MANUAL NO. AERB/NPP&RR/SM/O-1

MANUAL NO. AERB/NPP&RR/SM/O-1

GOVERNMENT OF INDIA

AERB SAFETY MANUAL

PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANTS AND RESEARCH REACTORS

ATOMIC ENERGY REGULATORY BOARD

AERB SAFETY MANUAL NO. AERB/NPP&RR/SM/O-1

PROBABILISTIC SAFETY ASSESSMENT
FOR
NUCLEAR POWER PLANTS
AND
RESEARCH REACTORS

Atomic Energy Regulatory Board
Mumbai-400 094
India

March 2008

Price:

Order for this manual should be addressed to:

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

FOREWORD

Activities concerning establishment and utilisation of nuclear facilities and use of radioactive sources are to be carried out in India in accordance with the provisions of the Atomic Energy Act 1962. In pursuance of ensuring safety of members of the public and occupational workers as well as protection of environment, 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. While some of these documents cover aspects such as siting, design, construction, operation, quality assurance and decommissioning of nuclear and radiation facilities, other documents cover regulatory aspects of these facilities.

Safety codes and safety standards are formulated on the basis of nationally and internationally accepted safety criteria for design, construction and operation of specific equipment, systems, structures 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 and guidelines elaborate various requirements and furnish approaches for their implementation. Safety manuals deal with specific topics and contain detailed scientific and technical information on the subject. Experts in the relevant fields prepare these documents. The Board and its advisory committees review them before they are published. The documents are revised when necessary, in the light of experience and feedback from users as well as new developments in the field.

The safety code on nuclear power plant design requires that design confirmation should be done by probabilistic safety assessment in addition to deterministic analysis. The safety code on nuclear power plant operation requires that the frequency of maintenance, testing, examination and inspection of structures, systems and components including computer based systems according to their importance to safety should be determined taking into consideration the probability of their failure to function, so as to provide assurance that they will satisfactorily perform their functions as and when required. Probabilistic risk assessment (PRA) or probabilistic safety assessment (PSA), is increasingly gaining importance in safe design and operation of nuclear reactors. The methodology has matured over the years. It complements deterministic analysis for design basis events. It also provides insights into beyond design basis events of very low probability and high consequences. This document gives comprehensive coverage of PSA, such as performance, regulatory review, failure database, different modelling and analyses, uses and validations of software packages, quality assurance in PSA preparation and review process. The information is primarily meant for nuclear power plants and research reactors although many of them could be usefully applied to other nuclear facilities. This document is prepared based on international practices in this field.

Appendices are an integral part of the document, whereas annexure and references/bibliography are included to provide information that might be helpful to the user. Approaches for implementation different to those set out in the manual may be acceptable, if they provide comparable assurance against undue risk to the health and safety of the occupational workers and the general public and protection of the environment.

Industrial safety is to be ensured through compliance with applicable provisions of the Factories Act, 1948 and the Atomic Energy (Factories) Rules, 1996.

This manual has been prepared by specialists in the field drawn from the Atomic Energy Regulatory Board, Bhabha Atomic Research Centre, Indira Ghandhi Centre for Atomic Research and Nuclear Power Corporation of India Limited. It has been reviewed by experts, relevant AERB advisory committees on codes and guides and the advisory committee on nuclear safety.

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 the task, along with their affiliations, is included for information.

(S. K. Sharma)
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 Occurrences

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

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

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 calculational tool that implements a mathematical model.

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.

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 Commission

An error that amounts to an unintended action, excluding inaction. It includes selection error, error of sequence, time error and qualitative error.

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 modes 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.

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 unremedied, 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.

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.

Man Machine Interface (MMI)

The abstract boundary between people and the hardware or software they interact with.

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 for restoration (or 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).

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.

Postulated Initiating Events (PIEs)

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

Predictive Maintenance

It is a 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)

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.

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 accidents or mitigation of accident consequences, reliability in protection of site personnel, the public and the environment from undue radiation hazards.

Safety System

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). It is also called the “safety critical 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

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 manual)

Accident Progression Event Tree/Containment Event Tree

Event tree generated for accident progression analysis in Level 2 PSA for various plant damage states.

Accident Sequence

Sequence of events leading to an accident.

Boundary

The physical or functional external interface of structure, system or a component.

Capability

The ability of an entity to meet a service demand with given quantitative characteristics under given internal conditions.

Capacity

The ability of the component to sustain a load measured in terms of load level (e.g., stress, moment or acceleration) below which the component continues to perform its functions.

Cognition

The capacity or mechanisms that lead to knowledge.

Common Cause Basic Event

In the context of system modelling, common cause events are a subset of dependent events in which two or more component fault states exist at the same time, or within a short time interval. A common cause basic event represents the unavailability of two or more components due to all shared causes that are not explicitly represented in the logic model as other basic events.

Common Cause Component Group

A group of (usually similar) components that are considered to have potential of failing due to the same cause.

Common Cause Event Model

A model, which is the basis for quantifying the frequency of common cause events. Examples include the beta factor, binomial failure rate, and basic parameter models.

Coupling Mechanism

An explanation of why and how a failure is systematically induced in several components.

Cumulative Distribution Function

Function F giving, for any value x, the probability that the random variable X will be less than or equal to x. $F(x) = P[X \leq x]$.

Degradation Failure

A failure, which is both a gradual failure and a partial failure. In time, such a failure may develop into a complete failure.

Dependability

The ability of an entity to perform one or several required functions under given conditions. It relates to the aspects of reliability, availability, maintainability, safety, durability, etc, or combinations of these abilities.

Diagnosis

The capacity or mechanisms to understand what is perceived and realise the implications of a perceived situation.

Down Time

The time interval during which an entity is in a down state.

Dual Failure

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

Early Failure

Failure occurring at the beginning of the life of an entity and whose rate decreases rapidly with time.

Failed State

State of an entity characterized by the inability to perform a required function.

Failure Rate

The limit, if any, of the ratio of the conditional probability that the instant of time, T, of a failure of an entity falls within a given time interval, $[t, t + \Delta t]$, to the length of this interval, Δt, when it tends to zero, given that the entity has not failed over [0, t]. It is also called as 'instantaneous failure rate'.

Failure Mechanism

The physical, chemical or other process, which has led to a failure.

Fragility

Conditional probability that a component would fail for a specified ground motion or response parameter value as a function of that value.

Gradual Failure

A failure due to gradual change of a given characteristics of an entity with respect to time.

Ground Acceleration Capacity

The seismic capacity of a component measured in terms of peak acceleration value at which the equipment will fail.

Human Error

The departure of a human behaviour from what it should be.

Hypothetical Accident

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

Importance Measures

Quantitative measure of importance towards risk contribution, derived from PSA results.

Independent Basic Events

Two basic events, A and B, are statistically independent if, and only if P(A and B) = P(A) * P(B) Where P(x) is the probability of event x.

Knowledge Based Behaviour

When symptoms are ambiguous or complex, the state of plant is complicated by multiple failures or unusual events, or the instrument gives only an indirect reading of the state of the plant, the operator has to rely on his knowledge and his behaviour is determined by more complex cognitive processes.

Lapse

An error in recall.

Large Early Radioactivity Release

A radioactivity release from the containment, which is both large and early. Large is defined as involving the rapid, unscrubbed release of airborne aerosol fission products to the environment. Early is defined as occurring before the effective implementation of the emergency response and protective action.

Latent Fault

An existing fault that has not yet been recognized.

Maintainability

The ability of an entity under given conditions of use, to be restored in or resulted to a state in which it can perform under given condition and using stated procedures and resources. The measure of maintainability is the probability that the above maintenance action can be carried out within a stated interval.

Markov Process

A process in which the probability that a system will transfer from one particular state to another depends only on the initial and final states of the transition. The terms of the equations for each state in this case depend only on the state itself, the possible immediately preceding and following states, and the rates of transfer between these states.

Maintenance Time

The time interval during which a maintenance action is performed on an entity either manually or automatically, including technical delays and logistic delays.

Performance Shaping Factor (PSF)

Any factor that shapes (influences) human performance to perform reliably or to make errors. It can be categorised into external PSFs (relating to situational characteristics, task and equipment characteristics), stressor PSFs (psychological and physiological)) and internal PSFs (characteristics of people resulting from internal and external influences).

Proximity Cause

A characterisation of the condition that is readily identifiable as leading to failure. It might alternatively be characterised as a symptom.

Precursor Event

Event whose occurrence makes it likely that another event having a probability and/or consequences larger than expected will exist.

Preliminary Hazard and Risk Analysis

An analysis which involves a preliminary hazard analysis together with an assessment of risk.

Probability Density Function

The derivative, if any, of the cumulative distribution function of a random variable.

Repair

The part of corrective maintenance in which maintenance actions are performed on the entity.

Repair Time

That part of active corrective maintenance time during which repair actions are performed on an entity.

Risk Coefficient

The lifetime risk or radiation detriment assumed to result from exposure to unit equivalent dose or effective dose (E).

Where, effective dose (E) defined as a summation of the tissue equivalent doses (H_T), each multiplied by the appropriate tissue-weighing factor (W_T);

$$E = \sum_T W_T H_T$$

Equivalent dose H_T is defined as $H_T = \sum_R W_R D_{T,R}$ and

$$H_{T,R} = W_R D_{T,R}$$

Where, $D_{T,R}$ is the absorbed dose delivered by radiation type R averaged over a tissue or organ T and W_R is the radiation-weighing factor for radiation type R.

Rule Based Behaviour

A (hypothesised) mode of behaviour that amounts to following situation action plans.

Or, Rule based behaviour is governed by a set of rules or associations, which are known and followed. A major difference between the rule based and the skill based behaviour stems from the degree of practice.

Screening Test

A test or a set of tests intended to remove or detect defective entities or those likely to exhibit early failures.

Secondary Failure

A failure of an entity caused either directly or indirectly by a failure or a fault of another entity and for which that entity has not been qualified or designed.

Seismic Hazard Curve

Frequency of exceeding a Peak Ground Acceleration (PGA) versus PGA, usually expressed on a per-year basis.

Single Failure Criteria

A criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

Skill

An ingrained ability or capacity toward specific action.

Skill Based Behaviour

In skill base behaviour, there is a very close coupling between the sensory input and the response action. Skill based behaviour does not depend on the complexity of the task, but rather on the level of training and the degree of practice in performing the task.

Slip

An error in implementing a plan, decision or intention.

Success Path

The path in a success diagram representing a combination of entity operating states, which ensure that the required function is performed.

Sudden Failure

A failure that could not be anticipated by prior examination or monitoring safety function (s) and any consequential failure (s), which result from it.

Super Component

A composite of related basic events modelled as single event for simplifying.

System

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

Taxonomy

A classification or way to classify.

Time Reliability Correlation

A relationship of probability of the (failure of) occurrence of an event to the time over which the event could occur.

Undesirable Event

Event (in the life of an entity) which should not occur or which should occur with a lower probability considering dependability objectives.

Unscheduled Maintenance

The maintenance carried out, not in accordance with an established time schedule, but after reception of an indication regarding the state of an item.

Walk down (plant)

A step or process during which data is gathered, assumptions on component capabilities are checked and analysis is performed. (e.g. walk down for PSA with respect to component capacity assessment).

Wear-out Failure

A failure whose probability of occurrence increases with the passage of time, as a result of processes inherent in the entity. It is also called ‘ageing failure’.

CONTENTS

1. INTRODUCTION

1.1 General

Probabilistic safety assessment (PSA), also known as probabilistic risk assessment (PRA), of nuclear reactors, essentially aims at identifying the events and their combination(s) that can lead to severe accidents, assessing the probability of occurrence of each combination and evaluating the consequences. PSA has been carried out for more than 200 nuclear power plants in the world and for most of the remaining ones, it is in various stages of development and completion. The studies confirm the benefit of PSA in identifying the plant strengths and weaknesses in its design and operation. In addition, it provides inputs to decisions on design and back fitting, plant operation, safety analysis and on regulatory issues. A major advantage of PSA is that it allows for the quantification of uncertainties in safety assessments together with the quantification of expert opinion and/or judgment. PSA is considered to complement the deterministic analysis for design basis events (DBEs) and for beyond design basis accidents (BDBAs) that consider multiple failures including operator errors and low probability events of high consequences.

In spite of the benefits, it is well recognised that PSA has its own limitations. The accuracy of the PSA depends on the uncertainties in aspects like data and models on Common Cause Failures (CCFs) and Human Reliability. CCFs can be eliminated to some extent by measures like providing diversity in design, physical separation between the systems and reducing the inter dependence. The influence of human error is reduced by automation and improved Man-Machine Interface (MMI). The benefits that accrue from PSA overweigh its limitations. So worldwide, utilities are performing the PSA of their plants and many regulatory bodies are using it as a risk informed approach in decision-making and some even following it as a risk based approach in decision-making. Over the years, the PSA methodology has matured and even new applications like Living PSA/Risk Monitor (LPSA/RM), Technical Specifications (TS) Optimisation, Reliability Centred Maintenance (RCM) and Risk Based In-Service Inspection (RB-ISI) have emerged. This makes it all the more useful in plant operation.

In order to achieve the goal of PSA, the PSA methodology integrates information on plant design, component reliability, operating practices and history, human behaviour, postulated initiating events (PIEs), accident sequences and potential environmental and health effects. This helps in focusing issues like deficiencies and plant vulnerabilities, risk contributors, sensitivity of governing parameters and uncertainties of numerical results. A full scope PSA is performed in three levels:

- A Level 1 PSA is the starting block of probabilistic safety assessment methodology, that arrives at core damage frequency by developing and quantifying accident sequences (event trees) with postulated initiating events (PIEs), together with system unavailability values derived from the Fault Tree analyses with inputs from failure data on components, common causes and human actions. This provides insights into design strengths and weaknesses and into ways of preventing core damage that could be a precursor to a large release of radioactive material.
- A Level 2 PSA taking inputs from Level 1 PSA results quantifies the magnitude and frequency of radioactive release to the environment following core damage and containment failure. It provides insights into severity of accident sequences resulting in core damage, consequent radioactive releases into containment, time and mode of containment failure, inventories of radioactivity released to the environment and ways of improving the mitigation and management of core damage accidents.
- A Level 3 PSA taking inputs from Level 2 PSA results, analyses the transport of radionuclides through the environment, the contamination of land, air, water and foodstuffs due to dispersion of radionuclides and assesses the public health and economic consequences of the accident. This is essentially a consequence analysis. In addition, it provides further insights into the relative effectiveness of the various aspects of accident management related to emergency response planning.

Fig.1.1 gives a schematic representation of a full scope PSA analysis.

The Level 2 and Level 3 analyses focus on risks to the environment and public health and societal loss and hence are being favoured by some users to be called PRA as compared to the terminology PSA for Level 1 analysis. In Level 1 PSA, risk to public does not arise but potential exists for containment degradation. However, both the terms PRA and PSA are interchangeably used and many favour use of the term 'PSA' for all three levels of analyses.

1.2 Objective

The objective of this document is to provide guidelines for conducting Level 1, Level 2 and Level 3 PSA studies taking into account internal and external events considering CCF Analysis, Human Reliability Analysis and Sensitivity and Uncertainty Analysis. Guidelines are also provided on the use of PSA in applications during various operational states of the plant and review of the PSA studies.

1.3 Scope

The document provides guidelines for performing PSAs for design and operation of NPPs as well as research reactors for all reactor states (shutdown, low power and full power) covering both internal as well as external Initiating Events (IEs). The guidelines include Level 1, Level 2 and Level 3 PSA and their specific applications to studies like LPSA/RM, RCM, TS Optimisations with regard to allowed outage time (AOT) and surveillance test interval (STI) and ageing management, RB-ISI, internal hazards due to dynamic effects and certain man induced external hazards, operator training and accident management. Guidelines are also given for Review and Quality Assurance (QA) of PSA.

These guidelines may be useful in carrying out safety analysis in other facilities like fuel storage, fuel reprocessing plant and non-nuclear facilities like chemical plants, refineries, etc.

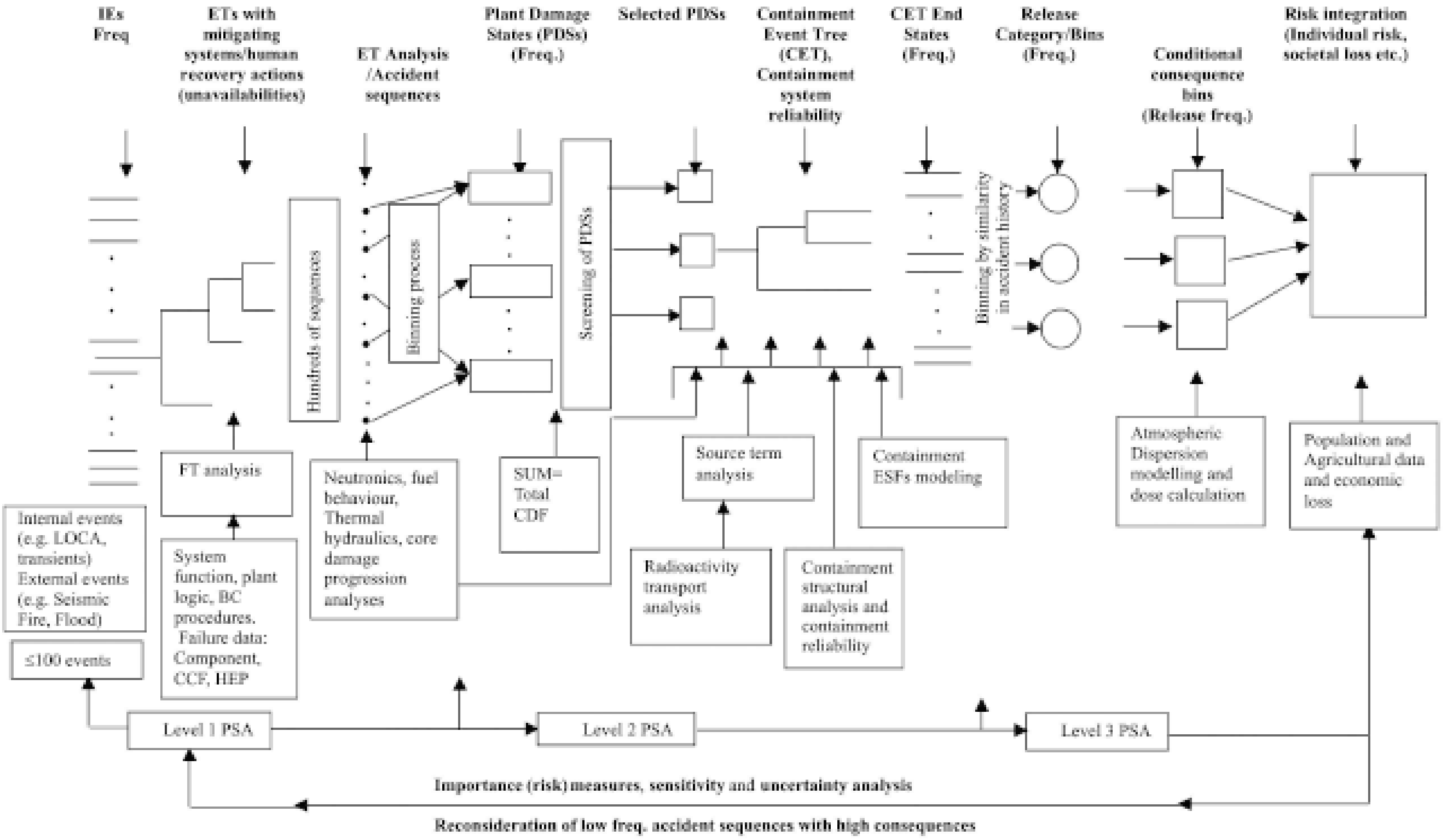


FIGURE 1.1 : SCHEMATIC REPRESENTATION OF A FULL SCOPE PSA ANALYSIS

2. QUALITY ASSURANCE

2.1 Introduction

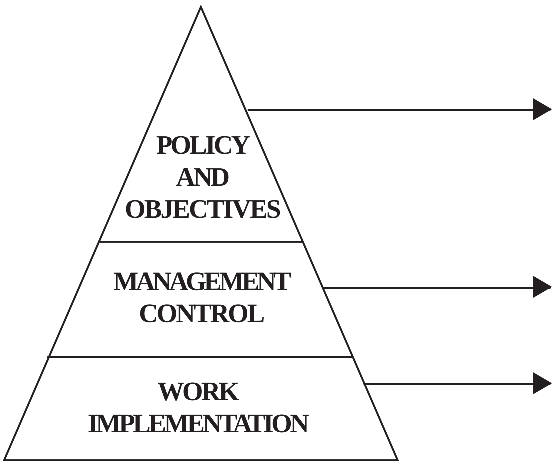
Performing a PSA of a nuclear plant involves a multidisciplinary teamwork of experts with intimate knowledge of plant design, operation and PSA techniques. Staff selection, project communication, computer software configuration and document control are crucial to the effectiveness and quality of PSA. Therefore, it is recommended that a detailed QA programme be established and made effective in every PSA project. The QA programme sets forth the methods, resources, controls and procedures, and defines the responsibilities and lines of communications for activities affecting the quality of a PSA. Inadequate QA measures employed in the early stages of a PSA may lead to loss of information and severely limit the usefulness of the PSA. The QA should include the project plan, QA assurance plan and QA procedure.

2.2 Management of QA Activities

The organisation should develop and implement a QA programme, which includes details on how the work in all the phases of PSA project is to be arranged, performed, assessed and associated management control. It covers QA planning, information control, the organisational structure, functional responsibilities, levels of authority for those managing, performing and assessing/reviewing the work. It addresses procedures that provided guidance on actual work performance.

2.2.1 Programme

The QA programme for a PSA project is illustrated in Fig. 2.1. The QA programme should be developed and documented to cover: (i) QA programme description, (ii) management documents and (iii) working documents



QA Programme Description
- A policy statement on PSA quality
- Missions and objectives
- Users, clients and reviewers of the PSA

Management Documents
- Management procedures
- Resources
- Organisational structure
- Functional responsibilities
- Job descriptions
- Interface arrangement

Working Documents
- Task procedures
- Plans and schedules
- Documentation
- Review procedures

FIGURE 2.1: TYPICAL DOCUMENTATION STRUCTURE OF THE QA PROGRAMME FOR PSA [1]

The following aspects are covered in the QA documentation as detailed below:

- Management aspects
- Resources
- Job descriptions
- Organisational structure

- Functional responsibilities
- Interface arrangement
- Information control
- PSA performance and control
- Verification and validation
- PSA review and assessment
- Standardisation

2.2.1.1 QA Programme Description

The QA programme description should establish a basis for the PSA project management by including the following:

(i) A statement of its applicability with regard to the overall QA programme of the responsible organisation including the possible interfaces with other QA programmes.

(ii) A summary on the mission, objective and scope of the PSA in terms of the result to be obtained and the uses to which the result are to be applied, the level of detail to be modelled, overall details required in the results and special features if any required.

(iii) Description of the functions, authority, responsibilities and accountabilities of units and individuals within the organisation and also the user, clients and reviewers of PSA including the interactions among the groups involved in PSA project and with other groups, for example review organisation.

(iv) The responsibilities of each organisation or group for the delivery of the different work packages including other aspects, which can affect the quality of the PSA, such as purchasing of items and services (e.g., consulting contracts) and mobilisation of adequate resources for completion of the PSA project.

(v) Description of required coordination of activities among the different organisations and groups and the interfacing between the constituent parts of the analysis.

(vi) Training of staff and levels of expertise required to achieve appropriate quality for each activity. Identification of the members of the team that will perform PSA, which may include system analyst, operational analyst and experts for specific PSA performance (e.g., seismic engineer for seismic PSA), besides PSA analysts.

(vii) A commitment to develop the necessary working documents.

(viii) Summary of the processes for evaluating the PSA work in relation to completeness, consistency, accuracy, document control and configuration control, including details of the QA for the software used.

(ix) Description of review processes including resolution of issues identified during review.

2.2.1.2 Management Documents

These documents are administrative in nature, and consist of the schedule of activities for the overall QA programme of the PSA project and for its management throughout the development, resourcing, performance, reviews, and applications of the PSA. Management documents include the following [2].

- Procedure for configuration management with regard to changes in all PSA related aspects such as models and data specification.
- Job descriptions
- Procedure for control of organisation, functional responsibilities and resources

- Procedure for organising and conducting performance and internal and external reviews.
- Procedure for handling interfaces.
- Training framework.
- Procedure for handling plant information.

2.2.1.3 Working Documents

QA programme working document covers PSA performance and control, verification and validation aspects, PSA output, PSA change control, PSA assessment and standardisation aspects, detailed task procedures, working documents and review procedures. The procedures include task specification, development of plans and schedules, review of all tasks, initiating event analysis, development of event trees i.e., procedure for each step of PSA. These work procedures and instructions include the following.

- Procedures for task specification
- Procedures for development of plans and schedules
- Procedures for review of all tasks
- Procedure for PIE analysis
- Procedures for sequence analysis and development of Event Trees (ETs)
- Procedures for system analysis and development of Fault Trees (FTs)
- Procedures for handling dependencies and CCFs
- Procedures for HRA
- Procedure for data collection, analysis, checking and computer input
- Procedure for developing/evaluating the hazard curve, fragility of components in case of external and internal hazard
- Procedure for severe accident analysis and source term evaluation
- Procedure for consequence analysis in Level 3 PSA with regard to effect on public health, environment impacts and social risk
- Procedures for FT/ET integration and quantification
- Procedure for uncertainty and sensitivity analysis
- Procedure for display and interpretation of results.

Outline of a PSA Project Plan and Technical Instructions Sample for System Analysis is given in Annexure-I and II respectively.

2.2.2 Programme Implementation

The QA programme should be implemented as per AERB codes and safety guides and other relevant international safety documents.

2.2.3 Organisation

The responsible organisation should establish the organisational structure, laying down clearly defined responsibilities and levels of authority and lines of communication. The PSA team, identified for PSA project, has the responsibility in the following areas:

(i) Establishment of the overall QA programme for the PSA

(ii) PSA project plan as given in Annexure-I.

(iii) Involvement in technical reviews

(iv) Approval of reports.

The position of the QA function in relation to project organisation should be clearly indicated, including lines of reporting to higher management and communication with other organisational units.

2.2.4 Interfaces

PSA project being complex, various internal and external interfaces should be carefully considered and defined in appropriate procedures. (See Annexure-III)

2.2.5 Staffing, Training and Qualification

Plant familiarisation and training in appropriate PSA aspects and PSA QA is essential for all personnel performing and verifying the activities affecting the quality of the PSA. Senior management should also be strongly committed to and be supportive of training.

2.2.6 Planning

PSA activities should be defined in the overall Project Plan of the responsible organisation. Task planning should take place well before the start of the PSA activities with reviews at appropriate levels in the organisation.

2.2.7 Non-Conformance Control and Corrective Action

Systematic control should be maintained over the identification, documentation and disposition of non-conforming items. Procedures and working instructions specify checks and reviews, which should identify deficiencies and provide assurance that only logical outputs are obtained. Non-conformance can come in the input data, modelling, target criteria (as set by Regulatory Bodies) and minimal cutset combinations, design aspects, operational aspects. Procedures and working instructions applicable should be used to handle non-conforming work. Results not confirming to design, operating framework (e.g. TS) or deviation in data modelling (e.g., failure data, CCFs, HRA) and PSG/PSCs set by analysts/ regulatory bodies, etc., should be appropriately resolved and documented.

2.2.8 PSA Document and Information Control

PSA document and information control should be as per written procedure. It should include the work proposed along with the background (of the project), general description of the plant, extent of the study, specifying the output product i.e., methodology, initiating event, event tree development, fault tree analysis, integration, etc.

2.2.8.1 General Considerations

The objective of this process is to control and document all the steps of the work. A large amount of information is available at the start of the project. This information must be quality assured and well documented. This information typically includes:

(i) Project scope, definition and objectives

(ii) Input data

(iii) Pre-performed analyses and calculations to be used for the PSA (deterministic analysis, success criteria, etc.)

During the actual work, information control covers items such as

(i) Documentation of assumptions

(ii) Data file control

(iii) Consistency of data used during the work

(iv) Traceability of the sources for information and data used in the different tasks

(v) Access to relevant information for all parties involved in the project (internal interfaces), and

(vi) Controlled documentation on changes, updating, new assumptions, that lead to iterations in the work process.

The outcome of the work can be intermediate or final. Proper quality in all results should be assured. The outcome consists typically of the PSA report(s) including the PSA model with all the corresponding data files. Special attention should be paid to the detailed documentation of input data from outside the PSA project and the detailed documentation of all assumptions, criteria and calculations including exclusion criteria or screening analysis, performed during the development of the model.

2.2.8.2 Source Information Control

The fundamental source of data for the PSA is the information from the plant. Thus a system should exist to assure that all the information needed for the PSA is received or made available to the PSA team. For consistency of the PSA models it is convenient that Plant Design and Operating documentation represent a picture of the plant at frozen date (snap shot of the plant).

2.2.8.3 Work Control

Control of information and documents developed during the projected processes needs to be subjected to appropriate QA. Regular updating of the PSA has to be subjected to a QA programme equivalent to the one applied during the development phase. PSA model can be subjected to iteration processes due to the following.

- Identification of errors or mistakes
- Refinement of assumptions, criteria or availability of additional input data
- Revision of input data (e.g., plant procedures, plant design, etc.) or further refinement after obtaining preliminary PSA results.

The iterations/modifications should be properly documented.

2.2.9 Configuration Management

The Purpose of PSA model configuration management is to ensure that any change in a part of the model is reflected in an appropriate manner in all other associated PSA parts,viz. identification, labelling, cataloguing and documentation of configuration. Configuration management is applied to PSA information and its documentation throughout the whole life-cycle to ensure that the models, data, specification, verification evidence, documentation and software used are all mutually identified and at a known status (issue revision/version, identifiers, date of stamp).

2.3 Carrying out PSA (Performance of PSA)

The basis for QA of a PSA project derives from (a) QA of the task inputs (i.e. technical basis), (b) QA of the task performance, and (c) QA of the task output at the completion of the task. QA for each task will entail verifications of compliance with the task instruction; verification of the technical accuracy of inputs and results and compliance with the required form and verification of content for input to other tasks.

2.3.1 Use of Verified Inputs

QA must not only embrace the work activities of the PSA, but must necessarily control the quality of the information input for each task. Information input will come from either the output of other tasks, or from outside the PSA project. QA of input data requires that information should be taken from a recognised approved and published source for its applicability to specific PSA. In case the design data did not meet this requirement the quality of the data must be established by acceptable/justifiable means.

2.3.2 Use of Verified Computer Codes

In order to ensure QA for the PSA, all computer codes used in the development of the PSA must be verified and validated, either in the course of their development or by the responsible organisation.

2.3.3 Verification and Validation of Analytical Work Products

Verification and validation should be performed in accordance with a pre-established plan. Each output of each task should be checked in the most appropriate manner prior to being released for use in other tasks. Whenever possible, the intermediate results should also be considered in the verification and validation process. The QA programme should define appropriate means for verification and validation of each work product. Persons appointed for verification and validation should be individuals competent in the area to be verified and validated and those who did not perform the original work.

2.3.4 PSA Reviews

A comprehensive review process for in-house review and regulatory review should accompany the PSA project for a quality PSA.

2.3.5 PSA Change Control

Changes in PSA models, data, information and results, including changes to requirement, scope, objectives and input data should be made in a controlled manner. The reason for a change should be documented. When carrying out a change, the modifications should be handled in the same way as for carrying out the complete PSA. Activities, which should be performed, include: (i) PSA information control, (ii) PSA configuration control, (iii) PSA documentation control, (iv) Verification and validation and (v) Review.

Depending on the type of changes, a new version or an update of the previous PSA version may be created.

2.3.6 PSA Outputs

PSA outputs for Level 1, Level 2 and Level 3 studies should be produced as given in Appendix-I.

2.4 Assessment

Measures should be in place for evaluating the PSA work in relation to the characteristics like: (i) Completeness, (ii) Consistency, (iii) Accuracy, (iv) Document control and (v) Configuration control.

This evaluation includes review at various levels and stages of the work performed. The activities should also include details of the QA of the software used in the PSA if necessary. It should include procedures for verification, documentation, and control of the software, whether procured from an external source or developed within the organisation. These procedures will apply to both the computer programmes used in the analysis and the models and data stored in electronic form. PSA results should be adequately reviewed by management to ensure that the PSA study has served its purpose.

2.5 Standardisation of PSA

The results of PSA may have uncertainties due to inherent variability in and limited availability of failure data, limitations in representations of system unavailability and event sequence for possible situations, uncertainties in modelling CCFs, HRA, Source Term and release consequences. Therefore, standardisation of various aspects like uses of proper failure data and models, including CCFs and Human Error Probability (HEP), methodology of quantification of end states/consequences, uncertainty analysis in the results and computer codes etc. are imperative for use of PSA insights meaningfully in risk informed decision making. Although, general QA aspects described above may ensure a certain minimum level of acceptable quality, this sub-section highlights recommendations in specific area/ aspects where standardisation can assure high confidence level in the performance/review of PSA studies. These areas/aspects are the following.

2.5.1 PSA Organisation

The team needed to conduct a PSA must include the following specialists.

System Analysts: Persons familiar with the plant design and accident analysis with regard to the DBA, severe accident progression, and containment performance under DBA/BDBA and computer codes for analysis of accident situations.

PSA Specialists: Persons familiar with event tree, fault tree methods and computer codes for analysis.

Plant Operation Specialists: Persons familiar with operating, test and maintenance procedures, administrative controls, control room layout and operating procedures for emergency conditions.

Data Analysts: Specialists in the collection and analysis of data.

Human Factor Analysts: Specialists in the collection and analysis of human reliability data and assessment.

Persons familiar with severe accident phenomena, uncertainty issues, containment performance, chemical and physical processes governing accident progression, containment loads, release of radionuclides.

Persons familiar with neutronics, source term evaluations, transport of radionuclides and dose evaluation.

Specialists in External Events: Persons familiar with external events for e.g., seismic PSA, expertise in earthquake engineering, structural design, evaluation of fragilities of components are required.

2.5.2 PSA Methodology

(a) Most commonly used and versatile techniques should be adopted for carrying out system and event sequence modelling. Fault tree methodology should be preferred for system unavailability analysis. Techniques allowing for modelling of the situation, as realistic as possible with less number of uncertainties and easy integration of models, which is essential in PSA, should be used. Core damage categorisation should be clearly discernible and as per the acceptable criteria.

(b) Since CCF analysis and HRA are very important in PSA, modelling techniques should take care of these aspects appropriately. Use of β-factor modelling should be limited to redundancies upto 3 components and independent failure probability should be the highest one of the values of these components. Where redundancies are more (4), it is recommended MGL model or α-factor model be used. As a thumb rule, to start with, HEP can be taken in the range of 1E-2 to 1E-4. A typical value could be 3E-03 [3], which can be modified by Performance Shaping Factors (PSFs) by expert judgement. Alternatively, a value in-between the range of 1E-02 and 1E-04 can be assigned in FT/ET quantification using a simple human error probability matrix. This can be developed by classifying jobs as simple, moderately complex and complex, human error attributes as less experienced, experienced and highly experienced and with the time availability for completion of jobs as more than half an hour, 10-30 minutes and less than 10 minutes. Once cutset shows the human error event as a dominant contributor, detailed human error modelling needs to be done to arrive at more realistic values. It should be ensured that the approximations and assumptions used in modelling techniques do not lead to erroneous results.

(c) Shared systems and passive safety features should be modelled appropriately. Considerations in shared system modelling include TS requirements with regard to the operability of units among which the Structure, System or Component (SSC) is shared, maintenance and surveillance aspects, capability to cater to unit requirements simultaneously or one at a time, human actions involved in successful operation, and operating procedures. The functional requirements that should be complied with, for success of passive system operation, should be carefully examined and accounted for. The unavailability values should be taken conservatively higher for passive systems, which may have not been experimentally verified.

(d) Support system/component and human actions should be modelled in FT level so that preferred small ET - large FT analyses can be done. However, one support system impacting two or more mitigating systems can be placed as header in the ET before these mitigating systems. Human recovery action should be modelled in ET level only. Credit for a human recovery action when needed especially in a short time should be justified (e.g., operator having undergone simulator training). In order to assess uncertainties in progression of severe accident, some reliance on numerical assignment of subjective probabilities is essential. Table 2.1 provides an example of probability values that could be assigned to various subjective descriptors.

TABLE 2.1 : PROBABILITY OF SUBJECTIVE DESCRIPTORS

Subjective descriptor	Probability
Certain	1.0
Likely to very likely	> 0.5 - < 1.0
Indeterminate, ambiguous	0.5
Very unlikely to unlikely	0.01 - < 0.5
Extremely unlikely	0.001
Impossible	0.0

2.5.3 Failure Data

As far as possible plant specific failure data should be used in a PSA. Wherever data paucity exists, failure data of similar plants and generic data may be used with discretion. Bayesian technique can be used to update the available data. For components relating to instrumentation e.g., sensors for which no failure is experienced in fairly long plant operation, very low value of unavailability below 1E-5 should not be used, unless adequate justification has been given.

2.5.4 Component Failure Models and Parameter Estimation

The failure model of components like repairable, tested, standby, non-repairable should be chosen in accordance with TS, plant layouts, accessibility considerations etc. Online testing of components in a safety system should be modelled considering the availability of the test override facility.

2.5.5 Sensitivity Studies

While carrying out sensitivity studies, acceptable increase in risk level can be referenced as a maximum of 10 %* increase in system unavailability level, 1 %* increase in CDF level and/or 0.1 %* increase in release frequency level in general and for risk based AOT/STI evaluations one order lower, unless otherwise specified by regulatory body as targets for risk informed decision. STI for a component in a safety system/mitigating system should be specified at least once in annual shutdown, even if risk based STI works out to be more than a year. (* Provisional)

2.5.6 External Events

While considering external events in PSA, simultaneous occurrence of two external events, or one external event inducing the other should be considered in PSA. Some external events (e.g., flood) may disrupt the evacuation routes and/or reduce the impact of radioactivity release/contamination and collective dose in public domain, etc. Such aspects of opposing nature should be addressed suitably in PSA modelling. Assessment of increased HEP under external hazards like flood, earthquake may not be addressed unless specifically called for, as modelling such interactions may be difficult and also uncertainty in estimation may be quite high. See table X-3 for contribution of IEs to CDF/CMF for published PSAs with complete seismic analysis.

2.5.7 Use of Computer Codes

The computer codes used for carrying out PSA should be state-of-the-art, user friendly, well verified, validated and documented. If the user intends to add new modules, the code should preferably have facility for this purpose. Such computer codes should contain modules for carrying out uncertainty, importance and sensitivity analyses. The uncertainty analysis technique can be by Monte Carlo simulation with Latin hypercube sampling method.

2.5.8 Quality of a PSA for Application

In the context of an application, the PSA is of an appropriate quality if it conforms to a set of attributes that are required for the application. Two types of attributes are defined in this section.

General attributes, which apply for a typical Base Case PSA apply for all PSAs and applications. Special attributes, which generally provide enhanced capabilities supporting certain applications of a PSA. These attributes need not be met in Base Case PSA. The general attributes represents a fundamental set of attributes that can be recognised as being associated with the performance of a technically correct PSA in accordance with the present state of art methodology and technology. Special attributes may arise because of the need to model specific impacts of changes proposed by the application which may require a higher level of detail for certain elements than required for the base case. They provide elevated capabilities in terms of resolution, specificity, scope, realism, and less uncertainty for the various applications.

There might be applications for which not all the attributes would need to be met or for which some attributes can be relaxed. These are applications for which either the risk information required is limited or for which the approach to decision making compensates for a lesser level of detail in the PSA by making a more conservative decision than would be the case for the more detailed plant specific model. Use of a more detailed and more plant specific PSA would allow more components to be classified as low safety significant when compared with what would result from use of a less detailed model. It should also be noted that the PSA results used by the decision making process may be adequate even if certain specific attributes are not met or not met fully. In this case ,special provisions should be made in the decision making process to compensate the lack.

3. PSA PERFORMANCE

3.1 General

As stated earlier, PSA is performed at three levels depending upon the scope of the study and requires large amount of information. Level 1 PSA requires the Safety Analysis Report including PSAR and FSAR, piping, electrical, and instrumentation drawings, descriptive information on various systems of the plant, procedures related to test, maintenance and operation of the plant components, generic and plant-specific data on PIEs, component failures and human errors. The additional information needed for a Level 2 PSA includes more detailed design information on the containment and associated Engineered Safety Features (ESFs). Level 3 PSA requires site-specific meteorological data for the radioactivity transport calculations, local population densities, evacuation plans and health effect models for risk evaluation. If external events are to be analysed, more information will be needed, depending on the external events to be included. For instance, detailed structural, seismic design of the plant and seismicity of the site are needed for a seismic analysis. Information on the compartmentalisation of the plant is necessary to analyse susceptibility to fires and floods [4]. The tasks associated with various levels of PSA involve project plan, input data, quality assurance, realistic assumptions, system analysis, containment analysis, analysis of radioactivity dispersion and deposition in the environment and consequences, external event analysis, uncertainty analysis, importance measure calculations, sensitivity analysis, development and interpretation of PSA results and documentation. The tasks involved in various PSA levels are briefly described below.

3.2 Procedure for Conducting Level 1 PSA

3.2.1 Scope and Objective of Level 1 PSA

The objective of Level 1 PSA is to calculate Core Damage Frequency (CDF) considering all PIEs, which may lead to core damage. Level 1 PSA can be used for (i) identification of dominant accident sequences, (ii) identification of systems, components and human actions important to safety, (iii) assessment of important dependences (system and man-machine) (iv) risk monitoring, (v) Technical Specification optimisation with respect to AOTs and STIs, (vi) Reliability Centred Maintenance, (vii) plant configuration management, (viii) prioritisation of inspection/testing activities, (ix) design modifications and plant back fitting, etc.

The scope of Level 1 PSA is to identify potential sources of radioactive release, to identify PIEs, which may lead to core damage, to identify core damage states and to evaluate CDF. If Level 2 PSA analysis is contemplated, all plant related features that are important to the analysis of containment response and source term, which are necessary input for carrying out Level 2 PSA analysis should be included in Level 1 PSA analysis.

The procedures for performing Level 1 PSA can be divided into four major steps [5], which are (i) identification of sources of radioactivity and accident initiators, (ii) accident sequence modelling, (iii) data assessment and parameter estimation and (iv) accident sequence quantification. Each of these is discussed below.

3.2.2 Identification of Sources of Radioactivity and Accident Initiators

A list should be made of all the sources of radioactivity (i.e. the reactor core, the spent fuel storage pool, the spent fuel handling facilities and the radioactive waste storage tanks) from which accidental releases could be postulated during different operational states of plant (i.e. full power operation, low power operation, shutdown stage, etc.) depending on the scope of the PSA being performed. The end result of the Level 1 PSA is CDF. An exhaustive list of accident initiators, also called ‘PIEs’, is identified. Several approaches are available for this task. The aim is to produce a list of PIEs and group these appropriately so as to ensure that the list is as complete as possible and includes bounding cases.

3.2.2.1 Approaches for Preparation of PIEs List

(a) Engineering evaluation

The plant systems and components are systematically reviewed to identify failure modes (e.g. failure to operate, spurious operation, breach, disruption and collapse) that could lead directly, or in combination with other failures, to core damage. Partial failures of systems, although they are generally less severe than complete failure, should also be considered. They are of higher frequency and are often less readily detected. Special attention should be given to common cause initiators.

(b) Reference of previous lists

It is useful to refer to lists of PIEs used for previous PSAs and accident analysis of similar plants.

(c) Deductive analysis

In this approach, core damage is made the top event in a diagram, which has the appearance of a fault tree. This top event is successively broken down into all possible categories of events that could cause it to occur. Successful operation of safety systems and other preventive actions are not included. The events at the most fundamental level are then candidates for the lists of IEs for the plant. Examples of such diagrams are the Master Logic Diagrams (MLDs) as shown in Annexure-IV.

(d) Operational experience

In this approach, the operational history (if any) of the plant under study and of similar plants elsewhere is reviewed for any events that should be added to the list of PIEs.

3.2.2.2 Identification of Safety Functions Required for PIEs

Once the exhaustive list of PIEs is prepared, detailed analysis of each PIE listed should be carried out to assess the causes and consequences and only important PIEs should be selected for the further analysis. This step is required because a larger list of PIEs would result in avoidable wastage of resources. Care should be taken for low frequency PIEs that can cause containment failure at high probability, if the scope of the PSA is to be extended to a Level 2 PSA analysis. Then grouping of the PIEs is done to reduce the effort required for the analysis of large number of PIEs, which may have the same consequences. This can be done if the demands these PIEs place on safety functions, front line systems and support systems are the same. Hence, the safety functions that need to be performed in order to prevent core damage for each PIE should be identified. Typical safety functions required for NPPs are: control of reactivity, core cooling and containment of radioactivity.

3.2.2.3 Assessment of Plant System Requirements

The performance required of a front line system depends in general on the PIE. Required performance means the minimum system performance that will allow for the successful fulfilment of its safety function under the specific conditions created by the PIE. The success criteria of front line systems are of particular importance for the PSA because they will define the top events or the starting point for the subsequent modelling. Success criteria for support systems cannot be so readily defined because in most cases they serve more than one front line system, and consequently each possible state of the system (e.g. two trains operating, one train operating, no trains operating etc.) has different effects on the front line systems that perform certain functions. A particular support system state could therefore lead to a safety function success or failure depending on the operational requirement of the front line system with which it is combined.

3.2.2.4 Grouping of PIEs

Once the task of assessing the requirements of the plant systems has been completed, the initiating events can be grouped in such a way that all events in the same group impose essentially the same success criteria on the front line system as well as the same special conditions (challenges to the operator, to automatic plant responses, etc.) and thus can be modelled using the same event/fault tree analyses. In the process of grouping, it will be clear that some categories of PIE need to be subdivided (e.g. Categorising LOCAs as Large Break LOCA and Small Break LOCA). One methodology of grouping is by functional aspects such as, increase of heat removal through secondary circuit, loss of primary coolant flow, reactivity and power distribution anomalies, increase of primary coolant inventory, decrease of primary coolant inventory, LOCA with leakage into atmosphere of secondary coolant system, radioactivity release from a subsystem or component and anticipated transients without scram. The main objective of grouping is to arrive at PIEs of manageable number that should represent each group appropriately including bounding cases for PSA modelling.

3.2.3 Accident Sequence Modelling

A typical accident sequence consists of a PIE group, specific system failures and successes, and their timings and human responses. Some of these accident sequences may result in plant damage states. The system failures/unavailabilities are in turn modelled in terms of basic component failures, CCFs and human errors to identify their basic causes and to allow for the quantification of the system failure probabilities (Unavailabilities) and accident sequence frequencies. Accident sequence modelling can be subdivided into (i) event sequence modelling and (ii) system modelling.

3.2.3.1 Event Sequence Modelling

An event sequence model provides sequences of events that, following an initiating event, lead either to a successful state or to a core damage state in which one or more design basis parameters are exceeded. The design parameters to be considered are those that include clad temperature, central fuel temperatures, design pressure for primary coolant, secondary (steam) system and containment, linear heat rating of fuel, departure from nucleate boiling, fuel enthalpy, clad strain, clad oxidation, percentage of fuel failure, hydrogen generation from metal water reaction, radiological dose and time available for operator action for emergency action (where a parameter cannot be identified for such assessment). Every accident sequence that does not lead to successful end state (safe reactor shutdown state as defined in the plant design and technical specifications for plant operation) is assumed to lead to core damage. There are several possible degrees of ‘core damage’; the severity is categorised on the basis of extent of core damage and the magnitude of the resulting radioactivity release from the core.

There are several methods available for event sequence modelling, viz., (i) Event trees; (ii) Cause consequence diagrams and (iii) Event sequence diagram.

(a) Event trees

Event Trees (ETs) are graphic models that order and reflect events according to the requirements for mitigation of each group of initiating events. Events or ‘headings’ of an event tree can be any (or combination of) safety functions, safety systems, basic events and operator actions. The event tree headings are normally arranged in either chronological or causal order. Chronological ordering means that events are considered in the chronological order in which they are expected to occur in an accident as depicted in (deterministic) Safety Analysis. Causal ordering means that events are arranged in the tree with ‘Cause’ relationship of the preceding to the succeeding events.

(b) Cause consequence diagrams

A Cause Consequence Diagram (CCD), a logic diagram that follows the chronological and causal order of the events, can contain more information than an event tree because it allows for more complex branching than the Yes/No logical operator allowed in the event trees. The use of CCD is typically limited to qualitative analysis, or as an intermediate modelling stage prior to event tree construction.

(c) Event sequence diagrams

Event Sequence Diagram (ESD) is a variation of cause consequence diagram. ESDs are developed for each group of IEs. The purpose of the ESDs is to illustrate all possible success paths from a particular PIE to a safe shutdown condition. The ESDs tend to include a significant amount of design and operational information and are used as intermediate steps prior to the construction of event trees.

3.2.3.2 System Modelling (Reliability/Availability Analysis)

Once the response of the plant to the PIEs has been modelled by one of the available event sequence modelling techniques, the details of the event sequence can be analysed through one of the available system models such as fault trees, state space diagrams, reliability block diagrams, go charts, etc. Before any specific method is applied, a very good understanding of the system operation as well as the operation of its components and the effects of their failure on system success is necessary. Such knowledge and understanding can be achieved through a qualitative analysis, e.g., a Failure Modes and Effect Analysis (FMEA).

(a) System fault trees

Fault Tree (FT) modelling is the most widely used method for representing the failure logic of the plant systems. It is a deductive failure analysis, which can be simply described as an analytical technique whereby an undesired state of the system is specified, and the system is then analysed in the context of its environment and operation to find all credible ways in which the undesired state could be brought out. The following aspects should be considered while constructing FTs.

(1) Methods and procedures for the construction of FTs should be agreed to at the beginning of a PSA and should be followed by all analysts. This is necessary in order to guarantee consistency of the analysis. Items to be considered in this context are system boundaries, logic symbols, event coding and representation of human errors and CCFs.

(2) All assumptions made in the process of constructing a fault tree should be documented together with the source (and revision number) of all design information used. In this way, consistency will be promoted throughout the analysis and traceability will be maintained.

(3) Clear and precise definitions of system boundaries are be established before the analysis begins. These definitions should be adhered to during the analysis and should be included in the final documentation covering systems modelling. The interface points between front line systems and various support systems could, for example, be located as follows.

- for electrical power supply, at the buses from which components within the system are fed
- for actuation signals, at the appropriate output cabinets of the actuation system
- for support systems providing various media (water, oil, air), at the main header line of the support system.

In cases where equipment or piping is shared between several systems, guidance with respect to proper establishment of boundary conditions is usually provided by system descriptions and drawings. This aspect should be carefully checked in order to avoid possible omissions and/or double counting.

(4) When systems are not modelled in detail and system level reliability data are used, failure events in common with other systems should be separated out and explicitly considered.

(5) Validated computer codes should be used for handling the solution and quantification of FTs to ensure consistency, comprehensiveness, efficiency and quality. Information on the available computer codes for level 1, level 2 and level 3 PSA is provided in Appendix-II.

(6) A standardised format should be employed for coding (naming) basic events in the FTs. Appendix-V gives suggested tables for basic events and gates. Whichever coding scheme is used, it should be compatible with the computer code selected for the systems analysis/event tree analysis and also enable the basic events to be clearly related to the following:

- Plant coding for the components
- Specific system in which the component is located
- Specific component identification and type, including 'House Event'
- Component failure mode.

To prepare the system models for a concurrent or subsequent evaluation of operating/accident environmental effects, the models will need to contain information on component location and susceptibility to the environmental effects of interest, e.g., high humidity and temperature, earthquake, fire or flooding. The information of this type should be encoded within the component name or provided in separate tables correlating events with applicable information.

(7) The FTs should reflect all possible failure modes of basic events that may contribute to the system unavailability. This should include contributions due to outage for testing and maintenance. When redundancies are involved, relevant technical specifications requirements should be taken into account. Human errors associated with failure to restore the equipment to its operable state following testing and maintenance and human errors associated with switching operations or valving operations should also be included in FTs.

(8) The following aspects of dependent failures should be reflected in the FTs.

(i) interrelations between IEs and system response

- common support system faults affecting more than one front line system or component through functional dependencies
- human errors associated with component test and maintenance activities
- components shared among front line systems.

(ii) Dependent events should be modelled explicitly and implicitly as reflected in the following points.

- Multiple failure events for which a clear cause-effect relation can be identified should be explicitly modelled in the system model. The root cause events should be included in the system fault tree so that no further special dependent failure model is necessary. This applies to multiple failures caused by internal equipment failure (such as cascade failures and functional unavailability events caused by components) and multiple failures due to clearly identifiable human error (such as human error in the steps of a prescribed procedure).
- Multiple failure events which are susceptible to dependencies, and for which no clear root cause event can be identified, can be modelled using implicit methods such as the parametric models, which are given in Appendix-III.
- Between the two previous extremes, there is a set of multiple failure events for which the explicit modelling of the cause, even if in principle feasible, is not performed because it would be too onerous; it is preferred to encapsulate the events in a parametric model. The decision to do this is taken by the analyst on

the basis of experience and judgement, taking into consideration the aim and scope of the analysis. Moreover, explicit modelling may in some cases be impracticable because the component failure data do not allow different failure causes to be distinguished. Explicit modelling should in principle go as far as reasonable, depending on, among other things, the resources for the analysis and the level of details needed. For the remaining dependencies, at least an upper bound should be assessed and for this parametric modelling can be used. The analyst should clearly document what has gone into the parametric modelling and what has been modelled explicitly.

(9) To permit proper quantification of accident sequences in which the IE may affect the operability of a responding system, the impact of IEs on the operability of the system should be explicitly included as appropriate in each system fault tree. In the small event tree/large fault tree approach, the impact of the IEs may occur at the component level. Alternatively, the failure probabilities for basic events will be modified in order to take account of the impact of the particular IE. In the large event tree/small fault tree approach, the initiators may appear as boundary conditions on the top event.

(10) To simplify and reduce the size of the FTs, certain events are often excluded owing to their low probability in comparison with other events.

(11) The testing procedures used in the plant must be closely examined to see whether they introduce potential failure modes.

(12) Trips of pumps and other safeguards intended to protect a component must be carefully identified. These can be a source of common mode failure. For example, spurious trips of auxiliary feed water pumps on low suction pressure can lead to system failure if recovery does not occur.

(13) Control and instrumentation systems (C & I) : Safety significant C & I systems including computer based systems in the NPPs and research reactors are necessary for safe and long-term reliable operation. There are certain difficulties in quantification of failure data for some of C&I components. Hence, care must be taken while developing Fault Trees for C&I including computer-based systems. These aspects have been further detailed in Appendix-IV.

(14) Shared systems : The impact of sharing of systems, between two or more units at a given site, on plant safety should be considered. The treatment of shared systems is based on the following aspects:

(i) Safety functions (including shutdown function) of any unit should not be affected beyond acceptable limits due to sharing of any system.

(ii) While the system is operating for one unit, mal-operation/failure of some component of the part of the shared system for the other unit, should not result into spurious (undesirable) actuation of the system into the other (operating) unit, or diversion of the flows etc. from the intended unit. This aspect can be modelled in the FT analysis.

(iii) Impact of non-availability of a shared system for one unit due to its being used by the other unit at that time is to be considered.

(iv) Impact of CCFs of these systems should be within acceptable limits.

(v) Checks should be made to assess whether the impact of sharing can be further reduced due to items such as those listed below:

- whether independent and physically separate control circuits are provided for operation of the shared systems for units.
- whether interlocks prevent simultaneous use of shared system by the units.

- whether operability of the shared pumps and the valves is tested periodically and proper log of these tests is maintained and reviewed at subsequent levels.
- whether follow-up checks are carried out after all the maintenance activities, to ensure that the normal state of the shared system components is restored back, in order to reduce probability of maintenance errors creeping in.

(vi) While modeling FT for shared systems, the following should be considered.

(a) Shared system may not be available because of the demand of the system for the other unit during the mission time for unit under consideration or system itself fails. This can be modelled by top gate of 'OR-gate' type.

(b) In the modeling of shared systems, human actions, CCFs and spurious actuations should be considered appropriately to account for the unavailability of the system.

(15) (a) Passive systems

One of the aims of using passive systems in NPPs is to add simplicity, reliability in functioning and cost reduction. Although passive systems are based on inherent properties of the physical processes, they may be vulnerable due to deviation from physical processes although to lesser probability than the active systems. Passive systems perform their intended functions once actuated and started, by following driving forces of nature. There are considerable uncertainties related to these forces in real situations. For example, heat transfer coefficients and pressure losses have to be studied with conditions in the plant. Final plant-specific conditions, layouts, configurations and human actions may be factors that affect the operability of the passive systems to a significant amount. These factors should be appropriately modelled in the FTs and values for each of these factors should be properly taken into account.

Basic FT symbols, illustration of 'House event' and sample FT are given in Appendix-V.

(b) State space diagrams and markov analysis

Markov process for State Space analysis can be a very useful tool for modelling scenarios in which system states change with time. It may be used for reliability/availability estimations, particularly for systems subjected to periodic testing and maintenance as well as failure and repair cycles. The state space diagram is a logic model depicting the various states of a system and the paths along which the system can transfer from one state to another. It is possible to represent a state space diagram by a set of simultaneous differential equations representing the change with time of the probabilities of the states. However, for a general case, it is not possible to obtain a closed analytical solution to such a set of equations. Hence, the simulation techniques would have to be used. In the case of systems with a failure, repair, test and maintenance cycle, it is possible to make a special case by assuming that the transfers from state to state follow a Markov process.

(c) Reliability block diagrams

Reliability block diagrams show the logical relation among system components in order to indicate which elements (blocks) of the system must operate successfully for the system to perform its intended function. Each block represents an individual component or a convenient grouping of components of the system. The block diagrams consist of blocks in series, parallel, series-parallel or in 'm out of n' configuration. Blocks representing redundant components are shown in parallel. Individual components whose failure causes system failure are placed in series. It is usually convenient to arrange blocks on a reliability block diagram in the sequence in which their functions are performed. The main disadvantages of reliability block diagrams are that it is difficult to model support systems adequately and causes of failure are not systematically identified (this is particularly relevant for human errors and CCFs).

(d) Go chart

The Go chart (Go) method is a success oriented system analysis technique. The Go method parallels that of the CCDs and ESDs in that it follows an inductive success oriented logic. Some key features of the Go method are [4]: (i) models follow the normal process flow, (ii) model elements have almost one-to-one correspondence with the system elements and handle most component and system interactions and dependencies, (iii) models are compact and easy to validate, (iv) outputs represent both success and failure states, (v) models can be easily altered and updated, (vi) fault sets can be generated without altering the basic model, (vii) system operational aspects can be incorporated, and (viii) numerical errors due to truncation are known and can be controlled.

The main advantage of the Go chart is that it is easily created from system engineering drawings and follows the normal flow path. It lacks, however, the inquisitive nature of the fault tree deductive logic, which asks, “how can it fail?”

3.2.3.3 Recommended Methodology

Use of combined event tree/fault tree method represents the recommended basic modelling approach. Other methods mentioned are to be regarded as supplementary and are of interest in specific modelling situations as explained earlier. One usual problem in selecting the method for a PSA is the determination of the level of event resolution at which event sequence modelling stops and system modelling begins. Two approaches have been identified in this regard: (i) small event tree/large fault tree approach and (ii) large event tree/small fault tree. Both approaches are acceptable since in principle they are equivalent.

(a) Small event tree/large fault tree approach

In this approach dependencies between front line systems and support systems do not appear in the ETs. ETs with safety functions as headings are developed and then expanded to ETs with the front line systems as heading. The front line system FT models are developed down to suitable boundaries with support systems. The support system FTs may be developed separately and integrated at a later stage into the front line system models. This approach generates ETs that are concise and that allow for a synthesised view of an accident sequence. Furthermore, subject to availability of computer codes, the small ETs may be more readily computerised. However, handling of large FTs requires more computation time and in some cases special codes.

(b) Large event tree/small fault tree approach

In this approach dependencies between front line systems and support systems do appear in the ETs. The top events on the FTs have associated boundary conditions; the boundary conditions include the assumption that the support system is in the particular state appropriate to the event sequence being evaluated. Separate FTs must be used for a given system for each set of boundary conditions. These separate FTs can be produced from a single FT that includes the support system and that, before being associated with a particular sequence, is ‘conditioned’ on the support system state associated with this sequence. This approach generates large ETs that explicitly represent the existing dependencies. Since they are associated with small FTs (i.e., front line systems without support systems), they are less demanding in terms of computer resources and code sophistication. However, the complexity of the ETs increases rapidly with the number of the support systems and the number of the support system states that are explicitly depicted in the ET.

3.2.3.4 Human Reliability Analysis (HRA)

Human performance and human reliability play an important role in nuclear reactor safety. Human factors considerations should figure not only in reactor operation but also in other tasks such as design, testing and maintenance. HRA should be primarily applied in PSA, where it is important to identify human errors, which have a significant effect on overall safety and also quantify the probability of their occurrence. The application of HRA in PSA requires quality data. The systematic collection and classification of human error and human reliability data is essential for quantifying the human error probability.

The main objective of treating human reliability in a PSA is to ensure that the key human interactions of typical crew/members are systematically incorporated into the assessment. The aim is also to make it as realistic as possible, by taking into account the emergency procedures, the man-machine interface, the training programme and the knowledge as well as the experience of the crews. It should be noted that PSA by itself cannot fully address all important human reliability and human factors. Issues relevant to nuclear safety, e.g., some aspects of management and organisation, are generally excluded.

The treatment of human reliability in a PSA is still evolving owing to complexity of human behaviour and general lack of relevant data. There is a growing consensus, however, on the need, usefulness and modelling of human reliability in PSA. The aspects of HRA and use of certain techniques are detailed in Appendix-VI.

3.2.3.5 Dependence Analysis

All the dependences should be listed separately and should also be properly included in the FT/ET models in order to evaluate correctly their impact on the level of risk. Multiple failure events that are susceptible to dependencies and for which no straightforward clear cause event can be identified should be modelled using implicit methods, such as parametric models categorised as CCF models. So, CCFs represent all dependences that are not explicitly modelled in the event sequence and system models, i.e., they are residual dependencies. CCFs can therefore belong to any of the below mentioned types of dependences. For all CCF contributions, a rather conservative joint probability of failure is assumed and the effect on the probability of the core damage is assessed. If the impact is substantial, then a more careful and detailed CCF analysis is performed. Dependences are categorised into the following types.

(a) Functional dependences

These dependences are among system, train, subsystem or component due to the sharing of hardware or due to a process coupling. Shared hardware refers to the dependence of multiple systems, trains, subsystems or components on the same equipment. In process coupling, the function of one system, train, subsystem or component depends directly or indirectly on the function of another. A direct dependence exists when the output of one system, train, subsystem or component constitutes an input to another. An indirect dependence exists when the functional requirements of the one system, train, subsystem or component depend on the state of another. Possible direct process coupling between system, train, subsystem or component includes electrical, hydraulic, pneumatic and mechanical connections.

(b) Physical dependences

There are two types of physical dependences.

- Those dependences that cause an initiating event (IE) and also possibly failure of plant mitigating systems due to the same influence, e.g., external hazards and internal events. Such events are certain transients, earthquakes, fires and floods, etc.
- Those dependences that increase the probability of multiple system failures. Often they are associated with extreme environmental stresses created by the failure of one or more systems after an IE or by the IE directly. Examples are fluid jets and environmental effects caused by LOCAs.

It should be emphasised that proximity is not the only ‘environmental’ coupling inducing physical dependence. A ventilation duct, for example, might create an environmental coupling among systems; trains, subsystems or components located in seemingly decoupled locations. Radiation coupling and electromagnetic coupling are two other forms not directly associated with a common spatial domain.

(c) Human interaction dependence

Two types of dependence introduced by human actions can be distinguished: those based on cognitive behavioural processes and those based on procedural behavioural processes. Cognitive human errors can result in multiple faults once an event has been initiated. Dependences due to procedural human errors include multiple maintenance errors that result in dependent faults with effects that may not be immediately apparent (e.g., miscalibration of redundant components).

3.2.4 Data Assessment and Parameter Estimation

This procedural step, aims at acquiring and generating all information necessary for the quantification of the FT model i.e. identification of the various models and the corresponding parameters that need to be estimated, determination of the nature and sources of relevant data, and compilation and evaluation of the data to produce the necessary parameter estimations and associated uncertainties.

3.2.4.1 Common Procedures

The procedural steps of data assessment and parameter estimation are concerned with the analysis of three major categories of data: (i) IE data, (ii) component failure, repair, test, maintenance and CCF data and (iii) human error data. For each of these categories the following common sub-tasks are distinguished.

- Event definition
- Model and parameter selection
- Identification of data sources and data gathering
- Selection and application of the estimation techniques.

3.2.4.2 Assessment of the Frequency of PIEs

The data required for quantification of the models that yield the frequencies of PIEs are the numbers of occurrences of the events and the total periods over which these events have been observed. Sources of such data are the plant logbooks, in which ‘significant occurrences’ are recorded, and licensee event records. If a plant specific assessment is not attempted, then the frequencies are taken from appropriate ‘generic’ lists or ‘databases’. Bayesian techniques, based on a more complicated model that estimates frequencies of occurrence by combining data from several plants, while taking into account the differences between the plants, can be applied.

3.2.4.3 Assessment of the Component Reliability

Component data analysis has as its objective the modelling of component failure, component repair, and component testing and maintenance. Component failure definition requires specifications of component boundary and mode of failure. The mode of failure is given as an undesirable state of component performance (e.g., a closed motorised valve does not open when required owing to a mechanical failure of the valve prior to the demand). Component testing and component repair and maintenance data are analysed to find out how often and for how long they render a component inoperable for the plant operating state. On-line testing, repair and maintenance are of primary concern in calculating system unavailabilities. However, leaving equipment in a failed or unavailable state following off-line testing or maintenance also has to be accounted for. Following aspects are to be kept in mind while assessing component reliabilities and generating failure database.

- Component description
- Failure mode

- Test interval
- Mission time
- Technical specification on AOT
- Maintenance times
- Failure rate (per hour) or failure per demand, expressed as mean or median values
- Upper and lower bounds (if a distribution is being used), high and low values, maximum and minimum values or other parameters (e.g. error factors) defining a possible range of failure rates
- Repair time.

(a) Component failure model and parameter selection

The models to estimate the probability that a component will not perform its intended function and depend on the mode of operation of the system to which the components belong. Some such models are described below.

(i) Operating systems

For operating systems, the reliability characteristic of interest is generally the probability that the system operates successfully for a given period of time T_M (the mission time). Operating systems contain two general types of components: non-repairable components and repairable components.

- Repairable and Non-repairable Components : The word ‘repairable’ means repairable without taking the total system out of service’. Thus, unless there is a redundant component, and unless the failed component is accessible for repair with the system operational, the component should be treated as non-repairable.

The expressions for component unavailability for operating systems are given below in Table 3.1

TABLE 3.1 : COMPONENT UNAVAILABILITY EXPRESSIONS FOR OPERATING SYSTEMS

Component Type/ Unavailability Mode	**Time Averaged Unavailability Expressions**	**Parameter Definition**	**Data Requirement for Parameter Estimation**
1. Non-repairable component	$1-e^{-\lambda_0 T_M}$	λo : Operating failure rate T_M : Mission time (obtained from success requirement)	λo Number of observed failures, total time to failure
2. On-line repairable component	$\frac{\lambda_0 T_R}{1+\lambda_0 T_R}$	T_R: Mean time to repair	T_R Observed individual times for repair

(ii) Standby systems

The unavailability of these components is a function of the standby time. If the component is tested periodically, then the average unavailability during the period of analysis is the average unavailability during the period between tests. The time dependent feature allows the inclusion in the model of the influence of the frequency of periodic testing. Depending on how a component is tested, we can distinguish three types of components of standby systems:

- Periodically tested standby components

  If components are found to have failed in a test, they are repaired. In addition, the components may be subjected to periodic scheduled maintenance. For these components there are five kinds of contributions to the component unavailability: hardware failure, unavailability due to testing, unavailability due to unscheduled repair/maintenance, unavailability due to scheduled maintenance; and unavailability due to interfacing maintenance. The expressions for these unavailabilities are given in Table 3.2. The parameters that must be estimated from data are the standby failure rate, the mean time to repair, and the mean time of on-line maintenance actions.

- Untested standby components

  If a standby component is not tested, then the averaged unavailability is given by the formula presented in Table 3.2. In this formula, the fault exposure time T_p (the time during which a failure can occur and the state of the component is unknown) is set equal to the life of the plant if no demand comes. However, it often happens that the component is indirectly tested or renewed. For example, if the system to which the component belongs is called upon to operate, the state of the untested component might be detectable when the system is demanded.

- Continuously monitored components

  Some components, although they belong to standby systems, are continuously monitored for their status. This is equivalent to assuming that a failure is detectable as soon as it occurs.

An alternative model that has been proposed for components during the standby period is that of constant unavailability or constant failure probability per demand. This model assumes that the failure of the component is only caused by immediate influences related to the demand.

(iii) Standby systems in operating mode after start-up

Standby systems are usually required to operate for a required mission time after successful start-up, the models can be handled analogously to operating systems. In principle, the systems can be regarded as repairable, provided that the conditions on repairability of operating systems mentioned earlier are fulfilled.

TABLE 3.2 : COMPONENT UNAVAILABILITY EXPRESSIONS FOR STAND-BY SYSTEMS/COMPONENTS

Component Type/ Unavailability Mode	Time Averaged Unavailability Expressions	Parameter Definition	Data Requirement for Parameter Estimation
1(a) Periodically tested components (time dependent failures)			
1.1 Hardware failure	$1-\dfrac{1-e^{-\lambda_S T}}{\lambda_S T}$	λ_s : Stand-by failure rate T : Component test interval	λ_s (ratio of number of failures to average standby duration) Number of failures observed in total standby periods under study, Test interval time, number of tests

TABLE 3.2 : COMPONENT UNAVAILABILITY EXPRESSIONS FOR STAND-BY SYSTEMS/COMPONENTS (CONTD.)

Component Type/ Unavailability Mode	**Time Averaged Unavailability Expressions**	**Parameter Definition**	**Data Requirement for Parameter Estimation**
1(a) Periodically tested components (time dependent failures) (Contd.)			
1.2 Test outage	$\frac{\tau}{T} q_0$	τ : Average test duration q_o: Override unavailability (if applicable) obtained from system analysis	Total component stand-by time q_o= No. of override failures/No. of override demands Observed test durations (τ)
1.3 Repair outage	$\lambda_s T_R$	T_R : Mean time to repair	Total repair time, No. of failures during standby period
1.4 Scheduled maintenance	$f_m T_m$	f_m : Scheduled maintenance frequency (includes interface maintenance) T_m: Mean time of scheduled maintenance action	T_m Observed individual times for repair and maintenance, including detection and waiting time
b) Demand failure	n/N	n = number of failures N = Number of demands	n, N
2. Untested component	$1-\frac{1-e^{-\lambda_S T_P}}{\lambda_S T_P}$	λ_s: Stand-by failure rate T_p: Fault exposure time	T_P: Inferred from replacement times of components due to other failures or if not replaced, then assume T_p= 40 years
3. Monitored component	$\frac{\lambda_S T_R}{1+\lambda_S T_R}$	T_R: Mean waiting time plus repair time	

3.2.4.4 Parameter Estimation

PSA work requires extensive collection of operating and maintenance data on failure of components of the NPPs. Plant specific data sources include plant design, operating and maintenance records and procedures, which provide information regarding most of the data items required for PSA. The basic data including human performance to be collected from these sources/records are summarised in Table 3.3. Representative record types and the title of contents of the records is given in Table 3.4. Where data paucity exists, Bayesian method or any other method can be used for estimation of parameters. For plant-specific data, estimation methods for component failure rate, repair time, test frequency and other parameters are explained in Appendix-VII.

TABLE 3.3 : BASIC DATA TO BE EXTRACTED FROM PLANT RECORDS

Data Required to be Extracted	Types of Data
Component failure data	Number of failures and failure mode, total exposure time
Component repair data	Duration of component repair including detection time and waiting time
Component test data	Frequency of tests and test duration times
Component maintenance data	Frequency of maintenance and maintenance duration times
Human performance data	Human related events

TABLE 3.4 : PLANT SPECIFIC DATA SOURCES AND RELATED INFORMATION

General Record Type	Specific Names	Content
1. Design drawing, design basis report, design basis information, design manual, Safety Rreport, Tech. Spec.	P&IDs. Process drawings, electrical drawings, fire zone drawing, design changes.	Type, number, identification, location, functional as well as physical interface of equipment in the plant and operating requirements.
2. Operating records and procedures	Operator (control room) logs, monthly status reports, licensee event reports (ERs, SERs), annual reports	Chronological record of events occurring during operation in various levels of detail and various reporting scopes
3. Plant system specification	System identification list, system operability matrix	Identification of system names, functions and boundaries, and identification of which systems are operable during which plant modes
4. Equipment records	Equipment lists, parts lists	Type, population, functional name, and system assignment of each component
5. Maintenance records	Maintenance logs, maintenance work requests, maintenance reports, job orders, in-service reports	Date, name, type and identification of component and system requiring maintenance action, problem observed, and action taken
6. Test records	Periodic test reports, plant test procedures, plant test schedule, (surveillance schedule)	Procedures, schedule, reporting of tests, and identification of components requiring testing
7. Calibration records	Calibration reports, calibration cards, calibration procedures	Procedures, schedules, reporting of tests, and identification of components requiring testing

Format for component failure data recording is given in Annexure-V.

3.2.4.5 Generic Databases

Whenever plant specific data do not exist for estimating the parameters of the plant models, data from a similar plant or applicable data compiled from national and international experiences can be used. These data are usually referred to as generic databases.

3.2.5 Accident Sequence Quantification

This procedural step includes all the tasks associated with the quantification of the accident sequences as given below.

3.2.5.1 Determination of Accident Sequence Boolean Equations

The determination of the Boolean equations for accident sequences requires the selection of the accident sequences to be quantified and the manipulation of the sequences to place them in a form suitable for quantification. The system models are also placed in the form suitable for the quantification. The selection of accident sequences also requires screening out of sequences at the system level because of their low contributions in comparison with those of other sequences. This screening takes place at the system level within the same plant damage category. For example, assume accident sequence IABC has been quantified and IABDE is to be quantified. If it is known positively that DE has no dependence with IAB and has a much lower probability (e.g., two orders of magnitude) than C, then IABDE might not need to be quantified. Care must be taken in determining that no dependence exists. The manipulation of ETs and FTs to obtain the minimal cut-sets (MCS) and the reduced Boolean equations are discussed in Ref. [4]. Annexure-VI gives basic laws of Boolean algebra.

3.2.5.2 Initial Quantification

The primary events and the frequencies of the IEs are initially quantified by using as point values, i.e. the mean values of the distributions that quantify the associated uncertainties. Where details are not available, conservative values can be used for the primary event data or the IE frequencies. If the conservative values result in significant contributors, then they can be more precisely evaluated. In this task, screening values are used for the Human Error Probabilities (HEPs) identified in ETs/FTs. Human errors, which contribute significantly to CDF, are then studied further as part of the HRA.

Post accident recovery, such as recovery of actuation faults or of pre-accident mispositioning faults, is not credited at this stage.

3.2.5.3 Final Quantification

The final quantification is obtained by using more accurate HEPs and other data values. Where necessary appropriate recovery actions are to be considered. The final results are to be calculated by applying an appropriate multiplicative factor to each cutset probability. This multiplicative factor, which is the non-recovery probability, accounts for the possibility that operator action will eliminate one of the faults in the cutset and thereby prevent core damage. Details of the recovery analysis are given in Appendix-VIII.

3.2.6 Uncertainty Analysis

The objective of uncertainty analysis is to provide qualitative measures of the uncertainties in the results of the PSA, for the frequency of core damage and system unavailability. In fact uncertainty analysis is required to be performed in Level 2 and Level 3 analyses also (see section 3.3.6 and section 3.4.2.10 respectively). Since the PSA model attempts to simulate reality, it is inevitable that there will be simplifying assumptions and idealisations of rather complex processes, phenomena and variability in the data. These simplifications and idealisations will generate uncertainties.

3.2.6.1 Major Sources of Uncertainties

Three major sources of uncertainties are as given below.

(a) Completeness

The main thrust of the PSA model is to assess the possible scenarios that can lead to undesirable consequences i.e., core damage for a Level 1 PSA. However, there is no guarantee that all possible scenarios have been identified and properly assessed. This lack of completeness, which is due to the difficulty to assess and/or quantify all possible scenarios, introduces an uncertainty in the results and conclusions of the analysis.

(b) Modelling adequacy

Even for those scenarios that have been identified, the event sequence and system logic models do not precisely represent reality. 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. These uncertainties are addressed as a part of the uncertainty analysis in the PSA, and sensitivity studies are usually performed to assess their relative importance. The uncertainty analyses and sensitivity studies are also required to be performed in Level 2 and Level 3 analyses.

(c) Input parameter uncertainties

The parameters of the various models used in the PSA are not exactly known because of scarcity or lack of data, variability within the populations of plants and/or components, and assumptions made by experts. These uncertainties can be represented by probability distributions.

3.2.6.2 Propagation of Uncertainties

The quantification of the input parameter uncertainties is usually done by considering a PSA result as the output of a model, in which input parameters are characterised as random variables. The probability distribution function assumed for each parameter then quantifies the uncertainty that is due either to lack of knowledge about the exact value of this parameter or to actual variations in the value of the parameter among the members of a certain population. Annexure-VII gives various uncertainty distributions and their associated parameters. The most widely used technique for propagating uncertainties is Monte Carlo simulation. In general, a Monte Carlo simulation consists of generating a random sample of the inputs of the model and determining the PSA output from each set of inputs in the sample. This process results in a random sample of the PSA output. Quantitative measures of the uncertainty associated with the output are then derived from this random sample. The various Monte Carlo techniques can be distinguished on the basis of the random sampling methods as follows.

(a) Simple random sampling (SRS)

Simple random sampling is the simplest of the sampling methods. In this method, every value of the sample is randomly sampled from its distributions. The main advantages of SRS are simplicity of generation, statistical analysis, and aggregation. With regard to aggregation, simple random samples obtained using the same models and parameter distributions can be combined to make larger samples. There is one main disadvantage of SRS. It requires many simulations, and hence it is time consuming.

(b) Latin hypercube sampling (LHS)

Latin hypercube sampling is one method of sampling a large number of input variables that yields estimators of model response more efficiently than SRS. The name of the sampling method derives from its similarity to certain fractional factorial sampling plans. LHS partitions a parameter range into discrete intervals. A parameter value within each interval is sampled using SRS. This approach reduces the sample size (relative to SRS) required to obtain estimates of a specified precision. The beneficial characteristics of LHS include its unbiased and efficient estimators. The efficiency of LHS versus the SRS has been demonstrated for cases in which the output is a monotonic function of the input variables, as is the case for PSA models when the rare event approximation is used. (In the rare event approximation, the frequency of core damage is expressed as a closed, monotonic function of the various input parameters, i.e., sums of MCS). Furthermore, sub-samples of LHS do not constitute a Latin hypercube sample and hence the LHS dose not exhibits the advantage of aggregation.

3.2.7 Importance Analysis

Importance analysis requires the determination of the importance of contributors to system unavailability, core damage frequency and accident sequence frequencies. However, it can also be extended to Level 2 and Level 3 analyses (e.g. for release frequency, consequence frequency). The importances, which are determinable from a PSA, can be grouped into two classes: (i) qualitative importances and (ii) quantitative importances.

3.2.7.1 Qualitative Importances

Qualitative importances are importances to CDF that are derived from the logic structure of the PSA models. The logic structure of the PSA includes the fault tree and event tree models and the failure combinations causing undesired events (minimal cutsets). The qualitative information in a PSA provides valuable criteria by which to evaluate the importances of risk contributors and changes.

3.2.7.2 Quantitative Importances

The quantitative importances are the importances of CDF contributors and changes that are derived from the quantitative results of the PSA. The quantitative importances utilise the estimated system failure probabilities, accident sequence frequencies or CDF. Although quantitative approaches can provide more detailed information than the qualitative importances, they are also subject to the greater uncertainty associated with the quantification. There are various types of quantitative measures, which have been defined for the interpretation of PSAs and for use in prioritisation of operational and safety improvements. Some of the measures of importance [6] are:

(a) Birnbaum Importance: It is the change in risk for a change in failure probability (1 to 0) for a component or system, i.e.

$$I_i^B = (\partial R/\partial p_i) \tag{3.1}$$

Where R is a measure of the risk that can be defined at various levels (either at the system level, accident sequence level, core damage level, radioactivity release level or consequence level) and p_i is the failure probability between 1and 0 of i^th^ component. Birnbaum importance identifies components/systems important to safety. But it does not consider the likelihood of component failure, i.e. highly important component in the model will have high Birnbaum Importance irrespective of their reliabilities.

(b) Inspection Importance: It is the Birnbaum Importance of a component multiplied by the probability of failure of that component. Inspection importance is the risk due to cutsets containing ith component i.e.

$$I_i^I= pi*(\partial R /\partial p_i) \tag{3.2}$$

(c) Fussel-Vesely Importance: It is the fractional change in risk for a fractional change in a component failure probability i.e.

$$I_i^{FV} = (\partial R/R) /(\partial p_i/p_i) = (pi/R)*(\partial R /\partial p_i) \tag{3.3}$$

(d) Risk Achievement Worth Ratio (RAWR): It is the ratio of the risk with the i-th component failed to the risk as modeled i.e.

$$I_i^{AR} = R_i^+/R \tag{3.4}$$

Where R_i^+ is the risk with ith component failed.

(e) Risk Achievement Worth Increment (RAWI): It is the incremental change in risk due to the failure of the ith component i.e.

$$I_i^{AI} = R_i^+ - R \tag{3.5}$$

(f) Risk Reduction Worth Ratio (RRWR):
It is the ratio of the nominal risk to that with i-th component perfect (Unavailability = 0) i.e.

$$I_i^{RR} =R/R_i^- \tag{3.6}$$

Where R_i^- is the risk with ith component perfect.

(g) Risk Reduction Worth Increment (RRWI): It is the incremental change in risk that results from i^{th} component being perfect (Unavailability = 0) i.e.

$$I_i^{RI} = R - R_i^- \qquad (3.7)$$

Where R_i^- is the risk with i^{th} component perfect.

The relationships among various importance measures can be deduced from their definitions [6].

3.2.8 Sensitivity Analysis

When risk or reliability analysis is performed, it is appropriate to inquire into the sensitivity of the results to input assumptions, models and data. It should be realised that importance and sensitivity of basic events are related. Basic events, which have high importance measures initially without recovery actions, will also display high sensitivity.

The purpose of sensitivity analysis is twofold: (i) to address modeling assumptions suspected of having a significant impact on the results and (ii) to determine the sensitivity of the core damage frequency/system reliability to possible dependences among component failures and among human errors. Sensitivity analysis should be extended to Level 2 and Level 3 PSA studies as required (see section 3.3.6 and section 3.4.2.10 respectively).

3.2.9 Treatment of External Events

External hazards/events are events that originate from causes external to the plant and create extreme environment common to several plant systems. The external hazards due to sabotage are addressed in section 4 of this document. External hazards are significant since they are ideal candidates for CCFs. External events can be considered at any level of PSA, depending on the scope and objectives of the study. However it is more applicable in general to Level 1 and Level 2. External hazards include earthquakes, floods, high winds, aircraft crashes, cyclones, etc. Table-3.5 includes a list of probable external hazards.

TABLE 3.5 : EXTERNAL HAZARDS [7]

Natural Events		
Origin	**Principal Phenomena**	**Associated Topic**
From earth	Earthquakes volcanoes	Capable faults, liquefaction, vibratory ground motion ejected missiles, lava, lahar (mud flow), poisonous gas, volcanic ash
	Soil failures	Slope instability, subsidence, swelling clays, karst collapse
From water	River floods Coastal floods	Dam failure, extreme rainfall, snowmelt Tsunami, seiche, wind generated high waves
From air	Extreme meteorological conditions	Temperature, rain, snow
	High winds Lightening Meteorites	Hurricanes, tornadoes, cyclones, sand storms, forest fire
Man Induced Events		
Transportation (airways, railways, highways, water ways)		Aircraft impact, explosion, missiles, vibration, fire
Nearby hazardous facilities (pipelines, petrochemical facilities, factories etc.)		Drifting clouds, explosions, missiles, vibration, toxic gases, fire

The external event analysis should address the influence of design errors (e.g. numerical errors, wrong assumptions, wrong mass in the seismic model, and error in material properties) and construction errors (e.g.,mistakes in size and material and defective installation), state of the art errors (e.g. loads not envisioned during original design and discovery of partial active fault in the vicinity) degradation effects and human errors due to operator action or inaction. Design and construction errors could be accounted for by using as built drawings, latest plant status and 'walk down' of the plant. The random equipment failures include uncertainty due to maintenance errors. Analytical models may need to be developed to handle effect of ageing and deterioration of electrical and mechanical components. Operator errors under external stress condition in accident situation arising from external event are difficult to model. Nevertheless an attempt can be made to impact these in the PSA model as realistically as possible.

The complete treatment of external event analysis should be carried out as per QA programme described in Chapter 2 as done for internal event analysis. The key elements in this regard include proper organisation and composition of PSA team, task breakdowns, documentation, peer reviews of methods and data and parameters elicited from experts' opinion and use of refined and validated software. Some of the important external events such as Fire, Seismic and Flood are discussed in Appendices IX, X and XI respectively. Aircraft crash and sabotage are addressed in section 4 of this document.

The standard approach for assessment of risk from external events involves IE analysis, or hazard analysis, analysis of effects (plant response analysis), evaluation of fragility/vulnerability of plant components, event sequence and plant system analysis and consequence analysis. Details of these are given below [4, 7, 8].

3.2.9.1 IE Analysis/Hazards Analysis

In hazard analysis, the frequency of occurrences of different intensities of external event called 'hazard intensities' are calculated and presented in the form of hazard curves. This is done in the following steps.

(a) Selection, screening and parameterisation of IEs

An extensive analysis of plant siting and design data needs to be done to list out the possible IEs from which the probable significant events with respect to plant safety can be screened. Since it is not possible to identify all site-specific features, external hazards assessments have been concentrated on a few of these hazards namely earthquake, flood and man induced events, which have emerged as important safety significant events. However, other site-specific IEs need to be considered based on experience and relevance. The preferred approach is to start from a full list and to narrow down the field based on expert judgement. This screening is qualitative. Screening can be done based on impact or based on the frequency of the IE. The reasons for using a particular screening criterion should be recorded. Screening based on assessed frequencies requires regulatory review. If not specified any, the natural hazard initiator that can be shown by detailed analyses to be less than 1.0E-07/year, are screened out.

IEs can be screened out if it can be shown that it is unlikely to have a significant effect on the plant safety.

The task of parameterisation of the events involves identifying the parameter(s) to describe a hazard, with a view to quantification of the damage potential of the event. In case of high wind, wind velocity resulting in dynamic loading is a parameter. Earthquake event can be measured in terms of parameters like frequency of occurrence, Peak Ground Acceleration (PGA). Tornado intensity can be measured on the Fujita Pearson intensity scale, pressure difference and possible missile impact loading. Fire can be measured by sizes (area/number of safety related equipment in a plant getting disabled). For man induced events, maximum amount of material released in transportation, mass and velocity of the impacting object in case of a collision, sizes (weight) and speed in case of aircraft crash, the inventory of material released, nature and pressure of the material for pipeline accidents and overspeed conditions under which missiles are generated under low trajectory turbine disintegration missile accident should be considered for calculation of damage potential.

The damage potential would also depend on the location of the effect in the plant. The effect of co-location of other equipment and structures nearby is to be addressed in fragility analysis, which is done later in plant vulnerability analysis. The simultaneous effect of another PIE resulting from one external hazard should also be considered as applicable. For example, wind speed, duration and direction, which can occur simultaneously with the flood, should be taken into account along with probabilistic assessment of wave action at lower levels, which can be more serious, depending on the site conditions. A severe storm can produce concurrent flooding, high winds and associated missiles and dam overtopping. Although, it is assumed that two external events are statistically independent and that the frequencies of simultaneous occurrence of two or more external event are small, related event sequences need to be considered. For example, seismically induced dam failures and pipe line failures are considered in the seismic analysis. Although two external events may not simultaneously exert stresses on a specific plant component, they may affect different components in the some accident sequence (i.e. an earthquake may fail the reactor components, whereas flooding may damage intake service water pumps).

(b) Hazard analysis

This task involves full hazard analysis that should be performed for each initiating event/ initiator, which has not been screened out or bounded in the earlier task. The objective is to generate a curve that relates the frequency or frequency of exceedance, or the probability to the different size/damage potential of the parameter selected for that particular initiator (external event). In fact a family of hazard curves are developed to take into account the uncertainties in the hazard parameter values and in the mathematical model of the hazard. Such a curve is drawn for a different non-exceedence probability level. A probability is assigned to each hazard curve and the summation of probabilities assigned over the family of curves is unity. This basic information, when combined with plant response analysis, provides the analysts with the information needed to determine the probability of an accident with significant consequences. The full hazard analysis will have to include aspects like warning time, location dependence and recognition of special issues concerning rare events. For example, with respect to warning time, if the reactor can be shut down and secured before the occurrence of the hazard, the risk will be greatly reduced. Such operational procedures should be taken into account by the analysts.

(c) Sensitivity analysis

Sensitivity analysis can explore those issues that concern the model used, the data or the approximations introduced. Sensitivity analysis is required wherever an issue or a parameter affecting the outcome of an analysis cannot be treated in a fully satisfactory way in the main analysis itself.

3.2.9.2 Plant Response Analysis

The plant response analysis covers analysis of the full spectrum of the possible undesirable plant responses in which hazard impact is translated into response (e.g. for earthquake, the response parameters could be displacement, shear moment, spectral acceleration, for extreme winds they could be force or moment on a structural element and deflections). For some external events like fire and flood, no specific response analysis is performed as manifestations, physical effects, response or hazard parameter value itself is significant for evaluation of fragility of SSCs. Plant response includes the response of component to the initiator and the response of the personnel and also the effect it may have on the pre-planned onsite/offsite emergency plan. The analysis will be different for different situations like existing operating power plant, plant under design stage and plant in siting stage since the results of PSA would reflect upon the decisions to be made regarding design aspects of the plants under construction. The information on the plant site, design, as built condition of the plant and operational aspects are required for plant response analysis.

3.2.9.3 Plant Vulnerability/Fragility Analysis

This involves evaluations of component fragility, i.e. ultimate capacity to which component can withstand without failure (functional disability, on the exceedence of which the component fails), which are the conditional frequencies of component failures for different values of the response parameter. Again some differences exist between external events depending on plant system and event sequence analysis. For example, in seismic PSA, fragility may be expressed as function of local response parameter (e.g. PGA versus frequency of failure) and evaluated separately for each component. In turbine missile risk analysis, the conditional frequency of failures from turbine disintegration missile impact is evaluated for different components in the accident sequence. Uncertainties in fragility evaluation arising due to insufficient understanding of the properties and failure modes of structural materials, error in the mathematical modeling for calculations of response, etc. use of generic data and engineering judgement in absence of plant specific data are represented by developing a family of curves for each component and assigning nonexceedance probability/confidence level to each fragility curve. The steps involved in component fragility evaluation are outlined below.

(a) Identification of vulnerable features

The key vulnerabilities are to be identified for the listed IE's. These are further discussed in detail in failure mode analysis and fragility analysis. The analysis should also address certain items that might be ruled out by proving their non-vulnerability to the IE and documented. The basis of considering the vulnerabilities for analysis should be documented for better clarity. For example, in case of flood, vulnerabilities of low lying areas of the plant and components therein should be considered.

(b) Generalised load analysis

The term load is a generalised term and includes conditions such as acceleration, impulse, impact, temperature, etc. or other adverse conditions because of the effect of the IE. For floods loads can be static (hydrostatic pressure, etc) or dynamic (wave action, water velocity etc.) and both should be considered. For translational wind, wind speed and aerodynamic considerations determine the loading. Pressure differential effects, which can produce very large load on structures, should also be considered for tornado type winds.

(c) Failure mode analysis

The objective of this task is to determine the specific failure modes that will cause each vulnerable component or structure to fail. A crucial aspect of this determination is to decide on definition of failure. For the purpose of PSA analysis, failure is always understood in context of function: each SSC has a safety function that it must perform and the failure means failure to perform or support the relevant safety function as per design intent.

Component may have 'n' different failure modes and different failures may lead to different subsequent effects. For example, for an electrical pump failure could be "fails to run" or "fails to start", mechanical failure (shaft seizure) and support failure. The different modes of failure of a component are to be listed out for each item under consideration. When making the evaluation, and particularly when reviewing the data, it might be possible to screen out some failure modes that are insignificant. The fragility curves have to be drawn for all failure modes for finding out the dominant failure mode.

(d) Fragility analysis

The fragility or vulnerability of a component is defined as the cumulative frequency of its failure (conditional failure probability) for hazard intensity (e.g., ground acceleration, over-pressurisation in an explosion, or wind speed) of less than or equal to specified value. The fragility is estimated from the actual capacity (ability to withstand the effect of initiator) in any given failure mode.

The objective of Fragility Analysis (FA) is to determine the probability of failure of specific components or structures because of the loads experienced due to external hazards. For FA, perform the following steps:

- Calculate the appropriate strength of component in failure mode(s) under consideration
- Calculate stress or load to the components resulting from the external initiator
- Provide a factor to account for inelastic absorption of energy
- Consider any additional loads from its operating environment and the external events resulting from secondary failures, e.g., safety valve operation, LOCA, turbine trip, collapse of wall, etc.
- Generate fragility curves considering uncertainties in capacity estimation of components.

(e) Event sequence and system analysis

The objective of this task is to identify and analyse the combinations of failures leading to an undesired end state for the ensemble of postulated accidents. This is performed by developing ETs/FTs with external events of particular hazard intensities and/or impacting external event in the component failure modeling for the range of hazard intensities defined in the problem and merging with internal event analysis. However, the analyst may treat, as required, the external events separately and calculate the frequencies of release categories resulting from external events. The FT/ETs developed for the internal initiator part of the analysis can also be used for external initiators, but this is not always the case. In some instances it would be necessary to develop special ETs or special FTs for the specific initiator under study. The important issue in this analysis is that of dependent failures. Another key issue is combining failures caused by external initiators with unrelated failures caused by internal plant faults or human errors.

(f) Consequence analysis

Various failure sequences leading to core damage are evaluated separately. Containment failure and specific release categories and consequences in the public domain are evaluated in Level 2 and Level 3 PSA analyses described in the later sections. The unconditional frequency of core damage/melt or of radionuclide release for a given release category is obtained by integrating over the entire range of hazard intensities. If the external event analysis is merged with internal event at the ET development stage, information should be provided on the IEs for each range of hazard intensity, necessary modification to the ET/FTs, changes to APET/CETs and differences in consequence analysis results. If the external event analysis is merged with internal event analysis at the consequence stage, the analyst should provide the probability distribution of the frequency of release for each release category. If the analyst decides to keep the external event analysis totally separate from the internal and other external event analysis, the probability distribution of frequency release categories is input into the consequence model developed for the external event analysis. Also, the effect of one external event may be inducing radioactivity release, whereas the other initiated/initiator external event may modify the parameter of consequence model. For example, a large earthquake or external flood may disrupt the communication network and damage the evacuation routes to account for the effect of large seismic events on roads, bridges, structures and communication. An extreme wind may carry radioactive material to more distant locations.

(g) Uncertainty analysis

There are many uncertainties in the analysis of external events. These arise from lack of data indicated and analytical models used in the analysis. In the hazard analysis the uncertainties to be considered are those in the frequency of occurrence of the hazard intensity. The characterisation of the phenomenon (e.g. line source or point source for seismic events, fault width and length for a tornado etc.) and transmission of effect (e.g. overpressure, missile impact ground acceleration, etc.) from the sources to the site. In the component fragility evaluations, uncertainties arise from an insufficient understanding of the properties and failure modes of structural materials, errors in the calculated response due to the approximation in modeling, and the use of generic data and engineering judgement in the absence of plant specific data. These uncertainties in this document are grouped into two categories as required with regard to the external event under consideration; one is the frequency/inherent or statistical randomness to represent the underlying randomness of variables and events and the other is 'uncertainty', 'probability' to represent modelling uncertainty accounting for current level of ignorance concerning these variables and events. As external events are analysed with plant level FTs, uncertainties are propagated by assigning probability distribution for each component failure frequency in Boolean expression. Usually a family of curves for plant level fragility for core damage/melt and for each release category is obtained. Integration over the hazard curve family gives the probability distribution for CDF and the frequency of each category. Integration can be accomplished by commonly used methods like discrete-probability distribution, arithmetic, moment methods, Monte Carlo error propagation or other statistical techniques.

3.2.10 Documentation of Level 1 PSA

The main objectives and format of the documentation of Level 1 PSA are given in Appendix-I.

3.2.11 Computer Codes

Some of the software packages or computer codes used for Level 1 PSA are mentioned in Appendix-II.

3.3 Procedure for Conducting Level 2 PSA

3.3.1 Objective and Scope of Level 2 PSA

The objective of level 2 PSA is to cover events occurring in accidents that generate thermal and mechanical loads on the containment boundary with the potential for causing structural failure and consequent release of radioactive material to the environment. Typical uses of Level 2 PSAs [9] are: (i) to gain insights into the progression of severe accidents and containment performance and identify plant vulnerabilities, (ii) to identify major containment failure modes and to estimate the corresponding release of radionuclides, (iii) to provide a basis for the evaluation of off-site emergency planning strategies, (iv) to evaluate the impacts of various uncertainties, (v) to provide a basis for accident management strategies, (vi) to provide a basis for the prioritisation of research activities for minimisation of risk and (vii) to provide insights to Level 3 PSA.

The scope of level 2 PSA is to analyse accident progression and phenomena leading to potential containment failure and release of radionuclides to environment. If a Level 3 analysis is contemplated, the input requirements such as the inventory of radioactive material released, its physical and chemical characteristics, and information on the time, energy, duration and location of the releases (ground level or stack level) must be accommodated in Level 2 analysis. The ultimate product of a Level 2 analysis is a description of a number of accident situations demanding containment integrity, a description of the possible containment responses and their estimated probabilities and an assessment of consequent releases to the environment.

3.3.2 Interface with Level 1 PSA: Grouping of Sequences

PSA level 1 identifies a very large number of accident sequences, which may lead to core damage. These sequences are grouped together into Plant Damage States (PDSs). PDSs group sequences that would be expected to have similar effects on containment response and fission product source terms. The grouping is based on the initiator type (e.g. large LOCA, transients), Reactor Coolant System (RCS) pressure at core damage, status of Emergency Core Cooling System (ECCS), status of containment's engineered safety features, and status of primary and secondary containment (like isolation/ bypass, failure). By doing so, the number of unique accident conditions that must be addressed in Level 2 is greatly reduced.

Broadly PDSs can be grouped into two main classes: those in which radioactive material are initially released to the containment and those in which the containment is either bypassed or ineffective.

(a) For PDS in which the containment remains intact, account must be taken of plant failures that are defined in Level 1 analysis that could influence either the containment challenge or release of fission products. This will include the following.

  (i) The type of initiator (e.g. LOCA) since this will affect the rate of discharge of fluid to the containment and timing of release of fission products.

  (ii) The mode of failure of ECCS (e.g. injection mode, recirculation mode) since this will influence the timing of core melt (early or late). Injection mode failure is likely to lead an early core melt. Whereas failure during recirculation will lead to a late melt.

  (iii) The circuit pressure at vessel failure (in case of PWRs) since this may influence the mode of vessel discharge and could challenge the containment (e.g. high pressure melt ejection, direct containment heating)

  (iv) The pressure at vessel failure which will be influenced by the size of the initial breach in the circuit (i.e. the initator type) as well as by the functionality of any depressurising system).

  (v) The status of containment's engineered safety features (e.g. containment pressure suppression system, containment filtration and pump back system, etc.)

  An Accident Progression Event Tree (APET, as mentioned in NUREG-1150 or Containment Event Tree CET, as called by some countries like Russia, TECDOC-1002) analysis will need to be performed. The terms APET/CET are used interchangeably in this document. Event trees generated in accident progression analysis in Level 2 for various plant damage states are called APETs/CETs.

(b) For PDSs with containment bypass, only source term analysis is required. Here the main consideration will be the identification of those attributes that influence the fission product source term. This will include the initiator type, status of ECCS (including failure time) and whether the leak is isolable after a period of time. For leaks into the auxiliary buildings, the status of the air conditioning and ventilation systems could be important. In principle, the extension of other initiators (internal and external hazards), could lead to the definition of a new set of distinct PDSs. In many cases, the hazards simply cause dependent failures of plant items and so are treated using the same plant models as are used for internal initiators. They will therefore yield the same PDSs. The area where there may be differences relates to direct containment damage. Events such as earthquake or external missiles may lead to containment failure as well as core damage. It may be necessary to create additional PDSs to cover these, but it may be possible to use existing PDSs which represent isolation failure.

  The extension of PSA to states other than full power introduces requirements to determine whether additional PDS, may be required. The significant differences occur primarily as a result of differences in inventory, primary circuit and containment state.

3.3.3 Accident Progression and Containment Analysis

The purpose of the accident progression and containment analysis is to track the physical progression of the accident from the IE until it is concluded that no additional release of radioactive material from the containment building will occur. The analysis tracks the impact of the accident progression on the containment building structure, with particular focus on the threat to containment integrity posed by pressure loadings or other physical processes. A typical list of the important accident phenomena for plant specific analysis, to be addressed in accident progression models, is given in the Appendix-XII.

An important part of Level 2 PSA is modelling of the severe accident phenomena that occur with onset of core damage and progresses to failure of containment and release of radioactive material from the containment to the environment. Core damage progression results in core debris formation, release of large heat source, hydrogen and radioactivity into containment threatening its integrity. The severe accident progression phenomena are highly complex set of physical and chemical phenomena [9]. The purpose is not to fully describe this complexity, the understanding of which is still going on as a research activity, but to place the phenomena within the overall structure to locate areas effectively, to model these into Level 2 PSA studies. These of course contribute to uncertainty in the analysis.

(a) Accident phenomena for LWR/PHWR accident sequences

The phenomena can be divided into three stages, viz., (i) Phenomenon within Reactor Pressure Vessel (RPV) and Reactor Coolant System (RCS), (ii) Phenomena within reactor cavity/vault and (iii) Phenomena within containment building.

(i) Phenomena within RPV and RCS

When means of removing decay heat are inadequate or lost, core heats-up and fuel clad material softens. Fuel clad gap gas pressure causes clad to swell (ballooning). Eventually cladding fails releasing gap inventories (‘Gap Release’) into RCS. At higher temperature clad will melt, interact with fuel, fuel can slump. As the core heats up in-vessel heat transfer and fluid flow are affected, which lead to steam formation and failure of RCS pressure boundary. With core-heat up, clad material (Zirconium) reacts with water/ steam to form zirconium oxide and hydrogen. The amount of hydrogen generated will depend on factors that include oxide layer, steam concentration, operator action, accident scenario, etc. As the fuel heats to its melting point more fission products would be released from the fuel (‘melt release’) and will be transported through RCS. With the heat-up process, melting of clad, fuel, control rod, other structural material and failure of RPV involving core degradation and loss of geometry will progress. The in-vessel core coolant reaction may cause steam explosion, missile generation and failure of reactor vessel. Vessel melt-through would otherwise result as core melt debris does not get cooling or becomes uncoolable. In some situations, consequent to high temperature and pressure, lower welding of RPV may rupture with sudden release of steam and molten core material (in reactor cavity/vault) and may cause vessel lift-off.

(ii) Phenomena within reactor cavity/vault

With core debris ejection from vessel, in absence of ex-vessel core catcher or failure of functioning of the core catcher, core-concrete reaction (Corium) takes place, with dispersed melts getting released into containment. This phenomenon is called High Pressure Melt Ejection (HPME) that causes Direct Containment Heating (DCH) and threat to the integrity of the containment.

In case of PHWR , core debris from vessel on getting into vault water, might cool off. In adverse condition, it may react with vault water and may cause steam explosion. If reactor vault including structural and biological shield fails, HPME will find way to containment. If the cooling to the core debris, having fallen on to the concrete at the bottom of the cavity/vault floor, is inadequate or the core debris is in uncoolable configuration, then concrete will heat up and break-up physically and decompose chemically. The chemical reaction will produce gases. The extent of the ablation of the concrete and rates of gas production are strongly dependent on the composition of the concrete aggregate. Basemat penetration is generally considered to be a less severe mode of containment failure, because (i) penetration rate is likely to be slow and cooling from the surroundings may arrest progression of basemat penetration and also

(ii) the fact that the fission products have to pass through the subsoil before they can reach the external atmosphere. The gases from corium bubble through melt, and take fission product vapours and aerosols with them and finally release to containment. Cooling/quenching of corium may take place with surrounding water or water introduced by engineered system and prevent or minimise the severity of further accident progression. However, possible formation of insulating crust on the top of the debris also needs to be examined also.

(iii) Phenomena within containment

The thermal hydraulic phenomena subsequent to release of heat and injection of gases into containment from core damage progression and operation of engineered safety features will govern pressurisation of the containment. Hydrogen, released into the containment with oxidising atmosphere there, can cause burning. Three different rates of combustion depending on concentration of hydrogen, concentration of steam and other gases such as CO or CO_2 can take place; local burning by diffusion flames, deflagration and detonation. Deflagration is a form of combustion in which the flame moves at a subsonic speed relative to the unburned gas. Local burning as well as deflagration may cause static or quasistatic pressure loads on the containment owing to extra heating of the containment atmosphere. Hydrogen detonations involve the reaction of hydrogen through the supersonic propagation of a burning zone or combustion wave. The pressure loads developed are essentially dynamic loads, which may cause a breach of the containment or damage to safety equipment. The ESFs to remove heat and steam may be water sprays, fan-cooling units, and ice beds. The ESFs to prevent pressure loads from hydrogen burning is hydrogen recombiners.

In PHWR the containment venting (Primary Containment Controlled Discharge System) to release containment pressure, filtration and pump back system to remove iodine activity and the containment isolation system to reduce ground level release of radioactivity are other containment ESFs. The radioactivity release in a severe accident occurring in stages are categorised broadly as in-vessel and ex-vessel release, and described later in this chapter under section 3.3.4.3.3.

It is essential to ensure that relevant accident phenomena are addressed in the plant specific analysis. If published data from experiments or reference plant analysis is used to evaluate certain phenomena, the relevance of that information to the plant being studied should be confirmed. If plant-specific analysis is performed the data used to perform the calculations should be checked.

(b) Phenomena in FBR accident sequences

In FBR, before the FP can reach core cover gas and subsequently to the reactor containment building (RCB), they may get removed by diffusion in sodium and reaction with structural material and sodium. Several models [11-12] have been developed on these phenomena but these have not been verified experimentally. Based on experiments conducted in several countries, following assumptions are made: (1) the fission gas release is total; (2) the volatile fission products release fraction depends on their physical-chemical properties and evolution of thermodynamic conditions during the development of accident, and (3) the non volatile FP and fuel released fraction is closely bound to the molten fuel coolant interaction and then to the coolant decontamination factor depending on many parameters such as bubble formation, pool depth, etc. It has been observed that for volatile FP, the iodine cesium vapor contribution to the source term in RCB is negligible compared to the iodine and cesium combined with liquid sodium aerosol contribution. For non-volatile radionuclide, the source term depends on the pool height above the core and on the obstacles present in the plenum.

The FP accumulated in core cover gas find path in the RCB through the penetrations to the top shield. Physical processes that take place in the RCB are agglomeration, sedimentation, thermophoresis, diffusophoresis and turbulent impaction. Wherever it is not possible to model the processes, the data from experiments are used to calculate the effect of the processes. It is found that gravitational sedimentation contributes maximum to the removal rate of the aerosols. The codes developed dealing in this aspects are given in References [13,14].

3.3.3.1 Modelling and Analysis of the Progression of Severe Accidents

The plant specific analyses of the progression of severe accidents are performed using any of the appropriate computer codes as given in Appendix-II or developed by the user (need to be validated). In addition, if available, literature for similar plants and containments could be used as a basis for establishing an adequate framework for the APET/ CET quantification. Deterministic accident progression analyses could be performed for dominant PDSs with respect to frequencies and PDSs that involve either direct containment bypass or early failure of the primary and /or secondary containment.

The user should identify the computational tools (codes) used to perform accident progression analysis depending on the objectives of the PSA study. The requirements for a meaningful code are

(i) most of the events and phenomena that may appear in the course of the accident are modelled,

(ii) interactions between various physiochemical processes are correctly considered and

(iii) computing time and resource requirements are reasonable.

Computer codes that address the entire spectrum of processes (integrated computer codes) provide an integrated framework for evaluating the timing of key accident events, thermodynamic histories of the RCS, core and the containment, and corresponding estimates of fission product (FP) release and transport. However, the broad scopes of these codes demand simplifications in many aspects of accident progression models so that they complete calculations in a reasonable short time.

In some studies, calculations with integrated codes are replaced or supplemented with calculations performed by other codes that address specific aspects of severe accident progression. These computer codes allow them to address important accident phenomena in a greater level of detail. The user should take note of the specified areas in which these codes are used, and determine whether results obtained with them are used, in conjunction with, or in place of, those obtained from integral code calculations. The user must be aware of the limitations and weaknesses of the codes.

3.3.3.2 Containment Performance

Calculations of severe accident progression generate pressure and temperature histories within containment during various accident sequences. To determine whether the containment pressure boundary will be able to withstand these loads, quantitative estimates of its structural performance limits (ultimate pressure/temperature capabilities) must be generated. This analysis should include all important elements and factors such as,

(i) specific design and features of the containment to be analysed (containment configuration, construction materials and reinforcement, penetrations of all sizes, their location in the containment structure and local reinforcement, penetration seal configuration and materials and local discontinuities in the containment structure),

(ii) specific material properties,

(iii) influences of surveillance tests, inspections, maintenance, repairs and effects of ageing,

(iv) assumptions (conservatisms used when information is limited or missing),

(v) initial (ambient pressure and temperature) and boundary conditions (transient pressure, temperature and heat flux etc.). Status of the containment elements depending on the plant’s operating conditions and initiating and consequential events in accident sequences,

(vi) failure modes and the extent of failures; failure criteria,

(vii) loads and phenomena impacting on the containment during accident sequences (pressure, temperature, thermo-mechanical erosion of concrete, missiles, shock waves, etc.),

(viii) performance of containment systems and equipment during accident sequences, and

(ix) accounting for uncertainties.

The typical containment failure modes and mechanisms are given in the Table-XIII-1 of Appendix-XIII.

(a) Structural response analysis

An analysis of containment structural response to imposed loads (such as pressure, temperature) should consider interactions between the containment structures and appended neighbouring structures, internal and external (e.g. reactor vessel and pedestal, auxiliary buildings).

A complete structural performance assessment should distinguish conditions that would result in catastrophic failure of the pressure boundary from those that result in small scale damage, and identify the anticipated location of failure. Two basic models have been used in PSA studies to characterise the loss of containment integrity resulting from structural failures.

(i) Threshold model: It defines a threshold pressure, with some associated uncertainties, at which containment is expected to fail, with a large rupture, with the potential for significant and rapid blow down of the containment atmosphere to the environment.

(ii) Leak before break model: It is pertinent to linear tear and penetration failure. Containment leakage is expected to precede major rupture. In general, leakage begins at a pressure below the ultimate capability pressure and progressively increases up to the ultimate capability pressure, at which point a catastrophic failure is expected to occur.

While internal pressure loading is the principal determinant of potential containment failure, consideration is also given to the possible effects of temperature on structural performance of containment. Containment temperature could affect the strength characteristics of the structural material as well as cause degradation of penetration seal materials.

If external events are considered in the PSA, containment structural response to postulated external events should be evaluated. Analysis of structural response to dynamic loads (i.e. shock phenomena, hydrogen combustion, etc.) should also be carried out. The containment structural performance must also take account the uncertainties associated with estimating the structural capacities for withstanding extremes of pressure and/or temperature. These uncertainties can be determined by standard techniques for uncertainty quantification and propagation.

(b) Containment bypass

In addition to structural failure of the containment pressure boundary, a thorough characterisation of containment performance should examine mechanisms and pathways by which FP released from the RCS may bypass the containment and be released directly to the environment. Typical bypass mechanisms include:

(i) interfacing system LOCAs (such as LOCA in FM system when connected to channel, LOCA in feed and bleed system),

(ii) steam generator tube rupture and

(iii) failures/leaks associated with personnel and material air locks.

3.3.3.3 Development and Quantification of APET/CETs

APETs or CETs are used to characterise the progression of severe accident and containment failure modes that lead to releases of fission products beyond the containment boundary. For a given core damage scenario, APETs/CETs are used in modelling the severe accident progression and containment response. Each branch point in APET/CET corresponds either to the availability of some containment system function or to the likelihood of occurrence of some physical phenomenon. A containment/ accident progression event tree can therefore be used to define sequences and serves to link core damage sequences with radiological source terms. In developing the event trees (APET/CET), following guidelines are required to be followed.

(i) The APET/CET structure must be logical, open to scrutiny, complete, consistent and to an appropriate level of detail.

(ii) The APET/CET nodal questions must determine the likelihood of whether the containment is isolated, bypassed, failed, vented or intact. Typical APET/CET nodal questions for a PWR are is given in Annexure-VIII.

(iii) It is desirable to keep the number of nodal questions reasonably small at a level consistent with the current understanding of severe accident phenomena.

APET/CET structure and nodal questions must address all the relevant issues important to the progression of severe accidents, containment response and failure and source terms.

(a) Accident recovery/management actions

Any recovery actions beyond the initiation of core damage (e.g. accident management actions) could be taken into account in APETs/CETs, provided that the following guidelines are followed.

(i) The recovery actions are those, which are beyond EOPs and which operators may be able to take as emergency measures, and also actions identified in EOPs for which analysts has not taken credit of. APET/CET quantification is based on a realistic human reliability analysis, thus providing an adequate base for selection of the branch probability estimates.

(ii) The effect of the environmental conditions resulting from a severe accident on the survivability of active components must also be considered (e.g. unavailability of pump due to excessive flooding).

(iii) Potential adverse effects (the potential for an energetic fuel-coolant interaction, fuel shattering, steam explosion, additional release of hydrogen and fission products) of recovery (e.g., injection of water into a degraded core, which can have adverse effect of fuel shattering, steam explosion) must also be considered as part of the event tree quantification.

(b) APET/CET quantification process

The quantification of the conditional probabilities for the branch point must be supported by documented analyses and recent data, including considerations of uncertainty issues for severe accidents. The determination of conditional probabilities (at each branch point) is based on deterministic analyses and expert judgement. The quality of this expert judgement is dependent on the analyst's current state of knowledge on a particular issue. However, sources of up to date information should be available to support the nodal probability (branch probability at each node) assignments, such as,

(i) deterministic analyses using severe accident codes or basic principles,

(ii) other PSA studies of similar plant, and

(iii) relevant experiments, reviews and analyses.

At present, there is no standard method for use of expert judgement and FT analysis as applicable in PSA process. Assignment of subjective probabilities to various events and phenomena is itself controversial. But in order to assess the uncertainties in the progression of severe accidents, some reliance on numerical assignment of subjective probabilities is essential.

(c) Threshold approach

The failure probability is a function of how close the parameter is to the failure threshold. An example, for failure of the RCS induced by natural circulation, is given below.

First, perform calculations for the accident sequence using a code and determine the structural temperature distribution. Second, on the basis of these calculations, and the body of evidence that exists in the literature, determine the likelihood of creep rupture failure by comparing temperatures. Third, find out how close is the calculated structural temperature to the yield point at a given pressure and assign the probabilities. If calculated temperature is much less than the yield point at a given pressure assign 0.01; assign 0.5 for structural temperature near to yield point and 0.9 for structural temperature greater then the yield point. The assignment of numerical values, is therefore, indicative of the analyst's judgement of and belief in the acceptability of the deterministic predictions of uncertain phenomena.

(d) Integral approach

In this approach, both the quantity of interest (pressure, temperature, etc.) and failure criteria (failure pressure, failure temperature, etc.) are treated as uncertain parameters. Probability density functions representing uncertainty distributions are arrived at on the basis of deterministic analyses and expert judgement. The failure probability is determined by the overlap/ interference of these two uncertainty distributions. An example of containment failure induced by DCH due to HPME is given below.

Perform parametric HPME and/or DCH calculations to arrive at containment pressure at vessel breach. Determine the upper bound pressurisation (based on parametric assumptions) and assume that it corresponds to the 90th or 95th percentile of the distribution. Determine the reasonable lower bound pressurisation and assume that it corresponds to the 5th or 10th percentile of the distribution. Construct an uncertainty distribution (distribution shape and/or type is judgemental and depends upon strongly on the extent of information available) for pressurisation loads inside containment due to HPME and/or DCH. On the basis of analyses of the structural performance of the containment, determine the uncertainty distribution for containment structural failure pressure. These uncertainty distributions determine the degree of belief (subjective probabilities) for failure.

3.3.3.4 Binning of Event Tree End States into Release Categories/Bins

The APET/CET produce a large number of end states, some of which are either identical or similar, in terms of key release attributes. These end states are often grouped together on the basis of appropriate attributes that affect fission product releases and accident consequences. These attributes are specific to the plant and the containment type. Table-XIII-2 of Appendix-XIII provides a list of important binning attributes for APET/CET end states.

In defining the attributes of the release categories, attention is paid to the requirement of Level 3 PSA. The source term information, that the Level 3 PSA analysis requires for each release category covers, the following.

(i) The radionuclides including the chemical forms of each radionuclide.

(ii) Frequency of each release category.

(iii) Amount of radionuclides released as a function of time.

(iv) Time of the release relative to reactor shutdown.

(v) Warning time (for implementation of counter measures).

(vi) Location of release (ground level or elevated release).

(vii) Energy content of release.

(viii) Particle size distribution of the released nuclides.

The rationale for a particular grouping scheme of the APET/CET end states into release categories must be thoroughly discussed and documented, as it could affect the results of a subsequent Level 3 PSA.

3.3.3.5 Treatment of Uncertainties in Accident Progression

Uncertainties arise in the Level 2 PSA as a result of several factors, including incomplete merit of possible scenarios, incomplete knowledge of severe accident phenomena, simplification in modelling, inaccuracy in grouping of Level 1 sequences in to PDSs as the input to the Level 2 and input parameters associated with the specific Level 2 PSA. There is no universally accepted approach to uncertainty analysis. In general, uncertainty analysis is carried out by the following three principal steps.

(a) Definition of the scope of the uncertainty analysis: The nature of uncertainties in the accident progression, containment and source term analysis must be considered. The choice of method depends on the requirement for uncertainty analysis in the overall PSA and the need to achieve compatibility with the other components of PSA.

(b) Characterisation/evaluation of each uncertainty issue: The issues may be derived from those which have been identified as a result of review process (by experts). The selection of issues is mainly achieved by sensitivity analysis and the analyst's judgement.

(c) Display and interpretation of the results: The results of uncertainty analysis should be carefully displayed carefully to strengthen the Level 2 conclusions using displays such as histograms, probability density functions, cumulative distribution functions and tabular formats showing the various quantities of the calculated uncertainties together with the distributional mean and median estimates. Evaluation of uncertainties are discussed in section 3.2.5 and 3.3.6.

3.3.4 Source Term Evaluation

A source term is defined as the quantity, timing, duration and characteristics of the release of radioactive material to the environment, following a postulated severe reactor accident. However, a distinction needs to be made here between the 'Accident Release Source' and the 'Source Term' as used in this document. The accident release source refers to the estimates made for an actual accident or to the measurements made for an actual accidental release and is specific to that particular accident. Source term analysis is performed under Level 2 PSA. The following are different aspects of the source term having bearing on the accident consequences.

(i) The rate and the total amount of radio-active material released: This is determined by the reactor inventory (which in turn depends on the design and operating power of the reactor) and the nature and severity of the accident.

(ii) The relative mixture of radionuclides released: This may be different from the composition existing in the core prior to the accident. It is determined by the chemical, physical, and radiological properties of the nuclides concerned.

(iii) The relative mixture of gases, volatiles and particulates released: The physical form of the activity released determines primarily its escape potential from the plant.

(iv) The environment of release and the accompanying energy: Atmospheric releases at high elevation, accompanied by high energy ensure a wide dispersal of radioactivity.

A simplified characterisation of the source is a first step in comprehending and analysing the consequences of release of radionuclides with a wide variety of physical and chemical forms, into the environment. The release may occur through the liquid route as well as the air route, the former generally considered as being less important and may result in the contamination of ground or surface waters. The nature of release may change over time, particularly if the release itself is prolonged.

Historical perspective of the source term evaluation is given in Annexure-IX.

3.3.4.1 Source Term Determination in PHWR Safety Analysis [111]

In the Source Term estimation for the DBA in a standardised Indian PHWR rather conservative assumptions are made as follows:

- Releases to the containment
  - 100 % of core inventory of iodine and noble gases is assumed to be released from the core. All FPs are assumed to be released instantaneously to the reactor containment.
  - For accident scenarios involving LOCA with failure of the ECCS water-trapping factor of 2 on iodine releases is considered in the Primary Heat Transport (PHT) circuit.
  - For a LOCA with availability of the ECCS, the water trapping factor for iodine is 2 x 10 ^{5}.
- Reduction factors for iodine during transport in containment
  - The iodine plate out half times for deposition in the containment are 1.5h in the primary envelope and 2.0h in the secondary envelope.
  - Once the air concentration of iodine in air has reached 10 % of the original value, further plate out of iodine is not considered
  - A plate out factor of 10 is considered for all leak paths in containment
  - The radioactive decay of FPs in the containment shall be permitted.
- Cleanup efficiency in ESF iodine filters shall be as follows.

-	Particulates in HEPA filters	:	99.9 %
-	Elemental iodine (I_2) in charcoal filters	:	90.0 %
-	Organic iodine (CH_3I) in charcoal filters	:	90.0 %

- Containment leak rate

  The containment leak rate for the primary and secondary envelopes shall be assumed as stipulated in the TS. An appropriate secondary containment bypass factor obtained by measurement or as considered in design shall be allowed.

Details of the FP core inventories for different types of reactors are given in Appendix-XIV.

3.3.4.2 Source Term (ST) Analysis Methodology

The starting point of ST analysis is a description of the accident sequences and damage states for the plant. This consists of collecting together groups of sequences, which are similar in their initiation, timing and state of plant damage into a limited number of source term or release categories. A single sequence, generally the one of highest ST which contributes a significant frequency within each category is then selected, and the ST evaluated for this is taken to be representative of the whole category. The core of a power reactor contains several million curies of radioactivity of hazardous nuclides built up during equilibrium power operation. Several barriers (e.g., fuel matrix, fuel cladding, RCS and reactor containment) must be breached before any significant part of this radioactivity can be released to the environment. Establishing the timing and nature of breaching of these barriers is an essential part of ST analysis.

Another requirement is an analysis of the chemical and physical behaviour of the radioactive material, which controls its release from the core and its transport through the plant to the environment. The aim is to find out what part of the activity originally released from the core will be retained in different areas of the plant, and what part will escape. Early containment failures are usually associated with high source terms. On the other hand, a delayed containment failure will ensure that a good part of the radioactivity reaching the containment is retained therein. It must be pointed out that the possibility of containment bypass - both partial bypass and total bypass - must be established, for that would result in high ST scenarios even when the reactor has a strong containment. All severe reactor accidents that result in large source terms must have two features; first the core must be grossly damaged, and secondly, the containment must undergo some degree of failure.

A generalised severe accident sequence would consist of the following parts:

- IE and response of the ESFs
- Core heat-up and reactor coolant system response
- Vessel penetration (if appropriate)
- Core-concrete interaction (if appropriate)
- Containment response.

An ET is drawn for each of the IEs with the postulated system responses, and a set of severe accident sequences is obtained, each one terminating in a different end-state. The end states are subsequently binned into a limited number of release categories.

(a) Computation of FP inventories and their grouping [15, 16, 17]

The second step in ST analysis is ascertaining properties of radionuclides and their grouping. In a nuclear reactor, there are several hundred radionuclides generated that can be grouped as FPs, actinides and activation products. The amount of actinides/transuranics increases with burn-up, and is particularly high for those reactors, such as the FBRs and LWRs, having high burn-ups. It should be noted that fuelling with mixed oxide fuel increases the inventory of transuranics due to the irradiation of plutonium throughout the cycle. In spite of the fact that 3 - 4 % of the transuranics were released in the Chernobyl accident in the initial disruptive phase, these are not expected, in general, to contribute significantly to source terms.

Based on the criteria of the quantity, release fraction, half-life, emitted radiation type and energy and chemical characteristics, these are reduced to 54 nuclides (24 elements). Table 3.6 gives the list of elements and nuclides. These are further arranged into eight groups, each comprising elements with similar chemical and physical properties (hence similar release and transport behaviour). This is shown in Table 3. 7.

A precise computation of FP inventories is a fairly complicated process, which involves finding the actual composition of the fissile nuclides (U-235, U-238, Pu-239) in the core mass, actual history of power operation, and the effects of formation by fission, radioactive decay, and neutron absorption. The nuclide growth and decay equation for all FPs are solved using elaborate computer codes, such as ORIGEN2 [17]. Some of the computer codes for computing fission product buildup in a reactor core can be modified to generate actinide and activation product inventories. These are finally grouped into three broad categories based on their volatility, which primarily governs the extent to which the core activities are released from the reactor fuel and escape from the primary system, with their chemical properties in the existing environment also playing a role.

TABLE 3.6 : LIST OF RADIONUCLIDES

1. Cobalt	^{58}Co, ^{60}Co
2. Krypton	^{85}Kr, ^{85m}Kr, ^{87}Kr, ^{88}Kr
3. Rubidium	^{86}Rb
4. Strontium	^{89}Sr, ^{90} Sr, ^{91}Sr
5. Yttrium	^{90}Y, ^{91}Y
6. Zirconium	^{95}Zr, ^{97}Zr
7. Niobium	^{95}Nb
8. Molybdenum	^{99}Mo
9. Technetium	^{99m}Tc
10. Ruthenium	^{103}Ru, ^{105}Ru, ^{106}Ru
11. Rhodium	^{105}Rh
12. Tellurium	^{127}Te, ^{127m}Te, ^{129}Te, ^{129m}Te, ^{131m}Te, ^{132}Te
13. Antimony	^{127} Sb, ^{129} Sb
14. Iodine	^{131}I, ^{132}I, ^{133}I , ^{134}I, ^{135}I
15. Xenon	^{133}Xe, ^{135}Xe
16. Cesium	^{134}Cs, ^{136}Cs, ^{137} Cs
17. Barium	^{140}Ba
18. Lanthanum	^{140}La
19. Cerium	^{141}Ce, ^{143}Ce, ^{144}Ce
20. Praseodymium	^{143}Pr
21. Neodymium	^{147}Nd
22. Neptunium	^{239}Np
23. Plutonium	^{238} Pu, ^{239}Pu, ^{240}Pu, ^{241}Pu
24. Curium	^{242}Cm, ^{244}Cm

TABLE 3.7 : GROUPING DONE IN RSS BASED ON SIMILAR PHYSICAL AND CHEMICAL PROPERTIES

Group	Element	Volatility
1	Noble gases (Xe, Kr)	Inert
2	Halogens (I, Br)	Volatile
3	Alkali Metals (Cs, Rb)	Volatile
4	Chalcogens (Te, Sb)	Volatile
5	Alkaline Earth (Ba, Sr)	Non-volatile
6	Noble Metals (Ru, Mo, Rh, Pd, Tc)	Non-volatile
7	Rare Earths (Ce, Sm, Pm, Pr, Nd, La, Y)	Non-volatile
8	Refractory Oxides (Zr, Nb)	Non-volatile

- Group 1 consists of the fission gases Xe and Kr, which are gaseous at normal temperatures

- Groups 2, 3 and 4 comprises halogens (in particular iodine), alkali metals (in particular, cesium), and the tellurium group elements. These are partially volatile at the reactor operating temperatures, and are likely to be rapidly released in substantial amounts in the case of fuel over-heating. I and Cs appear to be the most important in the Volatile group.

- Group 5, 6, 7 and 8 elements are relatively involatile even at fuel melting temperatures. These would be dispersed significantly only in the event of fuel melting temperatures being reached or as a result of chemical reactions. In the event of fuel vaporisation, the non-volatiles would condense to aerosols.

(b) Factors determining importance of radionuclide in ST analysis

The main factors determining the importance of a radionuclide are the total inventory of the nuclide in equilibrium, the nature of its radioactive emissions, chemical and physical properties determining its transport behaviour in the plant and in the environment, and its biological characteristics. Some of the factors mentioned are inherent to the radionuclide involved (such as fission yield, half-life, radioactive emissions, etc.), while others are dependent on the features of the reactor and the accident (such as the temperature profile of the core after an accident, the chemical environment in the release pathway, physical and chemical form of the radio-nuclide released, etc). However, in general, the fission gases and the volatiles (iodine, cesium and tellurium) are of importance in practically all severe accidents.

3.3.4.3 Release Stages [15,16]

The next step is to determine releases in different stages. In a severe accident, the initial heat-up and melting of the core occurs inside the RPV and the radionuclides released during this stage is called the In-vessel release. In the first stage of in-vessel release, processes involved are i) cladding rupture, ii) transport from the solid fuel matrix, iii) evaporation from molten fuel in core, iv) leaching of fuel following a cladding failure, and v) oxidation of fragmented fuel. The *second stage* of in-vessel release involves the transport and retention processes in the reactor coolant system. The *third stage* involves the transport and retention in the containment. The *fourth stage* is the leakage of fission product from the containment either through the intact containment or escape through the failed containment. If the containment is bypassed, some retention of radioactivity may still occur because of plate out in leakage path and/or if the bypass occurs into an auxiliary building.

If the accident progresses such that the molten core burns or melts through the vessel, or if there are severe accident phenomena such as steam explosion or high pressure melt ejection, then substantial quantities of the molten core will find their way directly into the containment (PWR/BWR plant). The release which takes place from this displaced fuel mass is called the ex-vessel release.

For PHWR plants, such ex-vessel release can take place, after reactor vault fails in damage progression in severe accident scenario. The chief mechanism of ex-vessel release is the molten core concrete interaction, which will drive additional active and inactive materials into the containment atmosphere. Moreover, the release of some materials is enhanced in the oxidising atmosphere of the containment.

3.3.4.3.1 Escape of Material From a Degraded Core

The in-vessel release of radioactivity from fuel constitutes the first stage of release in severe accidents. The initial inventory of radioactivity in the fuel can be calculated with relatively small uncertainty, as it depends on known parameters, such as the fuel type, core design, and the reactor operating history. For reactors with continuous refuelling, the equilibrium core inventory calculated at full power is considered. For other reactors, the end of cycle radionuclide inventory is considered in source term analysis. Severe accidents are characterised by high temperatures approaching fuel-melting temperatures (~2800° C).

Temperature is the primary driving force for release. In reactivity insertion accidents, core melt temperatures are reached in 1 s or less. In loss of coolant accident scenarios, the rise of core temperature is relatively slow.

(i) Gap inventory [16]

The gap inventory refers to the volatile fission products - stable as well as radioactive - that are released from the fuel matrix during normal reactor operation, and which reside in the gas plenum between fuel and fuel clad and cracks and voids available in the intact fuel pin. When the clad ruptures, the entire gap inventory may be released into RCS. For thermal reactors, this release usually represents < 1 % of the volatile FP inventory (see Table 3.8), but for LMFBRs the gap release may constitute > 50 % of the inventory. Practically no non-volatile material is expected to be found in the gap.

TABLE 3.8 : GAP INVENTORY FRACTION

Volatile species	LWR(1)	PHWR(2)
Xe, Kr	1.27 %	0.023 - 0.10 %
I	0.053 %	0.10 %
Te	-	0.088 %
Cs	0.025 %	0.022 %

(1) Fuel at 1200° C for 10-min, Lorenz model.

(2) Based on ANSI/ANS -5.4 model for all isotopes at equilibrium.

(ii) Release during heat-up to melt [16]

The volatile FPs - namely Xe, Kr, I, Cs and Te - are released more readily as the oxide fuel gets overheated. Both in-pile and out-of-pile release tests have confirmed that the noble gas elements, iodine and cesium show similar release behaviour, with rates that increase steeply with temperature. Tellurium shows a different release behaviour from the other volatile elements, being gettered and held up by zircaloy cladding until the latter is almost completely oxidised by the steam, when tellurium is released in a short burst. The release of the involatile FPs is significant only at high temperatures (~ 2000 °C).

(iii) Release following core slump [16]

While the UO_2 fuel melting takes place at ~2800° C, fuel liquefaction may occur well short of the melting point, as was demonstrated in the TMI 2 accident. Fuel liquefaction leads to loss of core geometry and slumping of the fuel channel into the core bottom and finally to the bottom vessel head in the case of LWRs.

In case of PHWRs, fuel melting leads to slumping into pressure tube, which may cause calandria tube to fail and eventually find way inside calandria bottom. Thus, a large pool of molten core materials may form on the lower head, discharging fission products and actinides, before it penetrates it. It is generally accepted that the residual amount of the volatile FPs will be rapidly discharged from the melt, while the release of the less volatile species is controlled by the combined effect of their vaporisation and transport through the molten pool. While the release rates of most species from the melt are expected to be high, considerable uncertainties exist regarding the chemical states of the active species, and these uncertainties are reflected in the prediction of in-vessel, and hence ex-vessel, release. Fig. 3.1 provides a qualitative perspective for sequence of events during core heat-up, meltdown and fission product release in LWRs.

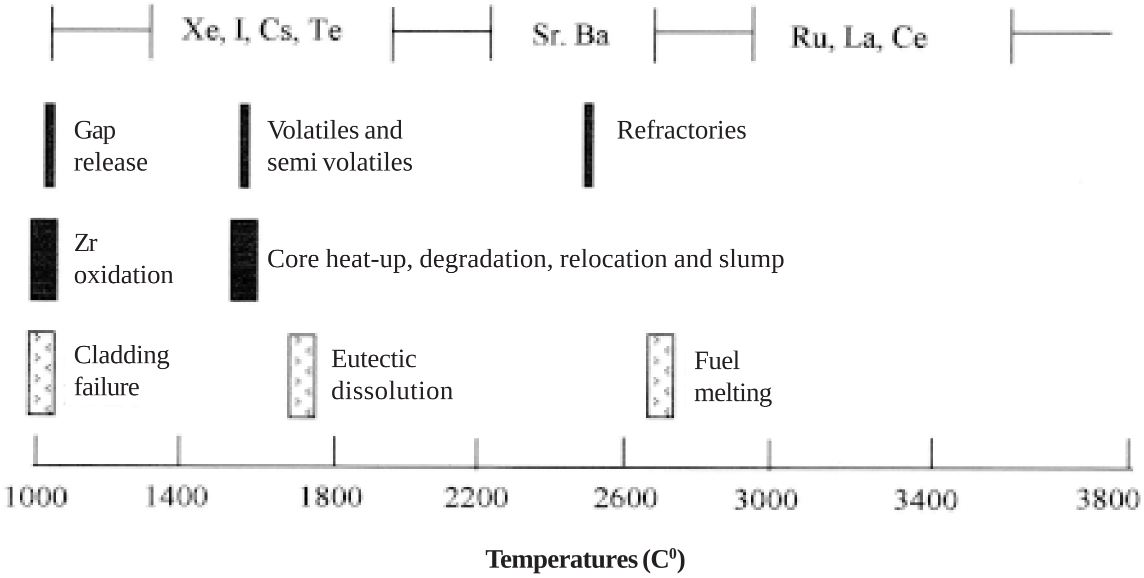


FIGURE 3.1 : QUALITATIVE SEQUENCES OF EVENTS IN MELT PROGRESSION AND RELEASE OF FPS [9]

3.3.4.3.2 Transport of Fission Products in Reactor Coolant System

(a) In water-cooled reactors, the main determinants of radionuclide transport in the primary coolant circuit are the temperature, the chemical environment, the nature of the wall surfaces, and the chemical and physical forms of the radionuclides. Upon release from fuel, the FPs exist as gas/ vapour and will change to the condensed forms as they encounter lower temperatures in the primary circuit. Most of the released mass will therefore pass through the primary circuit as aerosols. One key aspect of the behaviour of radionuclides in the primary circuit is the thermal-hydraulic condition corresponding to the particular accident sequence under consideration. Thus, a large break LOCA in the hot leg of a PWR will involve a short flow path from the core and involves little retention in the primary circuit. On the other hand, a cold-leg LOCA will involve a much longer and more complex flow path, with a correspondingly larger scope for retention. Once the flow path is established, then other information such as the system pressure, the rate of flow and composition of the gas, and the temperature change along the path etc., required as a function of time is obtained from the thermal-hydraulic codes. This is to be coupled with radionuclide transport codes for radioactivity transport analysis in primary coolant system and such fully coupled treatment of thermal-hydraulic and radionuclide transport is carried out in the state-of the art computer codes.

(b) Chemical and physical forms of radionuclides

The chemical and physical form of a radionuclide are very important since they decide whether it is in the primary circuit, and/or gets released into the containment. The initial form is in most cases either elemental or oxide or in other compound form; the physical form is either gas or vapour. The chemical form may change during transport if any interaction takes place with other materials. Similarly, the physical form initially released may change during transport.

It may be noted that the initial physical form of volatiles is vapour. It is transported by either convection currents or by continued boil-off to cooler parts of the RCS, where the vapour may saturate and condense, either forming aerosols by self-nucleation, or depositing on circuit walls or on other aerosols (say, the structural materials). Usually the process of conversion into aerosols is complete in the primary circuit. The analysis in the RCS is the analysis of the distribution of the radionuclides amongst the vapour phase, the aerosols in gas, aerosols deposited on surfaces, and vapour plated on surfaces, all as a function of time (Fig.3.2).

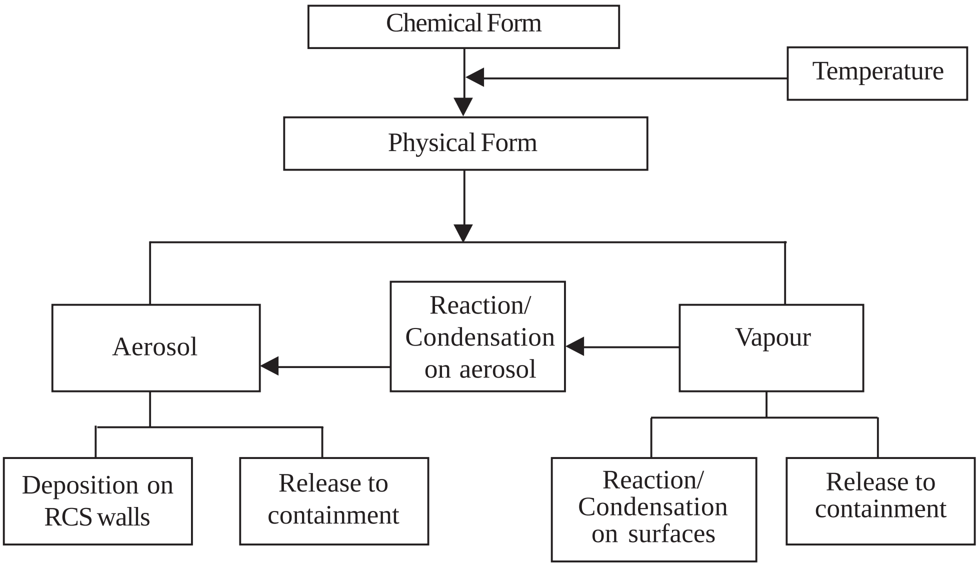


FIGURE 3.2 : IMPORTANT PROCESSES OF RADIONUCLIDES IN THE REACTOR COOLANT SYSTEM [16]

The aerosols may grow/deposit considerably in the primary coolant circuits. Most of the data on radionuclide transport in RCS has been obtained from small scale and large scale test facilities such as Marviken-ATT series (1985) at the Marviken nuclear plant, Studsvik in Sweden, LACE tests at Hanford, USA and STEP tests at the TREAT reactor at the ANL. These tests provide valuable database for validation of radionuclide transport in RCS modelling codes such as TRAP-MELT, VICTORIA etc.

(c) Release and attenuation behaviour of specific radionuclides in the RCS [18]

For noble gases, complete release can be assumed with no chemical or physical attenuation in the primary system. Iodine is most likely to be in the elemental atomic form in the matrix of the fuel, and cesium iodide in the fuel-clad gap inventory. When the iodine in the oxide fuel is released to the primary circuit, the most likely form is cesium iodide on account of the reducing atmosphere prevailing therein. Cesium iodide exhibits simple condensation either onto surfaces or on aerosols. However, there is doubt whether the cesium iodide can remain unchanged throughout its movement through the primary circuit, on account of the fact that volatile iodine (e.g., hydrogen iodide) is likely to be formed upon its interaction with boric acid (from borated water supplies or from the decomposition of the boron carbide control rods).

Cesium migrates in the fuel in the element form and will be released from the fuel rod into the reducing steam environment of a severe accident and will rapidly form cesium iodide and cesium hydroxide or cesium molybdate. The reaction of the iodide or hydroxide with boric acid leads to the formation of non-volatile cesium borates and hence attenuates the release. It is also likely that cesium hydroxide will react with structural materials (SS and Inconel) to diffuse into the inner chromium sesquioxide layer; this mechanism further attenuates the release of cesium.

Tellurium (Te) is as volatile as iodine or cesium but its release from the fuel rod is attenuated on account of the formation of zirconium tellurides. The release of Te depends on the degree of oxidation of the zircaloy cladding; if there is adequate oxidation, the release of Te occurs. Recent experimental data suggest that the eventual release of Te will occur as stannous telluride, formed by the reaction of the tellurium with the tin component of the zircaloy clad. Tellurium and hydrogen telluride could also be important vapour species depending on the thermal hydraulic conditions. However, if formed, they will interact rapidly with surfaces, and aerosols and will be attenuated.

Barium and strontium exist in the fuel as non-volatile oxides; their reaction with unoxidised zirconium could generate the elemental species. The latter species are relatively volatile, and will form hydroxides on reaction with steam. The hydroxides may also be formed by reaction of the oxides with high temperature and high-pressure steam. The hydroxides would behave in a similar manner to cesium hydroxide. Molybdenum will be present in the fuel as element, oxide and cesium molybdate. Formation of molybdenum oxide, cesium molybdate and molybdenum hydroxides will enhance the volatility of molybdenum.

The FPs (Technetium, Rruthenium, Rhodium and Palladium), are present in the fuel as element and will not be released to any significant extent. Also, no significant reactions with surfaces or with aerosols are predicted. Lanthanides and actinides are present in the fuel as non-volatile oxides. Any release is small and no significant interactions are likely to occur. Silver, cadmium, indium, tin, antimony, are relatively volatile, but as FPs have rather low fission yields. Hence, they will not contribute significantly to the radioactive source term. For FBR, it is observed that the contribution of iodine and cesium vapours in containment is small, as compared to the contribution of iodine and cesium combined with sodium aerosol. For non-volatile radionuclides, the source term in RCB depends on the sodium pool height above the core and obstacles present in the core [19].

3.3.4.3.3 Transport and Retention in Containment Systems [20]

Gases and aerosols coming from the RCS (in-vessel release) and from the reactor cavity after vessel melt-through (ex-vessel release) have to pass through the containment before escaping to the environment through the leak paths or containment opening. The aerosols may be accompanied by steam. The mechanisms of aerosol production involved here are the ‘vaporisation release’ and the ‘oxidation release’. The nature of the aerosols added in the latter process is qualitatively different from the former process. The mass of the aerosols in the containment is overwhelmingly inactive, being contributed by structural materials such as zircaloy, steel, control rod metals, boron, and concrete, and these have a decisive influence on aerosol behaviour in the containment. There are two sets of aerosol processes in the containment: those that serve to agglomerate the air-borne aerosols, and those that remove them. Agglomeration reduces the number density of the aerosols but not the air-borne mass concentration. The agglomerated particles have a larger probability of removal. In addition, increase of particle size on account of steam condensation is a strong growth process. The main aerosol removal processes in the reactor containment are: Gravitational settling, Diffusiophoresis, and Diffusion (laminar/ turbulent). Gravitational deposition is by far the most important removal processes in the containment. This process is assisted both by steam growth and by particle agglomeration. Thermophoresis, resuspension, and electrical effects are second order effects that are usually neglected. In FBR, sodium oxide aerosols in containment acts as scavenging agent for iodine. Iodine either in the form of sodium iodide or cesium iodide is carried by sodium oxide aerosols. Studies on leakage of aerosols from containment have shown that aerosols do not pass through leakage paths and plate out fully [21].

The function of a reactor containment is to reduce the probability of FP release to the environment, should they escape from the RCS under accident conditions. This is achieved by containment isolation and other ESFs provided to mitigate the effect of in vessel and ex-vessel radioactivity release (energy as well as radioactivity) in severe accident conditions. During the heat up process in the core, core slowly melts from the center and increases the load on the lower crust and the core support structure.

During core melt, quenching will form copious amount of steam, which produces a steam pressure spike and possible steam explosion. These internal missiles might fail the containment (a-mode containment failure). An energetic steam explosion can deliver shock loads, ejecting core debris as missiles, failing vessel and causing vessel lift-off in case of PWR and BWR. In PHWRs, the molten core after melt through calandria, comes in contact with vault water, cooling the core debris. It might cause steam explosion and direct radioactivity release along with core debris ejection can take place after reactor vault structure fails during accident progression. This direct core debris ejection to containment would result in an ex-vessel release of radioactivity into the containment.

In PWR and BWR, there are essentially three modes of ex-vessel release; High pressure melt ejection, core debris/concrete interactions, and steam explosions.

(a) High pressure melt ejection (HPME)

In the LWR high-pressure accident sequences, where the RPV and the RCS are at high pressure, if failure of a penetration in the lower head should also occur, then a high pressure jet of molten core material may be ejected directly into the containment or into a pool of water present in the reactor cavity/vault. In either event, the molten mass may fragment and become dispersed throughout the containment. Dispersion of core debris in containment can potentially induce numerous hazards. If hydrogen is present in the containment atmosphere, dispersion of the hot debris particles could serve as a catalyst to promote recombination of the hydrogen with free oxygen, even though hydrogen concentration may be below the conventional flammable limits. Direct containment heating (DCH) from the molten mass may threaten the containment integrity. In addition, the core melt to the containment atmosphere may result in oxidation reactions, which generate still more heat. If the melt falls or is ejected into the cavity under vessel, then steam explosion can occur. If core debris is finely fragmented in the containment atmosphere, either by steam explosion or HPME, an additional release of FPs may occur. The airborne radioactive inventory in the containment may suddenly increase by the following two mechanisms: one, of course, being the radioactive aerosol directly injected by the jet into the containment, and the second the enhanced release of certain FPs from the molten fuel on account of its oxidation in the air. A major source is likely to be tellurium, released after the zirconium has been quantitatively oxidised. A second source is likely to be ruthenium, which forms volatile oxides, RuO_x, and hydroxides under highly oxidising conditions.

(b) Molten core-concrete interaction (MCCI)

The molten core debris may melt through the lower head in a coherent manner, forming a large molten pool in the reactor cavity. The high temperature (> 2000° C) melt will rapidly interact with the concrete of the cavity floor. This process is called molten core-concrete interaction. The gases produced in the process (steam, carbon dioxide, carbon monoxide) will bubble through the melt and will transport the vaporisable part of the activity to the pool surface. This is called the ‘vaporisation release’. The released material, which may comprise both radioactive (FPs, fuel, actinides) and inactive (control rod, steel, concrete) materials, is discharged into the containment, where the vapours will form aerosols. If the containment is intact, these aerosols will enhance the aerosol inventory already present in the containment from in-vessel release. On the other hand, if the containment has already failed, then these may comprise a large additional source term.

(c) Steam explosions

A steam explosion refers to the reaction of the finely divided molten fuel matter with water coolant and is a potential threat to the reactor containment structure. An in-vessel steam explosion is postulated to occur as the molten core hits the water in the lower plenum, producing a large explosion, which sends a fragment of the RPV as a missile into the containment. An ex-vessel steam explosion occurs if the molten corium contacts a pool of water after emerging from the vessel. A steam explosion will enhance both the aerosol mass in the containment air as well as lead to enhanced release of radioactivity into the containment.

A steam explosion to be highly efficient would require at least three stages to be met; a) pre-mixing, b) triggering, and c) propagation. Pre-mixing is a requirement that the molten particles (about 1 cm in diameter) be dispersed in water; the particles will be blanketed initially by an insulating layer of vapour. The next requirement is that of the existence of an internal trigger, which would fragment the pre-mixed, hot molten droplets in the liquid water. Propagation across the interaction zone must follow to generate the shock wave associated with an explosion.

If a failure of containment should occur in severe accident, then the time and manner of the failure are decisive in determining the magnitude of a release. If a containment failure occurs just after the volatile fission products (I, Cs and Te) have been released into the containment and converted to aerosol, it is predicted that 80 % of the Cs and I core inventories would be discharged to the atmosphere. On the other hand, if five days were to elapse between the reactor vessel failure and the containment break, there would be adequate time for aerosols to deposit on the internal surfaces, and the calculated release of I and Cs would be only 10^{-2} % of the reactor inventory.

Along with the timing of failure, another factor in ST prediction is the size of the breach in the containment through which the release occurs. A large hole would result in a rapid discharge of the air-borne aerosol, while a small hole would considerably delay the discharge, thus enabling natural removal processes in the containment to cleanse the air to a greater extent. In the QUEST study, it was shown that the FP release to the environment varies by an order of magnitude as the breach effective area was varied from 0.001 m^2 to 10 m^2. The hole size is expected to have no effect on the release fraction beyond a certain value.

3.3.4.3.4 Releases Through Containment

The integrity of the reactor containment structure is of the prime importance in severe accidents. Normally containment will be designed to accommodate the postulated pressures and temperatures of a design basis accident. The transport paths in the containment usually lie through a large number of inter-connected compartments with opportunity for recirculation through these volumes. The default flow path is via suppression pool (in BWR/PHWR or ice condenser in PWR). Aerosols and iodines along with associated energy, in their transport, in reactor containments, are removed by natural processes, which are supplemented by the ESFs such as sprays, filter banks, building coolers. Besides, in modern double containment systems, the annular space between Primary and Secondary containment envelopes is held at negative pressure to prevent ground level leakage during accidents; Primary containment also has hydrogen recombiners as ESFs to reduce hydrogen concentration below hazardous level of deflagration/detonation.

The containment loads may be different in the case of severe accidents. Two categories of containment loading scenarios are postulated; the rapid pressurisation and relatively slow over-pressurisation.

Rapid pressurisation includes events such as steam explosions, steam spikes, or hydrogen burns. An in-vessel steam explosion is postulated to occur as the molten core hits the water in the lower plenum, producing a large explosion, which sends a fragment of the RPV as a missile through the containment. An ex-vessel steam explosion occurs if the molten corium contacts a pool of water after emerging from the vessel. A steam explosion will enhance both the aerosol masses in the containment air as well as lead to enhanced release of radioactivity into the containment. Hydrogen burns can cause detonations, which involve the hydrogen reaction through the supersonic propagation of a burning zone or combustion wave. The dynamic pressure loads created by hydrogen detonation may cause a breach of the containment or damage to important safety related equipment.

Relatively slow over-pressurisation includes events due to steam production and/or formation of non-condensable gases, including hydrogen, carbon dioxide, etc. In absence of containment ESFs, if a core-concrete reaction occurs the pressure will slowly start increasing. If the containment leaks before breaking, then the associated loss of gases will modify the thermal-hydraulics of the containment. During core melt accidents, Zircaloy as well as the other in-core metallic materials react at high temperatures with water or steam. Consequently, a large amount of hydrogen is produced. This hydrogen can get ignited through local burning by diffusion flames, deflagration or detonation. Local burning and deflagration may cause static or quasistatic pressure loads on the containment. Slow over-pressurisation can be caused due to compressed air in-leakage in the containment.

(a) Basemat penetration

In accident sequences, in which a large amount of the molten core debris falls on the concrete in the reactor cavity, a physical and chemical reaction occurs which gradually erodes the concrete, leading to a potential penetration through the basemat. The rate of melt penetration is estimated to be extremely slow, and given the basemat of considerable thickness, such an event is most unlikely. However, if such a penetration does occur over a time scale of hours or days, the radioactive aerosols would be attenuated considerably, through filtration in the engineering backfill, such that the resultant source term would be extremely low.

(b) Heat removal

In reactor containment, heat removal is by containment sprays, suppression pool, sump, cooling systems, and building air coolers. Such systems are normally protected from damage by steam jets, pipe whip or missiles. It is necessary to postulate the failure of these heat removal mechanisms in order to challenge the containment integrity in PSA Level 2 analysis.

Other considerations for containment accident progression that might lead to breach of containment integrity following a severe accident include: build-up of non condensable gas pressure, in-leakage of instrument compressed air to supplement other sources of pressurisation over the long-term, high temperature degradation effects on mechanical and electrical penetrations, failure to isolate containment, starting of fires in any combustible materials within the containment, and other possible events. Fig. 3.3 shows various accident phenomena in the containment building associated with source term calculation.

Some containments have engineered safety features to remove heat and steam from the containment atmosphere. These include water sprays, fan coolers and ice beds. These features can also accelerate the removal of fission products from the containment atmosphere. However, If hydrogen flame encounters a region containing obstructions, the turbulence induced by the obstructions can increase the burning rate and even cause a transition to detonation. Fan coolers, which not only induce turbulence in the gas, but also remove steam from the atmosphere at the same time, may be of concern when operating in the presence of hydrogen at elevated levels. Some examples of the ST evaluation are given in Annexure-X.

3.3.5 Containment Modelling Codes [15, 16]

The first modelling of aerosols within the containment was carried out with the CORRAL code, which assumed a single settling rate for the aerosols. Since the rates used in CORRAL were derived from the containment system experiments, which did not truly represent the reactor conditions, it's use is limited. Mechanistic aerosol codes were first developed for studies involving sodium fire under dry conditions in severe fast reactor accidents. There are essentially two types of containment codes; the discrete codes, which divide the size range into discrete size classes, and the log-normal codes, which make the more restrictive assumption that the size distribution is always log-normal. Comparison with test results have shown that there are systematic differences between the log-normal and the discrete codes, and that the results from discrete codes are in much better agreement with the experimental results. Some examples of discrete codes are: NAUA-5, CONTAIN, PARDISEKO III, AEROSIM-M AEROSOLS/B1, and those of the lognormal codes are HAA-4, HAARM-2 and CONTAIN-LMR. Containment aerosol modelling codes are highly developed, and it is currently believed that the uncertainties in the input data are larger than the uncertainties in aerosol modelling and computation. Many of these codes were verified and validated against small and large-scale containment aerosol tests [15, 16, 20].

3.3.6 Uncertainty and Sensitivity Analysis

Severe accident phenomena are highly complex, and so there are significant uncertainties in the prediction of what will happen. The mechanistic source term assessment is driven essentially by the phenomenology of the events involved in the accident sequences, and in spite of numerous tests and experiments, there are still certain areas which are not very well defined and judgement has to be exercised to define the parameters. It is in the modelling of these events that the maximum uncertainty arises in the value of the source term. Table 3.9 gives levels of uncertainties and sensitivities in severe accident phenomena. The uncertainties are graded high (H), medium (M) or Low (L). These are relative judgements. In some cases, where an M mark has been given, the uncertainty may be high, but the judgement is that this uncertainty is not as important as some of the other issues. Areas in which expert judgement is most likely to be necessary are indicated by (e).

A distinction is made between intrinsic and consequential uncertainties. When one phenomenon depends on initial or boundary conditions set by an earlier phenomenon, it will inherit the uncertainties from that earlier phenomenon. Here an attempt has been made to judge intrinsic uncertainties; those that would persist even if the initial conditions were known exactly. In discussing sensitivity, a distinction has to be drawn between different outputs and end uses of the calculation. In Table 3.9, we consider sensitivities on three aspects: assessing accident management procedures, assessing challenges to the containment and calculating source terms.

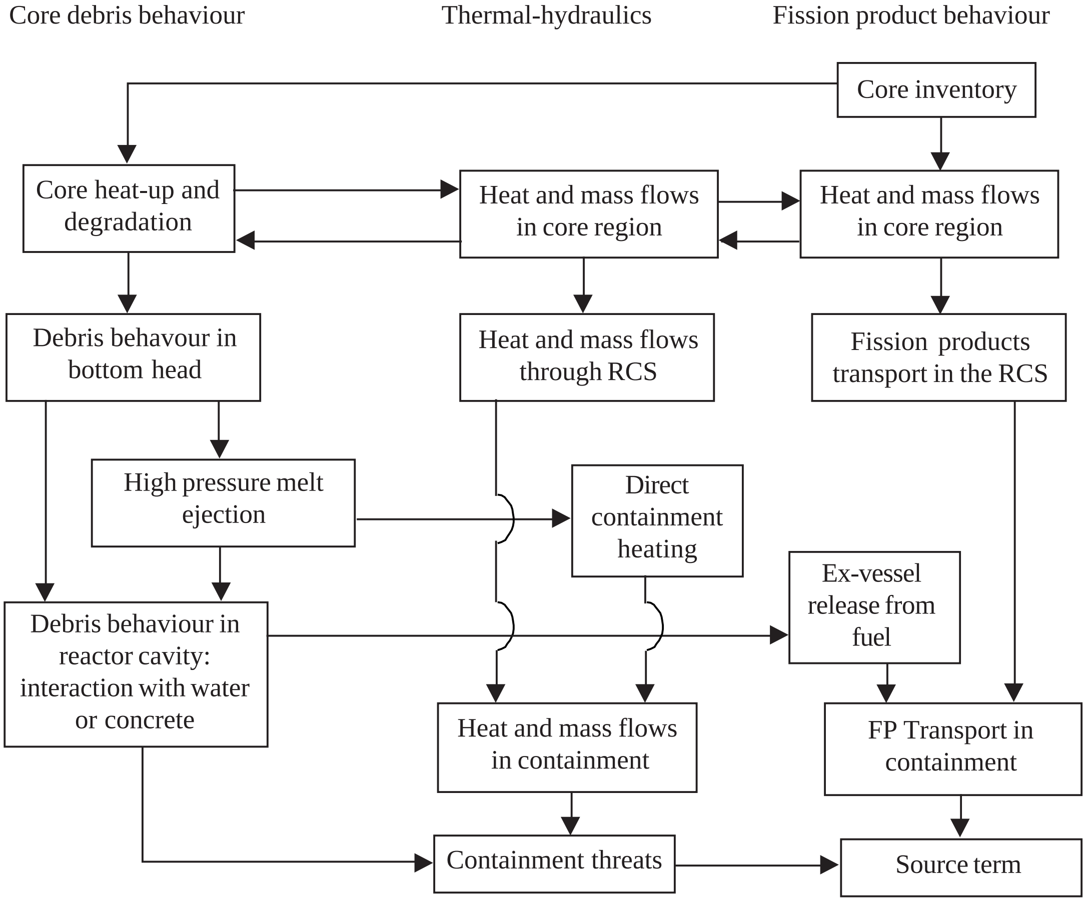

Core debris behaviour
Thermal-hydraulics
Fission product behaviour
Core inventory
Core heat-up and degradation
Heat and mass flows in core region
Heat and mass flows in core region
Debris behaviour in bottom head
Heat and mass flows through RCS
Fission products transport in the RCS
High pressure melt ejection
Direct containment heating
Ex-vessel release from fuel
Debris behaviour in reactor cavity: interaction with water or concrete
Heat and mass flows in containment
FP Transport in containment
Containment threats
Source term

FIGURE 3.3 : SEVERE ACCIDENT PHENOMENA IN CONTAINMENT BUILDING ASSOCIATED WITH SOURCE TERM

TABLE : 3.9 LEVELS OF UNCERTAINTY AND SENSITIVITY IN SEVERE ACCIDENT PHENOMENA

Severe Accident Phenomenon	**Intrinsic Uncertainty**	**Sensitivity**		
		Accident Management	**Containment Challenge**	**Source term**
Core Heat-up degradation	M$^{(e)}$	√	√	
In-Vessel thermal-hydraulics	M	√		
Hydrogen production	M	√	√	
RCS thermal-hydraulics	L	√	√	
In-vessel release of FPs	M			√
RCS fission products transport	M			√
Core loss of geometry	H$^{(e)}$	√	√	√
In-vessel core coolant interaction	H$^{(e)}$		√	
Vessel-melt through	H$^{(e)}$	√	√	
Vessel lift-off	L		√	
Debris ejection from vessel	H	√	√	
Direct containment heating	H$^{(e)}$	√	√	
Ex-vessel core coolant interaction	H$^{(e)}$		√	
Release of FPs in HPME	M			√
Core concrete interaction	M	√	√	√
Ex-vessel release of FPs	H			√
Debris quenching	M	√		
Containment thermal-hydraulics	L		√	
Hydrogen combustion	H		√	
Engineered Safety Features (ESFs)	L		√	
Transport of FPs in containment	M			√
Pool scrubbing	M			√
Effects of ESFs on FPs	L			√
Leak path retention	H			√
Containment venting: Unfiltered Filtered	 L L	 √ 		 √
Resuspension	M			√

Note : (e) Expert judgement

NUREG-1150 [10] has endeavoured to quantify the uncertainty by a method, which combines expert judgement on key ST issues and the associated parameter probability distribution, with a modified Monte Carlo sampling treatment to handle the wide variation in the values of the input parameters. For PWRs, the most important ST uncertainty contributors are found to be the magnitude of the core-concrete interaction release and the extent of the FPs initially trapped in the primary coolant circuit. Various computer codes used with regards to Level 2 PSA including on uncertainty analysis are given in Appendix-II.

3.3.7 Documentation of Level 2 PSA

The main objectives and format of the documentation of Level-2 PSA is in Appendix-I.

3.4 Procedure for Conducting Level 3 PSA

3.4.1 Objective and Scope

The objective of a full scope PSA is to assess the risk of public health and economic loss consequent to an accident and release of radionuclides from NPPs in as realistic a way as can reasonably be attained and to bound this assessment with upper and lower values. A Level 3 PSA provides insights into the importance of accident prevention and mitigation measures in terms of the adverse consequence to the public health, and the environment (i.e. contamination of land, air, water and foodstuffs). Therefore, some call it, in short, 'Consequence' Analysis.

To date, most of the experience with Level 3 PSAs is related to the assessment of the risk of potential NPP accidents. For this, the methodology is most formalised and several large, sophisticated codes are available. This document limits discussion to that type of analysis for which atmospheric release and dispersion of nuclides have been shown to be dominant, as compared to releases to aquatic or terrestrial environment. However, the general methodology is also valid for other nuclear facilities such as research reactors, reprocessing plants and spent fuel storage installations, although specific aspects of Level 2 and 3 PSA analyses may be different for these facilities.

3.4.2 Probabilistic Consequence Analysis [22]

The main elements of consequence analysis are shown in Fig. 3.4 [22]. Invariably, these elements are incorporated into a computer program, referred to as a Probabilistic Consequence Analysis (PCA) code.

3.4.2.1 Description of the Radionuclide Release

The starting point for a consequence assessment is the radionuclide release to the atmosphere, as produced by a level 2 PSA. This information, provided for each of the representative accidents to be assessed, obtained by grouping accidents with similar release characteristics together, referred to as the 'source term'. This specifies both the time dependent magnitude of the release and the manner of the release, the latter being defined by a number of release parameters. To aid realistic modelling of the dispersion and risk of accidentally released radionuclides, the following parameters are included in the ST of each category, in addition to its release fractions and its frequency:

- The time delay between the reactor shutdown and release of radioactive material to the environment, which reduces activity by radioactive decay, and also may influence the introduction of countermeasures before the release.
- The duration of the release, which influences the dispersion of released material
- Height of the release
- The thermal energy associated with the release.

These parameters are direct input for the atmospheric dispersion. Other characteristics of release (the physical form and chemical properties of radionuclides) are assumed to be constant in each release phase. It is assumed, that they are released in oxide form as aerosol particle with 1 mm activity median aerodynamic diameter (AMAD), except for noble gases, which appear in elemental form, and iodine, which may appear in elemental, organically bound, and particulate forms.

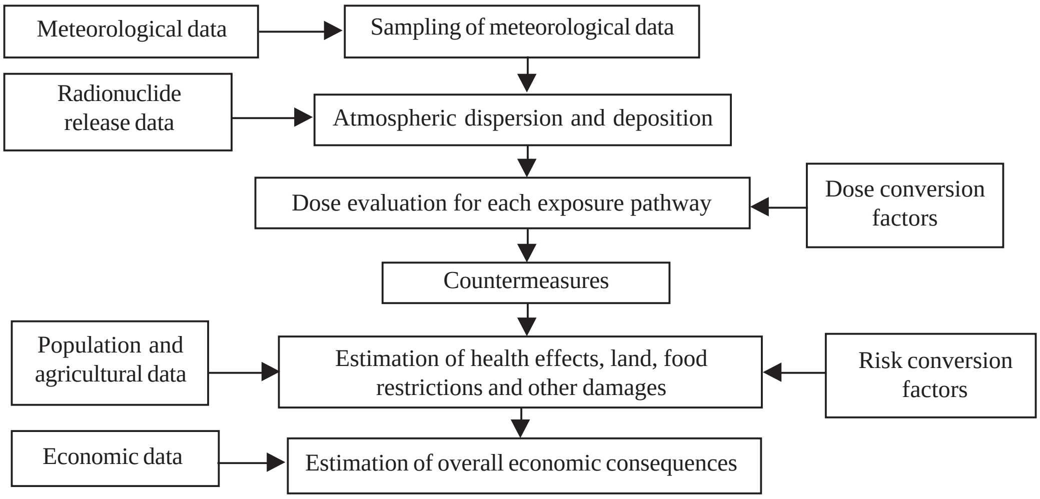

Meteorological data
Sampling of meteorological data
Radionuclide release data
Atmospheric dispersion and deposition
Dose evaluation for each exposure pathway
Dose conversion factors
Countermeasures
Population and agricultural data
Estimation of health effects, land, food restrictions and other damages
Risk conversion factors
Economic data
Estimation of overall economic consequences

FIGURE 3.4 : BASIC ELEMENTS OF PROBABILISTIC CONSEQUENCE ANALYSIS

3.4.2.2 Atmospheric Dispersion and Deposition

Material released to the atmosphere is transported downwind and dispersed according to normal atmospheric mixing processes. The diffusion-transport equation is commonly used for estimating dispersion in the atmosphere. Several models have been developed for this purpose using a variety of boundary conditions and simplifying assumptions. Many simple theoretical formulations of dispersion predict that the concentration profile will have a Gaussian shape. Additionally, they assume that the downwind transport goes along a straight line. Although the assumption of simple theories does not hold for real atmosphere, the Gaussian shape have been found empirically to be approximately valid in many situations and it forms the basis of the Gaussian plume model, which has been, and still is, widely used in consequence assessment.

The above description of plume dispersion is only a starting point for a model of behaviour of gases, aerosols and vapours in the atmosphere. Numerous other factors have to be taken into account. For example.

- Plume rise, due to buoyancy of the plume, arising from its inherent energy, is a very important factor in determining maximum ground level concentration from most sources since it typically increases the effective release height, by a factor of 2 to 10 times of the actual release height.
- When material is discharged from an elevated source, the plume will disperse and eventually reach the ground. On, reaching the ground the plume is reflected and effectively dispersed back up into the atmosphere. Dispersion in vertical direction is usually restricted to a certain height by an inversion lid (layer), which arises due to change in temperature gradient. Where a finite mixing layer exists, the dispersed material is trapped between the top of this layer and the ground. Reflections in this case occur, both on the ground and at the top of the mixing layer.
- Building wake and the effect of the topography on the dispersion of discharged material should be considered.
- Spatial and temporal variation in the wind direction should be taken into account.

The above description refers to plume dispersal without a decrease in the total amount of radionuclides it contains. In reality, the radionuclide content diminishes both by radioactive decay and through deposition mechanisms. Deposition mechanism fall into two categories: dry and wet. Dry deposition is the process by which material is removed from plume by impaction with the underlying surface or obstacle on it, such as vegetation. The rate at which material is deposited from the plume will depend on the nature of airborne material and the underlying surface. Wet deposition is the process in which material is removed by the process of precipitation and scavenging by the action of rainfall. Material may be removed from the plume by the action of rain falling through it. All these mechanisms are considered in consequence analysis.

3.4.2.3 Meteorological Data and its Sampling

It is a normal practice to use the meteorological data from the meteorological station nearest to the release point. Data compiled at other stations may, however, be acceptable if they are representative of the general condition experienced by the plume. Consequence analysis codes using atmospheric dispersion models other than Gaussian plume model may require additional meteorological data. Typically, such a code requires meteorological data at regular spatial interval, over the region of interest beyond site (so-called non-source meteorology); this is obtained by interpolation of available meteorological data. This process is complex and may need considerable judgement. The choice of meteorological data often represents a compromise between an ideal, the available and what is adequate for a particular assessment.

In PCA using various types of atmospheric dispersion models, the atmospheric dispersion and dose calculation must be repeated for a large number of sequences of conditions selected from the meteorological data file used to predict the full distribution of consequences, which may occur. Ideally the calculation may be performed for every possible sequence of weather conditions in the data file; in other words, a weather sequence each hour on the file. It is neither practicable nor necessary to consider every such sequence. Instead, one or more year’s data is sampled in such a way that a truly representative set of weather sequences is selected. The selection should be made in such a way that the sequences chosen represent the complete set of possible sequences, and yield the correct probability distribution of consequences. The simplest method of selecting starting times for the sequences is to do either at random or by selecting every nth sequence (cyclic sampling). These methods tend to sample common sequences frequently, whilst overlooking the more unusual ones. A more sophisticated method of sampling is stratified sampling, in which the intention is to group all those sequence of conditions on the meteorological data file, for which the consequences are similar. Sequences can be chosen at random from those within each of groups, and assigned a probability based on the number of sequences allocated to each group and the number selected from within each group.

3.4.2.4 Exposure Pathways and Dose Assessment

There are six principal pathways by which people can accumulate a radiation dose after an accidental release of radioactive materials to the atmosphere. For each pathway a dosimetric model is required to convert the concentration of radionuclides in the atmosphere, on the ground, in foodstuffs, or on skin and clothing, to dose to humans. These pathways are shown in Fig. 3.5 and briefly described below. If other parts of nuclear fuel cycle are considered, different exposure pathways may be dominant. For example, migration of radionuclide in soil and ground water, in case of waste storage and spent fuel storage facilities. In this regard details can be seen in AERB safety guide ‘Methodoligies for Environmental Radiation Dose Assessment’ (AERB/NF/SG/S-5).

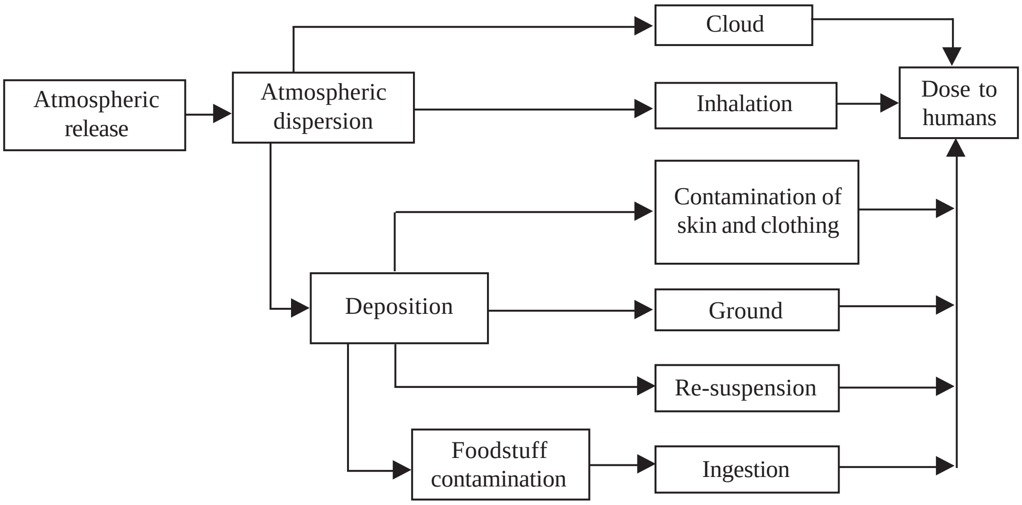


FIGURE 3.5 : PRINCIPAL EXPOSURE PATHWAY TO HUMANS FOLLOWING AN ATMOSPHERIC RELEASE

(a) External β and γ irradiation from materials in the cloud (cloud shine)

Both β and γ emitters in the passing cloud contribute to individual external exposure. The contribution of β dose is less significant due to their short range in air. Two models are commonly used for evaluation of dose from such exposure depending on the dimension of the plume and the distribution of activity within it; these are categorised as semi-infinite and finite cloud models respectively. Semi-infinite approach is based on the assumption that the air concentration is uniform over the volume of the plume from which photons can reach the point at which dose is delivered, and that the cloud is in radiative equilibrium. Correction factors for plume geometry and distance from the plume centreline should be taken into account.

The finite cloud model involves simulating the plume by a series of small volume sources and integrating over these sources. There are two stages in the calculation; the evaluation of photon flux at the point of interest and the conversion of photon flux to absorbed dose in air.

For people indoors, the structure of the building attenuates the gamma rays and so provides shielding. In evaluating the doses it is generally assumed that a certain proportion of population is indoors and the reminder outdoors at the time of release.

(b) Inhalation of material in the cloud

The direct inhalation dose is obtained as the product of inhalation rate, the time integrated air concentration and a pre-calculated dose per unit activity inhaled. These pre-calculated inhalation dose conversion factors, which are also age dependent, are obtained from the metabolic models.

The air concentrations inside and outside building may be different: evaluations should incorporate this by using an appropriate attenuation factor.

(c) External dose from radioactive material deposited on skin and clothing

Both β and γ emitters contribute to individual external exposure following the deposition of radioactive material onto the skin and clothing. The doses received from deposited material are evaluated using the pre-calculated data giving the dose rate per unit deposit and information on the physical half-life of the material on the skin. The dose response relationships for non-stochastic effects are applied with the small area of skin, and therefore the dose calculated can be used directly. However, for stochastic effects the average dose throughout the skin should be used in dose-response relationship. An allowance for only a part of body being contaminated in calculating this average skin dose should be included. The deposition density on skin or clothing is taken to be a function of that to the ground at the same location. It is standard practice to use a shielding factor to account for the shielding effects of clothing on β dose to skin.

(d) External γ irradiation from deposited radionuclides on ground (ground shine)

Both β and γ emitter radionuclides deposited on the ground contribute to individual external exposure. The evaluation of β dose is less significant due to their short range. This pathway is often evaluated by multiplying the deposit by a dose per unit deposit conversion factor, integrated to appropriated time period. These dose conversion factors are precalculated using simple formulae to account for long-term removal mechanism. These precalculated factors are stored in a data library. More complex models for generating the data library have been developed in recent years. The model used allows for shielding by ground roughness and the air in calculating photon fluxes above the ground. The doses from deposited γ emitters calculated with these factors are, therefore, appropriate for those people who are outdoors. The building shielding factors must be specified for the calculation of dose to people indoors.

(e) Inhalation of resuspended material

Resuspension can be caused by wind or by human activities (eg. traffic or ploughing). The relationship between the air concentration and the amount of material deposited is evaluated using a time-dependent resuspension factor.

(f) Ingestion dose

Ingestion doses are calculated from amount of activity deposited, the concentration of material in foods for unit deposition, the consumption rate and dose per unit activity ingested. Both the consumption rate and the dose per unit activity ingested are age dependent.

Food consumption is generally treated in one of two ways. One is based on assumption that all food is derived at the point of consumption, and that required amount of food is produced at each grid point. The second is based on assumption that all food produced is consumed outside the contamination zone.

3.4.2.5 Population, Agricultural and Economic Data

Calculation of exposure of the population in the path of a plume travelling over a region requires that the specific geographic population distribution around the release site be known. Evaluation of economic impact requires knowledge of not only the distribution of population but also the general nature of land use by sector. The real property loss due to damage, the agricultural damage and costs, and decontamination costs all involve knowledge of the percentage of the area used for agricultural and urban activities.

While compiling agricultural data, it is important to take into account the growth cycle of corps, so that seasonal effects, which can be significant, are properly taken into account. When agricultural data are not available, they can be approximated by using information on the land area used for farming within each grid element, in conjunction with information on the proportion of the farmland devoted to each agricultural product (in the region or the country). If food distribution is taken into account it is necessary to specify the regions of food production and consumption in the form as required (r, θ) or any other format).

3.4.2.6 Countermeasures

A variety of possible countermeasures or protective actions may be taken following an accidental release to reduce the impact of the accident on the environment and the public. A realistic estimate of the exposure of the population must therefore take appropriate account of these countermeasures.

The various protective actions available fall broadly into two categories, depending upon the time at which they are implemented and the effects, which they are designed to mitigate. Short term protective actions, sometimes termed 'emergency response' actions, include those measures, which might be implemented either before or shortly after a release to the environment. The primary objective of such measures is to limit the exposure of the population to both internal and external irradiation with the intention of preventing deterministic effects and minimising risks of stochastic effects. Short-term countermeasures include sheltering, evacuation, issuing stable iodine tablets, and the decontamination of people. Long-term countermeasures are designed to reduce chronic exposure to radiation, both externally from deposited material and internally from ingestion of contaminated food, with the intention of reducing the incidence of late health effects. Long-term countermeasures usually incorporated into PCA codes include relocation, land decontamination and food bans. There are other long-term countermeasures, which are generally not modelled, in current PCA codes. These include changes to agricultural practices, deep ploughing, alternate feed, cesium binders, alternative crops and alternate production.

Consequence analysis codes include intervention levels for imposing or withdrawing food bans. Generally, these intervention levels are based either on activity levels in food and drinking water or on maximum individual doses, which should be incurred although in some codes they are based on the level of ground contamination.

3.4.2.7 Health Effects

The exposure of individuals to ionising radiation can lead to health effects, which are generally classified as either 'deterministic' or 'stochastic'. Effects observed in exposed individuals, i.e. deterministic effects and cancers are termed 'somatic' effects, while those observed in their descendants are known as 'hereditary' (genetic) effects. Deterministic effects and stochastic effects are often referred to as 'early' effects and 'late' effects, respectively. The methods currently used in consequence analysis for evaluating the various health effects identified above are now briefly summarised.

(a) Deterministic effects

The probability or risk of an individual being affected, r, is given by 'hazard function'. Scott and Hahn developed a model of deterministic effects for the NRC [4];

$$r = 1 - \exp(-H) \tag{3.8}$$

Generally, H, the cumulative hazard, is given by a two-parameter Weibull function of the form:

$$H = 1n\,2 \left(\frac{D}{D_{50}}\right)^{s} \quad \text{for } D > T \tag{3.9}$$

where

D is the (average absorbed) dose to the relevant organ,

D_{50} is the dose, which causes the effect in 50% of the exposed population,

S is the shape parameter, which characterizes the slope of the dose-risk function,

T is the threshold dose.

Doses which are protracted over a period of time are less harmful than those delivered over a very short period. This is included in the model by summing over doses delivered in different time periods, with each normalised by an appropriate D50. The equation above is then replaced by:

$$H = 1n\,2 \left(\sum_{i} \frac{D}{D_{50}}\right)^{s} \quad \text{for } D_1 > T_1 \tag{3.10}$$

where

D_i is the dose delivered in the time period i,

$D_{i,50}$ is the dose which causes the effect in 50% of the exposed population if delivered in time period i,

T_i is the threshold dose for time period i.

Values of 'S' are given in Annexure-XI.

In a recent revision to the NRC health effects model, dose rate dependent models are proposed for fatal deterministic effects. These account for the fact that the dose received at a low dose rate is less harmful than the dose received at a high rate. This dependency is expressed by a medium lethal dose LD50 as a function of dose rate. This development is now being implemented in most current PCA codes.

The deterministic fatal effects usually calculated with the above model which comprises selective irradiation of the organs are. (i) Bone marrow (haematopoietic syndrome), (ii) Lung (pulmonary syndrome), (iii) GI tract (gastrointestinal syndrome) and (iv) Skin (skin burns).

In addition, the mortality of pre and neonates after exposure in utero is normally quantified. The above model also enables a wide variety of radiation induced injuries to be estimated (e.g. hypothyroidism, temporary sterility, microcephaly and cataracts)

(b) Stochastic somatic effects

The principal stochastic somatic effects are the increased incidence of cancers, both fatal and non-fatal, in the irradiated population. Their appearance is likely to be spread over several decades following an accidental release. Generally, for each cancer type the risk of cancer incidence r is given by a linear-quadratic dose response function of the form:

$$r = aD + bD^2 \tag{3.11}$$

where, D is the absorbed dose to the organ of interest and a and b are effect specific model parameters that quantify the risk per unit dose and are usually referred to as 'risk coefficients'. These coefficients are given in Annexure-XI.

In current consequence analysis codes it is usual to assume b=0, so that a linear dose response function is used. The application of such a no-threshold linear dose response function is in accordance with recent recommendations of the International Commission on Radiological Protection (ICRP) and may lead to an overestimation of the stochastic somatic effects at low doses. For low doses and dose rates below some threshold, some codes modify the parameter 'a' by a low dose and dose rate effectiveness factor (DDREF).

Two types of models are available for estimating the risk coefficients a and b, the relative and absolute risk models. The absolute (additive) risk model is based on the assumption that the probability of incurring radiation induced cancer depends only on the dose received and is independent of the cancer incidence due to natural and other causes. On the other hand, the relative (multiplicative) risk model assumes that the incidence of radiation induced cancer is related directly to the spontaneous rate, and that radiation acts multiplicatively to yield total risk. Which model is used depends on the type of cancer.

In the calculation of the number of stochastic somatic effects in the population as a result of an accident, the following aspects have to be considered.

(i) The life expectancy and age distribution of the exposed population,

(ii) As stochastic effects may not appear for some tens of years after a single exposure, some of the risks may not be expressed in the population, as people may die naturally before the possible radiation induced effect occurs,

(iii) Most of the routes of irradiation lead to doses protracted over a period of years or decades, with changing contributions of the various radionuclides released.

The calculation of the risk of stochastic somatic effects, allowing for the time variation of dose and the age and lifetime distribution of the population, requires, in principle, the evaluation of complex multiple integrals. Some codes, however, use a simple approximation.

(c) Stochastic hereditary effects

Hereditary effects may occur by changes arising in the base sequence in the DNA of a single gene, 'gene mutation', or by rearrangement of collections of genes within and between chromosomes; 'chromosomal aberrations'. Radiation damage to the male and female germ cells may increase the incidence of these effects; they range from being very obvious to being virtually undetectable. The above procedure can be used for evaluating stochastic hereditary effects in current consequence analysis code.

(d) Dose mortality criteria

Three dose-mortality criteria are proposed depending on the degree of medical treatment. The curves are reproduced from [43] in Fig. 3.6 and are denoted by A, B, and C for minimal, supportive, and heroic treatments, respectively. Mortality criteria are often stated in terms of the dose that would be lethal to 50% of the exposed population within 60 days (denoted by LD50/60). In Fig. 3.6, the LD50/60 may be read on the abscissa opposite the 50 % value on the ordinate. An early and commonly accepted value for LD50/60 is 300 rads to the whole body. This data was based on atomic bomb victims, who received only limited medical treatment at a time when radiation medicine was less advanced than today. As a result of the additional data accumulated over the years, it is recommended that LD50/60 would be 340 rads if only minimal medical treatment were available.

It is likely that, in the event of a serious reactor accident governments will mobilise medical resources throughout the nation to aid the exposed population. A major constraint would be the availability of specialised resources. For this reason, the medical advisors evaluated following two levels of medical treatment:

- Supportive: Supportive treatment would include barrier nursing, copious antibiotics, and transfusion of whole blood, packed cells, or platelets. For such people the LD50/60 would be 510 rads. Supportive treatment is not needed immediately following irradiation but can be started about 20 days later.
- Heroic: Heroic treatment includes, in addition to the therapy outlined for supportive, extraordinary procedures such as bone marrow transplantation. Heroic treatment should be initiated within 10 days.

3.4.2.8 Economic Consequences

Several models for predicting the economic impact of accidents have been developed and incorporated into consequence analysis codes. In general, these models include the cost of countermeasures, namely evacuation, relocation, sheltering, food restrictions and decontamination, and also the cost of health effects in the exposed population. The cost may also include the cost of decrease in the value of property, psychological effects, ecological impact, loss of revenue and capital, compensation, etc.

3.4.2.9 Presentation of Results

A complete consequence model can consider a spectrum of possible source terms and treats weather as a stochastic variable. Given a source term, the magnitude of consequences are estimated for a variety of meteorological conditions and wind directions, with associated probabilities based on observed

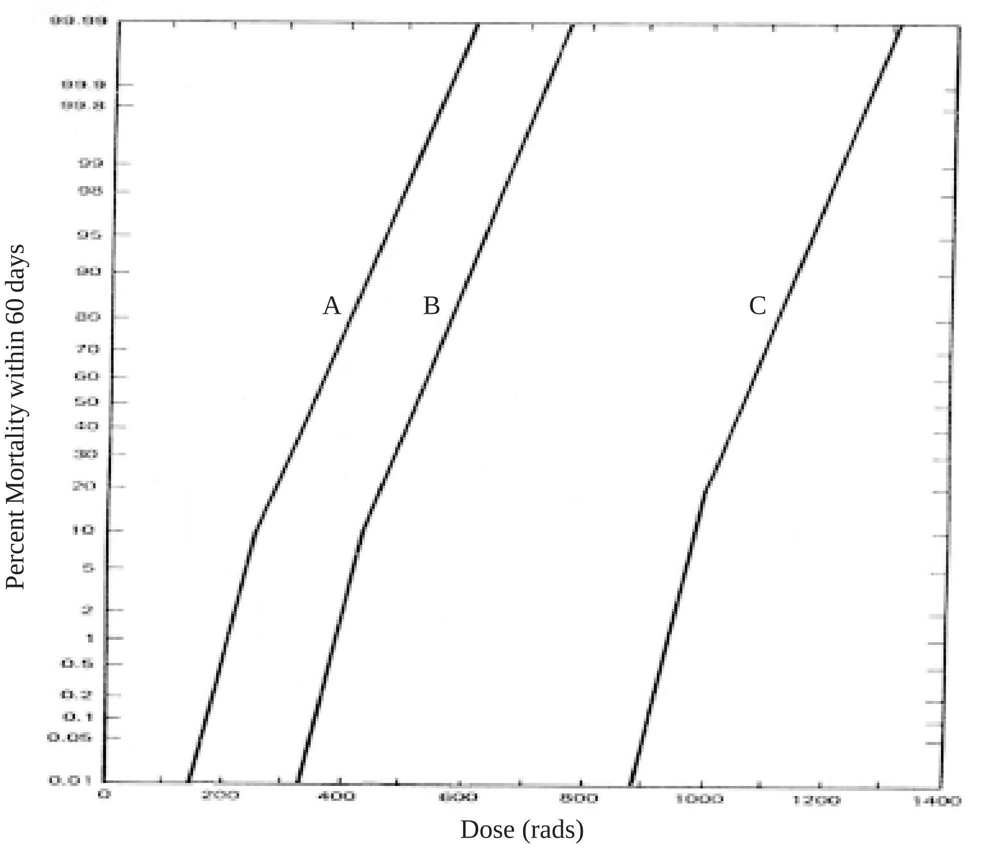


FIG. 3.6 : ESTIMATED DOSE-RESPONSE CURVES FOR 50% MORTALITY IN 60 DAYS WITH MINIMAL TREATMENT (CURVE A), SUPPORTIVE TREATMENT (CURVE B), AND HEROIC TREATMENT (CURVE C)

meteorological statistics. The most common way of presenting the resulting consequence magnitudes and probabilities is in the form of Complementary Cumulative Distribution Functions (CCDFs). An example is shown in Fig. 3.7. The ordinate is the probability of equalling or exceeding the consequence magnitude indicated by the curve. The abscissa is the value of the consequence, which may be any of the effects, such as number of early fatalities or injuries, the number of latent cancer fatalities, the size of the area contaminated to such a level, that decontamination is required, and so on. Logarithmic scales are employed on both sets of axes to accommodate the wide range of frequencies and consequences involved. CCDFs are often used as a measure of public risk. In addition, the expected (mean) value of the CCDF (which corresponds to the integral of the CCDF) is frequently used as a summary measure of risk.

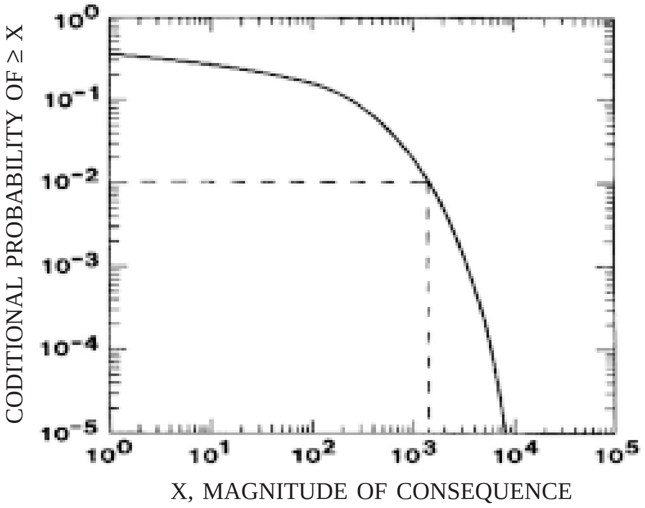


FIGURE. 3.7: AN EXAMPLE OF CCDF VS MAGNITUDE OF CONSEQUENCE

The expected value of the contribution corresponds to the integral of the curve. In this example, the consequence magnitude that would be exceeded in one out of one hundred releases (probability of 10^{-2}) is about 1500.

3.4.2.10 Uncertainty and Sensitivity Analysis

General aspects of uncertainty and sensitivity analyses are discussed earlier in section 3.2.6 and 3.2.8. With regard to PCA, uncertainties arise due to many factors that include usage of large number of complex models and parameters, assumptions made and judgement used in the calculations.

Uncertainty analysis is a highly labour intensive exercise, requiring several hundred runs of complex PCA codes [23]. Hence, a selection of the more important parameters affecting the various end points would be of great help. In the existing PCA codes, the identification of the sensitive parameters is performed at the sub-modular level, usually by the partial rank correlation coefficients, or the percentage contribution derived from R^2 values. As an example, in the Food Chain model of the COSYMA code, the following list of parameters was identified in [Table 3.10].

TABLE 3.10 : SELECTED INPUT PARAMETERS IN FOOD CHAIN MODEL OF THE COSYMA CODE [10]

Biological half-life, dairy cows, I	Processing loss, cereals
Daily intake of hay/silage, dairy cows	Processing loss, green vegetables
F_f transfer to meat, beef cattle, Cs	Resuspension factor, pasuture
F_f transfer to meat, dairy cows, Cs	Retention time, cereals, Cs
Soil fixation pasture, Cs	Retention time, green vegetables
F_f transfer to liver, dairy cows, Ag	Retention time, hay/silage
F_m transfer to milk, dairy cows, Cs	Root uptake, pasture, Cs
F_m transfer to milk, dairy cows, I	Soil migration, pasture, 3 migration rate constants, Cs
Interception factor, cereals	Soil contamination, green vegetables
Interception factor, hay/silage	Translocation , cereals, Cs
Interception factor, pasture	Translocation, potatoes, Sr
Interception factor, potatoes	

In the same manner, the list of sensitive parameters in all the sub-modules is collected. For the overall analysis, a brief list of the more important parameters is given in Table 3.11 below.

TABLE 3.11 : SENSITIVE PARAMETERS, IN THE OVERALL UNCERTAINTY ANALYSIS

1.	Dry deposition velocity to skin & ground, I and particulates
2.	Wet deposition washout coefficient
3.	Dispersion parameters, σ_y and σ_z
4.	Particle size distribution of the aerosols
5.	Risk coefficients for lung, colon, and other organs
6.	Occurrence of rain and wind slowdown
7.	$LD_{50,\infty}$ for bone marrow
8.	Fraction of skin affected by beta exposure
9.	Breathing rate
10.	Respiratory tract deposition and retention
11.	Residence times of materials on skin
12.	Cs and I retention parameters
13.	External dose and location factor
14.	Resuspension factors
15.	Sampling method for weather sequences
16.	Duration of release
17.	Timing of the initiation of counter-measures
18.	Biological half-life for dairy cattle for Iodine
19.	Daily intake of hay by dairy cows
20.	Interception factor, pasture.

Modelling uncertainties and the adequacy issue will require critical examinations of the model, and the way, these are combined in the overall assessment. This requires intensive peer reviews and discussion with experts.

3.4.3 Documentation of Level 3 PSA

The main objectives and format of the documentation of Level 3 PSA is given in Appendix-I.

3.5 Performance of Shutdown and Low Power PSA- SPSA [24, 25, 26]

This section highlights the important aspects pertaining to the PSA for the shutdown and low power operational states. PSA studies for NPPs considering shutdown and low power have shown that these states can contribute to the CDF at a level comparable to full power operations. One important reason is that, traditionally, less attention and importance are given for low power and shutdown states, compared to high power operational states of a reactor. The main risk significant characteristics for shutdown and low power operational states are the variability in plant configurations, simultaneous unavailability of safety significant systems and components, blocking of automatic actuation of safety systems and absence of specific clauses on limiting conditions of operations. PSA for shutdown and low power mode can provide useful insight and feedback with respect to (a) outage planning, (b) plant operation and procedures during an outage, (c) shutdown technical specifications, (d) outage management practices, (e) personnel training, (f) emergency planning and emergency operating procedures, and (g) hardware modifications. For such applications, risk from all operating states should be considered in an integrated manner. A write-up on Shutdown PSA is given in Annexure-XII.

3.5.1 Objective and Scope

The objective of including PSA of NPPs for shutdown and low power modes is to provide insight into the importance of various aspects of design, operating practices, maintenance, technical specifications, accident procedures and outage management with regard to the prevention of fuel and core damages, as well as releases of radioactive materials.

A full scope PSA should consider both the shutdown and low power operational states. This may be helpful in addressing cases such as shifting of maintenance activities from shutdown state to full power operations and changing the duration of AOTs in technical specification that can affect not only the shutdown PSA, but also the full power PSA. An isolated view based only on changes for individual applications without consideration of the risk impacts during different operational states, might be misleading.

3.5.2 Structure of PSA for Shutdown and Low Power Modes

The major procedural steps characterising a shutdown and low power mode PSA, should include the following.

(a) Identification of the potential source of radioactive release, generation of the list of operational states, and the IEs for the PSA for shutdown and low power modes, including quantification of IEs and identification of system dependencies (e.g. off-site power failure frequency may be higher in shutdown states).

(b) Accident sequence modelling using a combination of tools, such as ETs and FTs, that may differ from a corresponding PSA (due to the specific conditions during shutdown states) in terms of modelling of important tasks like human performance and dependence analysis. It should be noted, however, that in a low power/shutdown PSA, in which long mission times or recovery times are often applicable, use of Markovian techniques instead of standard FT/ET evaluation methods have the potential to yield more realistic results. Special care is required to be taken in choosing the appropriate success criteria.

(c) Data assessment to generate information necessary for the quantification of the model, including component reliability data, test and maintenance unavailability data and an assessment of CCFs.

(d) Inclusion of external IEs like earthquakes, flood; and internal events such as fire and flood, as well as heavy load drops during maintenance activities, dropping of reactor fuel assemblies (wherever applicable), etc. should be given due consideration.

(e) Accident sequence quantification may be performed using the same techniques as for a PSA for full power conditions. Sensitivity analysis should also be carried out for verification of the data, models and assumptions. Importance and uncertainty analyses should be performed, using the same techniques as for a PSA for full power operation.

On completion of the study, results should be reviewed to determine need for safety improvement measures in areas such as outage planning, operating procedures, technical specifications, accident procedures, emergency planning, hardware modifications, and training of personnel and management practices.

3.5.3 Outage Types, Plant Operational States and Accident Initiators

The current practice for modelling the changes in plant operational states during low power and shutdown PSA, is to define a number of plant operational states (POS) that are used to describe the operational stages during outages, and identification of IEs that are feasible in every POS. The different procedural steps or actions (Pre-POS), which occur during the outage, should be listed and grouped to form a shorter list of POS for consideration in the analysis. The POS/IEs combinations require screening and re-classification in order to achieve a manageable number of POS-IEs combinations (grouping). The emphasis given to this screening and grouping process, together with the large number of POS/IE combinations to be analysed are the key methodological differences compared to a PSA for full power conditions.

A clear interface should be defined between the POS modelled in the full power PSA and those to be modelled in the SPSA. The status of major safety functions may be more important than only the power level (or reactivity coefficient), for defining the interface. Two such important elements are; (i) Status of automatic actions and (ii) Status of support system. Typically, below a certain level (e.g., power level, PHT temperature, pressure or some combination of these parameters) automatic actuation of the main safety systems may be blocked to prevent inadvertent actuation. In some cases, as a plant approaches shutdown conditions, the essential support system configuration may change. Also containment may have been breached (e.g., interlocking doors of main airlock/emergency airlock may be open due to some maintenance job).

3.5.4 Identification of IEs

For shutdown conditions, a number of IEs are unique and different from those for the full power PSA. The major categories of IEs include: (a) Failures in the heat removal, (b) Loss of primary circuit inventory, (c) Event threatening primary circuit integrity, (d) Events affecting reactivity control and (e) Human activity related initiating events.

IEs may be grouped following the same criteria that are used for full power PSA and the following should be ensured in this regard.

(a) All IEs in the group have similar effect on safety and support system availability and operation

(b) All IEs in the group have similar success criteria for safety and support system

(c) All IEs in the group place similar requirements on the operation.

3.5.5 Quantification of IE Frequencies

As for full power, quantification of IE frequencies follows standard PSA practices. It is important, however, that the quantification of IE frequencies for shutdown and low power conditions account for plant specific items such as equipment configuration, availability, technical specifications, and outage management, including refueling operations (wherever applicable). IE frequencies also need to be POS specific, as discussed below.

In a shutdown PSA, IE frequencies are usually calculated on a 'per calendar year' basis. In other words, the IE frequency assigned to a particular POS takes into account both the expected hourly rate of occurrence of the initiator while in a particular POS and the duration of POS. When IEs are calculated on a 'per calendar year' basis, the core damage frequencies calculated for different POS are additive: the total core damage frequency is the sum of the core damage frequencies of the relevant POS.

Three different conceptual models can be applied for the IE frequency calculation in an SPSA, in order to generate 'per calendar year' frequencies:

(1) $f_{annual} = f_{hourly}$ x t_{POS}

(2) $f_{annual} = f\_\ precursor_{hourly}$ x P(IE|precursor) x t_{POS}

(3) $f_{annual} = n\_\ precursor_{POS}$ x $f\_\ POS_{yearly}$ x P(IE|precursor)

where,

f_{annual} = 'per calendar year' frequency of occurrence of initiator in POS (/year)

f_{hourly} = hourly rate of occurrence of initiator in a particular POS (/hour)

t_{POS} = duration of POS (hours in POS/year)

$f\_precursor_{hourly}$ = rate of occurrence of a precursor event per hour in the POS (/hour)

P(IE|precursor) = probability of an IE given occurrence of the precursor

$n\_precursor_{POS}$ = expected number of occurrences of a precursor in POS (/entry in POS)

f_POS_{yearly} = expected number of entries into POS (/year).

Model (1) is suitable for IEs, which may occur randomly at any time in a POS. In this case, the IE frequency is proportional to the time spent in the POS. This model is useful when IE frequencies are estimated directly from operational experience.

In model (2), the IE frequency is also dependent on the POS duration. This model is suitable when data is available on the occurrence of precursors, but not on the occurrence of the IE itself. A typical situation where this model might be used is for an IE which might arise from human error in some manipulation or manoeuvre, which is performed with a certain frequency in a particular POS. In this case, the conditional probability, P(IE|precursor), is the probability of the human error which would lead to the IE.

Model (3) is relevant for situations in which the IE frequency is not dependent on the duration of the POS. In this case, IEs arise due to errors or failures following an event which occurs a fixed number of times in the POS. For example, to model the frequency of an overdraining IE, $n\_precursor_{POS}$ would be the number of times a draining operation is performed in a particular POS (e.g. once) and P(IE|precursor) would be the probability of an overdraining per draining operation. It is important for the analyst to appreciate that situations of this type lead to IE frequencies, which are not proportional to POS durations and model these accordingly. Recognition of this type of situation is important because the risk from some IEs can be reduced by shortening the duration of critical POS, whereas the risk from others (e.g., overdraining) cannot.

There are basically three approaches for quantifying IE frequencies in a given POS: (i) direct estimation from operational experience (the plant being analysed, other plants of similar design, or generic reactor type), (ii) estimation from power PSA frequencies with supplementary analysis and (iii) use of a logical model including all the foreseen inputs leading to the IE.

3.5.6 Accident Sequence Modelling and Quantification

The methodology followed is more or less same as that followed for full power PSA. The front line safety systems may be different in low power and shutdown state of plants (e.g. ECCS for cold shutdown). In SPSA Level 2 analysis, further ET modeling of containment isolation and other containment safeguard systems may be required. This is particularly important for shutdown analyses as the availability of these systems is not necessarily assured in all stages of an outage. If the analysis is restricted to Level 1, it may still be useful to define POSs for grouping the accident sequences. Greater importance would then be associated with accident sequences involving failures of containment isolation and containment safeguard systems. It is recommended that an SPSA should always include, as a minimum, information on the status of containment integrity for each POS.

This step may involve six tasks:

(1) Event sequence modelling

(2) System modelling

(3) Human performance analysis

(4) Qualitative dependence analysis

(5) Impact of physical process on development of logic models

(6) Classification of accident sequences into POSs.

3.5.7 External Events

The following items should be considered during the performance of the external hazards analysis for the shutdown PSA.

- As for the internal events analysis, a table showing all systems required to perform the required critical safety function for each POS should be constructed.
- Structures and components that are only present in certain areas during some POSs, should be identified. For example, some plants have their vessel head parked close to the vessel or spent fuel pool, and if it is not fixed in place with seismically qualified restraints, it could be set in motion and impact upon critical safety equipment. Additional structures are often erected, which could jeopardise essential equipment if not suitably located or restrained. Identification of these configurations generally requires additional walkdowns of the plant during shutdown.
- For many plants the containment (equipment hatch) is open during many stages of shutdown operations. Under these conditions external hazards can add additional risk. Seismic events may preclude the rapid closure of an open equipment hatch. High winds may produce missiles that damage critical equipment within an open containment. Failures of building structures outside the containment may result in a direct pathway to the environment for radionuclide release.

3.5.8 Heavy Load Drops

PSAs normally focus on the failure to cool the core inside the reactor vessel or fuel stored in the spent fuel pool. But other more direct damage can occur, e.g. by heavy load drops onto the vessel, fuel pool or systems required to perform the critical safety functions.

Potential heavy load (e.g., confinement dome, RPV head, spent fuel cask, concrete shielding blocks) drops should be analysed in areas having the potential to damage systems required to perform the critical safety functions or having the potential to directly result in mechanical damage to fuel assemblies. If the load transport pathway is neither above fuel nor above regions containing critical equipment, screening out of particular heavy load drop initiators may be possible. However, screening out of all heavy load drop accident initiators is generally not possible because of the significant damage that can occur. Consequently, probabilistic analyses must be performed. The analysis should consider locations in addition to the reactor-refuelling floor where heavy loads are handled. For example, some plants (e.g., WWER-440) have open areas in the turbine hall where decay heat removal systems, which are vulnerable to heavy load drops, are located. Risk from dropping of shipping flask in spent fuel storage bay is addressed in sec. 4.4.5.

3.5.9 Accidents Involving Other Sources of Radioactive Materials

As for full power PSAs, potential accident sequences involving other in-plant sources of radioactive materials should be considered. Potential sources of radioactive material release include the spent fuel pool, radioactive waste tanks, processing facilities for radioactive waste, and on-site waste storage facilities including (dry) storage of fuel assemblies, etc. For these sources of radioactive materials, potential events or sequences of events, which could potentially lead to significant radioactive releases should be identified. For these events, a preliminary probabilistic analysis should be performed to quantify the frequency of a radioactive release and the potential magnitude of the radioactive material release estimated. A screening analysis should be performed to screen out events which have a low probability of occurrence (e.g. screening value lower than 1.0E-6 /year) or which lead to only small radioactive releases (e.g. screening value lower than the yearly allowed radioactive plant release). After this screening step, only the significant events need be analysed in detail.

Drain-down and loss of cooling events should be analysed for the fuel assemblies in the spent fuel pool. Identification of IEs should be performed, including a review of the operating procedures, which could lead to drain down, and loss of cooling IEs. Accident sequences which takes into account potential recovery actions taken by the operator, should be developed and quantified.

4. APPLICATIONS OF PSA

As mentioned earlier in section 1, PSA is now being widely used by utility and regulators all over the world. This chapter discusses some of the important applications of PSA.

4.1 Living PSA/Risk Monitor [27]

The configurations of nuclear facilities are subject to change with time. These changes can be physical (resulting from plant modifications, etc.), operational (resulting from enhanced procedures, etc.) and organisational. Therefore, if the PSA is to be of continuing use in the enhancement and understanding of plant safety, the PSA must be updated as necessary to reflect the above changes. This has lead to the concept of "Living PSA/Risk Monitor" (LPSA/RM). The purpose of LPSA/RM is to provide safety information on a plant for decision making about whether continued plant operation is tolerable under certain system function outages based on the impact it has on the plant safety. It may also support operations and be of help in deciding the maintenance strategies allowing immediate assessment of different plant configurations. A Living PSA is defined as a PSA of the plant, which is updated as necessary to reflect the current design and operational features and is documented in such a way that each aspect of the model can be directly related to existing plant information, plant documentation or the analysis assumptions in the absence of such information. The analysis in LPSA represents periodic updating of reference or base PSA and does not reflect plant configuration changes of short duration. The LPSA should be used by designers, utilities and regulatory personnel according to their needs. A risk monitor is a plant specific time analysis tool to determine the instantaneous risk, based on the actual status of the systems and components. At any given time, the risk monitor reflects the current plant configuration in term of the known status of the various systems and/or components out of service for maintenance or test. The risk monitor model is based on, and consistent with, the LPSA. The risk monitor is generally used by the plant staff in support of operational decisions.

The factors, which should be considered in deciding the scope of LPSA/RM are radioactivity source considered, IEs treated, plant operational modes analysed and Levels of LPSA/RM included (Level 1, Level 2, Level 3 PSA). SPSA should be used along with full power PSA for applications requiring decision based on comparison of risk at power with risk during shutdown state. The modelling approach for the development of LPSA/RM should be governed by the end application for which the LPSA/RM is intended. LPSA/RM model should facilitate updating as necessary to reflect the current design and operational features, and documentation in such a way that each aspect of the model can be directly related to the existing plant information, plant documentation or the assumptions. RM should cater to the on-line application of PSA model of the plant. RM should be updated at least with the same frequency as LPSA. Generally, updating or reconfiguration of the RM is performed on a daily basis or as often as necessary to monitor the operational risk of the plant.

This section provides the guidelines on the use of an existing PSA study as an input for developing a LPSA or RM tool. It covers the modelling, software and data aspects involved in the implementation of a LPSA/RM tool for on-line use.

4.1.1 LPSA Updating Process

4.1.1.1 Preliminary Assessment

Preliminary assessment of the importance of modifications on the LPSA model implies a qualitative analysis of the identified modifications with respect to the LPSA assumptions, evaluation models and data. This process allows the LPSA team to decide whether

(a) the impact of the identified modifications is judged not to require an immediate LPSA update, in which case, the preliminary assessment is logged and held for the next scheduled or necessary update.

(b) the impact of the identified modifications is judged to require an immediate LPSA update, in which case, the modifications and preliminary assessment are logged and an update is scheduled, taking account of the resources and support required.

4.1.1.2 Assessment of the Modification

For the assessment of how the modification relates to one or more elements of the model, it is necessary to evaluate the need to perform further analysis e.g., thermal hydraulic calculation or statistical data processing and take necessary action to collect all the required information to update the LPSA.

4.1.1.3 LPSA Updating

LPSA/RM should be updated as changes occur in any aspects of plant design or operation, or if there is improved understanding of the thermal hydraulic or accident phenomenology, new information leading to new revised data, or advances in analytical techniques.

In order to maintain LPSA, the documents, which should be maintained, are LPSA/RM updating procedure, LPSA/RM update database and LPSA/RM application guide. The LPSA/RM should be updated as frequently as necessary to ensure that the model remains an accurate representation of the safety of the latest plant configuration. While it is likely that each modification will be assessed on a case-to-case basis, it would be a good practice not to accumulate a backlog of such assessments for a period longer than one year.

The quality assurance procedure in LPSA/RM updating should be based on and consistent with IAEA QA guidelines [1]. These guideline indicate that changes in LPSA/RM models, data information and results, including changes to the requirements, scope, objectives and input data should be made in a controlled manner. The reason for the change should be documented and consideration should be given to the impact and implication of the changes.

4.1.1.4 Computer Codes

The development of computer codes for LPSA/RM application should be governed by functional requirements such as development and maintenance of LPSA/RM models, performance of LPSA/RM task including updating and management of LPSA/RM documentation.

The code should facilitate manipulation of not only reliability data but also data, which represent the FT/ET models, together with any other information which might be considered part of LPSA/RM model. The code should have required administration and protection functions such that the software provides required security and at the same time using access control features, allows authorised staff to carryout required functions. The code should provide graphical printing capabilities and should display a variety of results in the form of graphics and tables. If a separate code is used for Level 2 PSA analysis, it should be possible to import the sequence or cut-set definitions, frequencies, etc. from the Level 1 PSA analysis.

If the level 1 PSA code does not provide functionality to bin these sequences or cut-sets in plant damage states, this functionality should be provided by the Level 2 code. The Level 2 code should also provide sub-models other than FTs, provision of handling global variables (for example to allow tracking of hydrogen generation and combustion at different points in an accident sequence). The code should automatically bin containment ET end points into source term categories, in accordance with user-defined criteria. The code should facilitate tools for performing sensitivity studies. A formal uncertainty analysis capability, using Monte Carlo type or equivalent methods is desirable. It would be desirable to tabulate the frequencies of the source term categories and their contributors. Level 3 PSA model should consist of input files for PCA codes. The interface between Level 2 and Level 3 codes should be carefully defined in order to reduce the possibility of error.

4.2 Reliability Centred Maintenance (RCM)

Reliability Centred Maintenance is a systematic consideration of system functions, the way functions can fail, and a priority-based consideration of safety and economics with risk insights, that identify applicable and effective preventive maintenance tasks. Both passive and active components are included.

4.2.1 Objective and Scope

The main objective of the RCM process is to provide a systematic set of criteria, based on risk, for deciding which of the components considered in the process are to be defined as ‘risk-critical components’ for prioritisation of maintenance tasks. Only these risk-critical components are included within the scope of the RCM process. The second major purpose of the RCM process is to provide criteria and guidance for establishing RCM program for the risk-critical components identified in the process. The RCM concept, also called Risk Based Maintenance (RBM) or Risk-Focused Maintenance (RFM) should be applied to all categories of equipment that control off-site radioactive doses or that could adversely impact the ability of the plant to prevent or mitigate accidents or transients.

4.2.2 RCM Program [28]

The RCM program mainly consists of two steps; (i) identifying risk-critical components and (ii) determining what maintenance activities are required to ensure reliable operation of the risk-critical components identified. This guide describes general guidelines for the use of PSA in RCM. Level 1 PSA can be used to identify risk-critical components.

4.2.2.1 Identification of Risk-Critical Components (RCCs)

The process for identifying the RCCs begins with a consideration of the functions that must be performed for safe operation of NPPs. The next step is to identify major systems and components that provide these essential safety functions, including mitigation of accidents and components. Then the support systems for the functioning of frontline system are identified. There are two approaches to identify RCCs: (a) Non-(explicit) PSA method, which identifies components that enable performance of essential safety functions by the frontline and support systems, using system evaluations from design reports, FMEAs. (b) PSA method, which is a more recent quantitative approach based on risk evaluations using accident sequences to core damage, cutsets, sensitivity studies, importance measures of components. This is a risk-based approach for identifying RCCs using the Level 1 PSA results and is illustrated in Fig. 4.1.

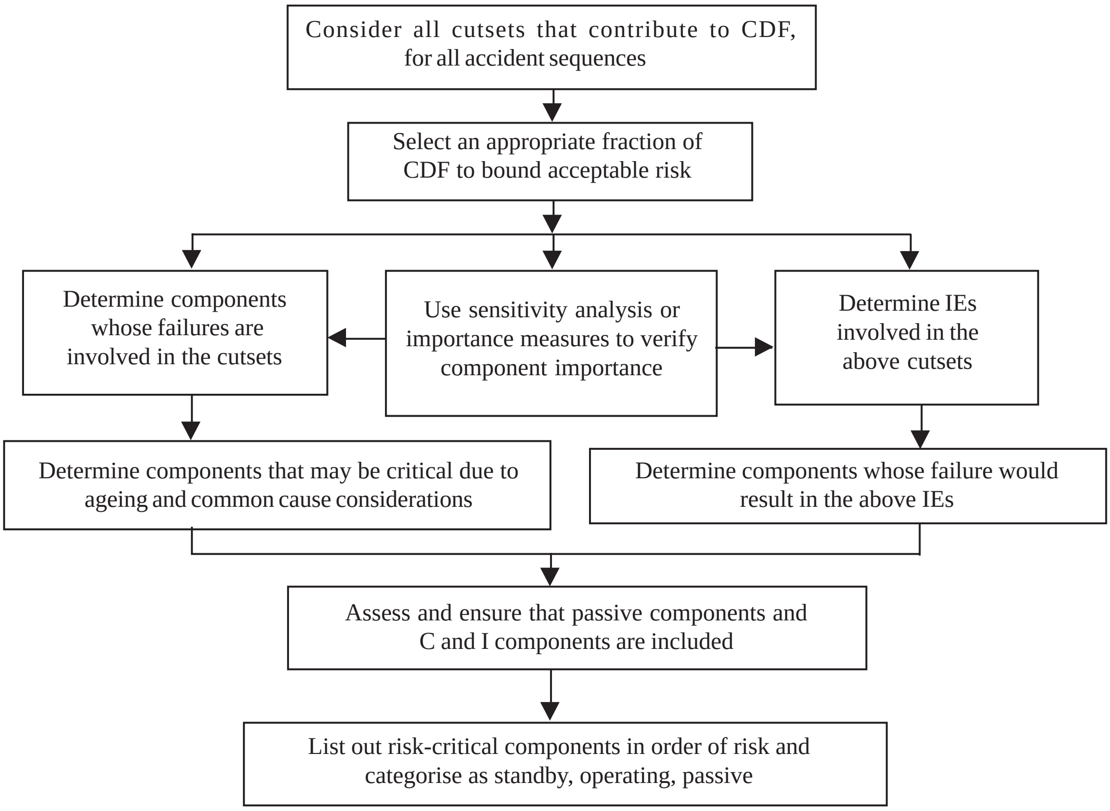
The following are the main steps for the use of PSA in a RCM program to identify RCCs.

(i) Choose a fraction of the CDF that represents the most likely accident scenarios. Identify the components whose failure modes are represented in this set of accident scenarios. These components are to be considered as RCCs including passive components (e.g. reactor pressure vessel, steam generators, accumulators) and standby components for which ageing or CCFs is a concern.

(ii) Identify RCCs from accident sequences, PIEs associated with these sequences using Minimal Cut-Sets (MCSs), components with failure modes that could result in these accidents, importance measures/sensitivities and rank them. For this purpose, any input used in deriving the system unavailability/frequency of PIE, core damage etc., such as plant specific data, plant incident records, corrective maintenance records, and station logbook, should be carefully considered and used in the analysis.

4.2.2.2 Determining Maintenance Activities for RCCs

In this step of the RCM program, maintenance activities required for the reliable operation of the RCCs determined in the first step are identified. There are mainly two steps in this task. The first step is to determine the dominant component failure modes. The second step is to determine maintenance activities for these dominant failure modes (which will be defended against). This should be worked out as a total maintenance activity that includes besides field maintenance activity, prioritisation as per ranking, purchase, stores and inventory control. Details are given in Ref. [28].



Consider all cutsets that contribute to CDF, for all accident sequences
Select an appropriate fraction of CDF to bound acceptable risk
Determine components whose failures are involved in the cutsets
Use sensitivity analysis or importance measures to verify component importance
Determine IEs involved in the above cutsets
Determine components that may be critical due to ageing and common cause considerations
Determine components whose failure would result in the above IEs
Assess and ensure that passive components and C and I components are included
List out risk-critical components in order of risk and categorise as standby, operating, passive

FIGURE 4.1 : DETERMINATION OF RISK-CRITICAL COMPONENTS USING PSA [28]

4.3 Technical Specifications (TS) Optimisation

4.3.1 Objective

One of the applications of PSA is to optimise TS with regard to Allowed Outage Times (AOTs) and Surveillance Test Intervals (STIs), to assure reliability in functioning of SSCs. TS requirements are generally based on deterministic analysis and engineering judgement. However, in some cases, the requirements may be unduly restrictive or not conducive to safety, and thus changes may be desirable. At the same time, there are certain requirements, which can improve safety if strengthened. PSA is a very useful tool to demonstrate whether the risk impact due to such changes is acceptable or not. This guide describes general guidelines and various methods for assessing the nature and impact of proposed TS changes on AOTs and STIs.

4.3.2 General Guidelines for TS Modifications

The following are the general guidelines for TS modifications.

(i) Identify the particular TS clauses that are affected by the proposed change and determine how the affected systems, components, or parameters are modelled in the PSA.

(ii) Provide the rationale that supports the acceptability of the proposed changes by integrating PSA insights with deterministic considerations and engineering judgement to arrive at risk-informed decisions.

(iii) Consider implementation and performance monitoring strategies formulated to ensure that no safety degradation occurs because of the changes to the TS and conclusions drawn remain valid.

4.3.3 Data Rquirements for TS Modifications

System FTs should be sufficiently detailed to include all the components for which surveillance tests and maintenance are performed. Since PSAs involve treatment at the component-level, they can be used to analyse changes in both AOTs and STIs. The data required for such analysis are as given below:

(i) Maintenance downtime data

(ii) Maintenance schedules and frequencies

(iii) Data relating to component testing such as duration of test, efficiency of the test, test strategy (staggered or sequential testing), test interval and any potential negative effects of testing.

(iv) Parameters for component unavailability like failure rate, maintenance/repair downtime, test downtime, human errors following test/maintenance and demand failure vs. standby failure contribution.

(v) For the analysis of AOT for shutdown/low power operation risk, the following additional data are needed.

   (a) CCF data for components/systems required for shutdown/low power operation of reactor

   (b) Time margin for recovery

   (c) Likelihood of Limiting Conditions for Operation/Shutdown related transients during power reduction/reactor cool down.

4.3.4 Assumptions in AOT and STI Evaluations

Using PSAs to evaluate TS changes requires consideration of a number of assumptions made within the PSA that can have a significant influence on the ultimate acceptability of the proposed changes. Assumptions that should be considered for AOT change evaluations can be summarised as follows [29].

(a) If AOT risk evaluations are performed using only the PSA for power operation, the risk associated with shutting the plant down because of AOT violations is not considered. For some situations (e.g. those requiring residual heat removal systems, service water systems, auxiliary feed water systems), comparative risk evaluations of continued power operation vs. plant shutdown should be considered.

(b) When calculating the risk impact (i.e. a change in CDF or LERF caused by AOT changes), change in average CDF should be estimated using the mean outage times for the current and proposed AOTs.

(c) When the risk impact of an AOT change is evaluated, the yearly risk impact that is calculated takes into account the outage frequency. An AOT extension may imply that the maintenance of the component is improved, which may reduce the component failure rate, and consequently, reduce the frequency of outages needed for correcting degradations or failure. Again, there are no experience data for the extended AOT; therefore, the assumption should be made that both the frequency of outage for corrective maintenance and the component's failure rate remain the same. Here, the beneficial aspect of maintenance is not quantified and this may give a slightly higher estimate of the yearly AOT risk measure for the proposed AOT.

(d) When AOTs of multiple safety system trains are extended, the likelihood of simultaneous outages of multiple components increases. The impact of such occurrences on the average plant risk, e.g. CDF, is small, but the conditional risk can be large.

Assumptions that should be considered for STI evaluations can be summarised as follows.

(a) The test-limited risk is estimated by assuming that a surveillance test of a component detects the failures, and after the test, the component's unavailability resets to zero or 'false' in the

Boolean expression. A few component failures, depending on a component's design and test performed, may not be detected by routine surveillance test. Usually, their contribution to risk is considered negligible.

(b) Generally, for most components, the increase of a STI beyond a certain value may reduce the component's performance (i.e. increase the failure rate). Experience data are not available to assess the STI values beyond which the component failure rate increases. If, in a risk-informed evaluation of surveillance requirements, the failure rate is assumed to remain the same, the assumption implies that the STIs are not being changed beyond the value at which failure rate may be affected. Care should be taken not to extend the STIs beyond such values using risk-informed analyses only.

(c) The risk impact of adopting different test strategies (e.g. sequential vs. staggered) should be evaluated to determine whether there is an impact on the evaluation of the change being considered.

(d) Downtime and errors of restoration are usually modelled in a PSA, unless they are negligible. Test-caused transients and wear of the equipment are applicable to a few tests, but they are not generally modelled separately in PSA. However, they can be evaluated using PSA models supplemented with additional data and analysis. Methods are available to quantitatively address these aspects; however, qualitative arguments can also be presented to support the extension of a test interval. If the adverse impact of testing is considered significant, such cases should be addressed quantitatively.

4.3.5 Methodology for TS Optimisation

The steps include the following. (a) identify the STIs and AOTs to be evaluated for consideration of changes, (b) determine the risk contribution associated with the subject STIs and AOT, (c) determine the risk impact from the change of proposed AOTs and STIs by evaluating risk measures of SSCs for which change in AOT/STI is sought, (d) ascertain the acceptability or otherwise of the risk impact (e.g., change in system unavailability, CDF, release frequency, etc) from target value established for risk informed decision (e) perform sensitivity and uncertainty evaluations to address uncertainties associated with the STI and AOT evaluation. The various risk measures and methodology for TS modifications related to AOTs and STIs are discussed here.

4.3.5.1 Measures Applicable for AOT Evaluations

(a) Conditional risk given the limiting condition of operation (LCO)

Increase in risk (DCDF or DLERF) associated with component outage is shown in Fig.4.2.

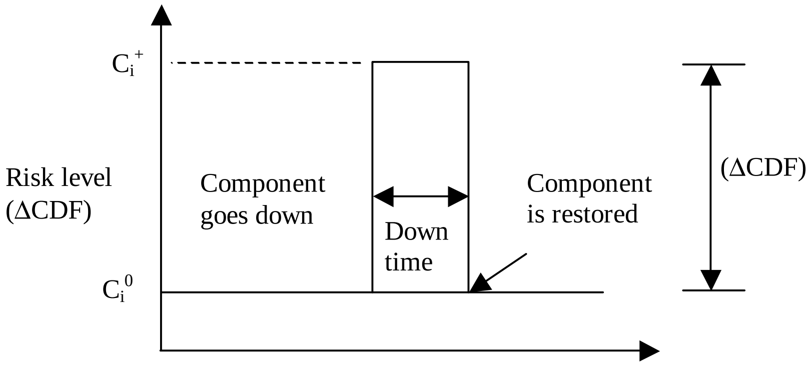


FIGURE 4.2 : INCREASE IN RISK ASSOCIATED WITH COMPONENT OUTAGE

(b) Incremental conditional core damage probability (ICCDP) or single down time risk

Increase in risk (e.g. single down time risk r_i of ith component is obtained by multiplying the increase in CDF by the duration of the configuration for the occurrence of a given configuration i.e., outage of ith component only).

$$r_i = \Delta C_i \times d = (C_i^+ - C_i^0) \times d_i \qquad (4.1)$$

r_i = Single downtime risk of the ith component

C_i^+ = CDF when component is known down including reconfigurations

C_i^0 = CDF when component is known up

d_i = Downtime

By imposing an acceptable limit (i.e., target or reference value for risk informed decision process) to the risk contribution of an AOT, a risk based AOT can be calculated, $d_{max} = r_{max}/\Delta R$ where ΔR is the change in risk (change in system unavailability, change in CDF (ΔC_i) or change in LERF). Then the risk based AOT can be compared to the real time duration of maintenance and to the AOT established in the TS.

(c) Yearly AOT risk

Risk increase from the projected (or expected) number of down times over 1 year period is yearly AOT risk. Fig. 4.3 shows the single down time risk and cumulative down time risk over some time period.

$$R_i = N_i r_i \qquad (4.2)$$

R_i = Yearly down time risk for ith component

N = Expected number of down time occurrences in a year = wT

w = Down time or maintenance frequency = $k\lambda$

Where, k = maintenance factor, λ = failure rate and T = time period, 1 year.

Maintenance frequency includes failure frequency and the frequency of maintenance due to degraded or incipient conditions.

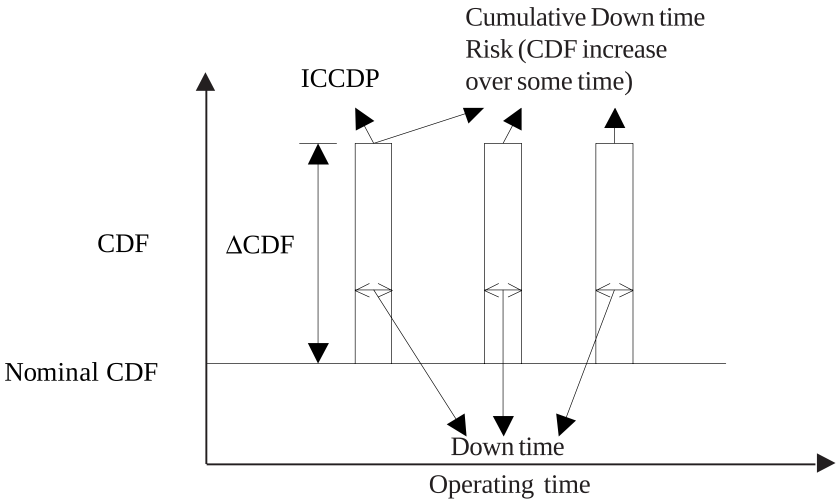


FIGURE 4.3 : ILLUSTRATION OF THE DIFFERENT RISKS ASSOCIATED WITH DOWN TIMES

When comparing the risk of shutting down with the risk of continuing power operation for a given LCO, the applicable measures are:

- risk of continued power operation for a given down time, similar to ICCDP and
- risk of shutting down for the same down time

The risk associated with simultaneous outages of multiple components, called configuration risk, is calculated as part of AOT changes. The applicable measures are similar to the AOT measures stated above.

4.3.5.2 Measures Applicable for STI Evaluations [30]

(a) Test-limited risk

The analysis of STIs is based on the risk contributions arising from failures occurring between tests and detected at the moment of the test. The STI risk contribution of a component is given by

$$R_D = ½\ \lambda_s T\ \Delta R \qquad (4.3)$$

where ΔR is the risk increase when the component is found failed at the moment of the test, λ_s is the standby constant failure rate and T is the STI. Similar to the AOT risk contributors, the STIs can be classified and set to a limiting value to the risk contribution,

$$T_{max} = (2R_{Dmax})/(\lambda_s \Delta R) \qquad (4.4)$$

(b) Test-caused risk

To evaluate and identify the test-caused risk, events should be analysed and those caused by a test should be identified. These could be due to failure in human interactions or component wear out on testing. Failure due to HEP can be modelled and quantified from detailed HRA (Appendix-VI). Component wear out can be addressed by ageing risk analysis (Sec. 4.8). However an integrated approach to work out such test caused risk is a developing subject and presently is beyond the scope of this document.

4.3.5.3 Measures for Multiple Technical Specification Changes

When multiple changes are requested, the total collective risk impact from all the changes should be evaluated. For example, for a group of AOT and/or STI changes, this includes the total impact of all the requested AOT changes, STI changes, or both.

If multiple changes are made, the impact of each change is assessed individually and then the total impact on the plant PSA is assessed.

4.3.5.4 Considerations in Quantification of Risk Due to TS Change

(a) In calculating the measures discussed for evaluating TS changes, two specific risk levels are discussed, which should be quantified using a PSA. Focusing on the CDF level, they are R1, the increased risk level (e.g., CDF) with the component assumed down and R0, the reduced CDF with the component assumed up. Depending on menu provided in the software it can be calculated from PSA end results (e.g., CDF) or MCS. It is to be ensured that the component down event appears in MCS significantly; this may call for changing truncation limit or re-manipulation in FT representations to make the relevant component more sensitive without violating plant logic.

(b) Contributions from CCFs need special attention when calculating the increased risk level R1. If the component is down because of a failure, the common-cause contributions involving the component should be divided by the probability of the component being down because of failure since the component is given to be down. If the component is down because it is being brought down for maintenance, the CCF contributions involving the component should be modified to remove the component and to only include failures of the remaining.

(c) If other components are reconfigured while the component is down, these reconfigurations can be incorporated in estimating R1 or RO, using the PSA. If other components are tested before repair or if maintenance is carried out on the down components, the conduct of these tests and their outcomes also can be modelled. If other components are more frequently tested when the component is down for the AOT, this increased frequency of testing also can be incorporated.

(d) In STI risk calculation, the contributions of CCFs should be appropriately modified. The common failure terms modelled, as a function of the test interval should be modified to reflect the new STI. Typically, CCFs are modelled using a-factor or Multiple Greek Letter model when the CCF of multiple components is a function of the STI. When changing STIs, care should be taken to change this term within the common cause contribution. The common cause of failing multiple components resulting from human error following a test is not a function of the STI, but may be affected by the test strategy used.

(e) When different test strategies are being evaluated, the human error term should be evaluated. Specific assumptions that were used in quantifying the human error common cause term should be identified and checked if they apply for the test strategy being analysed. For example, if the term was developed assuming a sequential test strategy, but a staggered test strategy is being analysed, the term should be modified to reflect this change. The failure probability from a common cause human error for a staggered test strategy is expected to be significantly lower than that for the sequential test strategy.

4.4 Risk Assessment for Internal Hazards Due to Dynamic Effects

4.4.1 General

The internal hazards (PIEs) in a plant other than fire and explosion, due to dynamic effects include pipe whip, jet impingement, missile, failure of critical components and dropping of heavy objects [36]. The effects of these could be any of the following

(a) Large pipeline displacement due to break (pipe whip) causing possible impact on adjoining SSC.

(b) Internal forces and reactive forces due to fluid jet leak from fracture/crack in piping, equipment, equipment housing, etc.

(c) Damage of safety significant components and loss of safety functions.

(d) Flooding and environmental consequences.

(e) Other PIEs of potential consequences.

(f) Release of radioactive/toxic material into the environment.

PIEs may cause direct damage called ‘primary effects’. In addition, they may cause indirect damage by means of failure mechanisms that can propagate the damage. These indirect damages are referred to as ‘secondary effects’ and in some cases may cause damage that exceeds those caused by the primary ones. Potential damage by secondary effects can be identified by studying plant layout drawings and walk-down. Important secondary effects could be any of the following.

(i) Secondary missiles: A missile or a pipe whip may produce secondary missiles such as pieces of concrete or parts of components, which may do unacceptable damage.

(ii) Falling objects: A pipe whip, jet impingement or a missile can damage a supporting structure of some heavy objects located above a safety component, creating falling object which may cause further damage.

(iii) Failure of high energy pipes and other components: Where a PIE can result in the rupture of a pipe or component besides causing loss of system inventory (possible LOCA), the fluid may cause further damage by any of the means like jets, pressure, temperature, humidity, pipe whip, flooding, secondary missiles, chemical reaction and radiation.

(iv) Flooding: Energetic missiles striking pipes, tanks, or pools normally filled with fluid may cause potential flood.

(v) Radiation dose: The release of radioactivity material may result from the impacts on items containing such material or necessary for control of radioactivity. The releases may also result from flooding.

(vi) Chemical reaction: Missiles or pipe whip impacts can release dangerous chemicals and may result in fire, explosions, exothermic reactions, accelerated corrosive attack, release of toxic materials, etc.

(vii) Electrical damage: Missiles, pipe whips or flooding may damage electrical equipment and/or result in malfunction including spurious actuation.

(viii) Damage to life lines: Some fluid commanded equipment and instrumentation needed for monitoring and/or control of important parameters/reactor state may be damaged due to missile, pipe whips or jet effects.

(ix) Fire: Some PIE may result in fires: For example an electrical arc produced by impact of a PIE in the proximity of flammable material.

(x) Personnel injury: A PIE may directly or indirectly cause injury to plant personnel.

The PSA for a plant requires consideration of such PIEs in the analysis for assessment of overall risk in a plant. The general approach for analysing risk from such internal hazards includes the following steps.

(i) Evaluation of the probability of occurrence of PIE (P1), (ii) probability of a possible threat to SSCs (P2), (iii) the probability of causing damage to SSCs with unacceptable consequences (P3) and finally (iv) the probability of unacceptable consequences (P) in the plant. Conservative design is a way of reducing P1. While evaluating P1, design features, inspection (surveillance including ISI), monitoring and possible operator action should be taken into considerations. Physical separation by appropriate layout is a means of reducing P2. While evaluating P2 (probability of SSCs being hit/affected), plant layout and barriers provided for protection of SSCs against possible strike effects should be taken into account. Comprehensive design and qualification of component is a way of reducing P3 (plant vulnerability/component fragility). For evaluation of P3, due considerations should be given to primary/ secondary effects, fail-safe features, qualifications, etc. Redundancy, other favorable designs and minimising CCFs are ways of reducing P. There is a variation in the level of confidence with which probabilities and consequences for such rare events can be determined. The consequence analysis should take into account ,besides physical separation and redundancy aspects, EOPs and operator recovery actions. The probability for successful recovery actions should be assigned, based on a number of factors that include expert judgement, insights from simulator training and operator PSFs like skill, knowledge and experience, and time availability for taking corrective actions. In order to cope with uncertainty in quantifying P1, P2, P3 or P, some studies should be performed, involving an appropriate combination of analytical and experimental work to determine the worst case and enable conservative estimate to be made.

Based on plant design and complying with design criteria and worldwide experience, some of these PIEs, viz., pipe whip, jet impingement, low trajectory turbine disintegration missiles, internal flooding, failure of some critical structures and fall of shipping flask, have been addressed in brief below for probabilistic risk assessment.

4.4.2 Pipe Whip and Jet Impingement

(a) Pipe whip

Pipe whip is an uncontrolled motion of a ruptured pipe. Cracks are postulated in weld areas of pipe (at bends, elbows, valves, etc.) and at nozzles to equipment, connections etc. The postulated rupture pattern is transverse or longitudinal. A transverse rupture is assumed an instantaneous circumferential break resulting in double ended guillotine rupture with chance of pipe ends to go away from each other. A longitudinal rupture is specified as a pipe line wall crack, located along the pipe axis, but without pipe parts going away from each other. This kind of rupture has the potential of impact by contact or jet impingement. Break probability depends on pipe diameter, service stress level, material crack location and size, leak detection capability (inside/ online) and corrective actions taken.

If axial stress component is at least 1.5 times the circumferential stress component, a transverse rupture is to be postulated. And vice-versa, if circumferential stress component is at least 1.5 times the axial stress component, the a longitudinal rupture is to be postulated.

The phenomenon of ‘pipe whip’ can only occur as a consequence of a double ended guillotine type break in high energy piping (internal operating pressure larger than or equal to 2.0MPa or operating temperature greater than 100^0C, and operation is at greater than 2% of unit normal power operation) and when pipe whip restraints of an effective design are not present or give away due to reaction forces.

On impact with other components or structures, the whipping movement is slowed down or stopped and the kinetic energy of the moving pipe branch is transferred partly or totally to the target, as an impact load. Such mechanical impact on other components would challenge the success of consequently needed safety functions like reactor trip, emergency core cooling, residual heat removal and containment isolation/control of radioactivity release, after an IE.

(b) Jet effects

A jet is a stream of fluid ejected from a leak or break in a pressure retaining system in a certain direction with significantly high velocity. Jets usually originate from a broken component such as pipe or vessel containing high energy pressurised fluid. The PIE is then a leak or break of that pipe or vessel. Jet effects can be excluded for low energy systems (<2 MPa and <100 ^{0}C) or if the reactor power is less than 2% FP. For each postulated break location and size, the jet geometry (shape and direction) and physical parameters (temperature, pressure) should be evaluated as a function of time and space. If the PIE generates more than one jet, possible interference of the jets should be taken into account. Either up-to-date computer code or a simplified approximation based on computational data or appropriate conservative assumptions, can be used for analysis of jet shape and properties.

Protection against dynamic effects from pipe whip, jet impingement, etc., against postulated pipeline rupture inside or outside the containment, is generally done in design by

(a) Ensuring physical separation of SSC from high energy components of other systems.

(b) Substantiating applicability of leak before break (LBB) concept

(c) Special design measure to ensure safety performances by

 (i) providing redundant system/multiple trains

 (ii) designing SSC with considerable capabilities to resist effects of postulated rupture.

 (iii) creating additional restraining support and barriers.

The following steps are involved in evaluating plant risk from these hazards.

(1) Identification of high-energy fluid pipes : High-energy pipes may cause pipe whip or jet impingement on surrounding SSCs. The broken pipe is powered by the thrust force of the cooling medium, which is calculated by detailed hydrodynamic analysis that produces time-force function. The pipe whip analysis is performed as one continuous calculation,

starting with the pipeline break and ending with the completion of the pipe movement, whereas evaluation of jet impingement effect involves a time history of jet impingement loads for the assumed jet shape and direction is determined. The force is a function of jet properties, such as quantity, velocity, cross-sectional area at the point of interaction with target, etc.

(2) Evaluation of frequency : The frequency for a double ended guillotine break of high energy piping (P1) is derived from operating experience, generic data and probabilistic fracture mechanics calculations and is available from evaluations for use in PSA. The probability of the initiating pipe break event considers also the existence of the pipe whip restraints in the piping system. A hazard curve may be generated for frequency of occurrence for different break sizes for pipe whip and those for different magnitude of force for jet impingement.

(3) Evaluation of probabilities that safety relevant piping or equipment will be hit (P2) : The whipping branches should be analysed geometrically in order to identify possible directions of movement that may potentially hit and endanger SSC targets, as well as to evaluate its kinetic energy. Any mechanical impact on the target should be investigated by an appropriate dynamic analysis, based on a detailed assessment of the system transient to quantify the discharge forces and the energy of the whipping pipe, as well as the fraction of energy transformed to the target with precision. In the case of pipe whip, it conservatively assumes a full circumferential rupture and that the pipe will form a hinge at the nearest rigid restraint. The analysis of the whipping pipe should also include the potential for a following break and for an impact on a possible target ejecting a secondary missile. Sources of missile can be single calculated masses such as valves and pumps. The usual approach is to model these into fault tree and assigning individual event probabilities based on expert judgement and considering the response of plant SSCs. Similar approach may be followed for evaluating P2 for jet impingement.

(4) Calculation of plant response : Probability that the SSCs affected will suffer unacceptable damage is P3. With input from step 2 above and insight from dynamic analysis, probabilistic fracture mechanics and/or expert judgement values for P3 need to be assigned.

(5) Computation of consequence probabilities : Quantification of each accident sequence from the IEs, including secondary effect initiated PIEs leading to core damage, source term and release consequences (P), can be done as required as per the methodologies of PSA Level 1 to 3.

Uncertainties arising in each step of analyses need to be propagated to arrive at vulnerabilities in consequence analysis.

4.4.3 Missiles [31]

4.4.3.1 Missile is the high energy mass generated by failure of high-energy components, as a primary and/or a secondary effect. The missile sources include the following.

(a) Off-normal/emergency modes of operation

(i) Ruptures of SSC operating under pressure (vessels, pipelines, and valves)

(ii) Destruction of equipment operating at high rotational speed (e.g. turbine rotor, pump flywheel)

(iii) Accumulation of explosive gases

(iv) Operator errors.

(b) Collapse and fall of large structure (height, mass as hazard parameters)

Possible PIEs of this category include the following

(i) Large structure failures (stack, turbine building, cooling tower, crane etc.)

(ii) Heavy equipment falls down (crane and lifted loads)

Although the plant is designed against these hazards from deterministic considerations, it is the randomness in the variables, which requires probabilistic considerations in the analysis. Pressure vessel rupture although not considered under PIEs in internal events PSA, is addressed under seismic PSA in Appendix-X. The following section addresses low trajectory turbine disintegration missile as regulatory bodies in many countries require besides deterministic evaluation, probabilistic risk analyses from these missiles, if safety significant SSCs are not located in the plant layout beyond turbine disintegration missile trajectory zone (typically 25^0 on either side of the plane of rotation).

4.4.3.2 Low Trajectory Turbine Missiles

The steam turbine, part of the turbo generator set, has the potential to generate massive, energetic missiles if a turbine disc were to fail catastrophically. The missile can be generated in two modes; at normal operating speed due to fatigue crack growth and destructive over speed failures. Upon sudden unloading of the generator, failure of the turbine over speed protection system and/or turbine stop and control valves, can cause the turbine to reach the destructive over speed. If a turbine disc fails and if a large portion of the disc is ejected from the turbine casing, it may be possible for the turbine missile to strike and cause damage to components or systems, that might possibly result in the release of radioactivity to the environment, following the accident.

From the above, the probability (P) of loss of safety systems due to low trajectory turbine missiles can be defined as the product of the following three probabilities.

$$P = P_1 \times P_2 \times P_3 \qquad (4.5)$$

$P_1 = P_{generation}$ = Probability of turbine missile generation

$P_2 = P_{striking}$ = Probability of turbine missile striking on a target (degradation/failure)

$P_3 = P_{impact}$ = Probability of turbine missile strike causing impact (resulting in failure/unavailability) on safety related equipment.

Furthermore, $P_{generation}$ is the sum of the following four probabilities (a to d).

(a) P_O = Probability of inherent defects during manufacture of turbine rotor that grow up to critical crack size. This comprises of the following four probabilities:

p1 = Probability that a forging will have a defect in spite of proven manufacturing process

p2 = Probability that this defect will not be revealed by tests during manufacturing of the forging

p3 = Probability that this defect will not be detected by incoming inspection and during turbine manufacture before delivery

$P_{manufacture}$ = p1 X p2 X p3

p4 = Probability that the crack will grow and will cause fracture before it is found out in operation

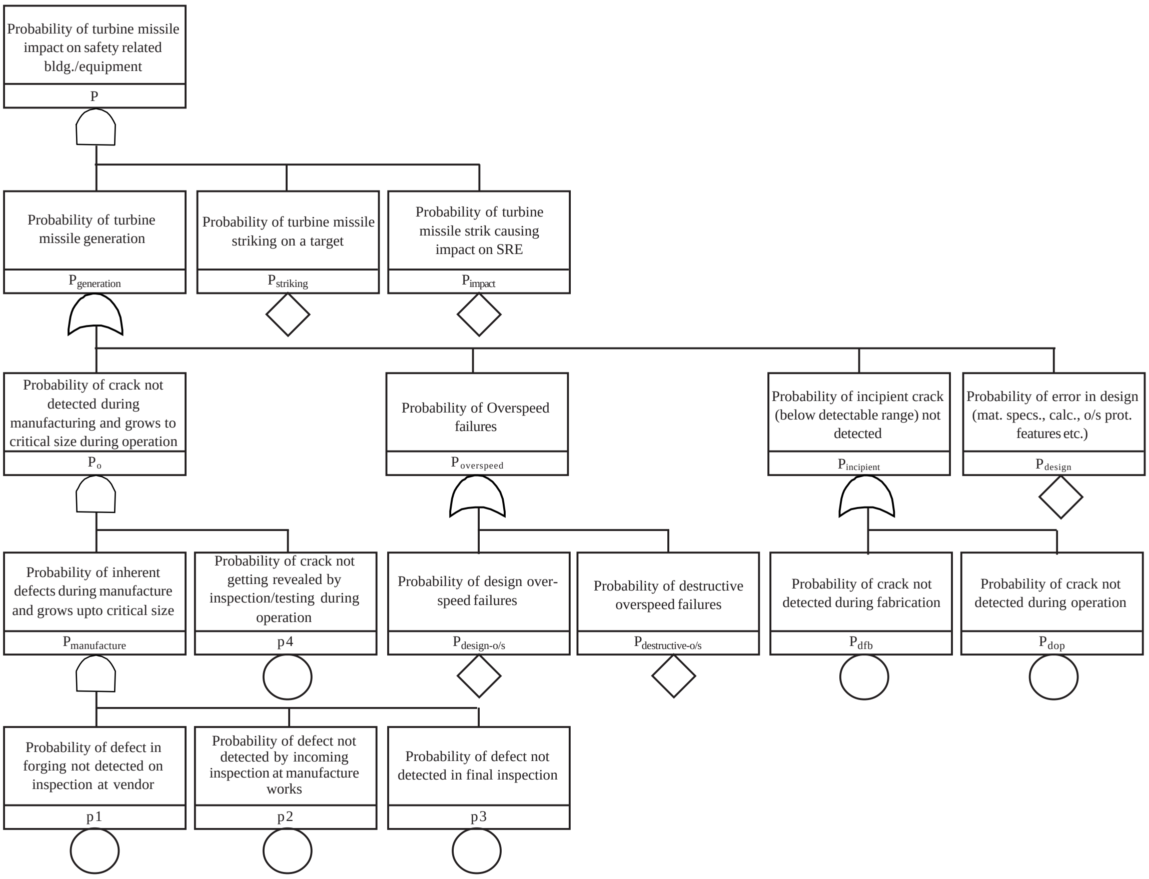
$P_o = P_{manufacture}$ X p4

(b) P_{design} = Probability of errors occurring during design

(c) $P_{overspeed}$ = Probability of turbine over speed

(d) $P_{incipient}$ = Probability of inherent defects below instrument detectable range which will grow and propagate to critical crack size during the service life

The typical values of p1, p2, p3, p4, P_{design}, $P_{overspeed}$, and $P_{incipient}$ are 2E-02, 1E-02, 4E-02,1E-01, 5E-2, 5E-9 and 8E-10 respectively for 1000 MWe turbine made by “Electrosila” [32]. This is shown in the Fault tree form Fig. 4.4



Probability of turbine missile impact on safety related bldg./equipment
P
Probability of turbine missile generation
Pgeneration
Probability of turbine missile striking on a target
Pstriking
Probability of turbine missile strik causing impact on SRE
Pimpact
Probability of crack not detected during manufacturing and grows to critical size during operation
Po
Probability of Overspeed failures
Poverspeed
Probability of incipient crack (below detectable range) not detected
Pincipient
Probability of error in design (mat. specs., calc., o/s prot. features etc.)
Pdesign
Probability of inherent defects during manufacture and grows upto critical size
Pmanufacture
Probability of crack not getting revealed by inspection/testing during operation
p4
Probability of design over-speed failures
Pdesign-o/s
Probability of destructive overspeed failures
Pdestructive-o/s
Probability of crack not detected during fabrication
Pdfb
Probability of crack not detected during operation
Pdop
Probability of defect in forging not detected on inspection at vendor
p1
Probability of defect not detected by incoming inspection at manufacture works
p2
Probability of defect not detected in final inspection
p3

FIG. 4.4 : TURBINE MISSILE GENERATION PROBABILITY CALCULATION

To determine $P_{overspeed}$ over speed protection system should be evaluated for reliability by developing and analysing FT. This includes instrumentation for detection of over speed, power supply, any valves, circuit breakers or other final control elements, protection mechanism hardware and software, and procedures involved in periodic calibration and readiness in testing, of the above. Details of calculation methodology for P2 and P3 are given in Ref.[33].

4.4.4 Failures of Some Reactor Components

4.4.4.1 Core Shroud Crack in BWR Plant

The reported cracks, predominantly in horizontal welds in core shroud, in overseas BWR plants during 1990-1995 necessitate, besides deterministic evaluation to ensure availability of adequate margin in structural integrity, PSA of core shroud having 360^0 circumferential through-wall crack undergoing displacement under dynamic effects, and possible decapitation of safety functions. The PIEs considered for dynamic effects are MSLB, recirculation line break or SSE.

The hazard (P1), i.e. frequency of failure and displacement, can be calculated from generic data and/or fracture mechanics approach and fault tree methodology considering propagation of circumferential cracks on the equipment welds, especially horizontal ones, to catastrophic failures and failure of other restraining features (like stabilizer pins) as provided in the design. The plant response; that is probability of safety significant SSCs getting affected consequent to such displacement (P2), should be evaluated with insights from thermal hydraulic analysis and expert judgement. The safety functions likely to get affected involve core cooling via normal and emergency spray injection modes, control rod insertion, and emergency poison injections for safe shutdown capability. The system unavailabilities (P3) and event sequences leading core damage probability (P) can be evaluated from ET modelling and Boolean reduction. The release consequence, if required, can be evaluated, as per Level 2 and Level 3 analyses using failure probabilities/frequencies for SSCs/PIEs.

4.4.4.2 End Shield Rupture in PHWR

Rupture of end shield due to embrittlement and crack propagating to catastrophic failures on continued operation in adverse environment, and loading (transient, accidental), may entail damage of lattice tubes housing coolant channel resulting into loss of inventory of end shield cooling water and LOCA. The hazard (P1) i.e., probability of such rupture and size of rupture need to be evaluated. The size of rupture can be defined from the extent of damage affecting a number of coolant channels and/or rate of inventory loss of end shield cooling system. The value of P1 may be estimated by considering a number of factors, which include FT methodology, existing crack configuration (size, orientation etc.), embrittled condition of end shield, and environmental condition and insights from fracture mechanics approach. The plant response and fragilities of components that rupture, would cause unacceptable damage to coolant channel and/or end shield cooling can be evaluated by system analysis and probability values can be assigned from fragility studies and its randomness, uncertainty along with expert judgement. The quantification of event sequences leading to core damage should be done by impacting increase in frequency of LOCA IE, loss of end shield cooling system inventory, any secondary effects of end shield rupture and operator recovery actions. The consequence (P) can be evaluated as per PSA Level 2 and Level 3 analyses.

4.4.4.3 Control Rod Housing Rupture

Damage to control rod housing/mechanism outside the core may lead to SBLOCA and possible control rod ejection in some PWR plant designs (e.g., KK project) The probability of such hazard (P1) can be evaluated using FT methodology and can be modified based on factors that include expert judgement. Bayesian approach, degradation mechanism, surveillance and fault detection techniques. This PIE, if not already considered in the existing PSA module, needs to be evaluated along with other PIEs to arrive at CDF and further source term and consequence to public domain. The contributions from this PIE and dominant contributors to the occurrence of such event and other plant risk contributors can be evaluated from MCSs obtained at the different stages in the analyses. The uncertainties associated with FT/ET modeling and quantification should be propagated to the top event probability.

4.4.5 Dropping of Shipping Flask in Spent Fuel Storage Bay (SFSB)

The hazard due to dropping of shipping flask weighing over 25 T into the SFSB involves possible pool liner failures and/or damage to the spent fuel stored in the racks of the storage bay, resulting release of radioactivity to outside environment through leakage paths. The probability of dropping shipping flask (P1) and its effect (strike) probability (P2) can be evaluated using FT methodology, considering various design features such as interlocks, fail safe mechanisms, operating procedures and possible human errors, and impacting failure rate based on plant experience and generic data as available. The damage or failure probability P3 should be evaluated individually both for the pool liner and spent fuel stored in the bay from users expert judgement, based on insights from structural analysis/probabilistic fracture mechanics. Probability of the consequence of release to the outside environment (P), should be evaluated by modelling various design features provided in the SFSB, leakage paths and possible operator actions to mitigate the situations, into the ETs, and integration of the quantifications of accident sequences leading to release.

4.4.6 Flooding from Internal Events

The treatment of flood in general has been highlighted in Appendix-XI. This part highlights only internal flooding caused as secondary effect by all PIEs, which result in a release of a liquid (usually water) consequent to leaks/breaks of pipes, vessels or tanks, as well as events which lead to actuation (spurious or desired) of a spray system (e.g. containment spray or fire extinguisher sprays). It also includes flooding caused by human error during maintenance. Flooding means not only water pools on the room floor but also collection of liquid in upper locations (e.g. spray or condensed steam collection in cable tray).

While evaluating hazard (P1), i.e., liquid level as a function of time and frequency of occurrence, possible blockage of drain, drainage system in the plant, cracks in floor, walls, etc. should be kept in view. While evaluating P2 and P3 for plant response and vulnerabilities and for event sequence, secondary effects by flooding such as electrical hazards, and possible pressure excursion when liquid comes in contact with hot object, where applicable, should be considered. Standard FT methodology can be used, assigning for events, plant specific/generic data supplemented by expert judgement. In consequence modelling, detecting systems, mitigating measures including OPECs and possible operation recovery actions should be considered and quantification can be done using PSA ET, Level 2 and 3 analyses. Uncertainties arising in different stages of estimation should be propagated to arrive mean and deviations for the top event probability.

4.5 Risk Based Regulatory Inspection

One important use of PSA insights is regulatory inspection of NPPs in operation and under construction. Regulatory inspection is an involved job, and is done with periodicity to get some first hand knowledge on the safety status of the plant. Therefore, it needs to be optimised with regard to resources of manpower, money and time. PSA can provide valuable insights as regards where efforts need to be concentrated on for optimised benefits. It starts with identifying critical components based on consideration of dominant accident sequences and risk importance measures, and review of analysis of risk based technical specifications on allowed outage time, surveillance test intervals and in-service inspections of SSCs, including computer based systems hardware and software. From these details, schedules of inspection are worked out, giving emphasis to items important to safety ,as per the risk categorisations, high, medium and low, and spending efforts in accordance with risk hierarchy.

4.6 Risk Based Backfitting / Plant Upgrades / Modifications [35]

Use of insights obtained from PSAs of operating NPPs for identifying potential safety modifications and supporting the selection, design, installation and licensing of plant upgrades, is perhaps one of the most important applications of PSA. If the results show that CDF or severe off-site release is largely dominated by a very limited number of accident sequences, effective backfits may be proposed to prevent or to mitigate these scenarios. Similarly, backfits may also be suggested if PSA results show that a plant does not meet recommended or established national or international PSG/PSCs. Proposed backfits may involve changes to system designs and installation of new hardware, changes to operational procedures, development of specific accident management procedures, or changes in operator training.

PSA can only be used to identify which safety improvements are most effective to reduce overall plant risk within the limitations of the PSA models and scope of analysis. However, final selection of the backfits may also take into consideration of deterministic design criteria, cost-benefit evaluations, and other factors including applicable codes/guides, regulatory requirements/new policies.

Deterministic analyses and a detailed Level 1 PSA (with internal and external events) are necessary pre-requisites for evaluation of proposed modifications. The analysts should be aware that the proposal of changes may also affect the risk in other operating modes, and, as a minimum, a qualitative analysis of the impact of the proposed changes on the risk associated to other modes of operation should also be performed. Sometimes proposed backfits that may not significantly contribute to CDF reduction may still be very effective to reduce the frequency of off-site releases. Considerations on the containment vulnerabilities are also important for this application in such cases. Hence, it would be useful for the scope of analysis to include at least a limited scope Level 2 PSA in such cases.

The first step in the evaluation of the proposed backfit or upgrade is a qualitative assessment of its impact on risk. Comparative evaluation of proposed backfits requires that the PSA results should realistically account for actual plant operating experience. To the extent possible, the PSA should use plant specific data. Since, the accumulated operating experience is often not sufficient to justify the use of only plant specific values for the majority of components and failure modes, the PSA should use a consistent method to combine plant specific experience and generic data. Decisions about proposed plant improvement options should be based on a thorough review of the PSA event sequences and examination of different measures of importance. Recommended improvement options should consider the inherent uncertainties in the PSA methods, models, and results. In some cases, additional analyses are necessary to refine the PSA results and, if possible, to reduce important sources of uncertainty before specific plant modifications are recommended.

4.7 Risk Based Operator Training [35]

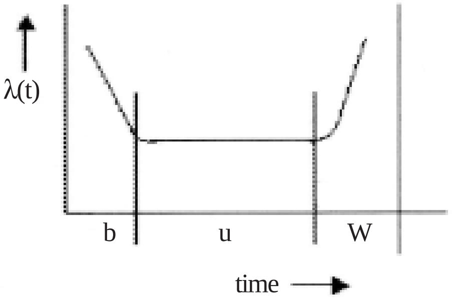
Operator training in any nuclear plant plays a key role in reducing the operator error probability. Operator training should be extensive and continuous. It should consist of a combination of classroom lectures, assignments, simulator exercises, training in emergency operating procedures (EOPs) and also in-plant actions to the extent possible and appropriate. Periodic testing of the operator capabilities for satisfactory performance, individually and also as a team, helps in improving operator performance.

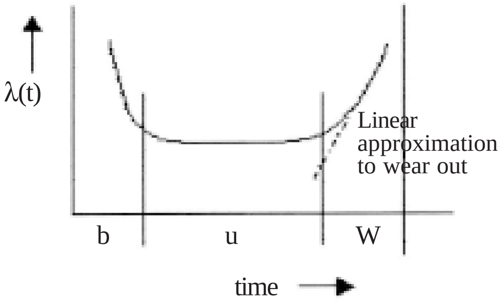
Level 1 PSA results highlight the significant contributors to core damage. Many of these contributors are human errors. Sometimes, the high probabilities for such human errors arise from deficiencies in training. This important insight can be used to help in selection of accident scenarios for training. Accident sequence frequency and risk significance of operator actions in terms of relative contribution to CDF can be used as selection guides. Similarly, the relative consequences of various operator errors and PSA results could be used to select those actions that would benefit from emphasised training. By performing sensitivity analyses, PSA analysts can determine how enhanced training can contribute towards reducing risk. PSA can be used to improve operator training for emergency conditions because it can help to select and rank the accident scenarios based on established criteria, such as accident sequence contribution to core damage, fractional contribution of human errors in the sequence, etc.

Both high frequency-low consequences and low frequency-high consequences are important considerations in risk assessment. Hence, operator training should include both sequences. For this reason, Level 2 PSA can be of great advantage because it provides information on consequences as well as on frequency. Level 2 PSA can be useful in understanding complexities and uncertainties of severe accident processes, containment response, consequences of failures of containment ESFs and identification of possible human recovery actions for operator training, expected plant specific responses and limitations of the instrumentation and protective systems in such circumstances. However, the impact of enhanced training programmes cannot be directly evaluated with PSA, if the analysis of operator errors does not include the impact of training as one of the PSFs considered in the quantification of HEPs.

4.8 Risk Based Ageing Management

Frequent failures of components increase plant risk by increasing component unavailability/failure frequency, increasing frequency of process system upsets including initiator and hence more plant risks such as increase in probability of core damage. Failures of components beyond their useful life are more than random failures on account of ageing. Fig. 4.6 [36] shows the familiar bathtub failure curve for components, related to power supply, control and instrumentation. Fig.4.7 [37] shows the failure rate curve for mechanical components; nature of failure rate is slightly different, not so flat, even during its useful life, and failure rate increasing significantly particularly in the later half. The useful life as specified by designer/vendor is affected by factors like operational transients, environmental conditions and maintenance and test schedules. History dockets, trend analyses are helpful in assessing whether ageing of a component is contributing to failure rate. This is the phase, management has to decide, whether to go for repair with more surveillance or replace the component. This is besides the consideration of obsolescence. PSA can provide valuable insights in this regard. It evaluates risk impact of ageing of components. It can be performed at a system level or CDF or release frequency level; more relevant being consideration of impact on CDF in Level 1 PSA. It models random failure with ageing induced failures derived from fracture mechanics approach and works out risk factors, i.e., combined (random plus ageing) risk importance measures, by sensitivity studies.





b - Burn in, u - Maturity or Useful life, W - Wear out

Figure 4.5 : Failure Rate Curve for Electronic Components

Figure 4.6 : Failure Rate Curve for Mechanical Components

The root cause of increase in failure rate can be any of an ageing phenomenon, fatigue or corrosion of components or systems. The other type of ageing phenomenon is a process that gradually degrades characterisation of the component, such that it no longer fulfils its design requirements. Examples include snubbers that lose their damping capacity with increase in fluid leakage through the seals, or heat exchangers losing heat transfer capacity as oxidation layers/scales are formed on the tubes/shell surfaces and reactor vessel losing pressure capacity as fluence and number of power transients increase threshold value. Determining risk significance of this degradation is more complex as it involves combining probabilistic load distribution with fragility curves and considering the impacts of the different failure modes. However, bounding calculations can be performed. Such an analytical approach is a developing field. Basic mathematical approach for determining risk sensitivity to component ageing is given by

$$\frac{dR}{dt} = \sum_j \frac{dR}{dq_j}\frac{dq}{dt} \tag{4.6}$$

where, $\frac{dq}{dt}$ = Rate of change of component j's unavailability q_j and R = Risk

Component unavailability is given by,

$$q_j = q_{oj} + (q_j - q_{oj}) \tag{4.7}$$

where q_{oj} = component unavailability with ageing contribution not included.

Rate of risk change due to ageing for ageing for all components in a plant is given by

$$\left(\frac{dR}{dt}\right)_A = \sum_j \frac{dR}{dq_j}\frac{d(q_j - q_{oj})}{dt} = \sum_j r_j \tag{4.8}$$

$$\left(\frac{dR}{dt}\right)_A = 0, \text{ where no ageing (i.e., } q_j = q_{oj}) \tag{4.9}$$

where $r = \frac{dR}{dq}\frac{d(q-q_0)}{dt}$ and q_0 being unavailability with no ageing (4.10)

The component ageing risk sensitivity contribution = (Risk importance of the components) X (the extra rate of change of component unavailabilities due to ageing) (4.11)

A specific formula is to be used for q and q_o to obtain specific expressions for component ageing risk sensitivity r at time (t). Unavailability (q) including ageing contribution, for a component is given by

$$q = 1 - \exp\left(-\int_o^t \lambda(t')dt'\right) \tag{4.12}$$

The expression for qo for random failures will be different depending on component modelling i.e. for irrepairable component.

$$q_0 = 1 - e^{-\lambda_0 t} \tag{4.13}$$

where λ(t') is the time dependency component failure rate with ageing and λ_0 is the constant failure rate assuming no ageing.

4.8.1 Simplified Methodology

A variety of time dependent component failure rate models exist for treating potential ageing effects, which include Weibull distribution, gamma distribution, truncated normal distribution etc. They require knowledge of detailed time to failure data, which cannot be retrieved from gross failure data. The linear ageing failure rate is the best time dependent failure rate that can be derived from gross data. The linear failure rate can be simply viewed as a straight line fit to the wear out portion of the curve (Fig. 4.6 and 4.7). Further the linear rate ageing model is suitable for modelling ageing mechanisms which cause a cumulative degradation in the component, so as to continually increase failure rate, and hence is applicable to such ageing processes as linear wear, linear material build-up and linear elastic related phenomena. It can also serve as a first order linear approximation, even where degradation build-up is not linear or independent of the previously accumulated damage, such as that due to vibration. The inaccuracies due to using the linear model will often be shadowed by the data uncertainties. The simplistic approach that can be followed in evaluating risk impact of ageing is as presented below.

It involves calculating appropriate risk of components having significant impact on plant risk, i.e., importance measures from usual PSA and combining them with ageing effects determined from ageing models to determine the CDF impacts of ageing. The methodology permits detailed models of testing and maintenance to be incorporated, thus allowing ageing evaluations, the risk effectiveness of maintenance programmes and ageing management programme and to prioritise the task in ageing management.

Basic formulae are given below and sensitivity study of risk impact of ageing of NPP, is illustrated in tables subsequently.

The failure rate, λ(t) as a function of time (or number of cycles) is expressed as $\lambda(t) = \lambda_0 + at$

where λ_0 = constant failure rate (random) contribution and a = appropriate component ageing rate [37].

NUREG/CR-4769 describes the basis for the linear ageing model and its applicability. The ageing rate values are obtained from expert opinion and checked with certain plant data. NUREG-1362 [38] describes the data used. The unavailability increase, Δq due to ageing [59] of a component is given by:

$$\Delta q = \frac{1}{4}a(L-T)T + \frac{1}{6}aT^2 \tag{4.14}$$

Where L= Replacement interval (MTBF) and T= Surveillance test interval

The CDF increase (ΔC) due to ageing can be expressed as sum of contribution term from successively higher order of ageing interactions [39].

$$\Delta c = \Sigma\, S_i\, \Delta q_i + \Sigma\,\Sigma\, S_{i\,j}\, \Delta q_i\, \Delta q_j + \ldots\ldots\ldots + \Sigma\,\Sigma \ldots\ldots \Sigma\, (S_{ij}\, i_2 \ldots i_m)\, \Delta q_{i1}\, \Delta q_{i2} \ldots\ldots \Delta q_{im} \ldots \qquad (4.15)$$

Where $i_1 > i_2 > \ldots . > i_m$

S_i = CDF importance of component i, identified to be having significant effect on plant risk

S_{ij} = CDF joint importance of components i and j

$S_{i1\ i2\ldots im}$ CDF joint importance of components $_{i1\ i2\ldots im}$

Δq_i = Ageing effect in component i

$\Delta q_i\ \Delta q_j$ = Product of ageing effects in components i and j

S_i, S_{ij} …..etc. can be computed from presently available PSAs (considering random failure) which do not include ageing effects. Then, the ageing effects Δq_i can be calculated from the separate ageing model stated above. The risk importance factors, S_i, S_{ij} …..etc. thus need to be calculated once from reference PSA. As different ageing effects or different maintenance programmes are evaluated for their effectiveness in controlling ageing, only the ageing effects Δq_i need to be changed and substituted in Δq_i (4.15) to determine the resulting CDF changes, Δc.

The specific additional risk based ageing related maintenance activity involves carrying out scheduled overhauls at given intervals and carrying out improved surveillance tests on the risk dominant ageing contributors. The illustrations (given in Annexure-XIII) show that ageing can have large CDF impacts, but these can be controlled effectively by introducing additional ageing management activities for the risk dominant contributors.

4.9 Accident Management

Accident Management is essentially accident prevention and mitigation of their consequences. The objectives of the accident management are to prevent or minimise core damage, to maintain the integrity or delay the failure of the RCS, to maintain the integrity or delay the failure of the containment and to mitigate the release of radioactive material [41]. The full scope PSA can support the development, of strategies to deal with the identified vulnerabilities, and of calculational aids that would be used to assist in the selection and application of the strategies. Here, only the severe accident management is addressed. These measures include reliable prevention and/or mitigation of containment threatening phenomena, so that dose to the public is minimised and/or emergency measures can be taken for public safety. Three source terms have been identified accounting to the delay in containment failure and fission product retention capability of the release pathway [40].

- S1 corresponding to early containment failure and a direct pathway.
- S2 corresponding to delayed (24 h) containment failure and a direct pathway.
- S3 corresponding to delayed release through pathways that provide retention of radionuclide.

Containment function can be improved by accident management procedures like

(a) monitoring containment integrity and making effort to restore the containment function, if degraded, by complementary action,

(b) prevention of an early basement leakage by drain filling, and

(c) implementation of a containment filtered venting system (e.g., PCCD)

From the point of view of emergency plans (e.g. evacuation in 5 km range and confinement in a 10 km range) a delay between 12 to 24 h is compatible only with a S_3 source term. Three types of management strategies can be employed to limit the consequences to the level compatible with emergency plan measures for public protection.

(1) Prevention of accident sequence leading to S1, by eliminating risk of hydrogen combustion, steam explosion and direct containment heating.

(2) Reduce S2 source term below S3 level by,

- taking corrective measures against containment breach,
- reducing containment failures by over-pressurisation beyond design limit pressure, and
- eliminating basement ablation by molten core concrete interaction.

(3) Implementation of the national crisis management organisation and elaboration of severe accident guides for crisis management teams, in order to manage the core damage situation with a priority oriented to the containment function protection.

Accident management strategies associated with timing of containment failure (S1 or S2/S3) are as follows.

4.9.1 Early Containment Failure

(a) Hydrogen risk management

As soon as severe accident is initiated, hydrogen production is unavoidable. To prevent unacceptable consequences from hydrogen combustion, either one can increase the volume of containment or inertise the containment atmosphere or use hydrogen passive auto catalytic recombiners (PAR) or igniters in such a way that explosion is impossible or any possible explosion would not threaten the containment.

(b) High pressure core melt risk management

Core melt relocated in the lower head can lead to vessel melt through. If pressure is high before melt through, a high pressure melt ejection in reactor cavity can lead to transfer of fragmented molten mass into the containment. Associated heat transfer in the containment atmosphere could lead to high pressure peak beyond the containment integrity pressure limit. Further, in most of the high pressure core melt situations, secondary side of steam generators (SG) is empty of water. This can lead to SG tube creep rupture and subsequently to containment bypass. For high pressure core melt situation, the following accident management is envisaged.

In most of the situations, the fuel bundles fail. So, in the early stage of the accident, the operator is to inject cold water appropriately, so as to avoid the core melt.

(c) Steam explosion risk management

In-vessel steam explosion risk is studied in PSA Level 2. Ex-vessel steam explosion or potential loads resulting from melt pouring in a flooded reactor cavity/vault are also considered. However, feasibility and efficacy of flooding reactor vessel/cavity, during melt progression in severe accident situations, for in-vessel/ex-vessel core melt cooling need to be evaluated as accident management measures, to prevent further core disruption or corium formation and propagation.

4.9.2 Long Term Containment Failure Risk

The prevention of high pressure melt ejection risk is considered for management of in-vessel to ex-vessel accident progression. But there are no specific measures to manage ex-vessel corium progression. However, in order to mitigate potential consequences of sub-soil contamination in case of basemat ablation, short and long-term isolation of reactor subsoil is envisaged to prevent contamination of underground water. Provisions for in-vessel/ex-vessel needs to be made to prevent core-melt progression reaching to basement. Concerning source term evaluation, two topics are important: (i) Kinetics of basemat ablation for long term and (ii) iodine behaviour in the primary circuit and containment. For S3 source term evaluation, corium concrete interaction assessment is important. Calculations indicate large discrepancies concerning properties and rate of the time of basemat melt through. Regarding iodine source term, studies show that large fractions of gaseous iodine exist in hot leg of the circuit. Due to sump radiolysis, iodine production is only low and in the long term, organic iodides released from the painted surfaces in the gas phase would dominate the volatile iodine fraction.

4.10 Risk Based In-Service Inspection (RB-ISI)

4.10.1 Introduction

In-Service Inspection (ISI) ensures reliable functioning of components important to safety. Current ISI programmes are based on past experience and engineering judgement with deterministic approach. Service experience has indicated that failures are dominated by corrosion or fatigue mechanisms and typically occur in areas, which might not have been included in ISI programs. Risk based ISI (RB-ISI) approach provides insights into the contribution of components to plant risk for a certain ISI programme. It also provides insights into the optimal use of scarce resources for ISI, i.e. less inspection/testing towards low risk significant components, and focussing more attention on components having high risk [41,42,43,44,49].

The RB-ISI evaluates risk with the insights from component degradation mechanism and establishes an effective plant integrity management programme, which maintains plant safety, while at the same time reducing the burden associated with existing ISI requirements. It also reduces man-rem exposure and achieves economic benefits.

4.10.2 Current Inspection Categorisation Philosophy

Current ISI philosophy considers the determination of inspection areas and the degree of inspection by taking into account the safety margins and magnitude and type of failure. Inspection categories are function of size of failure, stress ratio and fatigue usage factor [45]. The size of failure is expressed as the ratio (RE) of the maximum energy release rate from the failure being considered, to maximum energy release rate from the most severe failure considered during design of the system, that directly transports heat from the nuclear fuel. This ratio is denoted by RE. The failures are categorised as large, medium and small depending on calculated value of RE.

$RE < 0.1$ ————————>	Small
$0.1 < RE < 0.3$ ——————>	Medium
$RE > 0.3$ ————————>	Large

Fatigue usage factors shall be determined by the rules given in ASME BPVC Section III. Stress Ratio is defined as the ratio of calculated stress to allowable stress as per PHWR practices (CANDU standard). The criteria for developing inspection programmes are derived from stress ratio and fatigue usage factor matrix. According to the above criteria, four categories are defined viz. A, B, C1 and C2 signifying decreasing order of severity. Table 4.2 and 4.3 represent four categories for the matrices of fatigue usage factor and stress ratio for medium and large size failures respectively. Depending on the category in which each component falls, the inspection method, quantum of inspection and interval are determined. Regarding inspection interval, first inspection will be carried within first 5 years of reactor operation and subsequent inspections are to be done for time intervals that do not exceed 1/3 of the design operational life of the plant or 10 years, whichever is less.

TABLE 4.1 : DETERMINATION OF CATEGORY FOR MEDIUM FAILURE SIZE

		FATIGUE USAGE FACTOR		
		0.01 **(Low)**	**0.1** **(Medium)**	**1.0** **(High)**
STRESS RATIO	**High** (1-2/3)	C1	B	A
	Medium (2/3-1/3)	C1	B	B
	Low (1/3-0)	C2	C1	C1

TABLE 4.2 : DETERMINATION OF CATEGORY FOR LARGE FAILURE SIZE

		FATIGUE USAGE FACTOR		
		0.01 **(Low)**	**0.1** **(Medium)**	**1.0** **(High)**
STRESS RATIO	**High** (1-2/3)	B	A	A
	Medium (2/3-1/3)	C1	B	A
	Low (1/3-0)	C2	C1	C1

4.10.3 Methodology of RB-ISI

The whole RB-ISI process can be summarised in the following steps [47,48,50,51].

(1) Determine the scope

Identify the SSCs to be included so as to adequately reflect the risk implication of component failure.

(2) Develop PSA model

Leaks and breaks are modelled as initiators in PSA. A detailed modelling of plant system and event sequence modelling are required in order to identify contributors having a significant impact on plant risk.

(3) Develop component details

Distinct component boundaries should be identified at branching points or size changes where a significant difference in consequence or failure probability occurs, or the break probability is expected to be markedly different due to environment or other factors.

(4) Determine initiatiors of component failures

This involves the identification of initiators of a component failure and identifying the effects on mitigating systems.

(5) Assess component failure potential

Estimate the failure potential of each component, its failure mechanism, degradation mechanism and ageing effects, which have to be used in PSA calculation for final CDF value.

(6) Assess consequence, for failure of each component

Effect of failure of each component should be analysed.

(7) Categorise components and select component locations for inspection

Prioritising components for determining an effective inspection program that maintains the component failure probabilities below the target values.

(8) Assess change in risk (e.g. CDF, Source Term)

Generally risk impact is analysed at CDF level; where containment related contributors are to be addressed for ISI programme, effect on release frequencies is to be assessed. However, most of the components in ISI programme relate to Level-1 analysis, and this section will generally be devoted to this application. The methodology can be extended to cover containment related components.

4.10.3.1 Risk Categorisation Based on Importance Measures

A new parameter called inspection importance measure has been developed, in order to prioritise the systems for ISI, viz. a system level ranking based on inspection importance measure (I^w). Inspection importance (I^W) of a component is defined as the product of the birnbaum importance (I^B) times the failure probability [43].

$$I^W_{sys} \;=\; I^B_{sys} \;*\; P_{f_{sys}} \tag{4.16}$$

$P_{f_{sys}}$ = System failure probability due to structural integrity failures

The inspection importance is an approximation of the Fussel-Vesely (FV) importance of pipe break for the system and has all the useful properties of the Fussel-Vesely importance measure for establishing the inspection priorities.

Birnbaum and Fussell-Vesely importance measures have been suggested by ASME for risk informed in-service inspection. In most of the applications, the exact ranking is not important. Guidance and experience for applying importance measures for in-service testing/in-service inspection is mainly based on expert opinion. A sample categorisation is given below, where RAW refers to risk achievement worth [6].

Risk Category	Criterion
High	FV > 0.001
Potentially high	FV < 0.001 and RAW > 2
Low	FV < 0.001 and RAW < 2

These categorisation can however be only applied to safety system components. In order to overcome this limitation, another importance measure called Differential Importance Measure (DIM) has been suggested [44],

$$DIM_{x_i} \;=\; \frac{\delta CDF_{x_i}}{\delta CDF} \tag{4.17}$$

$$\delta CDF_{x_i} \;=\; CDF\left(x_i + \delta x_i\right) \;-\; CDF_0$$

$$\delta CDF \;=\; \sum_i \delta\, CDF_i$$

which can be applied to components in process as well as safety system. Differential importance measure (DIM) can be defined as the fraction of total change in risk or core damage frequency that is due to a change in parameter x_i.

4.10.3.2 Risk Categorisation Based on Risk Matrix

Risk based decision regarding ISI, involves determining the inspection programme based on risk information with inputs from deterministic insights. As a first step it is required to estimate likelihood failure frequency/failure probability of components (e.g. failure rate, unavailability)[50,51]. The estimation of likelihood failure frequency/failure probability of the component can be done broadly through three approaches; statistical analysis, structural reliability analysis and expert elicitation. Statistical analysis involves rigorous data collection programme and analysis of collected data. Structural reliability analysis is based on fracture mechanics methods. Various codes like PRAISE, PIFRAP, etc. are available for estimation of likelihood failure frequency/failure probability from the structural reliability analysis. From experience, it has been found that likelihood frequency is influenced by the degradation mechanism prevailing on the component. Electrical power research institute (EPRI) has adopted likelihood failure frequency and degradation mechanism information as the deterministic criteria [44].

The risk information provides an estimate of consequence of failure of a component using PSA models. Consequence can be quantified through the estimation of conditional core damage probability (CCDP). The risk from failure of a component on failure of a specific joint i (e.g. a particular weld) is expressed in terms of $CCDP_i$. The consequence evaluation group is organised into two basic impact groups; (i) initiating event and (ii) loss of mitigating ability.

In IE impact group, the event occurs when a pressure boundary failure occurs in an operating system. This could occur as a result of loss of fluid in a frontline system (LOCA, feed water line break), or in support system (like service water cooling). The importance of every initiating event, caused by a component failure, needs to be assessed in order to assign it to its appropriate consequence category. The $CCDP_i$ for a component failure from 'i'th joint, can be directly obtained from the PSA results, by dividing the CDF due to the specific IE by the frequency of that IE.

In the loss of mitigating ability group, the event involves the component failures in safety system. Safety system can be in two configurations, standby and demand. While in standby configuration, the failure may not result in an unsafe situation, but degrades the mitigating capabilities. After failure is discovered, the plant enters into the configuration of AOT, i.e., the time available for component to be restored to service or to effect plant shutdown otherwise for safety considerations. In consequence (risk) evaluation, AOT is referred to as exposure time.

$$CCDP_i = [CDF_{(qi = 1)} - CDF_{(BASE)}] * T_E \qquad (4.18)$$

Where, $CDF_{(qi = 1)}$ = CDF given the component failure from joint i

$CDF_{(BASE)}$ = Base or reference CDF

q_i = Component failure/unavailability due to failure from joint i.

T_E = Exposure time (detection time + AOT)

While in demand configuration, the failure occurs when the system/train operation is required in an actual demand. Here, instead of exposure time, mean time between the tests/ inspection intervals or demands is to be considered. The expression can be written as

$$CCDP_i = [CDF_{(qi = 1)} - CDF_{(BASE)}] * T_t \qquad (4.19)$$

Where, $CDF_{(qi = 1)}$ = CDF, given the component failure due to joint i

$CDF_{(BASE)}$ = Base or reference CDF

q_i = Component failure unavailability due to failure of joint 'i'

T_t = Mean time between tests or demands

Risk matrix is designed with different categories, depending on the risk (change in CDF) values and degradation mechanism for determining the inspection interval. Risk matrix is defined as the decision matrix that is used to categorise the components based on degradation mechanism and consequence of its failure (Table-4.3). From international experience [46], a basis has been established for ranking component rupture potential as high, medium or low, simply by understanding the type of degradation mechanism present (Table-4.4).

Each component is assigned the appropriate category depending on its ΔCDF and degradation mechanism and seven categories of inspection programme strategy are developed. This inspection programme will include prioritisation of components for inspection, inspection interval, method of inspection and scope/volume of inspection.

If a component falls in risk category 1, 3 or 5, it has to be inspected under existing flow accelerated corrosion (FAC) programme since the failure frequency may be dominated by FAC degradation mechanism. Similarly, if a component falls in risk category 2 or 5, it has to be inspected under existing inter granular stress corrosion cracking (IGSCC) programme since the failure frequency may be dominated by IGSCC degradation mechanism. For the risk category 4, there may not be any prominent degradation mechanism, but consequence wise it requires attention. Risk categories 6 and 7 may not be falling under any inspection programme, and no volumetric or surface examinations are required. Irrespective of risk categories, all components should be pressure or leak tested.

TABLE 4.3 : RISK MATRIX [51]

	Consequence Category (CCDP)			
Likelihood frequency of component failure due to 'i'th joint failure	**None** **$<10^{-8}$**	**Low** **10^{-8}<CCDP<10^{-6}**	**Medium** **10^{-6}<CCDP<10^{-4}**	**High** **$>10^{-4}$**
High ($>10^{-4}$)	Low 7	Medium 5	High 3	High 1
Medium (10^{-7}<CCDP<10^{-4})	Low 7	Low 6	Medium 5	High 2
Low (10^{-7})	Low 7	Low 7	Low 6	Medium 4

TABLE 4.4 : CLASSIFICATION OF DEGRADATION MECHANISM

Component failure potential (F)	**Degradation Mechanism**
High($>10^{-4}$)	Flow accelerated corrosion, vibration fatigue, water hammer
Medium (10^{-7}<F<10^{-4})	Thermal fatigue, corrosion fatigue, stress corrosion cracking, pitting, erosion cavitation
Low($<10^{-7}$)	No significant degradation mechanism (Component failure could be due to other causes e.g. over pressurisation)

4.10.3.3 Evaluation of Risk Impact for ISI Strategy

ISI strategy includes inspection interval, method of inspection and extent/volume of inspection. In order to evaluate the impact of risk from changes in in-service inspection interval, the change in CDF from both the inspection programmes has been used as a risk measure. The model described in equation 4.20 is based on the influence of component failure frequency at a location j due to the inspection program. The change in the core damage frequency at location j, that is impacted by the changes in inspection program can be estimated as.

$$\Delta CDF_j = (F_{rj} - F_{ej}) * CCDP_j = (I_{rj} - I_{ej}) * F_{0j} * CCDP_j \quad (4.20)$$

Where, $F_{Aj} = F_{0j} I_{Aj}$ (4.21)

F denotes failure frequency of component from failure of joint at j location.

I refers to effectiveness of inspection methodology

$CCDP_j$ = Conditional core damage probability from component rupture at location j

The subscripts "rj" refers to proposed strategy (with risk informed approach) and "ej" refer to existing strategy.

The subscripts "Aj" refers to any inspection strategy A for location j

F_{Aj} = Frequency of component failure at location j subject to inspection strategy A

F_{0j} = Frequency of component failure at location j subject to no inspection

I_{Aj} = Inspection effectiveness factor (between 0 and 1)

This is the probability that the flaw is detected. It can be derived from the inspection effectiveness curve developed from various data collected from experience and tests for different inspection methodologies like visual, ultrasonic, radiography, etc.. It is also assumed that flaws detected by inspection methodologies will be attended to by necessary corrective actions before returning to service and that would in turn effectively reduce the probability of failure (initiated by the failure at the location, under consideration)

After the estimation of risk impact (ΔCDF), depending on the acceptable target criteria for ΔCDF, the decision shall be made regarding the adoption of inspection strategy. (The decision criteria suggested by EPRI is to ensure that the cumulative change in CDF is less than 1E-7/yr/system for the employment of the new methodology).

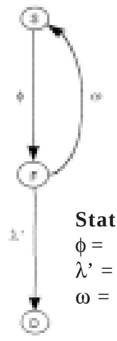
The frequency of a failure of a component subjected to no inspection or contemplated after a long time during plant operation can be evaluated from generic data or from software developed and validated for similar plant and/or with expert judgement. The probability of a flaw below detectable range of inspection/ test instrument growing to a critical size and resulting into catastrophic failure before detection (or with no online leak detection instrumentation, ISI programme) can be estimated using fracture mechanics approach. The uncertainties arise in the different stages of analyses, and besides random failures, use of risk matrices for potential failure frequency vs degradation mechanism, development of inspection strategy based on risk matrix categorisation, assigning inspection effectiveness factor and arriving at failure frequency from statistical data and with fracture mechanics insights, also need to be quantified and propagated to the final output for refinement and assuring high confidence level, in the assessment.

4.10.3.4 Incorporating ISI Changes in Failure Probability Calculations

The objective of Markov modelling approach is to explicitly model the interactions between degradation mechanisms and the inspection, detection, and repair strategies that can reduce the probability that failure occurs or the failure will progress to rupture. This Markov modelling technique starts with a representation of "piping segment" in a set of discrete and mutually exclusive states. At any instant of time, the system is permitted to change state in accordance with whatever competing processes are appropriate for that plant state. In this application of Markov model the state refers to various degrees of piping system degradation or repairs, i.e., the existence of flaws, leaks, or ruptures [55]. The processes that can create a state change are failure mechanisms operating on the pipe and process of inspecting or detecting flaws and leaks, and repair of damage prior to progression of failure mechanism to rupture.

(a) Three state Markov model

This model would be applied to a pipe element such as a weld or small section of pipe that is uniquely defined in terms of the presence or absence of degradation mechanisms, loading conditions, and status in the inspection program. The model in Fig. 4.7 is developed to examine the singular role of the in-service inspection program, which can influence the total failure rate of pipe segments but has little if any impact on the conditional probability that a failure will be a rupture. A limitation of this model is that it does not distinguish between leaks and ruptures, cannot model leak before break, and cannot be used to examine the role of leak detection as a means to reduce pipe rupture frequencies. Another limitation is that leaks and ruptures are only permitted once the system is in the flaw state. This limitation makes the model suitable for degradation type failure mechanisms, but not for severe loading condition related causes, such as vibration fatigue or water hammer. These limitations are removed in the next section in which a four state model is developed and more possibilities are introduced for leaks and rupture transitions from the success state. However, to build up the knowledge about pipe reliability modeling in a step by step fashion, it has been found instructive to analyse this more simplified model to understand some basic properties of this approach to reliability modelling such that the necessary details can be built up in an organised fashion.



Piping System States

S = Success
F = Flaw
D = Degraded
(Leak or Rupture)

State Transitions

φ = Occurrence of Flaw
λ' = Occurrence of Leak or Rupture
ω = Inspect and Repair Flaw

FIGURE 4.7 : THREE STATE MARKOV MODEL

ω is the Markov model that accounts for the inspection process and can be further defined according to the following model.

$$\omega = \frac{P_I P_{FD}}{(T_{FI} + T_R)} \tag{4.22}$$

where: P_I = probability that a piping element with a flaw will be inspected per inspection interval.

P_{FD} = probability that a flaw will be detected given this segment is inspected. This term is often referred to as the 'probability of detection' or POD.

T_{FI} = mean time between inspections for flaws, (inspection interval)

T_R = mean time to repair once detected.

(b) Four state Markov model

This model consists of four states of pipe segment reflecting the progressive stage of pipe failure mechanism; the state with no flaw, development of flaws or detectable damage, the occurrence of leaks and occurrence of pipe ruptures. As seen from this model (Fig. 4.8) pipe leaks and ruptures are permitted to occur directly from the flaw or leak state. The model accounts for state dependent failure and rupture processes and two repair processes. Once a flaw occurs, there is an opportunity for inspection and repair to account for in-service inspection program that search for signs of degradation prior to the occurrence of pipe failures. Here the leak stage L does not indicate actual leak, but represents a stage in which pipe wall thickness is in a slightly reduced state.

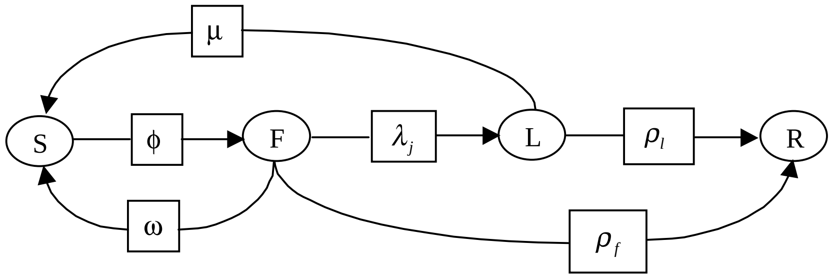


FIGURE 4.8 : MARKOV MODEL FOR PIPE ELEMENTS WITH IN-SERVICE INSPECTION AND LEAK DETECTION

S = Success; F = Flaw; L = Leak stage; R = Rupture

Another parameter is introduced in four state Markov model to represent the leak repair.

Repair rate $\mu = P_{LD} / (T_I + T_R)$ (4.23)

P_{LD} = probability that leak in the element will be detected per detection period.

Mainly the rupture state is defined as failed state. Accordingly the component failure probability is defined as the probability of finding the system in that state. This failure probability will be used is our PSA models for risk informed in-service inspection.

4.11 Sabotage

Sabotage (Nuclear) is any deliberate act directed against a nuclear facility, nuclear transport cask or nuclear material and associated fission products, which could directly or indirectly endanger the health and safety of the worker, the public, and the environment by exposure to radiation [56]. Specific acts of sabotage include: vehicle bombs, deliberate aircraft crash against containment, explosive attacks against a reactor core, cooling system, and shutdown, diversionary arson, kidnapping or murder of critical personnel, etc. Sabotage may be classified into three general categories viz.: radiological, operational, and personnel.

4.11.1 Primary Targets and Threat Objectives

For radiological sabotage, the target at an NPP includes fresh fuel, the reactor core, and spent fuel. The threat objectives in attacking this target include irradiating people and contamination of the site and the environment. Sabotage against personnel would include as targets critical NPP personnel, such as the plant manager or the control room operators, other plant personnel, and any other people who may be on the site. Attacks against personnel targets have the objectives both of causing fatalities and of impacting plant operations. For operational sabotage, the target would be any equipment that would impact power production, or risk to the operations of the plant.

4.11.2 Physical Protection System Design and the Relationship to Risk

To prevent sabotage, plant physical protection system should be analysed to be adequately reliable. The analysis of a physical protection system includes the determination of the physical protection system objectives, characterising the design of the physical protection system, the evaluation of the design, and possibly, a redesign or refinement of the system. The process must begin by gathering information about the facility, defining the threat and then identifying targets. Determination of whether or not the assets are attractive targets is based mainly on the ease or difficulty of acquisition and desirability of the material. The next step is to characterise the design of the physical protection system by determining the elements of detection, delay, and response. The physical protection system is then analysed and evaluated to ensure it meets the physical protection objectives. Evaluation must allow for features working together to assure protection rather than regarding each feature separately.

The basic premise of the methodology described here is that the design and analysis of physical protection must be done from a systems standpoint. In this way, all components of detection, delay, and response can be properly weighted according to their contribution to the physical protection system (PPS) as a whole. Without a methodical, defined, analytical assessment, the PPS might waste valuable resources on unnecessary protection or, worse yet, fail to provide adequate protection at critical points of the facility. Due to the complexity of protection systems, an evaluation usually requires computer modelling techniques. If any vulnerabilities are found, the initial system must be redesigned to correct the vulnerabilities and a re-evaluation conducted. Then the system overall risk should be calculated. This risk is normalised to the consequence severity if the adversary could attain the target. The facility is then able to make a judgement as to the amount of risk that exists and if this is acceptable.

The risk approach to physical protection system should attempt to work out the probability of interruption (PI) of the defined adversary along the most vulnerable path in the facility. This PI should be acceptable.

However, a question may be addressed as regards how much risk the facility is willing to accept versus the cost of reducing risk. If the facility and regulators understand that there are a limited amount of resources to be applied to physical protection of everything at the facility, then each application of a portion of those resources must be carefully and analytically evaluated to ensure a balanced risk. This section briefly explains the method of risk identification and mitigation [Sandia National Laboratories]. The risk equation used is:

$$R = P_A * [1 - (P_I)] * C \tag{4.24}$$

where the terms are as follows:

R = Risk to the facility of an adversary gaining access to, or stealing, critical assets. Range is 0 to 1.0, with 0 being no risk and 1.0 being maximum risk.

P_A = Probability of an adversary attack. This may be difficult to determine, but generally there are records available to assist in this effort. The value of this probability is from 0 (no chance at all of an attack) to 1.0 (certainty of attack). Usually in the calculation of risk, we assume $P_A = 1.0$, which means that it is a 'conditional risk' calculated given that that an attack on a facility will occur.

P_I = Probability of interruption. This is the probability that the defined adversary will be interrupted by the response force in time to stop the adversary from accomplishing their objectives. The principle of timely detection is used in calculating this probability from 0 (the adversary will definitely be successful) to 1.0 (the adversary will definitely be interrupted in their path).

C = Consequence value. This has a value from 0 to 1 that relates to the severity of the occurrence of the event. This is the normalising factor, which allows the conditional risk value to be compared to all other risks across the site. A consequence table (Table 4.5) of all events could be created which would cover the spectrum of loss, from highest to lowest. Therefore, by using this consequence table, the risk can be normalised over all possible events. Then the limited PPS resources can be appropriately allocated to ensure that the risk is acceptable across the spectrum.

If we assume that P_A is equal to 1 (there will be an attack), this term drops out of the equation. If we then also assume that C is equal to 1, that is, the consequence is the highest we can imagine, this term also drops out. This leaves a conditional risk, R, that is determined solely by the effectiveness of the PPS, which can be useful in establishing the 'worst case' risk i.e. an attack by the most capable adversary on the most valuable target. It is then possible to go back and use different consequence values to determine the risk to the enterprise for lower consequence losses. This will allow a prioritisation of targets and appropriate protection. Finally, the probability of attack may also be varied, based on available data where possible, and a realistic assessment of risk can be obtained. This three-step process can help in simplifying the complexity of the risk assessment by varying only one term at a time, allowing an appreciation about the influence of each factor on the outcome.

TABLE 4.5 : RADIOLOGICAL AND TOXICOLOGICAL SABOTAGE CONSEQUENCE VALUES

Consequence Impact of Effects on the public, Employees, and the Environment	Value from acts of radiological or toxicological sabotage
Catastrophic on-site and off-site fatalities and injuries, long term denial of facility (> 2 years) due to damage or radiation contamination, and off-site denial of food, water, or habitat due to contamination for more than 1 year	1.0
High off-site injuries and on-site fatalities and injuries, on-site facility denial for 1-2 years, and off-site denial of food, water, or habitat due to contamination for less than 1 year.	0.8
Moderate on-site injury (no off-site injury), on-site facility denial for 6 months to 1 year, and denial of food, water, or habitat due to contamination for less than 6 months.	0.5
Low on-site injury, on-site facility denial for less than 1 month, and no impact on food, water supply or habitat.	0.2

Once the risk value is determined, the security manager can justify the expenditure of funds based on a scientific, measurable and prioritised analysis. This information can be presented to executive management of the corporation or facility to demonstrate how the security risk is being mitigated and how much risk exposure remains. The analysis can then form the basis for a discussion on how much security risk can be tolerated or how much to increase or decrease the budget based on risk. This analysis can also serve to demonstrate to any regulatory agencies that a careful review of the security of the facility has been performed and that reasonable measures are in place to protect people and assets. The analysis will allow the facility to state the assumptions that were made (threat, targets, risk level), show the system design, and provide an analysis to show system effectiveness.

4.11.3 Analysis

The DEPO [56] process is used with the Graded safeguards table to evaluate risk. In general, the DEPO process or any similar methodology is satisfactory for analysing the physical protection system at a NPP. There are many path models available, such as EASI and SAVI in the United States, and EVA in France, for use in the analysis process. These path models are used to construct adversary sequence diagrams, which predict the most vulnerable pathways into a facility, the detection probability, and the time for an adversary to access the target. The analysis is usually stopped when the saboteurs reach the target, and denial is the response force strategy. As an enhancement to the usual analysis, NPPs might consider including reactor safety and accident prevention experts in the process. Considering the proposed new target types and sabotage categories, their input could be invaluable in identifying new ‘vital’ areas. In addition, it should always be borne in mind that any human error, equipment malfunction, or procedure that could result in problems for the NPP might also be used by a saboteur.

4.11.4 PSA to Physical Security Management [57]

Physical security at a NPP must address a broad spectrum of potential incidents, ranging from minor intrusions to radiological sabotage. A process must be developed that uses risk information contained in its PSA to modify the physical security plan. The risk information contained in PSA is used to focus the contingency plan and thereby support an efficient use of risk security resources [58]. The safeguard contingency plan contains a predetermined set of decisions and actions to arrest a potential saboteur and assigns decisions and actions to specific security personnel. Fulfilment of this plan also determines the number of security personnel required to protect the plant.

By using the risk information developed for PSA, a list is generated of sets of critical equipment, whose successful defense would prevent core damage and hence radiological sabotage. This list can be used to prioritise the allocation of guards to critical locations within the plant. The risk information can also be used to list sets of equipment whose concurrent destruction would cause core damage. Finally, these sets can be used to develop scenarios for training the security force.

4.12 Aircraft Crash [59,60]

Prevention of possible catastrophic effects as a result of aircraft falling down on the NPP, requires certain protection measures to be built in the plant. As these measures may be extremely expensive it is necessary to ensure that the protection measures taken are optimal and adequate for the real danger, which could be expressed in terms of probabilities of the external destructive impacts (risks). In order to protect important and potentially dangerous ground objects against the accidental aircraft impacts, special air traffic zones could be imposed where the aircraft flights are forbidden or restricted. This measure reduces probability of the accidents caused by the aircraft impact onto the objects but it does not eliminate it completely. Therefore, it is necessary to assess the probability of external hazard of aircraft impact to assure adequate protective measures engineered for the NPPs. Air traffic can be characterised by the average distance from NPP, altitude, airplane velocity, fuel storage capacity of aircrafts in flight, and number of flights, angles of flight of the aircraft and the standard deviation of these parameters.

4.12.1 Risk Identification

The analysis of flight safety statistics revealed the following types of aircraft accidents, which could be hazardous for ground objects.

(i) Airplane destruction and fragmentation during its flight at safe altitude.

(ii) Loss of controllability and inability to continue the flight along the route at safe altitude.

(iii) Loss of space orientation under conditions of low visibility.

(iv) Aircraft direct impact and fire consequence in its flight at unsafe altitude.

(v) Aircraft impact, fragmentation and fire during take-off and landing.

The hazard listed under (iv) could be due to extremely low probability gross error of pilot or more probable by sabotage/terrorist suicidal actions, probability of latter type could be assigned by expert judgement based on existing political situation. The last type of accident occurrence (listed under v) probability is ruled out (P1 = 0), based on siting criteria for NPP, viz., by screening distance value (SDV)-typical value being 10 km and/or screening probability level (SPL)-typical value being less than 10^{-06}/R-y aircraft crashing probability, on an area of 10,000 m^2 anywhere in the country. However, if due to changing circumstances such as political, military and international airport authority regulations, the NPP happens to come to be within the zone of take-off/landing, this probability of occurrence need to be accounted for.

4.12.2 Hazard Analysis

The probability of an event with an aircraft falling onto the NPP as a result of an aircraft accident (hazard) for the above first three types is determined as

$$P_{12} = \sum_{i}^{3} \sum_{j} P_{ij} \tag{4.25}$$

$$P_{ij} = P_{AAij} \times P_{nij} \tag{4.26}$$

where P_{AAij} is the probability of the fact that the aircraft accident (AA) of the i^{th} type with class j aircraft occurs in the vicinity of the object. The class of aircraft can be categorised based on factors that include aircraft weight and fuel storage capacity.

P_{nij} is the conditional probability of an aircraft or its fragments falling onto the object as result of the aircraft accident.

Probability P_{AAij} is determined according to Poisson's law,

$$P_{AAij} = 1 - \exp(-P_{Fij} * \tau) \quad (4.27)$$

Where P_{Fij} is the flight safety parameter, which equals to the probability of an accident within an hour of flight and is found according to:

$$P_{Fij} = nij/ T \quad (4.28)$$

where nij is an average number of aircraft accidents of the i type with the aircraft of j class per year (y).

T- is the flight hours of j class aircraft, hours/year

τ - the time, aircraft is staying within its reach of the ground object and is determined by the equation:

$$\tau = H * K * N / V \quad (4.29)$$

Where H - flight altitude, K- aerodynamic efficiency of aircraft, N-number of flights along the given air routes and V-flight speed

A study on the probability of occurrence of an aircraft crashing on the NPP (Pnij) shall be made and the value of Pnij can be assigned, taking account the flight frequencies at the nearest air field and its distance from the site, expert's judgement and data base generated globally from both domestic and international flights.

4.12.3 Plant Response and Component Fragility Evaluation on Aircraft Crash

Aircraft crash may result into direct impact and missile effects, fuel burning and resulting consequences.

4.12.3.1 Direct Impact and Missile Generation

The load/time functions for the direct impact of the aircraft on the items important to safety should be established. This should include considerations like areas of crash surfaces of the main body of the aircraft and of the aircraft and of the secondary missiles made of parts of the aircraft, from which they have become separated, impact velocity and also angle of impact. The evaluation should include analyses of the potential for structural failure by shear and bending, for perforation of the structure, for spalling of concrete within the structures, for damping of SSCs and for propagation of shock waves that could affect items important to safety. The aircraft may break up into parts like engines, wings, fuselage tail section, each of which becomes a separate missile with its own trajectory. An analysis of the missiles that could be produced and their significance, should be made on the basis of engineering analysis, with due regard to the possibility of simultaneous impacts on separate redundant systems. The impact velocity, weight of aircraft and also angle of impact (typically 10° to 45° to horizontal) are parameters for load/time evaluation.

4.12.3.2 Effects Caused by Aircraft Fuel Burning

The following consequences that may result from release of fuel carried by the crashing aircraft should be taken into account:

(i) Burning of aircraft fuel outdoors generating high energy and temperature and causing damage to exterior plant components important to safety.

(ii) Explosion of part or all of the fuel externally to buildings

(iii) Entry of combustion products into ventilation or air supply systems, thereby affecting personnel or causing plant malfunctions such as electrical faults or failures in emergency diesel generators

(iv) Entry of fuel into the building through normal openings, through holes which may have been caused by the crash, or as a vapour or aerosol through air intake ducts, leading to subsequent fires, explosions or unwanted side effects such as the over speeding of diesel engines.

While evaluating the effects of fuel burning, parameters on amount and type of fuel carried by the crashing aircraft are important. The amount of fuel to be considered for energy release calculation should be based on the type of aircraft, typical flight plans (paths) and flight travel time and velocity.

4.12.3.3 Event Sequence and Consequence Analysis

The conditional probability of these SSCs getting damaged to unacceptable consequences should be assessed based on load/time function, insights from structural engineering, fracture mechanics and expert judgement. The core damage consequence can be evaluated by event sequence development and quantification of the same after impacting failure probabilities of components, both at FT and ET level, as appropriate. The source term should be worked out with Level 1 PSA inputs and APET/CET analysis, also considering the fact that there could be direct radioactive release probability by simultaneous damage of containment and other SSCs like reactor block, PHT pipeline breaks, etc. The overall release consequence to public domain can be evaluated from PSA Level 3 analysis taking into account any possible effect on implementation of counter measures. The uncertainties associated with each stage of evaluation should be appropriately addressed.

4.13 Probabilistic Structural Integrity Assessment

4.13.1 General Approach

There are numerous sources of uncertainty in structural design and the absolute safety of a structure cannot be guaranteed due to unpredictability of future loading, variations of material properties as they exist in the structure, simplifications to analysis methods for predicting behavior and human factors. However, the risk of a failure with unacceptable consequences can be reduced to an acceptably low number. Estimation of this level of risk is evaluated using the methods of probabilistic structural integrity assessment.

The fundamental concept for reliability analysis is that resistance and load factors are statistical quantities with a central tendency (mean), dispersion about the mean (variance) and some form of distribution (probability density function, e.g. Normal). When combined together via an expression to describe the limit state (such as fracture or collapse) there will be a finite probability that the load will exceed the resistance. This defines the probability of failure (Pf) and since reliability is equal to 1- Pf, the inherent reliability of the component against a particular failure mode, and with given resistance properties, is defined.

Initial concepts in this area of structural reliability were developed in the nuclear and offshore industries in the 1980s, applications that have associated with them a very high consequence of failure. More recently, these methods have begun to be used in structures that are more conventional and guidance now exists in many design and integrity analysis codes. This may be either in the form of a direct reference to such methods, their use to derive partial safety factors or their application to maintenance and inspection. Public perception and understanding of risk, the associated role of regulatory bodies and the necessity for a common basis on policy where safety is an issue have further strengthened the move to reliability-based methods. The advantage of such methods in integrity analyses is that the use of pessimistic assumptions for data inputs is avoided, and the compounding effects of such assumptions can be minimised. This compound effect makes the results of deterministic analyses often very conservative leading to a lack of credibility in their results. The methods can be applied to any mode of failure (e.g. fracture, collapse, fatigue, corrosion, creep and buckling) provided the limit state can be described by an equation(s) and that one or more of the variables in the equation is statistically distributed.

A high probability of failure can be accepted where the consequences of that failure are low; conversely, a high consequence of failure must be allied to a low probability of occurrence. Societal and governmental acceptance of risk dictates that different industries and structures will have different combinations of probability of failure and consequence of failure, There are also targets of what is considered to be negligible risk, unacceptable risk and a region in between where risk is treated in terms of 'ALARP' (As

Low As Reasonably Practical). High risk can be treated in terms of mitigating either the frequency of occurrence or reduction of consequence. The interpretation of failure probability must be made in the context of the type of structure or component. Mass produced components (pumps, valves, electrical devices) can be assessed in terms of failure frequency, or time to failure, due to the numbers involved and the fact that they generally comprise parts which wear out, rather than fail by some unexpected or complex mechanism, which may involve human factors. In contrast, engineering structures tend to be unique in their structural form and location and are subjected to a range of operating conditions, which can cause failure, by one failure mode or a combination of many.

The concept used for structures is therefore to sample from the input distributions many times and theoretically create similar structures under the full range of operating conditions. For the case of an existing structure, information can be gained on its behavior and this can be used to refine the calculations of risk, a form of reliability updating, which is not possible with newly, designed structures. The assessed reliability is not solely a function of the structure itself, but is also dependent on the amount and quality of information available for the structure.

The general concept behind all probabilistic methods is that some or all of the inputs contain inherent uncertainty and these can combine to give an uncertainty rating for structural performance. For general structural assessment purposes, it is standard practice to assess safety by comparison of load and resistance effects using established design rules to predict the likelihood of failure. Where there are uncertainties in the input variables, or scatter in the material properties, reliability-based methods can be employed to determine the probability that the load effects will exceed the resistance effects. Inherent scatter in a material property will affect the failure probability and it is therefore not only the mean value of a property which is important, as in deterministic analysis, but also its variance and the type of distribution used to represent the dataset.

Depending on the failure mode, material properties, temperature, geometry and loading will influence the reliability of the component. It is more usual to assess failure modes, which contribute to the ultimate limit states rather than serviceability limit states. These include yielding, fracture, fatigue, creep, corrosion, stress-corrosion cracking, bursting and buckling.

4.13.1.1 Hierarchy of Structural Reliability Methods

It is generally accepted that reliability methods can be characterised into one of 4 levels:

Level 1: uses partial safety factors to imply reliability and is used in simple codes.

Level 2 : is known as second moment, First Order Reliability Method (FORM). The random variables are defined in terms of means and variances and are considered to be normally distributed. The measure of reliability is based on the reliability index b. In advanced Level 2 methods, the design variables can have any form of probability distributions.

Level 3 : have multi-dimensional joint probability distributions. System effects and time-variance may be incorporated. They include numerical integration and simulation techniques.

Level 4 : includes any of the above, together with economic data for prediction of maximum benefit or minimum cost.

4.13.1.2 Types of Uncertainties

Formal uncertainties can be classified into three categories; physical, knowledge based and human.

The first represents natural randomness intrinsic to a variable and is known as objective uncertainty, such as wind loading. The second, subjective uncertainties, can be reduced at a cost by collecting more data or adopting more realistic models while the third category is hardest to quantify and modify.

Knowledge based uncertainty can be further subdivided into statistical, model and phenomenological uncertainties. Statistical uncertainty arises due to a limited number of observations being used to make up a sample, which is then taken to represent a population. Generally, a sample does not perfectly represent the full population but the degree of imperfection is never known, although it can be estimated. Modelling uncertainty is caused by the use of simplified relationships between variables to represent real behavior. Methods are used to simplify loads and structural responses. Limit state equations are examples of modelling uncertainties. Phenomenological uncertainty arises because unimaginable phenomena occur which affect structural failure. Examples include wind-induced resonant effects and frequencies of earthquake loading and since such phenomena has not been previously encountered, they are particularly important for novel structures or those which attempt to extend the state-of-the-art.

The difference between 'real' experienced risk of structural failure and the modelled or predicted failure probability (which is lower) is usually referred to as the adjunct probability of failure. It is mainly attributable to human error and modelling uncertainty. As long as these remain there will always be a gap between predicted and experienced risks, this gap is generally 1 to 3 orders of magnitude, although accounting for modelling uncertainty alone in fracture analyses gives a difference of one order of magnitude and for these reasons, predicted reliability levels are best referred to as notional, rather than absolute, levels and are better suited for comparison purposes.

4.13.1.3 Use of Reliability Methods in Nuclear Industry

The probabilistic structural integrity evaluation in nuclear industry covers predominantly fracture, fatigue, creep and corrosion failure processes. These methods are applied for inspection scheduling, life extension, design and change in operating conditions. Fracture is the most important postulated design basis event for the Indian PHWR.

4.13.2 Probabilistic Fracture Mechanics

The R5 [61] and R6 [62] methodologies are the most widely applied for high and low temperature failure assessments respectively, and both can be treated probabilistically. R5 reliability analysis is currently at the development stage, while examples of R6 application in reliability are well documented. Application of R6 to estimate probability of failure of Indian 540 MWe nuclear reactor is presented in [63-64]. The use of the R6 method in support of safety cases, and determination of acceptable levels of reserve factors, has however demonstrated that it is usually the lack of high quality input data, particularly defect size distributions, that limit the usefulness of the approaches rather than any inherent limitation of the methods themselves.

The R6 method uses the well-known failure assessment diagram (FAD), which enables simultaneous analysis of fracture and collapse for a component with a flaw (Fig. 4.10).

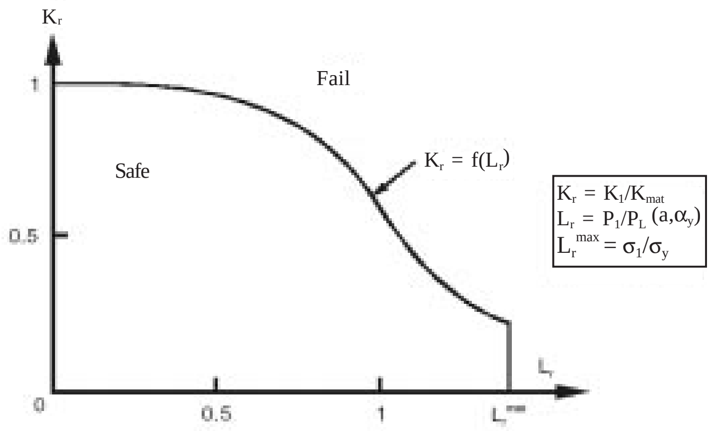


FIGURE 4.9 : BASIC PRINCIPLE OF THE FAILURE ASSESSMENT DIAGRAM (FAD)

Material properties and flaw sizes are usually treated probabilistically, while applied and residual stress is deterministic. Ideally, full conditional probabilities for material properties should be established since strength and toughness are related but alternatively realistic lower tails can be imposed on the distributions to reduce the level of pessimism. By using the actual composition from a test certificate, and based on knowledge of the performance of different compositions, a more realistic estimate of failure probability can be obtained than if the minimum or maximum allowable limits of each element had been assumed.

The failure assessment diagram (FAD) gives a graphical representation of the potential effect of a defect on the integrity of a structure. The FAD is a two-dimensional plot and indicates the propensity of the defect to cause failure by plastic collapse and brittle fracture. The basic FAD has two axes, K_r and L_r where:

K_r = Applied stress intensity/fracture toughness

L_r = Applied stress/yield stress
or
Applied load/limit load

K_r is known as the brittle fracture parameter and L_r the plastic collapse parameter. The safe region is bounded by these two axes and a curve known as failure assessment line (FAL). The simplest case of R6 called Option gives the equation of FAL by equation (4.30).

$$\begin{aligned} &K_r = [1-0.14L_r^2][0.3+0.7e^{(-0.65L_r^6)}] \\ &for \quad L_r \le L_r^{\max} \\ &K_r = 0 \quad for \quad L_r > L_r^{\max} \\ &L_r^{max} = \sigma_f / \sigma_y \end{aligned} \tag{4.30}$$

The three principal inputs, which are necessary for a basic deterministic calculation to be performed, are crack size, stress and fracture toughness. If all three are known, the safety of a structure can be evaluated, while if any two are known the critical level of the third parameter can be determined. The brittle fracture parameter can also be defined in terms of J Integral or crack tip opening displacement (CTOD) -based fracture toughness. Once the co-ordinates of the analysis point has been evaluated and plotted on the FAD, further information can be gained depending on the relative position of the analysis point in FAD space. The FAD locus divides this space into 'safe' and 'unsafe' regions, the shape of the locus allowing for the interaction of yielding and fracture. Furthermore, depending on where the analysis point falls the most likely failure mode can be estimated; the regions of 'fracture-dominated', 'collapse-dominated' and 'intermediate' behavior are divided up according to the ratio of K_r/L_r. Another feature of the FAD is that some element of work hardening is allowed for since the L_r cut-off level of 1.0 represents an allowable maximum stress equal to the mean of yield stress and UTS.

4.13.3 Target Reliability Levels

Target reliability levels depend on the consequence and the nature of failure, the economic losses, the social loss or inconvenience, environmental consequence and the amount of expense and effort required to reduce the probability of failure. Target levels are usually calibrated against well-established cases that are known from experience to have adequate reliability, although novel types of structure require formal approaches to define appropriate levels. The reliability index of a structure is often quoted rather than failure probability since there is a substantial difference between the notional probability of failure in the design procedure and the actual failure probability. An acceptable frequency of failure in case of nuclear piping can be taken as lower than that of the "Core Damage Frequency". This value is normally quoted as of the order of 10^{-6} per year.

4.13.4 Types of Analysis : Simulation v Transformation Methods

In simulation methods, a number of random samples are drawn and the probability determined by simple ratios. In transformation methods, the integrand is transformed into a standard type of distribution, which can then be analyzed using the particular properties of the distribution. Decision of relevant failure modes and their limit states are common to both classes of analysis, as is interpretation of the consequences of failure. The methods differ in the middle step of determination of failure probability from distributions of applied and resistance factors.

4.13.4.1 Simulation Based Methods

(a) Monte-Carlo simulation (MCS)

MCS is a relatively simple method, which uses the fact that failure probability can be expressed as a mean value of the result of a large number of random combinations of input data. An estimate is therefore given by averaging a suitably large number of independent outcomes (simulations) of this experiment. The basic building block of this sampling is the generation of random numbers from a uniform distribution. Simple algorithms generate random numbers repeating after approximately 2 x 10^3 to 2 x 10^9 simulations and are therefore not suitable to calculate medium to small failure probabilities. Once a random number u, between 0 and 1, has been generated, it can be used to generate a value of the desired random variable with a given distribution. A common method is the inverse transform method. To calculate the failure probability, one performs N deterministic simulations and for every simulation checks if the component analysed has failed. The number of failures is NF, and an estimate of the mean probability of failure is the ratio of NF to N. A schematic of the MCS method is shown in Fig. 4.10 below.

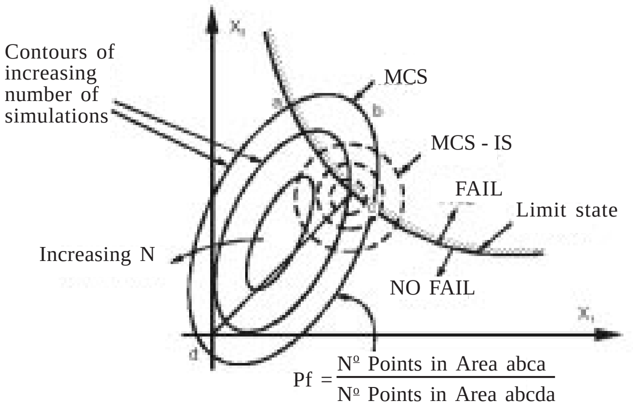

X_1
Contours of increasing number of simulations
MCS
a
b
MCS - IS
FAIL
Limit state
Increasing N
NO FAIL
X_1
d
Pf = Nº Points in Area abca / Nº Points in Area abcda

FIG. 4.10 : SCHEMATIC OF MCS AND MCS-IS METHODS

An advantage with MCS, is that it is robust and easy to implement into a computer program, and for a sample size tending to infinity, the estimated probability converges to the exact result. Another advantage is that MCS works with any distribution of the random variables and there are no restrictions on the limit state functions. However, MCS is rather inefficient, when calculating failure probabilities, since most of the contribution to Pf is in a limited part of the integration interval. In addition, for very low failure probabilities, a large number of simulations is required for the result to converge to the actual value, in these case FORM is preferred or the method of importance sampling (MCS-IS) can be used.

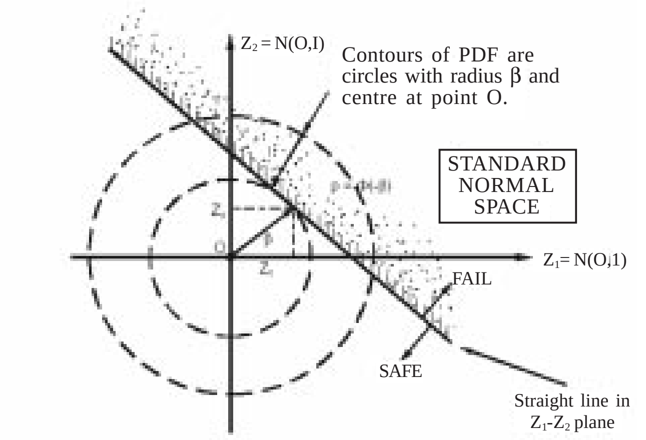
(b) Monte-Carlo simulation with importance sampling (MCS-IS)

MCS-IS is an algorithm that concentrates the samples in the most important part of the integration interval. Instead of sampling around the mean values, as in MCS, sampling is made around the most probable point of failure. This point, called MPP, is generally evaluated using information from a FORM/SORM analysis and as such, the MCS-IS has limited application except for cases where convergence in FORM cannot be achieved due to complexity of the limit state.

4.13.4.2 Transformation Based Methods

(a) First order reliability method (FORM)

FORM uses a combination of analytical and approximation methods and comprises three stages. Firstly, independent of whether each parameter has been defined as a Normal, Log-Normal or Weibull distribution, all variables are first transformed into equivalent Normal space with zero mean and unit variance. The original limit state surface is then mapped onto the new limit state surface. Secondly, the shortest distance between the origin and the limit state surface, termed the reliability index β, is evaluated; this is termed the design point, or point of maximum likelihood, and gives the most likely combination of basic variables to cause failure. Finally, the failure probability associated with this point is then calculated via the relationship between β and Pf. This is shown schematically for the case of a linear safety margin in Fig. 4.11 below.



$Z_2 = N(O,I)$
Contours of PDF are circles with radius β and centre at point O.
STANDARD NORMAL SPACE
$Z_1 = N(O,1)$
O
β
FAIL
SAFE
Straight line in Z_1-Z_2 plane

FIG. 4.11 : FORM ANALYSIS WITH LINEAR LIMIT STATE

Transforming the variables into equivalent Normal variables in standard Normal space (mean = 0 and standard deviation = 1) gives the joint probability density function as the standardized multivariate Normal which has many useful properties; This is known as the Hasofer-Lind Transformation and by its application the original limit state surface g (x) = 0 then becomes mapped onto the new limit state surface g_u (u) = 0. Calculation of the shortest distance between the origin and the limit state surface, β, requires an appropriate non-linear optimisation algorithm. A modified Rackwitz and Fiessler algorithm, used as the default algorithm in most reliability analyses, works by damping the gradient contribution of the limit state function. It is a robust algorithm and converges quite quickly for most cases. Finally, the failure probability is calculated using an approximation of the limit state surface at the most probable point of failure. FORM is more efficient than MCS in terms of computing time and accurate results can be obtained even when the failure probability is low. All the random parameters must however be continuous and large errors can also result if there are local minima in the limit state or high non-linearity at the design point. Despite these limitations, FORM is the most popular reliability analysis method. It can be easily extended to non-linear limit states and has a reasonable balance between ease of use and accuracy.

(b) Second order reliability method (SORM)

The approximation of the limit state at the design point as a straight line is a step, which leads to errors in FORM analyses, the magnitude of which depends on the degree of non-linearity of the limit state equation. In SORM, a parabolic, quadratic or high order polynomial is used to describe the limit state surface, centered on the design point. This leads to higher accuracy but is not generally considered necessary for the majority of engineering applications.

For description of these methods in detail refer to [65], [66] and [67].

5. PSA REVIEW

5.1 Introduction

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 of the PSA may be performed by the regulatory body. 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.

5.2 Scope

The guidelines are given to address issues such as the timing and the extent of review, review of aims and objectives of the PSA, review and audit of the utility's PSA production process, and the documentation of the findings of the review.

5.3 Levels of Review

There are four levels of review in the organisation; (i) Study-team review, (ii) Plant operating personnel review, (iii) Peer review and (iv) Management review [4]. These are briefly described below.

5.3.1 Study Team Review

The review of all work done should be carried out by the team leader and the internal peer group. Although this review should cover all aspects of the study, it is at this level that methodological mistakes, if any, are identified with the greatest confidence.

5.3.2 Plant Operating Personnel Review

It is desirable to have the PSA reviewed by persons most familiar with the plant design, operation and utility operating practices. It is at this level that technical mistakes concerning representation of the plant and site characteristics are identified with the greatest confidence.

5.3.3 Peer Review

This review should be carried out by true peers, that is, persons who are not involved in the study but have capabilities essentially equivalent to those of the persons performing the study. The peers should span the range of disciplines required for the study. In general, this review should concentrate on the appropriateness of methods, information sources, judgements, and assumptions.

5.3.4 Management Review

This level of review should concentrate on perspective, scope and product suitability in meeting program objectives. The reports from the peer review should be a part of the management review.

5.4 Review Process

There are mainly four steps in this process: (i) Approach to the review, (ii) Review of aims, objectives and scope of the PSA, (iii) Review of the methods and assumptions used in the PSA, and (iv) Review/ audit of the utility's PSA production process [77].

5.4.1 Approach to the Review

5.4.1.1 Timing of the Review

There may be an on-line or an off-line review depending on the time when the review is carried out. An on-line review is carried out immediately after the PSA team has finished one particular task and it has the advantage that many of the findings of the review can be incorporated in the PSA and significantly reduces the amount of reworking. The disadvantage is that the reviewed reports may change significantly as the analysis proceeds and may need further review. An off-line review starts after the submission of the final report on PSA to the regulatory body. The advantage of this approach is that the PSA documents are reviewed once. The disadvantage is that the review may find significant problems that could have been identified and corrected more easily at an early stage of the analysis. An on-line review is recommended for first two levels of the review and off-line review is recommended for third and fourth levels of review.

5.4.1.2 Extent of the Review

The extent of the review can range from an extensive review to a much more limited review. During an extensive review, the PSA would be reviewed in considerable detail to make sure that the models and data used are good representations of the actual plant design and operational practices. This approach has significant advantage in terms of learning, building confidence in the PSA and reducing the efforts required for reviewing PSA applications. During a limited review, the aim would be to ensure that all aspects of the event sequences leading to end states are modelled adequately and the data to determine the frequencies of the event sequences is representative of the plant. The advantage of this approach is that it is less intensive in resources for the regulatory body but leads to lower levels of learning and confidence. An extensive review is likely to be required if it is intended to use the PSA as a basis for risk-informed decision making.

5.4.1.3 Documentation for the Review

The documentation for the review would include systems descriptions, associated flow sheets and drawings, operating procedures, test and maintenance procedures, accident management procedures, and the documentation of the PSA itself. It is recommended that regulatory authority agrees with the utility on the format and content of the PSA documentation before the start of the PSA

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 event/fault tree analysis. This would allow reviewers

(i) to use the PSA as a basis for risk informed regulation

(ii) to search for specific information in the model

(iii) to perform spot checks on the model and its quantification

(iv) to carry out importance analysis to identify the areas of the PSA on which the review should be focused

(v) to carry out their own sensitivity studies to determine how changes in assumptions can affect the results of the PSA.

5.4.1.4 Setting Up the Review Team

It is important that the review team be experienced in the techniques for carrying out state-of-art PSAs. The range of expertise should be sufficient to address all the issues, which are likely to arise during the review of the PSA. Where necessary, additional training may be provided as required. The review team should include experts with experience in deterministic analysis.

5.4.1.5 Identification of/Focus on Important Issues

The reviewers should identify the issues, which have the highest risk significance such as IEs and system/component failures. This may be done by using the importance measures, sensitivity studies and uncertainty analysis.

5.4.1.6 Comparison With Other PSAs

The reviewers may consider it useful to compare the results of the PSA with those of other PSAs. For example, in PSA Level 1 analysis, CDF, dominant sequences and their initiators, dominant systems, etc., can be compared with the results of the PSAs of similar plants. However, there could be differences in design among the plants compared; neither the similarity, nor the lack of similarity, of the results is a clear indication of correctness or incorrectness of the PSA, but it can stimulate thinking about areas to review in more detail.

5.4.1.7 Research

In the course of the review, the reviewers may identify areas that they see as promising candidates for research to develop the state-of-the-art, for example, reducing uncertainties, increasing confidence, and reducing conservatism.

5.4.2 Review of Aims, Objectives and Scope of the PSA

If the PSA is going to be presented to regulatory authority for the review, it is advisable that before the PSA is started both parties agree on aspects of the PSA such as its aims, objectives and scope.

5.4.3 Review of Methods and Assumptions

It is recognised that PSA methods are still evolving in certain areas. However, it is important that both the regulatory authority and the utility determine what the state-of-the art is in PSA and this should be agreed upon by both parties.

5.4.3.1 Methods of Analysis

It is necessary for the reviewers to determine whether the methods used for the analysis are adequate to meet the aims and objectives of the PSA. Wherever method or tool different from the state-of-the-art is identified, this matter is to be raised immediately with the utility as a significant area of concern. The reviewers need to check that best estimate methods, assumptions and data have been used in the PSA wherever possible. With the aim of best estimates throughout the PSA, it is important to check that the conservatisms present are not so great that they lead to an unacceptable bias and distortions in the results of the PSA. The reviewers should confirm that all the sources of data have been identified and are relevant. The aim is to ensure that plant specific data are used wherever possible. Where this is not possible, use of data from the operation of the same type of reactor system or generic data is acceptable. Where no relevant operating data are available or data paucity exists and judgement has been used to assign the IE frequency, the basis for this judgement is to be stated and shown to be valid, as far as possible.

5.4.3.2 Verification and Validation of Computer Codes

The computer codes used in the PSA are to be validated and verified. In this context, verification is defined as providing the theoretical examination to demonstrate that the calculation methods used in the computer code are fit for purpose. A code that solves a differential equation might be tested on a known analytical solution of the equation to confirm that it is indeed giving solutions to an acceptable level of accuracy. Validation is done to ensure that the controlling physical and logical equations have been correctly translated into computer code which represent accuracy and reality of the situations/ phenomena. It is necessary for the reviewers to determine whether the codes, which have been selected by the PSA team, are fit for purpose, and that the users of the codes are experienced in their use and fully understand their limitations. The set of computer codes to be used by the utility should be in agreement with the recommendations of the Regulatory Body.

5.4.4 Review/Audit of the Utility’s PSA Production Process

In addition to carrying out a review of the technical issues involved in a PSA, the regulatory authority may also carry out a review/audit of the utility’s PSA production process and the procedures being used. The reason for this is to give confidence that those parts of the PSA, which have not been reviewed in detail, have been performed satisfactorily. The reviewers usually check that the utility has procedures in place for the production of the PSA, which set out the basic principles and methodologies to be followed, and that they are adequate to produce a state–of-the-art of PSA. The reviewers determine whether the utility has QA program in place for the production of the PSA. It is necessary for the reviewers to check that the PSA is being produced and documented in a way that makes it easy to update and to extend its use to other applications.

5.5 Review of Level 1 PSA [68]

The technical issues that need to be addressed in carrying out the review of the Level 1 PSA are discussed below.

5.5.1 Identification and Grouping of IEs

The reviewers need to check that a systematic procedure has a been used to identify the set of IEs used in the PSA. The set should include internal events, internal and external hazards. For twin or multiple unit sites, some safety systems may be shared or cross-tied. In this case, the reviewers should check that those IEs that can affect both units have been identified and the PSA takes account of the shared systems that are required by both/ all of the units (instead of available fully for one unit). Missiles from turbine disintegration could strike a vulnerable part of the other unit, and this event should have been identified, even though it may be screened out later after analysis.

The set should include partial failures of equipment that may make significant contribution to the risk. The reviewers are expected to check the criteria used for including events into or excluding them from the set. Reviewers should compare the set with that for similar plants. The reviewer should ensure that any IEs that have actually occurred are included in the set of IEs addressed in the PSA.

The reviewers need to check that the corresponding ET has been developed to envelop all potential sequences and consequences of these IEs with appropriate success criteria for mitigating system. However, where such IEs are grouped, the reviewers should satisfy themselves that this does not introduce undue conservatism into the analysis.

5.5.2 Event Sequence Analysis

The reviewer has to check whether the safety functions are identified along with the success criteria for the safety systems. The success criteria should identify the operator actions that are required to bring the plant to a safe, stable shutdown state. Reviewers should also check the mission times for the safety systems based on the accident analysis carried out. If any operator action is considered in the event tree, reviewer should check that it appears in chronological order since the probability of error will be conditioned by whole sequence of events up to that point. If the different system success requirements in ETs are modelled by means of house events in the system FTs, the house event descriptions should be reviewed and the interfaces with the respective ETs should be checked.

The reviewers should check that the PDSs are appropriately grouped taking into account each core damage sequence having influence on the containment response or the release of radioactivity to the environment. These PDSs should be consistent with what has been done in previous PSAs for similar plants.

5.5.3 System Analysis

It is necessary for the reviewer to check that FTs have been developed for each of the safety systems identified in the ETs. When a system success criteria is different for different event sequences, a single FT may be developed for that system using house events with appropriate description. Reviewers should check that all the individual basic events, which could lead to system unavailability, either directly or in combination with other basic events, are modelled in the FTs. Reviewers should also ensure that all support systems including electrical systems, cooling systems, I&C requirements, etc are included in the FTs. Passive components whose failure could fail the system (e.g., filter blockage, pipe break etc.) also should be modelled and should not be screened out on the basis of very low probability. Where components are grouped into super components, the failure modes of each of the elements should have the same effect on the system. Also, all super components should be functionally independent in that no component appears in more than one super component, or elsewhere as a basic event. Reviewers should ensure that the CCFs, which can affect groups of redundant components, are identified and modelled in the FTs. Adequate justification is to be provided for these common cause failure probabilities. Where possible, they are to 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. Reviewers should also ensure that modelling of maintenance unavailability in the FTs does not violate the TS requirements. Reviewers should ensure that the shared systems have been appropriately modelled. It is necessary for the reviewers to check that the HRA has been performed in a structured and logical manner and that all the steps of the analysis are documented in a traceable way. The reviewers need to check the HRA process used in PSA to ensure that all the necessary steps are included in the PSA.

5.5.4 Data Used in PSA

The reviewers should ensure that the maximum use has been made of plant specific data, but should compare this with the recent or updated generic data and satisfy themselves that there are reasonable explanations for any notable differences. This is necessary even when the two sources are combined by Bayesian approach or any other method. Data from the operation of similar plants are preferred to more generic data, such as that from all PHWRs, but may not have been readily available to the PSA analysts. In any case, the data used should be sufficiently well justified in the PSA documentation.

For IEs 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 judgement. The reviewers need to ensure themselves that bases for the judgments on these numerical estimates have been given and are acceptable. The estimation of the number of demands, operating hours or standby hours is important in the analysis of specific plant records. The reviewers need to check this estimation for selected components.

5.5.5 Computer Based Systems

For a computer-based system, the failure rate will generally be dominated by errors in the software, with the contribution from hardware faults being relatively small. The software failure rate of a large computer based systems like protection system, may be judged, taking account of the following factors.

- the size and complexity of the system (the number of lines of computer code is an indication),
- the novelty of any of its features,
- whether it identifies a safety kernel,
- the degree of conformance with procedures and standards in the production, checking and testing processes,
- the independence of the teams performing the static analysis and the dynamic testing,
- the number of errors found in these two processes,
- the extent of use of formal analysis tools in the static analysis,
- the number of dynamic tests carried out,
- the experience of the designers of the system, and
- experience with similar systems in service.

If software failure rate is claimed to be very low (e.g. < 1E-04/demand), the reviewers should ensure proper justification. Where a control system and protection system are both computer based, consideration is to be given to software dependencies between them. There may be potential for a software error to give rise to a control fault (IE) and also disable the protection against that fault.

5.5.6 Sensitivity, Uncertainty and Importance Analysis

The reviewers should check that sensitivity analyses have been performed on all the appropriate assumptions and data. The reviewers should check that uncertainty introduced by incompleteness, modelling inadequacy and input parameters have been properly calculated and ensure that the uncertainties have been propagated through the model correctly. The reviewers should check that the importance analysis results are logical and in agreement with the sensitivity analysis, qualitatively, as applicable.

5.5.7 Review of Results

The results of the Level 1 PSA are expected to give the numerical estimate of the CDF and include sufficient information to give insights into what are the main contributors. This would typically include CDF, contribution to the CDF from each of the PIE groups, dominant accident sequence, results of sensitivity, uncertainty and importance analysis, etc.

The reviewers should ensure that the results of the PSA are logical, correct and the overall objectives and requirements of PSA are met. The assumptions made in the PSA should have proper basis. In particular, where relevant experiments have been carried out, the reviewers should compare the experimental results with the assumptions made in the PSA. In addition, where major expert opinions have been formed in previous PSAs, any deviations should be identified and explained. The reviewers need to check whether the contributions to the risk from issues such as operator error and the CCFs, and the benefits from carrying out accident management measures are reasonable in relation to the results of the other PSAs.

5.6 Review of Level 2 PSA [69]

The technical issues that need to be addressed in carrying out the review of the Level 2 PSA are discussed below:

5.6.1 Identification of Plant Damage States (PDSs)

The reviewers should check PDSs identified and grouped appropriately. The reviewers should check that total frequency of event sequences below the cut-off value is a small fraction of the total CDF (e.g. less than 5 %) and that the accident sequences that could potentially lead to large consequences (i.e. containment by-pass sequences, steam generator tube rupture accidents, sequences with containment isolation failure) are not systematically removed from the PDS grouping and addressed appropriately.

5.6.2 Accident Progression Models

Deterministic analysis of reactor and containment behaviour during postulated accident sequences represents the principal basis for event quantification in a Level 2 PSA. The probabilistic framework of a Level 2 PSA is the mechanism for delineating and quantifying uncertainties in deterministic severe accident analyses.

5.6.2.1 Computational Tools

The reviewers should identify the computational tools used to perform accident progression calculations. In some studies, a single integrated severe accident analysis computer code is used to model all aspects of severe accident progression (e.g., MAAP, MELCOR, ESCADRE and THALES-2), and reviewers should be familiar with the applicability and limitations of the computer codes.

5.6.2.2 Review of Treatment of Important Accident Phenomena

The reviewers should ensure that all important accident phenomena are addressed by plant-specific analysis or by application of information from other credible and relevant sources. For each accident phenomenon, the reviewers should be able to identify the computer code or data source used to address it. If published data from experiments or reference plant analysis is used to evaluate certain phenomena, the relevance of that information to the plant being studied should be confirmed. If plant-specific analysis is performed using the computer codes, the data (e.g. volume of water coolant, volumes of various compartments in containment, other basic data to define the configuration, geometry and material composition of the plant) used to perform the calculations should be checked. The reviewers should examine the level of detail used to develop a nodal thermodynamic model (i.e. lumped parameter control volumes) including RCS and containment nodalisation schemes as well as the core nodalisation structure. The reviewers should confirm that the spatial nodalisation schemes used by the analysts are consistent with contemporary approaches used for other, similar plants.

The reviewers should compare the calculated results of the analysis with the severe accident calculations, performed with computer codes and published in the literatures. This provides a useful basis for gauging the extent to which unique plant design or operating characteristics influence severe accident progression. In the absence of such information (e.g., for unique plant designs), the reviewers should check global results by means of simple hand calculations; e.g., mass/energy balances to estimate the timing of key events. The reviewers should check whether uncertainty/sensitivity analyses are performed. Without such analyses, the Level 2 PSA is incomplete.

5.6.3 Containment Performance Analysis

Calculations of severe accident progression generate pressure and temperature histories within containment during various accident sequences. To determine whether the containment pressure boundary will be able to withstand these and other loads, quantitative estimates of its structural performance limits must be generated. The reviewers should check that following features of the containment pressure boundary are included in the analysis:

- containment configuration, construction materials and reinforcement (e.g., free-standing steel shell, concrete-backed steel shell, pre-tensioned or reinforced concrete; post-tensioned),
- penetrations of all sizes, their locations in the containment structure and local reinforcement (e.g., equipment and personnel hatches, piping penetrations, electrical penetration assemblies, ventilation system penetrations),
- penetration seal configuration and materials, and
- local discontinuities in the containment structure (e.g., shape transitions, wall anchorage to floors, changes in steel shell or concrete reinforcement).

5.6.3.1 Structural Response Analysis

The reviewers should check that the analytical tools used to develop containment failure criteria are of accepted industry standard or validated. Alternatively, experimental results can be used directly. The reviewers should also examine the terms in which containment failure criteria are stated. A complete structural performance assessment should distinguish conditions that would result in catastrophic failure of the pressure boundary from those that result in smaller scale damage, and identify the anticipated location of failure.

If the external events (e.g. seismic) are considered in the PSA, containment structural response to postulated seismic events should be reviewed. As with other mechanisms for containment failure, the relationship between seismic intensity and the location and size of containment failure should be readily identified in the study.

5.6.3.2 Containment Bypass

In addition to structural failure of the containment pressure boundary, the reviewers should also examine analyses performed to identify locations, pathways and associated sizes of bypass mechanisms such as containment isolation failure, interfacing system LOCAs and steam generator tube rupture. With regard to steam generator tube rupture, the reviewers should also check that such events are not only treated as PIEs, but are also considered as an event that may occur during in-vessel core degradation.

5.6.4 Quantification of CETs/APETs

The reviewers should carefully check that the technical basis used to quantify events and the probabilities generated from them represent an unbiased characterisation of accident behaviour. Appropriate consideration should be given to the uncertainties that accompany deterministic calculations of severe accident phenomena. There are many approaches to transforming the technical information concerning containment loads and performance limits to an estimate of failure probability, but three approaches are most often used in contemporary studies. In the first approach, expert judgement is applied in translating qualitative terms expressing various degrees of uncertainty into quantitative (point estimates) probabilities. For example, terms such as “likely” or “unlikely” are assigned numerical values such as 0.9 and 0.1 respectively. In the second technique, probability density functions are developed to represent the distribution of credible values for a parameter of interest (e.g. containment pressure load) and for its corresponding failure criterion (e.g. ultimate pressure capacity). The basis for developing these distributions is the collective set of information generated from plant-specific integral code calculations, corresponding sensitivity calculations, other relevant mechanistic calculations, experimental observations, and expert judgement. The conditional probability of containment failure is then calculated as the convolution of the two density functions. In the third technique, the probability density functions representing uncertainty in each term of the containment performance logic model are propagated throughout the entire model to allow calculation of statistical attributes such as importance measures. It is particularly important for the reviewers to note which method is used to quantify events that are found to be important contributors to risk measures, such as the frequency of early containment failure, or the frequency of large fission products releases.

The technical basis for the event quantification is available from computer code calculations of severe accident behaviour, interpolation of results from code calculations, applications of relevant experiments, hand calculations, expert judgement and engineered system and human reliability analysis. Information derived from the containment system analysis (system unavailabilities, non-recovery probabilities, and human error probabilities), should be reviewed with special attention paid to modelling consistency with relevant Level 1 PSA models.

5.6.5 Source Term (ST) Characterisation

The attributes used to define source term bins should be reviewed to determine if accident progressions that are grouped into a common ST bin would, in fact, have similar radiological release characteristics and potential off-site consequences. The reviewers should examine the accident progressions selected for representative ST calculations, and agree with rationale used by the PSA analysts that other accident progressions within the same release category would result in a similar ST. The reviewers should examine the method used to calculate radionuclide release to the environment, and be confident that the radionuclide grouping scheme is consistent with current, state-of-the-art practices. If the frequency of the following accident conditions is significant, the corresponding STs should be reviewed with particular care.

- Release from unisolated SG tube ruptures can span a very range. Very large releases can accompany accident sequences in which the SG secondary inventory is depleted; conversely, moderate release may result if the ruptured tube is submerged.

- Release from accidents with unisolated containment; depending on the size of the failed isolation, and on the path of release, estimates may vary from small to very large.

- Releases from accidents with late containment failure; depending on the containment capacity, late failure may occur anywhere between 10 hours and 48 hours after core damage. Over these long time periods, revaporisation of volatile species I, Cs and Te from dry, overhead surfaces can dominate the source term.

- Releases from accidents with scrubbing provided by containment sprays; the effectiveness of containment spray in reducing airborne radionuclide concentrations can span several orders of magnitude, depending on spray water temperature, droplet size and spray distribution within the containment atmosphere.

5.6.6 Review of the Results

The reviewers should check that the results of the Level 2 PSA are logical and correct and the overall objectives and requirements of the PSA are met. The reviewers should check that a sufficient range of sensitivity studies have been carried out which relate to the aspects of the analysis which are most significant in determining the level of risk, and those which have the highest uncertainty. The reviewers should check that the results of the sensitivity studies demonstrate that the conclusion of the analysis and the insights derived from it are still valid. The results of the Level 2 PSA study should be compared with those for similar plants and any differences identified. The reviewers should check the assumptions and their justifications made during the study.

The results should include sufficient information to give insights into main contributors to the risk, and the uncertainties in these estimates of the risk.

5.7 Review of Level 3 PSA [22]

The technical issues that need to be addressed in carrying out the review of the Level 3 PSA are discussed below.

5.7.1 Interface with Level 2 PSA

Reviewers should check the assumptions, methodology and computer codes used to calculate the ST.

5.7.2 Atmospheric Dispersion and Deposition

Radionuclides released to the atmosphere as a fine aerosol or gas will create a plume, which is carried downwind. Reviewers need to check which model is used in the Level 3 analysis. Generally, Gaussian model is used for its simplicity and less computational time. Although, choice of atmospheric dispersion model is not major contributor to the difference in the final results, reviewers should see that data required for the chosen model are available in detail. Reviewers need to check that deposition mechanisms are properly modelled in the analysis.

5.7.3 Meteorological Data and Its Sampling

Reviewers should check that the data used in the analysis is taken from the meteorological station nearest to the release point. However, data from the other stations may be acceptable if they are representative of the general conditions experienced by the plume. Stratified sampling minimises the chances of omitting significant but rare weather sequences. Reviewers should ensure that this sampling method is used in the analysis or satisfy themselves with the justification given for the use of other sampling methods.

5.7.4 Exposure Pathways and Dose Assessment

Reviewers should check that correct dosimetric model is used to convert the concentration of the radionuclides to dose in humans for each of the possible exposure pathways. Reviewers should check that proper geometrical correction factors are used for the modification of the semi-infinite cloud results to obtain approximate finite cloud results. Reviewers should ensure that persons indoors and outdoors are considered separately in estimating acute health effects rather than averaging the shielding factors in order to avoid underestimation. Reviewers should promote generation for Indian sites and based on this information, PCA codes should be modified, if possible, to get realistic results.

5.7.5 Population, Agricultural and Economic Data

The spatial distribution of the population, agricultural production and economic data are important elements of PCA codes for the calculation of the health effects and economic impact of implementing countermeasures, such as relocation and food bans. These data (population, agricultural and economic data) may be available in different forms. Reviewers should check that these data are properly mapped into the compatible format of the PCA code used for the analysis.

5.7.6 Countermeasures

Reviewers should check that both short term and long term countermeasures have been properly accounted for the realistic estimate of the exposure of the population. In current PCA codes, decontamination process is modelled with the decontamination factors, which should be checked by the reviewers.

5.7.7 Health Effects

Both deterministic and stochastic health effects are calculated based on the models used by the PCA codes. Reviewers should check that various parameters (average dose, absorbed dose, threshold dose, etc.) of the model equations are properly calculated and the risk-coefficient factors used are latest and supported by proper justifications.

5.7.8 Review of the Results

The results of the Level 3 PSA are expected to give various factors such as concentrations of important radionuclides, radiation doses (individual and collective), health effects (individual and collective), areas, persons and amounts of agricultural produce affected by countermeasures as a function of time, and economic costs. In consequence models it is traditional to present results as complementary cumulative distribution functions (CCDFs), also known as complementary cumulative frequency distributions (CCFDs). Along with producing CCDFs, it is also standard practice to produce the expectation and various percentile values for each CCDF. Reviewers should check that these results are provided appropriately.

5.7.9 Sensitivity and Uncertainty Analysis

Consequence analysis codes endeavour to produce 'best' estimates of the various consequence end points, i.e. without undue conservatism. In order to assist in the interpretation of these results, they should be associated with an estimate of the uncertainties. Reviewers should identify various sources of uncertainties at different stages of the analysis. The reviewers should check uncertainty introduced by incompleteness, modelling adequacy, and that input parameters have been properly calculated and ensure that the uncertainties have been propagated through the model correctly.

5.8 Review of Low-Power and Shutdown PSA [24]

Shutdown and low power operations can contribute to CDF at a level comparable to full power operations. The technical issues that need to be addressed in carrying out the review of the shutdown and low power PSA are discussed below:

5.8.1 Interface with Full Power Operation

Reviewers should recognise that not only the power level of reactor but also the status of automatic actuation and status of front line and support systems are also important from the safety perspective. For example, in VVERs, the large LOCA signal is inactive below 245 °C primary temperature. In some Westinghouse PWRs, an automatic RPS actuation signal will be blocked below 7 % power. In PHWRs, ECCS is blocked during low power and cold shutdown. For example, during turbine trip, power is transferred from the main transformers to auxiliary transformers. These different plant configurations in shutdown state decide the IE, which can lead to various core damage states.

5.8.2 Identification of PIEs

For shutdown conditions a number of PIEs are unique and different from the PSA for full power operation, for example, heavy load drops. The major categories of PIEs, which can threaten critical safety functions are events which affect normal heat removal, events causing a loss of primary circuit inventory and integrity and events affecting reactivity control. Human activity related PIEs are more important during shutdown states. Reviewers should check whether these PIEs are properly taken into account.

5.8.3 Quantification of PIE Frequencies

In a shutdown PSA, PIE frequencies are usually calculated on a 'per calendar year' basis. These frequencies are estimated by any of three methods (i) based on direct estimation from operational experience, (ii) based on full power PSA frequencies with supplemental analysis and (iii) using system modelling techniques (i.e. Fault Tree Analysis, Markovian technique etc.). Reviewers should check the justification given for the selection of the method for estimating PIE frequencies. When PIEs are calculated on a "per calendar year" basis, CDF calculated for different plant operating states (POSs) are additive (i.e., the total CDF is the sum of the CDFs of the relevant POSs). Reviewers should check that all possible POSs are identified, and for each of these POSs, PIEs are calculated.

5.8.4 Event Sequence Modelling

The analysis of human interactions during shutdown is complex. Hence, reviewers should check while developing the ETs, issues such as HRA are appropriately addressed. If the existing full power PSA, ETs are modified for shutdown PSA, reviewers should check the success criteria for the safety systems modelled into ETs, according to the TS requirement applicable to shutdown state.

5.8.5 System Modelling

Success criteria (number of trains required), operating condition (stand-by or operating), mission times and actuation mode (i.e., automatic or manual) are different (for the same system) during full power operation and shutdown states. Hence, reviewers should see that such differences are taken into account in the systems modelling. For example, if "House event" is used to modify the existing FTs, reviewers should carefully examine that top gates of the FTs meet the required success criteria of the systems under consideration. The methodology for the CCF analysis is same as for full power operation. However, reviewers should be aware that testing and maintenance activities might create new sources of dependencies.

5.8.6 Uncertainty, Importance and Sensitivity Analysis

The same techniques are used as for a full power PSA. Hence, Reviewers can see whether consistency has been maintained in both the full power PSA and shutdown PSA.

5.9 Documentation Format for Review Report

The format, content, and structure of the report may depend on the scope of the review. The review report should cover the objective, approach, and a description of the review process. The report should summarise the PSA study carried out and briefly describe the plant features. A list of the reviewers and plant staff and PSA team involved in the whole review process may be pertinent. The review findings should be thoroughly documented, and should include the following:

- The acceptability of the PSA
- The adequacy of the methods and measures used
- The completeness of and consistency in the study
- The major findings and suggested ways to resolve the issues
- Conclusions and recommendation to enhance the plant safety.

For the completeness and future reference, it would be a good practice to document the discussions held with the PSA/utility team and the responses/justification provided by the PSA/utility team to the questions asked by the reviewers.

5.10 Checklist for Review of PSA Related Studies

Table 5.1 shows the checklist to facilitate review process.

TABLE 5.1 : CHECKLIST FOR REVIEW OF PSA RELATED STUDIES

1. Purpose of PSA studies			
1.1	Conceptual/early design stage		
1.2	Detailed design stage		
1.3	The plant at commissioning stage		
1.4	The plant for construction clearance as part of PSAR		
1.5	Operation authorisation as a part of FSAR		
1.6	Operating plant for the first time (PSA Level 1/2/3) or update (PSA Level 1/2/3) of analysis		
1.7	Plant modifications		
1.8	Technical specifications evaluation with risk basis as applicable.		
1.9	Changes in AOT or STI		
1.10	Low power and shutdown risk (SPSA)		
1.11	Configuration management (Living PSA/Risk Monitor)		
1.12	Accident management plan		
1.13	Plant ageing risk		
1.14	Risk based maintenance		
1.15	Risk evaluation of radioactive storage		
1.16	Prioritisation of tasks		
1.17	Others (please specify)		
2. General objective			
2.1	Is the objective clearly specified in the report ?		
2.2	Assess the level of safety of the plant		
	2.2.1	To identify the most effective area(s) of improvement	
	2.2.2	To compare the level of safety with acceptance criteria, target values, etc.	
	2.2.3	To assist plant operation	
3. Specific objective			
3.1	Identification of dominant accident sequence		
3.2	Identification of items important to safety		
3.3	Identification of human actions important to safety		
3.4	Assessment of important dependence (s) (CCF)		
3.5	Identification and evaluation of new safety issues		
3.6	Analysis of severe accidents		
3.7	Decision on back fitting of generic items		
3.8	Decision on back fitting of plant specific items		
3.9	Design modifications		
3.10	Plant modifications		
3.11	Prioritisation of operational tasks		
	3.11.1	Surveillance	
	3.11.2	Testing activities	
	3.11.3	Configuration management, etc.	
3.12	Prioritisation of regulatory tasks		

TABLE 5.1 : CHECKLIST FOR REVIEW OF PSA RELATED STUDIES (CONTD.)

	3.12.1	Inspection, etc.	
3.13	Prioritisation of research studies		
3.14	Evaluation of plant technical specifications		
3.15	Evaluation of operating experience		
	3.15.1	Near misses	
	3.15.2	Extended outage of a component, etc.	
	3.15.3	Skipping a surveillance test	
3.16	Accident management		
3.17	Maintenance scheduling		
3.18	Obsolescence/replacement of ageing components		
3.19	Risk evaluation of critical components for continuing operation beyond its design life		
3.20	Risk evaluation of a repository		
3.21	Others (please specify)		
4. Scope of the PSA report			
4.1	Plant operational states considered		
	4.1.1	Full power operation	
	4.1.2	Low power operation	
	4.1.3	Intermediate power level operation	
	4.1.4	Reactor shutdown - hot stand-by	
	4.1.5	Reactor shutdown - cold stand-by	
	4.1.6	Others (please specify)	
4.2	Potential sources of radioactive releases considered		
	4.2.1	Reactor core	
	4.2.2	Spent fuel storage facility	
	4.2.3	Spent fuel handling facility	
	4.2.4	Radioactive waste storage facility	
	4.2.5	Others (please specify)	
4.3	Category of core damage identified		
	4.3.1	One final category (e.g. core damage involving pressure vessel breach for BWR, significant fuel failures in the core for PHWR, etc.)	
	4.3.2	Multiple category causing partial core damage. (For e.g., partial core damage involving fuel failures in a few channels, core damage involving pressure vessel breach)	
4.4.	Initiating events considered		
	4.4.1	Internal events	
		- Internal events including off-site power failure	
		- Internal events including internal flood	
		- Internal events including internal fire	
		- Internal events including internally generated missiles, etc.	
	4.4.2	External events	
		- Seismic hazard	

TABLE 5.1 : CHECKLIST FOR REVIEW OF PSA RELATED STUDIES (CONTD.)

	- Flood			
	- Fire			
	- Other external events (air craft crash, tornadoes, sabotage etc)			
4.5	Extent of analysis of special issues			
	4.5.1	Assessment of human error, identification, modelling, etc. used		
		4.5.1.1	Whether all kinds of human errors are considered, i.e. error of omission, error of commission, etc.	
		4.5.1.2	Whether conservative screening method used	
		4.5.1.3	Whether best estimate human error probabilities used	
		4.5.1.4	Whether operator and/or maintenance personnel error considered	
		4.5.1.5	Whether repair actions considered	
		4.5.1.6	Whether operator recovery considered	
		4.5.1.7	Any others (please specify)	
	4.5.2	Extent of dependence analysis (CCF)		
		4.5.2.1	Whether accident sequences were analysed to identify human error dependence	
		4.5.2.2	Whether explicit modelling of impacts of environmental conditions associated with specific IEs	
		4.5.2.3	Whether equipment dependence is explored through fault tree linking	
		4.5.2.4	Models used for CCF (e.g. Beta factor, MGL, shock model etc)	
	4.5.3	Release of radioactivity		
	4.5.4	Impact on occupational worker/public domain		
		4.5.4.1	Individual risk	
		4.5.4.2	Societal risk	
		4.5.4.3	Environmental risk	
	4.5.5	Uncertainty analysis		
	4.5.6	Sensitivity analysis		
	4.5.7	Importance (risk) measures		
	4.5.8	Time duration of analysis (mission times)		
		4.5.8.1	Whether mission times following each IEs mentioned	
		4.5.8.2	Whether the bases for mission times considered are appropriate (Consistent with technical specification, deterministic and accident analysis studies)	
5. Level 1 PSA				
5.1	System analysis			
	5.1.1	All PIEs and their frequency of occurrence considered with bounding cases in a systematic manner		
	5.1.2	All related system reliability/unavailability analysis carried out including computer based and shared systems		
	5.1.3	FT modelling and analysis		
		5.1.3.1	Human actions identified	

TABLE 5.1 : CHECKLIST FOR REVIEW OF PSA RELATED STUDIES (CONTD.)

		5.1.3.2	CCF	
		5.1.3.3	Software used for analysis	
	5.1.4	Event tree analysis		
		5.1.4.1	Modelling of accident progressions with success/failure criteria done.	
		5.1.4.2	Identification of plant damage states	
		5.1.4.3	Software used for analysis	
5.2	Failure data used for analysis (generic/plant specific)			
	5.2.1	At component level		
	5.2.2	Human error		
	5.2.3	C CF		
5.3	Adequacy/Acceptability of human error modelling/data			
5.4	Adequacy/Acceptability of CCF modelling/data			
5.5	Uncertainty analysis			
5.6	Rationality of assumptions made in modelling			
5.7	Adequacy of sensitivity studies			
5.8	Adequacy of importance risk measures			
6. Level 2 PSA studies				
6.1	Accident progressions modelled			
6.2	Codes used for core damage progression (e.g. reactor physics model, thermal hydraulics codes including system, sub-channel and porous media, computational fluid dynamics code, etc.)			
6.3	Source term analysis and code used			
6.4	Containment analysis (analysis and adequacy of structural code used)			
6.5	Software for accident progression in the core			
6.6	Software for radioactive release and retention from the containment			
6.7	Adequacy/Acceptability of human error modelling/data			
6.8	Adequacy/Acceptability of CCF modelling/data			
6.9	Uncertainty analysis			
6.10	Rationality of assumptions made in modelling			
6.11	Adequacy of sensitivity studies			
6.12	Adequacy of importance risk measures			
7. Level 3 PSA studies				
7.1	Atmospheric dispersion model for radioactivity transport to public domain and dose code used.			
7.2	Estimation of risk to public/individuals/environment			
7.3	Uncertainty analysis			
7.4	Rationality of assumptions made in modelling			
7.5	Adequacy of sensitivity studies			
7.6	Adequacy of importance risk measures			
8. Fire PSA				
8.1	Identification of interfaces with internal events			

TABLE 5.1 : CHECKLIST FOR REVIEW OF PSA RELATED STUDIES (CONTD.)

8.2	Data collection and processing		
8.3	Hazard analysis: identification of critical areas, screening method, establishing of frequency of occurrence		
8.4	Propagation analysis		
8.5	Plant system analysis		
8.6	Release frequency		
8.7	Models, software, verification and validation		
8.8	Uncertainty analysis		
9. Seismic PSA			
9.1	Hazard analysis		
	9.1.1	Establishing parameters and hazard analysis	
	9.1.2	Computer codes used	
9.2	Plant response analysis		
	9.2.1	Selection of components for fragility evaluation, methods used	
9.3	Plant system and event sequence analysis		
	9.3.1	Initiated events	
	9.3.2	Dependent failures	
	9.3.3	Simultaneous occurrence of external events	
	9.3.4	Quantification of system unavailabilities and ETs	
9.4	Consequence analysis		
10. Flood PSA			
10.1	Selection of PIE		
10.2	Parameter identification		
10.3	Flood hazard analysis		
10.4	Plant fragility evaluations		
10.5	Plant and system analysis		
10.6	Consequence analysis		
11. Other external events: (to be developed inline with item 9 above)			
12. Application oriented PSA studies			
12.1	Related PSA levels, target/acceptance criteria		
12.2	Modelling		
12.3	Assumptions, reference documents, softwares used		
12.4	Sensitivity, uncertainty studies etc.		
12.5	Others depending on application areas		
13. QA aspect of PSA			
13.1	13.1.1	QA programme description aspects • Policy statement • Mission and objectives • Users, clients and reviewers of the PSA	

TABLE 5.1 : CHECKLIST FOR REVIEW OF PSA RELATED STUDIES (CONTD.)

	13.1.2	Management aspects • Development, implementation and maintenance of QA program (methods, planning, scheduling, control, procedure, organisation, responsibilities, line of command, interfaces, etc) • Adequacy of staff, qualification of staff • Documentation and configuration control-adequacy (highlighting policy, objectives, management control, work implementation, task performances, etc.) • Non-conformance control and corrective action procedures- adequacy		
	13.1.3	Performance aspects: • Work process detailing, task flow structures adequacy • Selection of methods, extent of data used- satisfactory • Modelling- adequacy • Analysis done by the state-of-the-art methodology • Software used is state-of-the-art • Validity of assumptions made in modelling/analysis • Verification and Validation of codes/software used- adequacy • Standard criteria followed-acceptability		
	13.1.4	Assessment aspects • Measuring effectiveness of management processes • Adequacy of work performances • Audit (Peer Review) - by Internal agency - by External agency		
14. Regulatory review				
14.1	Involvement and review aspects			
	14.1.1	Composition of PSA production team		
	14.1.2	Composition of PSA review team		
	14.1.3	Participation of outside expertise • In production process • In review process		
	14.1.4	Process of review • On-line review • Off-line review		
	14.1.5	Extent of review • Limited • Extensive		
14.2	Assessment of results of PSA			
	14.2.1	Analysis results meet with:		
		14.2.1.1	Objectives	

TABLE 5.1 : CHECKLIST FOR REVIEW OF PSA RELATED STUDIES (CONTD.)

		14.2.1.2	Acceptance criteria • Basic acceptance criteria • Secondary acceptance criteria • Analysis acceptance criteria • Specific acceptance criteria for - AOT - STI - Critical component identification - Risk based modification - Dominant accident sequences - Others	
	14.2.2	Any other remarks to aid in regulatory decision making		
	14.2.3	Consideration of the target values • Unavailability of critical components • Safety system unavailability • CDF • Early release probability of radioactivity/hazardous material beyond plant boundary • Individual risk of fatality • Societal risk • Others		
14.3	Analysis is acceptable/(meets objectives, adequacy, further studies required, etc)			
14.4	Studies identified for research and development works			
14.5	Agency to carry out identified R&D work			
14.6	Time stipulation for submission of further studies as identified			
15. Name, Affiliation and Signature (with date) of Review Team Including Leader/Members				

APPENDIX-I

FORMAT OF DOCUMENTATION FOR PSA RELATED STUDIES PERFORMED

Objective of the documentation

The primary objective of the PSA documentation is to fulfil the requirements of its users and be suitable for review and the applications under consideration. The documentation of PSA should be well structured, clear and easy to follow, review and update. In addition, the document should provide means for possible extension of the analysis including integration of new topics, use of improved models, broadening of the scope of the PSA, and its uses for additional applications. Assumptions, exclusions and limitations of extending and interpreting the PSA should be explicitly presented. It is recommended that

- Uncertainties in the data and sensitivity analysis and important analysis be well documented.
- Conclusions are clearly brought out.

Documentation format

1. Cover sheet (title, year/date of transmittal, organisation name, etc.)
2. Preface
3. Table of contents
4. Summary report
5. Main report
    - 5.1 Introduction
    - 5.2 QA program in PSA
    - 5.3 Brief description of plant type and related systems
    - 5.4 IEs/hazards considered in the study
    - 5.5 Data used in the study
    - 5.6 Modelling
    - 5.7 Quantification of analysis
    - 5.8 Sensitivity, uncertainty and importance analysis
    - 5.9 Computer codes used - verification and validation
    - 5.10 Results and insights
    - 5.11 Conclusions and recommendations
    - 5.12 Audit/Peer reviews of PSA studies
6. Appendices/Annexures
7. Abbreviations
8. References
9. Bibliography

Summary report and main report for the level 1, level 2 and level 3 PSA studies are given below, as examples:

Summary Report

1. Introduction
2. Objective and scope of the study
3. Overview of the approach (methodology, computer codes, etc.)
4. Results of the analysis depending on the scope of the study

    4.1 Level 1 PSA

    - 4.1.1 System unavailabilities
    - 4.1.2 Accident sequence frequencies
    - 4.1.3 Core damage frequency
    - 4.1.4 Dominant contributors and ranking as necessary
    - 4.1.5 Uncertainty, importance and sensitivity analysis

    4.2 Level 2 PSA

    - 4.2.1 Containment failure modes
    - 4.2.2 Radiological source terms and their frequencies (cumulative and distribution functions)
    - 4.2.3 Uncertainty, Importance and sensitivity analysis

    4.3 Level 3 PSA

    - 4.3.1 Concentrations of important radionuclides at different locations and times
    - 4.3.2 Radiation doses
    - 4.3.3 Health effects
    - 4.3.4 Economic and social impacts
    - 4.3.5 Complementary cumulative distribution functions
    - 4.3.6 Uncertainty, importance and sensitivity analysis

5. Plant vulnerabilities to severe accidents, and interpretation of results
6. Conclusions and recommendations.
7. Organisation of the main report

Main Report for Level 1 PSA

1 Introduction

- 1.1 Background
- 1.2 Objectives and scope of the study
- 1.3 Project organisation and management
- 1.4 Composition of the study team
- 1.5 Overview of the approach (methodology, software used, etc.)
- 1.6 Structure of the report

2 QA program in PSA

2.1 Objective and scope

2.2 Project organisation, responsibilities and resources of units and individuals

2.3 Coordination among different organisations and groups

2.4 PSA production process

2.5 Peer reviews

3 Description of the plant systems

3.1 System function

3.2 Design basis

3.3 Test and maintenance

3.4 Technical specifications

3.5 Success/Failure criteria

3.6 Assumptions in the modelling

4 Identification of radioactive sources, accident initiators and plant response

4.1 Sources and conditions of radioactive release

4.2 Selection and screening of PIEs

4.3 Grouping of PIEs

4.4 Evaluations of hazard intensities, plant response and component fragility for external events

5. Accident sequence modelling

5.1 Event sequence modelling

5.2 System modelling

5.3 Human reliability modelling

5.4 Qualitative dependence modelling

5.5 Classification of plant damage stages

6. Data assessment and parameter estimation

6.1 IE data and frequencies

6.2 Component data and parameters

6.3 Human reliability data and parameters

6.4 CCF data and parameters

7. Accident sequence quantification

7.1 Quantification of system reliabilities

7.2 Quantification of accident sequences and over all CDF

7.3 Uncertainty, importance and sensitivity analysis

7.4 Computer codes used in the analysis

8. Display and interpretation of results

   8.1 Dominant contributors to CDF

   8.2 Results of uncertainty, importance and sensitivity analyses

   8.3 Interpretation of results and engineering insights

   8.4 Conclusions and recommendations

   8.5 Findings of peer review team

Appendices

- Data used in the analysis
- Plant logic diagrams, flow sheets, schematic diagrams, control circuit diagrams, etc.
- Detailed reliability analysis, event trees and quantification
- Basis for choice of different models (CCF, HRA, component failure modes)
- Detailed results of uncertainty, sensitivity and importance analyses
- Basis for uncertainty/sensitivity ranges
- Appendices and annexures, as applicable

Supporting documents to be submitted for review as required

(i) Design basis report

(ii) Design manuals

(iii) Safety analysis reports

(iv) Technical specifications

(v) Operating procedures for emergency conditions

(vi) Verification and validation of software

Main Report for Level 2 PSA

1. Introduction

   1.1 Background

   1.2 Objectives and scope of the study

   1.3 Project organisation and management

   1.4 Composition of the study team

   1.5 Overview of the approach

   1.6 Structure of the report

2. QA program in PSA

   2.1 Objective and scope

   2.2 Project organisation, responsibilities and resources of units and individuals

   2.3 Coordination among different organisations and groups

2.4 PSA production process

2.5 Peer reviews

3. Description of the design of the plant and the containment

3.1 Plant design features including containment and its ESFs mitigating severe accidents

3.2 Technical specifications and operating requirements

3.3 Description of plant and containment system modifications

4. Interface to level 1 PSA

4.1 Grouping of sequences with justifications

4.2 PDSs for internal initiators and uncertainties

4.3 PDSs for external initiators and uncertainties

4.4 PDSs for other power states and uncertainties

5. Analysis of the containment structural performance

5.1 Description of the structural design and failure modes of the containment

5.2 Structural response and fragility results

5.3 Fragility analysis for containment performance including uncertainty analysis

5.4 Evaluations of hazard intensities, plant response and component fragility for external events

6. Accident progression and containment analysis

6.1 Severe accident progression analysis

6.1.1 Scope of the analysis

6.1.2 Method of the analysis (codes, models etc.)

6.1.3 Summary of release into containment for analysed PDSs (estimates of quantity and probabilities)

6.2 Accident progression ETs/Containment ETs

6.2.1 APET/CET development using operating procedures and recovery actions

6.2.2 APET/CET quantification

6.2.3 Binning of APET/CET end states

6.2.4 Treatment of uncertainties

6.2.5 Results

7. Source term

7.1 Grouping of fission products

7.2 Method of analysis (codes, models, etc.)

7.3 Summary of point estimate results for analysed PDSs

7.4 Treatment of uncertainties

7.5 Results

8. Sensitivity and importance analyses

8.1 Identification of sensitivity issues

8.2 Results of sensitivity analysis

8.3 Importance ranking of issues

9. Conclusions

9.1 Key insights on severe accidents and containment response characteristics

9.2 Design features and inherent mitigatory benefits

9.3 Conclusions relative to PSA objectives

9.4 Recommendations

Appendices

- Detailed containment structural fragility evaluations.
- Detailed APET/CET and reliability analysis and quantification
- Results of deterministic severe accident analyses
- Basis for choice of different models used in the analysis
- Detailed results of uncertainty/sensitivity analysis
- Basis for uncertainty/sensitivity ranges
- Appendices and annexures, as applicable

Supporting documents to be submitted for review as required

(i) Design basis report

(ii) Severe accident analysis reports

(iii) Technical specifications

(iv) Operating procedures for emergency conditions

(v) Verification and validation of software

Main Report for Level 3 PSA

1. Introduction

1.1 Background

1.2 Objectives and scope of the study

1.3 Project organisation and management

1.4 Composition of the study team

1.5 Overview of the approach

1.6 Structure of the report

2. QA program in PSA

2.1 Objective and scope

2.2 Project organisation, responsibilities and resources of units and individuals

2.3 Coordination among different organisation and groups

2.4 PSA production process

2.5 Peer reviews

3. General aspects of level 3 PSA

3.1 Description of the radionuclide release and source term

3.2 Atmospheric dispersion and deposition

3.3 Meteorological data and its sampling

3.4 Exposure pathways and dose assessment

3.5 Population, agricultural and economic data

3.6 Countermeasures (short term and long term)

3.7 Health effects

3.8 Economic and social consequences

4. Description of the consequence analysis

4.1 Brief description of the code

4.2 Input data

4.3 Computational models and parameters

5. Display and interpretation of results

5.1 Results of the analysis

5.2 Results of uncertainty and sensitivity analysis

5.3 Interpretation of results and engineering insights

5.4 Conclusions and recommendations

Appendices

- Basis for selection of the probabilistic consequence code
- Basis for data used in the analysis
- Basis for uncertainty/sensitivity distributions/ranges
- Basis for choice of various models used in the analysis
- Appendices and Annexures, as applicable

Supporting documents to be submitted for review as required

(i) Reports on meteorological, population, agriculture and economic data

(ii) Off-site Emergency plan

(iii) Verification and validation of software/computer codes

APPENDIX-II

COMPUTER CODES FOR PSA STUDIES

Various features of the computer codes used for different levels of PSA (i.e. Level-1, Level-2 and Level-3) are described here for information. Analysts can choose any computer code from this list or in-house developed computer code for the PSA study. However, suitable verification and validation of the computer code should be performed as per QA requirement.

II-1 Level 1 PSA Computer Codes

TABLE II-1 : LEVEL 1 PSA COMPUTER CODES [70]

Code	Analysis	Brief Description	Computer type	Availability Source
IRRAS	PSA study and update 'LPSA'	Integrated reliability and risk assessment tool to build, modify, text edit, FT linkage and quantification, importance and uncertainty analysis (Monte Carlo)	PC single user	EG & G Idaho, USA USNRC
PSA PACK	PSA study, training and decision making	PSA package, menu driven interactive system. FT/ET construction and quantification, MCSs (30000) editing and quantification, uncertainty (Monte Carlo) and importance analysis, includes reliability data base for failure rates	PC/AT single user	IAEA
PNC code network (QUEST)	PSA study and update, decision making	PSA code network including IE identification and quantification, FT/ET construction and quantification, SETS code FT analysis, drawing, modularisation, importance and uncertainty	PC	PNC Japan
RISA	FT time dependent uncertainty, importance	Integrated PSA package, unlimited gates and events, no formal limits on MCSs, modularises trees and demodularises the cutsets, graphical FT/ET editing and plotting interface with a component failure data base. FT/ET integration.	CDC, VAX, SUN, PC-DOS, PC-EXT.DOS	Inst. for Process Technology Tech. Univ. Berlin, FRG
SAIC package	PSA study and risk oriented decision making	Fully integrated PC based workstation for PSA FT/ET construction, FT linking and reduction, MCS equation editing and quantification	PC	SAIC USA (commercial)
Fault tree+ V9.0	PSA study	Integrated package for PSA, Markov models can also be linked in FT/ETs, CCF analysis, importance, uncertainty and sensitivity analyses, efficient MCS algorithm, graphs, plots, pie charts and time profile histograms	MS windows 95/98 and windows NT	ISOGRAPH, UK

TABLE II-1 : LEVEL 1 PSA COMPUTER CODES [70] (CONTD.)

Code	Analysis	Brief Description	Computer type	Availability Source
Risk spectrum PSA professional	PSA study (level 1 and 2) and 'LPSA'	Integrated PSA package, graphical FT/ET editors, standard windows help system, multiple document interface, powerful functions of editing, copying , renaming, searching, replacing, sorting, and extracting all kinds of data, house events and exchange events for complex variations of the base model, different CCF models, uncertainty, importance, sensitivity and time-dependent analyses, fast MCS algorithm, high quality report generator for printing	PC, single user, windows based, user friendly	Relcon AB, sweden

II-2 Level 2 PSA Computer Codes Used for Severe Accidents

The codes that model the phenomena of severe accidents can be divided into three types according to their capabilities and intended use, viz., mechanistic codes, PSA codes and simple parametric codes. Mechanistic codes (e.g. SCADAP-RELAP-5, CONTAIN) attempt to model the phenomena in as much detail as possible, without regard for how long the code takes to run. Generally these codes are multipurpose finite element codes for structural, dynamics and/or static analysis. The codes can usually model both local (e.g. crack propagation) and global responses of the loaded structure. In contrast PSA codes (e.g. MAAP) are designed to run fast, so that these can calculate many sequences (and a number of times for a single sequence if uncertainty analyses are required). For example in the mechanistic codes a numerical solution is found for the integral differential equation for aerosol agglomeration and deposition, giving the aerosol size distribution at each time step. In contrast, the MAAP code for PSA application uses a correlation approach for aerosol behaviour. There are so called simple parametric codes based on simple parametric models intended for specific PSA application, such as estimation of radioactivity release from containment, where more runs are needed than can be reasonably handled even by PSA code. Table II-2 lists out some mechanistic and PSA codes of international repute. This section provides a brief description of some specific codes, currently in use for Level 2 PSAs.

TABLE II-2 : SEVERE ACCIDENT COMPUTER CODES

Country	Computer Codes	In-Vessel Phenomena				
		Thermal hydraulics	Core melt progression	Release from fuel	Transport in RCS	Vessel Failure
USA	MELCOR	+	+	+	+	+
	MAAP	+	+	+	+	+
	SCDAP - RELAP 5	+	+	+	+	+
	STCP	+	+	+	+	+
France	ESCADRE	+	+	+	+	+
	CATHERE - CARE	+	+	+	+	+
Japan	THALES	+	+			+
	ART			+	+	
	THALES - 2	+	+	+	+	+
Germany	ATHLET - CD	+	+	+	+	+
EC	ESTER 1.0	+	+	+	+	

TABLE II-2 : SEVERE ACCIDENT COMPUTER CODES (CONTD.)

Country	Computer Codes	Ex-Vessel Phenomena					
		HP melt injection	Core concrete interaction	FP release from debris	FP transport in containment	Hydrogen combustion	Containment response/loads
USA	MELCOR	+	+	+	+	+	+
	MAAP	+	+	+	+	+	+
	CONTGAIN		+	+	+	+	+
	STCP	+	+	+	+	+	+
France	ESCADRE	+	+		+		+
Japan	THALES		+			+	+
	ART	+		+	+		+
	THALES - 2		+	+	+	+	+
Germany	COCOSYS	+	+	+	+	+	+
EC	ESTER 1.0		+	+		+	

II-2.1 WASH-1400 Computer Codes, NRC_BMI Code

The first generation source term computer codes that became available with the RSS in 1975, essentially included ORIGEN, to calculate the reactor core inventories; MARCH, to compute the thermal-hydraulics in the HT system and the containment and CORRAL to perform the aerosol removal calculations in the containment. The radioactivity transport in the HT system was not modelled. The computer codes were only loosely coupled. NRC-BMI Code, the second-generation source term code suite was developed, in the early 1980s, in the Battelle Memorial Institute, and appeared as BMI-2104 essentially in response to the TMI-2 accident. These codes were subsequently revised and accepted by the USNRC, and are now known as STCP. The bulk of the calculations in the Source Term Code Package (STPC) are done in ORIGEN2/ MARCH3/ TRAPMELT2/ NAUA codes. The third generation codes currently under development in the US include MELPROG/ TRAC/ VICTORIA/ CONTAIN; these follow a fully integrated approach to thermal hydraulics and radioactivity calculations

II-2.2 Source Term Code Package (STCP) [71]

Accidents modelled with the STCP include small- and large-break LOCAs, transients with loss of AC power, ATWS, and loss of make-up water, heat removal, and ECCS. The STCP is a linked set of modules that comprises the codes MARCH3, ORIGEN2, CORSOR, TRAPMELT3, NAUA MOD5, VANESA, SPARC and ICEDF.

(i) MARCH3 : It models thermal hydraulic behaviour (overall behaviour of reactor coolant system, molten core and containment). It is a combination of MARCH 2 thermal hydraulic code, CORCON/MOD2 core-concrete reaction and CORSOR - M for in-vessel fission product release from overheated fuel.

(ii) ORIGEN2 : It is not a part of the STCP suite, but is required for the computation of the radioactivity in the reactor core. There are several computer codes capable of performing this function, ORIGEN2 is commonly used among these.

ORIGEN2 calculations use a database, which comprises of three types of data, viz., (i) radioactive decay (radionuclide half-lives and branching fractions), (ii) photon energies per decay and (iii) cross-sections for neutron absorption including FP yields for the fissionable species.

The user supplies the code with the reactor type, the fuel inventory, and the average specific power in the core (or neutron flux). The code outputs include radioactivity, mass, fractional isotopic composition, thermal power, toxicity, neutron absorption and fission rates, neutron and photon emission rates, and total heat. The code can output 700 activation products, 880 fission products and 132 actinides (total <1676 radionuclides).

The accuracy of the radionuclide inventory output by ORIGEN2 is poor; the uncertainty in the results is about ± 30% under ideal conditions for individual isotope concentrations. The calculated decay power curve of LWRs matches reasonably well with the ANSI-ANS-5.1 (1979) curve from one minute to several months.

(iii) CORSOR : It is for calculating release of fission products from the fuel. In addition to the temperature profile of the core as obtained from a thermal hydraulic code, the user of the CORSOR code has to provide the inputs like the number of axial and radial nodes, the inventories of the various core materials, the radial and axial power peaking factors, the volume distribution factors for the annuli, the release model (default/modified) to be used in calculations, the time steps to be used and the degree of detail desired in output.

The main output from the code is the cumulative amount of material released up to a given time into the heatup transient. The release curve is subsequently reduced by piecewise linearisation into a table of time vs. release rate, which is the input for TRAPMELT.

Limitations of CORSOR

- it is a purely empirical release model, strictly applicable only to the high burn-up LWR fuel to which the default data corresponds;
- the effect of fuel burn-up, power history, etc., is not explicitly available;
- the effect of change of geometry of fuel during heat-up is not considered; the code is not applicable for melt releases;
- the effect of chemical environment and interactions among the species released is considered only to a limited extent (the application is limited to tellurium);
- the effect of UO_2 oxidation, leading to hyper-stoichiometric UO_{2+x}, in which the volatile atom mobility is considerably higher, is not explicitly considered;
- the possible effects of gas flow rates, system pressures, etc. on FP release are not included;
- the effect of radio-active half-life is not reflected in the composition of the released materials;
- the initial burst release observed in release experiments is not modelled;
- the burst release expected during the re-wetted stage of the LOC transient is not modelled.

(iv) TRAPMELT3 : It is a combination of MERGE code and TRAPMELT2. MERGE provides more detailed flow rates and temperatures in the RCS and TRAPMELT calculates the FP transport and deposition in RCS.

The TRAPMELT3 computer code calculates the radionuclide transport through, and retention in, the primary coolant system under severe conditions in Light Water Reactors. The thermal-hydraulic conditions are provided by the MERGE code, while the transport and deposition models are provided by TRAPMELT.

TRAPMELT3 requires as input extensive thermal-hydraulic data such as steam mass flow rates, steam and surface temperature, steam qualities, pressures, etc. as a function of time. It also needs source data (from CORSOR) in the form of mass rates by species, phase and location.

TRAPMELT3 determines particle number, median size and logarithmic variance of the mass for each location and each control volume at the end of each time step.

Limitations of TRAPMELT3

The code contains a number of approximations, which compromise its accuracy. These are as follows.

- It considers only steam in the carrier gas, ignoring hydrogen, which has a considerably different kinematic viscosity. TRAPMELT3 violates the well-mixed assumption and the validity of several rate equations governing aerosol behaviour.
- Re-evaporation is neglected.

(v) NAUA MOD5 : It is advanced multi-compartment aerosol behaviour analysis code [72] for use in reactor containments (BWR) following core melt accidents (LWR). The version used in STCP was NAUA MOD4, which was further modified, essentially to study FP aerosol transport and removal in the containment following a core meltdown accident in a LWR. The code has a strong experimental base.

NAUA can be applied with equal ease to both dry and condensing steam atmospheres. NAUA requires as input containment dimensions, shape factors for different processes, information on the number of particle size classes and the lower and upper particle size limits, aerosol processes to be included in the run, aerosol and steam source rate, mean aerosol size and gsd for each release phase, and leakage rate from the closed volume. NAUA generates as output at each time step, the amount of steam and aerosol removed by each removal mechanism, the amount and characteristics of the aerosol remaining air-borne, and that leaked out from the containment.

Some of the aerosol phenomena not included in NAUA are: turbulent agglomeration, thermo-phoresis, electrostatic effects and re-suspension. The limitations of NAUA are as follows.

- Only physical processes are calculated; chemical effects cannot be included.

  In NAUA, FP materials, such as iodine, whose behaviour is strongly controlled by its chemistry cannot be directly modelled. Similarly, soluble aerosol materials cannot be handled. Furthermore, only the natural aerosol phenomena are handled by the NAUA code. Code modification would be required if aerosol is removed by containment ESFs such as containment sprays, particulate/iodine filters, coolers, and suppression pools. NAUA does not have an integral containment thermal-hydraulics model.
- NAUA MOD4 excludes thermo-phoresis, and turbulent diffusion.
- The code requires input values for the steam deposited on suspended aerosol mass.
- NAUA is basically a single-component code, and treats only water as a separate constituent in the co-agglomerated aerosol mass.

(vi) VANESA : It calculates the ex-vessel fission product release and aerosol generation from the core concrete interaction. VANESA code (in conjunction with the thermal-hydraulic code CORCON) provides a mechanistic model for the release of aerosol, which escapes during the core-concrete interaction.

The VANESA code requires as input the melt temperatures, composition of melt, chemical composition of concrete, gas generation rate (CO_2 and steam) and other inputs supplied from CORCON. It contains a library of thermodynamic properties for about 125 chemical species (mostly elements, oxides and hydroxides) from which vapour pressures of the species can be calculated. The code outputs include essentially the rate of ex-vessel aerosol formation, and the mass composition and mean particle size of the materials liberated as particles.

Limitations of VANESA

The main omission from the code is the effect of an overlying water mass, with potential crust formation on the melt, together with the scrubbing of the released mass in the pool. Also, the presence of chlorides, fluorides and sulfides in the melt is not considered, which could lead to higher escape rates from the melt.

(vii) Suppression Pool Aerosol Removal Code (SPARC) [73] : It models the scrubbing of the vent gases bubbling through the suppression pool. SPARC focuses on the aerosol removal processes that are related to gas bubble transit through the suppression pool. These processes include sedimentation, inertial deposition, diffusion, and diffusio-phoresis. The effects of jet impingement on the water surface and the discharge of contaminated water into the air space, as the bubbles burst at the pool surface are modelled. The scrubbing efficiency depends on particle size, pool depth, steam quality, and the pool temperature. Higher Decontamination Factors (DFs) are obtained with small, oblate bubbles saturated with steam, in colder and deeper pools. SPARC accepts as input the size and shape of the rising bubbles, the temperature and depth of the pool, the characteristics of the carrier gas and the aerosol parameters. The code outputs include the pool-scrubbing factor, the characteristics of the aerosol discharged into the air space, and the resultant pool temperature.

Limitations of SPARC

SPARC does not calculate the iodine-scrubbing factor. A comparison of SPARC with other suppression pool scrubbing codes indicates that it under-predicts DFs by a factor of 2-4.

(viii) ICEDF : It models aerosol behaviour in ice containment (PWR)

It is now being superseded by the more advanced integrated code MELCOR, which addresses the weaknesses of the STCP, such as (i) inadequate or inconsistent modelling of the important phenomena or plant features, (ii) inability to address sensitivities or uncertainties, (iii) an inflexible structure that does not facilitate introduction of new models or improvements in the existing ones and (iv) interfaces between code modules that do not take into feedback effects.

II-2.3 MELCOR [74]

MELCOR (Version 1.8.5, October 2000.) is a fully integrated, relatively fast-running code that models the progression of accidents in LWRs. The MELCOR code includes following.

- Thermal-hydraulic response of the primary coolant system, the reactor cavity, the containment and the confinement structures;
- Core uncovery, fuel heat-up, cladding oxidation, fuel degradation, and core material melting and relocation;
- Heat-up of RPV lower head due to relocated fuel materials, the thermal and mechanical loading and failure of the lower head, and transfer of core materials to the reactor vessel cavity;
- Core-concrete interaction and the ensuing aerosol generation;
- Forming of non-condensable gases, combustion gases and direct containment heating (DCH-heat transfer from high pressure melt ejection and thus reaction in containment in severe accidents)
- In-vessel and ex-vessel hydrogen generation, transport and combustion;
- FP release, transport and deposition;
- Behaviour of radioactive aerosols in the containment building, including scrubbing in water pools and containment behaviour in the containment, and
- Impact of ESFs on thermal-hydraulics and radionuclide behaviour.

MELCOR facilitates sensitivity and uncertainty analyses through the use of sensitivity coefficients. The new MELCOR models include: an iodine chemistry model, a passive autocatalytic recombiner model, many improvements to the core degradation modelling, updates to several of the code default values, and improvements to the hygroscopic aerosol model. Core re-flood modelling is in progress.

II-2.4 Modular Accident Analysis Program (MAAP) [9]

The Electric Power Research Institute's (EPRI's) Modular Accident Analysis Program (MAAP3.0B), developed as a PSA tool, is a fully integrated code that couples thermal-hydraulics with FP release and transport. It has been used for most of the US individual plant examination programmes. It analyses the accident progression from a set of IEs either to a safe, stable and coolable state, or to structural failure of the containment and radioactive release to the environment. The design intent for this code for PSA application results in major differences in modelling assumptions, in comparison with the mechanistic codes. For example, the debris pool in core-concrete interaction is modelled as a homogenous molten debris pool, in contrast with the mechanistic code representation of a stratified pool which requires more complex modelling of under layer heat transfer.

MAAP uses a control volume and flow path approach in which the geometry of the control volumes (called regions) is pre-specified and different for a PWR and a BWR. The primary system is divided into region; upper and lower plenum, reactor core and down-comer; and for PWRs, cold and hot legs, and steam generator loops. Separate mass and energy conservation equations are solved for each of the regions. The PWR containment is divided into regions; upper and lower compartment, cavity, annular compartment, pressuriser relief tank, pressuriser, possibly two extra compartments for an ice condenser, and primary system. The containment is divided into two regions; reactor pedestal cavity, dry well, wet well, possibly an upper and a lower containment compartment, and primary system. The equations are lumped parameter, non-linear, first order, coupled, and ordinary differential equations. The core is divided into concentric radial rings and axial segments. MAAP uses a single core relocation model. Features are included in the code such that limited sensitivity studies can be carried out on the core melt behaviour and hydrogen generation. With regard to hydrogen combustion, MAAP does not distinguish between flame ignition and flame propagation. The incomplete burning model is one-dimensional. MAAP models the transport and retention of FPs. The materials released from the core are divided into 6 groups. The FP states modelled are: vapour, aerosol, and deposited and contained in-core or molten core material. Re-vaporisation is included as a transfer between the states. The retention rate is calculated using a correlation, which is a function of the aerosol concentration. Agglomeration of aerosols is calculated using a correlation derived from experiments.

An updated version MAAP 4, apart from general modelling enhancement, is designed, to evaluate potential accident actions, and also for applications in ALWR studies.

II-2.5 THALES/ART [9]

The THALES/ART codes developed by JAERI consist of THALES for severe accident thermal-hydraulics and ART for PFP release and transport. The package analyses the accident progression from a set of PIEs to the ultimate containment failure and radioactive release to the environment, with sensitivity analyses on source terms, accident mitigation analysis and Level 2 PSAs. Separate versions are available for PWRs and BWRs. In its hydrogen combustion modelling, THALES does not distinguish between flame ignition and flame propagation. Burning occurs only in the compartments where ignition conditions are reached and global burning is assumed to occur. The THALES core-concrete model is one-dimensional. ART uses the same control volumes as THALES and models the transport and retention of FPs.

THALES2 is the second version of the THALES/ART code package, which takes into account the feedback effect of FP behaviour on thermal-hydraulics and FP re-vaporisation.

II-2.6 CONTRAN

Containment transient analysis code for pressure and temperature transients in the containment following LOCA and MSLB, (BARC, INDIA) [75].

II-2.7 HYRECAT

For the analysis of hydrogen mitigation phenomena in the containment using catalytic recombiners, (BARC, INDIA) [76].

II-2.8 Mechanistic Code for Containment Response:

DYNA3D, ABAQUS, NASTRAN, etc.

II-3 Level 3 PSA Codes for Probabilistic Consequence Analysis [77,78]

The first accident consequence analysis code developed is CRAC during the Reactor Safety Study in 1975. Since then a number of complex packages have been generated, such as ARANO (NEL, Finland, 1977), CRAC2 (USNRC, 1982), CONDOR (NRPB, 1984), MACCS2 (USNRC, 1990), LENA (SRPI, Sweden, 1993), MECA (PUM, Spain, 1993), COSYMA (KfK & NRPB, 1995).

II-3.1 CRAC2

CRAC2 is a revision of the CRAC (Calculation of reactor accident consequences) program. It estimates reactor accident consequences. CRAC2 requires an inventory of radioisotopes released from the reactor containment to the environment and a description of the accident conditions as input. It (1) models the meteorological dispersion of the cloud of radioactive material, (2) determines the health effects of the material upon the surrounding population, and (3) estimates the costs to the public from the accident. CRAC2 samples specific meteorological conditions from a set of representative reactor locations and probabilistically combines the results to form frequency distributions of consequence from a reactor accident. It requires detailed meteorological, population, economic, and health data. In addition, CRAC2 models emergency planning procedures, such as evacuation. Detailed parametric and sensitivity studies can be simply accomplished in one computer run. Data utilised by some of the models have been upgraded; (1) latent cancer fatality risk factors have been changed to reflect the lifetime risk of latent cancer from radiation exposure, and (2) economic data have been upgraded to reflect 1980 economic statistics for the United States.

II-3.2 CONDOR

CONDOR is a joint venture of the then United Kingdom Atomic Energy Authority (UKAEA), the Central Electricity Generating Board and NRPB. CONDOR estimates the consequences of hypothetical accidental releases of radionuclides to the atmosphere allowing for the range of atmospheric conditions. It considers the impact, both on the population, in terms of doses and health effects, and on the foodstuffs.

As inputs, the code requires size, type and timing of the released activity, locations of the release together with information on the population and agricultural products grown in the surrounding area, subsequent distribution of the foodstuffs to other locations, and mitigating actions required to reduce exposure of the population (countermeasures). e.g., evacuation of sections of the population, banning foodstuffs based on location or predicted dose/activity levels, and meteorological conditions under which the released material will travel, through the atmosphere.

CONDOR outputs several indicators of consequences of the release, which include spatial and temporal distribution of activity levels or individual doses, collective doses to the population as a whole, numbers of people affected by the following countermeasures : Evacuation, sheltering, relocation, taking of stable iodine tablets, individual decontamination, areas of land interdicted or decontaminated, quantities of foodstuffs banned, number of cases of individual types of health effect in current and future generations e.g. early deaths or injuries, fatal and non-fatal cancers and hereditary effects, and individual risks of being affected by a particular countermeasure or of contracting a particular health effect.

II-3.3 MACCS2

MACCS2 is a major enhancement of the previous MACCS 1.5.11 package. The principal phenomena considered in MACCS are atmospheric transport, mitigative actions based on dose projection, dose accumulation by a number of pathways including food and water ingestion, early and latent health effects, and economic costs. MACCS can also do sensitivity studies and cost benefit analysis.

A MACCS calculation consists of three phases: input processing and validation, phenomenological modelling and output processing. The phenomenological models are based mostly on empirical data, and the solutions they entail are usually analytical in nature and computationally straightforward. The modelling phase is subdivided into three modules. ATMOS treats atmospheric transport and dispersion of material and its deposition from the air utilising a Gaussian plume model with Pasquill-Gifford dispersion parameters. EARLY models consequences of the accident to the surrounding area during an emergency action period. CHRONC considers the long term impact in the period subsequent to the emergency action period. The atmospheric model included in the code does not model the impact of terrain effects on atmospheric dispersion. The code also does not model dispersion close to the source (less than 100 meters from the source) or long range dispersion. The economic model included in the code models only the economic cost of mitigative actions.

II-3.4 COSYMA

The probabilistic Accident Consequence Assessment (ACA) code COSYMA was principally developed by FZK and NRPB but with significant inputs from a number of other contractors within the EC MARIA (Methods for Assessing the Radiological Impact of Accidents) research programme.

The endpoints calculated by the code are:

- air concentration and deposition at specific locations and as a function of distance from the site,
- numbers of people and areas affected by countermeasures, and their time integrals,
- amounts of food banned,
- the duration of countermeasures at particular locations,
- the probability of implementing countermeasures, both at specific locations and as a function of distance from the site,
- doses received in selected time periods, both at specific locations and as a function of distance from the site,
- the individual risk of early and late fatal and non-fatal health effects, both at specific locations and as a function of distance from the site,
- the numbers of early and late fatal and non-fatal health effects, and
- the economic costs of the off site consequences of an accident.

COSYMA can be used for deterministic or probabilistic assessments. Deterministic assessments give detailed results for a release in a single set of atmospheric conditions; probabilistic assessments give results taking account of the full range of atmospheric conditions that may be experienced and their respective frequencies of occurrence. The input is menu driven, and sub-divided according to the steps of an ACA calculation. The user must provide information on the characteristics of the released material, the location where the release occurs, details of the countermeasure strategy adopted, and the endpoints required. The user may also change the values of some of the parameters used in the models. Default values are provided for all parameters. The system includes data libraries for many of the quantities required, such as dose per unit intake or food chain concentrations per unit deposit. Gridded population and agricultural data for the whole of Europe, and two example sets of atmospheric conditions, are also provided. Detailed information on the population distribution near the site and on site-specific atmospheric conditions can be included by the user if available. The major features of the PCA codes are shown in Table II-3.

TABLE II-3 : MAJOR FEATURES OF THE CONSEQUENCE LEVEL-3 PSA CODES INVOLVED IN THE OECD/NEA-EUROPEAN COMMISSION CODE COMPARISON EXERCISE

Features	PCA codes					
	ARANO Finland	CONDOR United Kingdom	COSYMA Germany	LENA Sweden	MACCS USA	OCCAAR Japan
Atmospheric dispersion						
Gaussian plume	√	√	√	√	√	–
Trajectory	–	–	√	√	–	√
Time variant	–	√	√	–	√	√
Disposition						
Dry	√	√	√	–	√	√
Wet	√	√	√	√	√	√
Meteorological sample						
Stratified	–	√	√	√	√	√
Other	√	√	√	√	√	√
Exposure pathways						
Cloud shine	√	√	√	√	√	√
Ground shine	√	√	√	√	√	√
Skin	–	√	√	√	√	–
Inhalation	√	√	√	√	√	√
Re-suspension	–	√	√	√	√	√
Ingestion	√	√	√	–	√	√
Countermeasures						
Sheltering	√	√	√	√	√	√
Thyroid blocking	√	√	√	√	–	–
Evacuation	√	√	√	√	√	√
Relocation	√	√	√	√	√	√
Food ban	√	√	√	√	√	√
Health effects						
Early	√	√	√	–	√	√
Late	√	√	√	√	√	√
Economic consequences						
	√	√	√	√	√	–

APPENDIX-III

COMMON CAUSE FAILURE ANALYSIS

III-1 Introduction

This section presents a brief description of various common cause failure models available and a systematic procedural framework for CCF analysis. CCFs are a subset of dependent events in which two or more component fault states exist at the same time, or in a short time interval, and are a direct result of a shared cause. From a probabilistic point of view, the importance of common cause failures is that their existence implies that two or more components are not probabilistically independent and P(A and B) > P(A) P(B) for two events A and B. CCFs are classified as due to design, construction, procedural and environmental causes. These can be further sub-divided as due to functional deficiencies, realization faults, manufacturing, installation, test and maintenance, operation, human error, normal extremes and energetic extremes. The predominant causes are design (30-50%) operation and maintenance errors (30%), and remaining due to normal and extreme environmental causes (30%).

Multiple failure of events, for which a clear cause-effect relationship can be identified should be explicitly modelled in the system model. This applies to multiple failures caused by internal equipment failures and multiple failures due to clearly identifiable human errors. Multiple failures for which no clear root cause event can be identified, can be modelled using implicit methods such as parametric models. The analyst should decide based on experience and judgement, taking into consideration the aim and scope of analysis, which of the two approaches should be chosen.

III-2 Procedural Framework of CCF Analysis [79]

The procedure for the CCF analysis is divided into three phases; (I) Screening Analysis (II) Detailed Qualitative Analysis and (III) Detailed Quantitative Analysis

Phase 1 - Screening Analysis	
Steps	
1.1	Plant familiarisation, problem definition and system modelling
1.2	Preliminary analysis of CCF vulnerability
1.2.1	Qualitative screening
1.2.2	Quantitative screening
Phase 2 - Detailed Qualitative Analysis	
Steps	
2.1	Review of operating experience
2.2	Development of root cause-defence matrices
Phase 3 - Detailed Quantitative Analysis	
Steps	
3.1	Selection of probability models for common cause basic events
3.2	Data analysis
3.3	Parameter estimation
3.4	Quantification
3.5	Sensitivity analysis
3.6	Reporting

III-2.1 Plant Familiarisation, Problem Definition and System Modelling

In this stage FT models of the various systems are developed considering system success criteria, TS limitations, detailed plant design and operating practices.

III-2.2 Preliminary Analysis of CCF Vulnerability

The objectives of this stage are to identify the groups of systems components to be included in or eliminated from the CCF analysis, and to prioritise the groups of system components identified for further analysis, so that time and resources can be best allocated during the CCF analysis. These objectives are accomplished through the qualitative and quantitative screening steps.

III-2.2.1 Qualitative Analysis

In this step, a search is made for common attributes of components and mechanisms of failure that can lead to common cause events. Past experience and understanding of the engineering environment are used to identify signs of potential dependence among redundant components. The analyst should focus on identifying those components of the system, which share one or more of the attributes, such as same design, same hardware, same function, same installation, maintenance, or operation staff, same producers, same location and same environment.

An effective qualitative analysis for CCF should review detailed plant design and operating practices and identify defences built in plant. The defences such as ‘diversity’ (functional, equipment and staff), ‘barriers’ (spatial separation, physical protection, interlocks, removal, or introduction of administrative control, cross ties), ‘testing and maintenance’ (staggered) and ‘additional redundancy’ (in the context of limiting the size of Common Cause Component Group (CCCG) or providing operational diversity), can eliminate or reduce the coupling among component failures.

A systematic and automated method for identifying plant vulnerabilities to dependent failures is known as the generic approach. According to this approach the generic causes are divided into two groups; generic environment such as humidity and temperature, and common links such as maintenance and manufacturer. Tables III-1, III-2 and III-3 provide a list of some location-dependent generic environments and Table III-4 contains some possible common links other than location, which help in identifying sources of dependency.

TABLE III-1 : ELECTRICAL OR RADIATION GENERIC ENVIRONMENTS

Generic Cause	Example Sources
Electromagnetic	Welding equipment, rotating electrical machinery, lightning interfaces, power supplies, transmission lines
Radiation damage	Neutron sources, charged particle radiation, gamma radiation
Conducting medium	Moisture, conductive gases
Out-of-tolerance	Power surge voltage, short circuit, power surge current

TABLE III-2 : MECHANICAL OR THERMAL GENERIC ENVIRONMENT

Generic Cause	Example Sources
Temperature	Fire, lightning, welding equipment, cooling system faults, electrical short circuit
Grit	Airborne dust, metal fragments generated by moving parts with inadequate tolerances, crystallised boric acid from chemical control system
Impact	Pipe whip, water hammer, missiles, earthquakes, structural failure
Vibration	Machinery in motion, earthquake
Pressure	Explosion, out-of-tolerances system changes (pump over speed, flow blockage)
Humidity	Steam pipe breaks
Moisture	Condensation, pipe rupture, rainwater
Stress	Thermal stress at welds of dissimilar metals, thermal stresses and bending moments caused by high conductivity and density of liquid sodium
Freezing	Liquid sodium solidifying, water freezing

TABLE III-3 : CHEMICAL OR MISCELLANEOUS GENERIC CAUSES

Generic Cause	Example Sources
Corrosion (acid)	Boric acid from neutron control system, acid used in maintenance for removing rust and cleaning
Corrosion (oxidation)	A water medium or around high temperature metals (for example, filaments)
Other chemical reactions	Galvanic corrosion; complex interactions of fuel cladding, water, oxide fuel, and fission products; leaching of carbon from stainless steel by sodium
Carbonisation	Hydrocarbon (hydraulic fluid, lubricating oils, diesel fuel) in liquid sodium
Biological	Poisonous gases, explosions, missile hazards

TABLE III-4 : COMMON LINKS RESULTING IN DEPENDENCIES AMONG COMPONENTS

Common Links	Example Sources
Energy source	Common drive shaft, power supply
Calibration	Misprinted calibration instruction
Installation	Same subcontractor or crew contractor
Maintenance	Incorrect procedure, inadequately trained personnel
Operations	Overstressed or disabled operator, faulty operating procedures
Proximity	Location of all components of a cut set in one cabinet (common location exposes all of the components to many unspecified common causes)
Test procedure	Faulty test procedures which may affect all components normally tested together
Energy flow paths	Location in same hydraulic loop, location in same electrical circuit

III-2.2.2 Quantitative Screening

In this step, a conservative value is assigned to the probability of each basic event in the system FT, including the independent as well as the CCF events. For this beta factor model is used, which provides a conservative approximation to CCF frequencies regardless of the number of redundant components in the CCF group. The system unavailability is evaluated using conservative values and the dominant contributors to the system unavailability are identified. These dominant contributors will be emphasised in Phases 2 and 3.

III-2.3 Review of Operating Experience

This step enables the analyst to develop insights regarding the failure causes and mechanisms, and more importantly root cause of such failure mechanisms relating to the physical and operational characteristics of SSCs, maintenance program, training of personnel, quality control and several others.

III-2.4 Development of Cause-defence and Coupling Factor-defence Matrices

An effective way to present the results of a detailed qualitative analysis is the so-called cause-defence matrix. In developing a plant-specific cause-defence matrix the analyst must be very familiar with the specific characteristics of the plant, knowledgeable about large number of causes of failure, and familiar with the defences that have been used to defend against them.

One set of matrices needs to be developed for each of the component groups identified as the result of the screening phase, and those that may have been added to the list as the result of the plant walk-through and data review in this phase. This step is very useful in event impact vector analysis for parameter estimation using operating data. This is explained in the next subsequent subsection (III-2.6). A comparison between the generic and plant specific matrices will help prioritise the list of CCF vulnerabilities and quantify the contribution of CCFs.

III-2.5 Selection of Probability Models for Common Cause Basic Events

Common cause basic events (CCBEs) are events that represent multiple failures of components from shared root causes. The objective of this step is to provide a transition from the FT logic model in Phase-1 to a model that can be quantified. This is done by associating a probability model, such as the constant failure rate model or the constant probability of failure with demand model with each basic event (common cause or independent).

Although historical data collected from the operation of NPPs, indicate that common cause events do not always fail all redundant components, experience from using b factor model reveals that, in some cases, it gives reasonably accurate (only slightly conservative) results for redundancy levels up to about three or four. However, beyond such redundancy levels, this model generally yields results that are conservative. With the current state of data that involve large uncertainties, the numerical impact of selecting one model over another is not significant, given a consistent treatment of data in all cases. However when interest centres around specific contributions from third or higher order trains, more general parametric models like MGL or alpha -factor model are suitable. The models can be classified into two major categories; (i) Non-shock models and (ii) Shock models [79]. These are described below.

III-2.5.1 Non-shock Models

Non-shock models are CCF models that estimate multiple failure probabilities without postulating a model for the underlying failure mechanism. Examples : The basic parameter model, the beta-factor model, MGL model, and the alpha-factor model.

III-2.5.1.1 Beta Factor Model

The beta factor model is a single parameter model; i.e. it uses one parameter in addition to the total component failure probability to calculate the CCF probabilities. This model assumes that a constant fraction (β) of the component failure rate can be associated with common cause events shared by other components in that group. Another assumption is that whenever a common cause event occurs, all components within the common cause component group are assumed to fail.

$$Q_I = (1-\beta)Q_t$$
$$Q_m = \beta Q_t \tag{III-1}$$

This implies that $\beta = \dfrac{Q_m}{Q_I + Q_m}$ (III-2)

Where, Q_t is the total failure probability of one component ($Q_t = Q_I + Q_m$), Q_I is the independent failure probability of the single component, Q_m is the probability of basic event failure involving m specific components, and *m* is the maximum number of components in a common cause group. To generalise the equation, it can be written for m components involving failure of k components (k ≤ m) as,

$$Q_k = \begin{cases} (1-\beta)\ Q_t & k = 1 \\ Q_k = 0 & 2 \le k < m \\ \beta Q_t & k = m \end{cases} \tag{III-3}$$

Where Q_k is the probability of basic event involving k specific components.

A practical and useful feature of this model is that the estimators of beta do not explicitly depend on system or component success data, which are not generally available. Also, estimates of the beta parameter for widely different types of components do not appear to vary much compared to Q_k. These two observations and the simplicity of the model are the main reasons for its wide use in risk and reliability studies. However, application of this model would be limited up to certain values of m.

III-2.5.1.2 Multiple Greek Letter Model

The MGL model is an extension of the beta-factor model. The MGL model was the one used most frequently in the international common cause failure reliability benchmark exercise. In this model, other parameters in addition to the beta factor are introduced to account more explicitly for higher order redundancies and to allow for different probabilities of failures of subgroups of the common cause component group.

The MGL parameters consist of the total component failure probability Q_t, which includes the effects of all independent and common cause contributions for all component failure and a set of failure fractions. These fractions are used to quantify the conditional probabilities of all the possible ways a common cause failure of a component can be shared with other components in the same group, given that a component failure has occurred. For a group of m redundant components and for each given failure mode, m different parameters are defined. For a 4-component group, MGL model has 4 parameters and they are expressed as follows.

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^m$$

$$Q_t = Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)} \tag{III-4}$$

$$\beta = \frac{3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}}{Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}} \tag{III-5}$$

$$\gamma = \frac{3Q_3^{(4)} + Q_4^{(4)}}{3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}} \tag{III-6}$$

$$\delta = \frac{Q_4^{(4)}}{3Q_3^{(4)} + Q_4^{(4)}} \tag{III-7}$$

β = Conditional probability that the cause of a component failure will be shared by one or more additional components, given that a specific component has failed.

γ = Conditional probability that the cause of a component failure that is shared by one or more components will be shared by two or more additional components, given that two specific components have failed.

δ = Conditional probability that the cause of a component failure that is shared by two or more components will be shared by three or more additional components, given that three specific components have failed.

For a general case,

$$Q_k^{(m)} = \frac{1}{\begin{pmatrix} m-1 \\ k-1 \end{pmatrix}} \prod_{l=1..k} (\rho_l)(1-\rho_{k+1})Q_t \tag{III-8}$$

Where $\rho_1 = 1,\ \rho_2 = \beta,\ \rho_3 = \gamma, \ldots\ldots,\ \rho_{m+1} = 0$

The following equations express the probability of multiple component failures due to common cause, Q_k, in terms of the MGL parameters, for a 4-component group:

$$Q_1^4 = (1-\beta)*Q_t \ ; \ \ Q_2^4 = \frac{\beta(1-\gamma)*Q_t}{3} \ ; \ \ Q_3^4 = \frac{\beta\gamma(1-\delta)*Q_t}{3} \ ; \ \ Q_4^4 = \beta\gamma\delta * Q_t$$

III-2.5.1.3 Alpha - factor Model

The alpha factor model defines common cause failure probabilities from a set of failure frequency ratios and the total component failure frequency, Qt. In terms of the basic event probabilities, the alpha factor parameters are defined as:

$$\alpha_k^{(m)} = \frac{\begin{pmatrix} m \\ k \end{pmatrix} Q_k^{(m)}}{\sum_{k=1}^{m} \begin{pmatrix} m \\ k \end{pmatrix} Q_k^{(m)}} \tag{III-9}$$

Where $\begin{pmatrix} m \\ k \end{pmatrix} Q_k^{(m)}$ is the frequency of events involving k component failures in a common cause group of m components, and the denominator is the sum of such frequencies. In other words, $\alpha_k^{(m)}$ is ratio of the probability of failure events involving any k components over the total probability of all failure events in a group of m components, and $\Sigma_k \alpha_k^{(m)} = 1$. The basic event probabilities can be expressed in terms of Q_t and the alpha factors as follows.

$$Q_k^{(m)} = \frac{k\alpha_k^{(m)}}{\begin{pmatrix} m-1 \\ k-1 \end{pmatrix} \alpha_t} Q_t \quad \text{Where } \alpha_t = \sum_{k=1}^{m} k\alpha_k^{(m)} \tag{III-10}$$

III-2.5.1.4 Extended β Factor Model

The extended β model is based on that developed by R. A. Humphreys. The method involves the scoring of the system design against eight criteria, namely (i) separation, (ii) similarity, (iii) design complexity, (iv) analysis, (v) procedures, (vi) training (vii) environmental control and (viii) environmental tests. The total score is then converted on a regression basis, into a β value. This model reflects levels of redundancy, by defining generic β factors for different levels of redundancy. For instance redundancy level 2 or 3 uses β_1 and level 4 or 5 uses β_2 and levels above 5 use β_3, with $\beta_1 > \beta_2 > \beta_3$. These β factors are selected based on comparison between the failure probability of redundant components as obtained by this method and the more precise MGL method [80].

III-2.5.2 Shock Models

Shock models are CCF models that estimate multiple failure probabilities by postulating a shock that impacts the system at certain frequency to cause multiple failures. Example : Binomial failure rate model.

The BFR model considers two types of failures. The first represents independent component failures; the second type is caused by shocks that can result in failure of any number of components in the system. According to this model, there are two types of shocks: lethal and non-lethal. When a non-lethal shock occurs, each component within the common cause component group is assumed to have a constant and independent probability of failure. The name of this model arises from the fact that, for a group of components, the distribution of the number of failed components resulting from each non-lethal shock occurrence follows a binomial distribution. The BFR model is, therefore, more restrictive because of these assumptions than all other multi-parameter models presented here. When a lethal shock occurs, all components are assumed to fail with a conditional probability of unity. Application of the BFR model with lethal shocks requires the use of the following set of parameters:

Q_I - independent failure frequency for each component

μ - frequency of occurrence of non-lethal shocks

p - conditional probability of failure of each component, given a non-lethal shock

ω- frequency of occurrence of lethal shocks

m- total number of components in common cause group

Thus, the frequency of basic events involving k specific components is given as:

$$Q_K = \begin{cases} Q_I + \mu\, p\, (1-p)^{m-1} & ; k=1 \\ \mu\, (p)^k\, (1-p)^{m-k} & ; 2 \leq k < m \\ \mu\, p^m + \omega & ; k=m \end{cases} \qquad \text{(III-11)}$$

III-2.6 Parameter Estimation

Input required to estimate the parameters of the common cause probability models described above is, information about the number of applicable events of single and multiple failures and the number of failed components.

III-2.6.1 Data Analysis (Data Collection, Classification and Screening)

The sources of data available to an analyst are event reports, operating logs, maintenance history dockets, etc. indicating both single and multiple equipment failures. Since plant specific data on multiple equipment failures are rare, it is necessary to extend the search to other plants. Also, recourse could be taken to data sources, specifically developed at international level for dependent analysis on components like pumps (NUREG/CR-2098), valves (NUREG/CR-2770), instrumentation and control assemblies (NUREG/CR-3289), control rod and drive mechanism (NUREG/CR-1331), diesel generators, breakers (EPRI NP-3967) etc. However, since other plants may be designed or operated differently, events that occurred at one plant designed or operated differently, may not have occurred or be unlikely to occur at another. Thus, the data should not be used blindly, but should be carefully reviewed for applicability. Once the failure event reports are identified for each of the CCCG, they should be classified on cause (observed and root causes), coupling factor, failure mode and a number of other characteristics, including defensive strategies in place at the plant. These are useful in developing a statistical database. There are several sources of uncertainty, including the interpretation of the data to elicit causal mechanisms, the assessment of their impact, and uncertainty about how the data were obtained. Consequently, it is essential to not only provide a point estimate but also to characterise this uncertainty numerically.

III-2.6.2 Parameter Estimation Using Operating Data

To complete the description of the event impact at the original plant, the analyst needs to identify (i) Component group size, (ii) Number of components affected, (iii) Shock type (lethal or non-lethal) and (iv) Failure mode.

III-2.6.2.1 Development of Impact Vector for Original Plant [79]

The outcome of the event classification can be represented in the form of an Impact Vector. This impact vector of an event that has occurred in a component group of size m has m+1 elements, each representing the number of components, which did or could have failed in the event. If in an event, k components fail, the k-th element of the impact vector is 1 while all other elements are 0. The general form of the impact vector is

$I = \{ F_0, F_1, F_2 \ldots\ldots F_m \}$ (III-12)

For e.g., I = {0, 0, 1} represents an event in a system of two components (m=2) in which both components failed due to a shared cause ($F_2 = 1$).

Experience with database and event reports indicates that in a large number of cases the event descriptions are not clear, the exact status of components are not known, and the causes and coupling factors are seldom identified. Therefore, the classification of the event, including the assessment of its impact vector, may require establishing several hypotheses, each representing a different interpretation of the event. In such cases a probability is assigned to each hypothesis, representing the analyst's degree of confidence in that hypothesis. For example, in an event involving a group of three components, the description does not indicate how many components have actually failed. The analyst presumes that two components might have failed with 90 % confidence and three components might have failed with 10 % confidence. Then the impact vector for this event can be given by

$I = \{I_0, I_1, p1*I_2, p2*I_3\}$, Where, $I_0 = 0$, $I_1 = 0$, p1 = 0.90, $I_2 = 1$, p2 = 0.10 and $I_3 = 1$ (III-13)

III-2.6.2.2 Development of Impact Vector for Plant Being Analysed

Having developed the impact vector of the event in the original plant in which it occurred, the next step is to determine what that implies for the plant and system being analysed (target plant). This requires a two-step adjustment of the original impact vector to account for qualitative and quantitative differences between the original system and the target system.

For qualitative adjustment, analyst checks the cause and coupling mechanism of the event with respect to the target plant and decides whether the event is applicable to target plant or not. If analyst is unable to decide, based on the available information, he can assign an “event applicability factor”, r (0 < r < 1). Then the resulting modified impact vector is

I' = r*I. Table III-5 gives some suggested values for r.

TABLE III-5 : SUGGESTED VALUES FOR APPLICABILITY FACTORS

Strength of Target Plant Defenses Compared with Original/Average Plant	Applicability Factor (r)
Complete defense	0.0
Superior defense	0.1
Moderately better	0.5
Weaker or no defense	1.0

For quantitative adjustment, the impact vector must be 'mapped up', 'kept unchanged' or 'mapped down', depending on whether target system 'size' (number of component in a CCCG) is larger, equal or smaller than the original system.

A complete set of formulae for mapping down data from systems having four, three, or two components to any identical system having fewer components is presented in the Table III-6. In this table, $P_k^{(m)}$ represents the k-th element of the average impact vector in a system (or component group) of size m.

TABLE III-6 : FORMULAE FOR MAPPING DOWN EVENT IMPACT VECTORS

Size of System Mapped From	Size of System Mapped To (Number of Identical Trains)		
	3	2	1
4	$P_1^{(3)} = (3/4)\, P_1^{(4)} + (1/2)\, P_2^{(4)}$	$P_1^{(2)} = (1/2)\, P_1^{(4)} + (2/3)\, P_2^{(4)} + (1/2)\, P_3^{(4)}$	$P_1^{(1)} = (1/4)\, P_1^{(4)} + (1/2)\, P_2^{(4)} + (3/4)\, P_3^{(4)} + P_4^{(4)}$
	$P_2^{(3)} = (1/2)\, P_2^{(4)} + (3/4)\, P_3^{(4)}$	$P_2^{(2)} = (1/6)\, P_2^{(4)} + (1/2)\, P_3^{(4)} + P_4^{(4)}$	
	$P_3^{(3)} = (1/4)\, P_3^{(4)} + P_4^{(4)}$	$P_1^{(2)} = (2/3)\, P_1^{(3)} + (2/3)\, P_2^{(3)}$	
3		$P_2^{(2)} = (1/3)\, P_2^{(3)} + P_3^{(3)}$	$P_1^{(1)} = (1/3)\, P_1^{(3)} + (2/3)\, P_2^{(3)} + P_3^{(3)}$
		$P_2^{(2)} = (1/3)\, P_2^{(3)} + P_3^{(3)}$	
2			$P_1^{(1)} = (1/2)\, P_1^{(2)} + P_2^{(2)}$

Mapping up the impact vector introduces uncertainties. To reduce the uncertainty inherent in upward mapping of impact vector, event is classified into three categories; (i) independent event, (ii) non-lethal shocks and (iii) lethal shocks. The following relationships can be given for independent events and lethal shocks. General formulae for mapping up non-lethal shocks are given in Table III-7.

For mapping up an independent event, $P_l^{(l)} = (l/k)\, P_l^{(k)}$, where l and k is the sizes of the target system and original system respectively.

By definition, a lethal shock wipes out all the redundant components present within a CCG. Hence, $P_l^{(l)} = P_k^{(k)}$.

TABLE III-7 : FORMULAE FOR UPWARD MAPPING OF EVENTS CLASSIFIED AS NON-LETHAL SHOCKS

Size of System Mapped From	**Size of System Mapped To (Number of Identical Trains)**		
	2	**3**	**4**
1	$P_1^{(2)} = 2\,(1\text{-}\rho)\,P_1^{(1)}$	$P_1^{(3)} = 3\,(1\text{-}\rho)^2\,P_1^{(1)}$	$P_1^{(4)} = 4\,(1\text{-}\ \rho)^3\,P_1^{(1)}$
	$P_2^{(2)} = \rho\ P_1^{(1)}$	$P_2^{(3)} = 3\rho\,(1\text{-}\ \rho)\,P_1^{(1)}$	$P_2^{(4)} = 6\,\rho\,(1\text{-}\ \rho)^2\,P_1^{(1)}$
		$P_3^{(3)} = \rho^2\,P_1^{(1)}$	$P_3^{(4)} = 4\,\rho^2\,(1\text{-}\ \rho)P_1^{(1)}$
			$P_4^{(4)} = 6\,\rho^3\,P_1^{(1)}$
2		$P_1^{(3)} = (3/2)\,(1\text{-}\rho)\,P_1^{(2)}$	$P_1^{(4)} = 2\,(1\text{-}\rho)^2P_1^{(2)}$
		$P_2^{(3)} = \rho\ P_1^{(2)} + (1\text{-}r)\ P_2^{(2)}$	$P_2^{(4)} = (5/2)\rho\,(1\text{-}r)P_1^{(2)} + (1\text{-}\rho)^2\,P_2^{(2)}$
		$P_3^{(3)} = \rho\ P_2^{(2)}$	$P_3^{(4)} = \rho^2\ P_1^{(2)} + 2\,\rho\,(1\text{-}\rho)P_2^{(2)}$
			$P_4^{(4)} = \rho^2\ P_2^{(2)}$
3			$P_1^{(4)} = (4/3)(1\text{-}\rho)\ P_1^{(3)}$
			$P_2^{(4)} = \rho\ P_1^{(3)} + (1\text{-}\rho)P_2^{(3)}$
			$P_3^{(4)} = \rho\ P_2^{(3)} + (1\text{-}\rho)P_3^{(3)}$
			$P_4^{(4)} = \rho\ P_3^{(3)}$

A maximum likelihood estimator for r is r = k/m, where k is the number of components affected in the event, and m is the size of the original system.

III-2.6.2.3 Development of Event Statistic From Impact Vectors

Once the impact vectors of all the events in the database are assessed for the system being analysed, the number of events in each impact category can be calculated by adding the corresponding elements of the impact vectors. That is,

$$n_k = \sum_{i=1}^{m} P_k(i) \tag{III-14}$$

where n_k = total number of basic events involving failure of k similar components, and

$P_k(i)$ = the k-th element of the i-th impact vector

By using this n_k , the parameters (α, β, δ, and γ) in various CCF models can be calculated.

(a) Estimator for the β - factor model parameter

Although the β - factor was originally developed for a system of two redundant components and the estimators that are often presented in the literature also assume that the data are collected from two - unit systems, a generalised β - factor estimator can be defined for a system of m redundant components. Such an estimator is based on the following general definition of the b - factor (identical to the way it is defined in the more general MGL model).

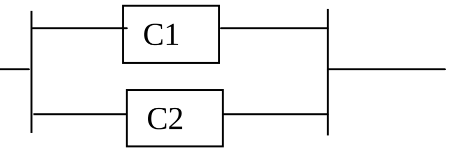
$$\beta = \frac{1}{Q_t}\sum_{k=2}^{m}\binom{m-1}{k-1}Q_k \text{ . The estimator } \beta = \frac{\sum_{k=2}^{m} kn_k}{\sum_{k=1}^{m} kn_k} \tag{III-15}$$

Example for beta factor model

Data: No of demands = N_D = 1000

No of times C1 or C2 alone failed = n1= 30

No of times both failed = n2=3



Parameter estimation

$\beta = 2\, n_2 /(n1+2\, n2) = 0.17$

Calculation of failure probabilities

$Qt = n1 + 2\, n2 /(2\, N_D) = 1.8E - 2$ /d

$Q2 = \beta * Qt = 3E$-3

(b) Check list based estimator

If failure data is scarce, then checklist-based estimation of β could be used [89]. The main advantage of this method is that it provides an auditable trail of assessment and also details the scope of improvement directly. The checklist method is as follows. CCF are mainly influenced by factors like physical separation, redundancy level, design complexity, environmental control, environmental testing, maintenance, operating procedures and training level. Quantitative scores are awarded to each of this qualities. The accumulated grade is converted to β based on suitable scaling.

(c) Estimators for the MGL parameters

Based on the definition of the MGL parameters, the simple point estimators are

$\rho_l = \dfrac{\sum_{k=l}^{m} kn_k}{\sum_{k=l-1}^{m} kn_k}$ (l = 2, 3,..m), where n_k is defined as the number of events involving the failures of exactly k components.

Example for MGL model:

Data:

ND = 1000

Redundancy level = m =4

No of independent events = n1 = 50

No of events involving 2 components = n2 = 10

No of events involving 3 components = n3 = 4

No of events involving 4 components = n4 = 1

Parameter estimation

$\rho_2 = \beta = \dfrac{\sum_{k=2}^{4} kn_k}{\sum_{k=1}^{4} kn_k} = 0.42$, $\rho_3 = \gamma = \dfrac{\sum_{k=3}^{4} kn_k}{\sum_{k=2}^{4} kn_k} = 0.44$ and $\rho_4 = \delta = \dfrac{4n_4}{\sum_{k=3}^{4} kn_k} = 0.25$

$Qt = n1 / 4N_D + 3.\, n2 / 6.\, N_D + 3.\, n3 / 4.\, N_D + n4 / N_D$

$= 2.15E - 2$ /d

Calculation of failure probabilities

$Q_1^4 = (1-\beta) * Q_t = 1.25E\text{-}2$; $Q_2^4 = \dfrac{\beta(1-\gamma) * Q_t}{3} = 1.68E\text{-}3$

$Q_3^4 = \dfrac{\beta\gamma(1-\delta) * Q_t}{3} = 9.9E\text{-}4$; $Q_4^4 = \beta\gamma\delta * Q_t = 9.9E\text{-}4$

(d) Estimators for the α - factor model parameters

An estimator for each of the α - factor parameters (α_k) can be based on its definition as the fraction of total failure events that involve k component failures due to common cause. Therefore, for a system of m redundant components,

$$\alpha_k = \frac{n_k}{\sum\limits_{k=1}^{m} n_k}$$

Example for α - factor model:

Data : From example (b)

Parameter estimation

$$\alpha_1 = \frac{n_1}{\sum\limits_{k=1}^{4} n_k} = 50/65 = 0.769$$

$$\alpha_2 = \frac{n_2}{\sum\limits_{k=1}^{4} n_k} = 0.154; \ \alpha_3 = \frac{n_3}{\sum\limits_{k=1}^{4} n_k} = 0.062 \ ; \ \alpha_4 = \frac{n_4}{\sum\limits_{k=1}^{4} n_k} = 0.015$$

Calculation of failure probabilities

$$Q_2^4 = \frac{2\alpha_2}{\begin{pmatrix}3\\1\end{pmatrix}\alpha_t} Q_t \quad \text{with Qt = 2.15E -2 and } \alpha_t = 1.325$$

Q^4_2 = 1.67E - 3 /d

(e) Estimators for BFR model

The main parameters of the BFR model are Q_I, λ_t, ω and p . Let λ_t = rate of non-lethal shocks that cause at least one component failure, and

$$n_t = \sum_{k=1}^{m} n_k \tag{III-16}$$

Where n_k is the number of basic events involving k components. n_L is the number of lethal shocks, n_I is number of individual component failures, excluding that due to lethal and non lethal shocks.

$$Q_I = \frac{n_I}{mN_D} \tag{III-17}$$

$\lambda_t = n_t / N_D$

$\omega = n_L / N_D$ and p is the solution of the following equation,

$$\sum_{k=1}^{m} kn_k = p \frac{mn_t}{1-(1-p)^m} \tag{III-18}$$

An estimator for μ can be obtained from the above estimators as follows

$$\mu = \frac{\lambda_t}{1-(1-p)^m} \tag{III-19}$$

Example for BFR

Data: From example (b)

$nt = 65$, $\lambda t = 6.5E - 2$

$\omega = 1E\text{-}3$, assuming one lethal shock.

$p = 0.18$ (using polynomial solver)

$\mu = 0.1168$

$Q_1 = 1.25E - 2$

$Q_2 = 2.5E - 3$

$Q_3 = 5.6E - 4$

$Q_4 = 1E - 3 + 0.12 * 0.18^4 = 1.13\ E - 3$

III-2.7 Parameter Estimation With no Operating Data

With the current status of databases, it is not possible to determine parameters by analysing operating data for all the components of interest in risk and reliability analyses of NPPs. There is, therefore, a practical need for estimating parameter values based on engineering judgement. Table III-8 provides a suggested set of generic values for the parameters of the Alpha factor and MGL parameters, which may be used when a more detailed evaluation of CCF events is not possible.

TABLE III-8 : GENERIC PARAMETER VALUES [79]

System Size (m)	**Alpha Factors**				**MGL Parameters**		
	a_1	a_2	a_3	a_4	b	d	g
(2)	0.95	0.05	-	-	0.10	-	-
(3)	0.95	0.04	0.01	-	0.10	0.27	-
(4)	0.95	0.035	0.01	0.005	0.11	0.42	0.4
Generic Beta Factor value = 0.1 [81]							

III-2.8 System Quantification

The purpose of this stage is to synthesise the key output of the previous stages to effect a quantification of system failure frequency, and the interpretation of results. The event probabilities obtained for the common cause events are incorporated in the solution for unavailability of the systems or into event sequence frequencies in the usual way cutsets are quantified. The results of this step include the numerical results and the identification of key contributors.

III-2.9 Result Evaluation and Sensitivity Analysis

Since there is considerable uncertainty in the estimation of common cause failure probabilities, an uncertainty analysis is done to integrate the individual uncertainties into a combined result. It is also useful to see how significant such uncertainties can be by using sensitivity analyses to determine the direct relationship between the input values for the common cause basic events and the overall system results.

III-2.10 Reporting

The final step is the reporting of the analysis. It is particularly important to be clear in specifying what assumptions have been used and to identify the consequences of using these and other assumptions.

III-2.11 Additional Considerations

When CCF data availability is scarce, β factor could be used with the beta estimated using a checklist method. However when interest centres around specific contributions from third or higher order redundancies, more general parametric models like MGL or alpha factor model are suitable. The framework described above is expected to result in a consistent, reproducible and defensible CCF analysis.

APPENDIX-IV

RELIABILITY ANALYSIS OF CONTROL AND INSTRUMENTATION SYSTEMS

IV-1 Introduction

There is an increasing trend in the use of computer-based control and instrumentation (C & I) both for safety and non-safety related systems in NPPs. Typical safety significant C & I systems in NPPs and Research Reactors are : (i) Neutron flux and process parameter sensors and associated signal processing equipment, (ii) Reactor power control and process control systems (e.g. RRS, PCS), (iii) Control room and important parameter monitoring equipment, and (iv) Safety parameter sensing, safety system actuation and operation (e.g. reactor trip (shutdown) system, ECCS).

International standards like IEC-1226, IAEA-50-SG-D1 and AERB Safety Guide AERB/SG-D1, give the safety classification of C&I systems used in the NPPs. The basic purpose of safety classification is to identify the possible target reliability values, the requirement specifications for QA, and reliability testing and design features.

Defence-in-depth, redundancy, fault-tolerance through redundancy, single failure criteria, diversity and fail-safe design philosophy are important in the design considerations for C&I systems. C&I systems in the recent times use microprocessors that contain both hardware components and software.

The important aspects to assure quality and reliability of the C&I systems include the following.

(i) QA in the procurement of Electronic Components (ECs) including cables, relays, etc.

(ii) Environmental qualification /testing of ECs

(iii) Reliability screening tests (100%) for all the components

(iv) Standard practices for the design of circuit hardware and software (e.g. IEC-880, IEC-987, IEC-125, IEC-1226, draft AERB guide-D-25, etc.)

(v) Redundancy and diversity concepts for subsystems, channels and sensors

(vi) Verification and validation testing for both hardware and software

(vii) Man-Machine interface considerations in design, operation and maintenance

IV-2 Reliability Analysis Methods

Reliability and safety assessments for computer-based systems are done using an integrated combination of deterministic and probabilistic techniques. C&I systems contain both hardware and software.

IV-2.1 Hardware Reliability

The failure rate of electronic components follows a systematic characteristic bath-tub curve,[Fig 5.6, Pg 89] where-in life pattern can be broadly divided into three regions; (a) Initial high failure rate period (few weeks to one year), (b) Constant failure rate period (usually 10-15 years), and (c) Wear out increasing failure rate period. Failure of electronic components could be by open mode, short mode, degradation, etc. and dominant failure mode needs to be identified for operational safety.

Reliability analysis methods include (i) MIL-217 Methodology for Electronic Equipment (applicable to electronic hardware of non-redundant components, sub-system or channel of duplicated/triplicated system), (ii) Fault Tree Model Technique, (iii) Block Diagram (cutset/tie-set method), (iv) Markov Model, (v) Go Chart Model (vi) Fuzzy Logic, (vii) Petri Nets and (viii) Neural Network Methods and Dynamic Fault Tree modelling. Block diagram method is mostly used for small systems. The Fault Tree methodology is widely used; its greatest advantage being incorporation of CCF/CMF models. Markov model and Go chart model represent system states including failure and repair conditions. Mathematical expressions for reliability assessment are available for moderately small size C & I system.

IV-2.1.1 MIL-HDBK-217F Method

An updated version of this, MIL-STD-217F, is used for failure rate assessment of electronic component or circuit modules [82]. Failure rate models are given for a very broad category of electronic components, in which base failure rate values are given, and failure rate of each type of component is calculated by multiplying the base failure rate by stress factors for the given application. Stress factors for the component models are given in the Handbook [82], for factors like environment, power consumption, voltage and thermal stresses, quality, construction etc., for the application of C&I systems in NPPs.

If for a typical electronic component, base failure rate is expressed as λb, then final failure rate of the component is expressed as $\lambda_{comp} = \lambda_b * \prod_{I=1}^{n} (SF)_I$. Where $(SF)_I$ is ith stress factor of the component and 'n' is total number of stress factors.

In a similar way, failure rates of all the components in the equipment or circuit board are estimated, and as an approximation, a series component model is assumed to estimate the failure rate of the equipment. This information becomes an input to the FT model.

IV-2.1.2 Dynamic Fault Tree (DFT) Analysis [83]

The traditional FT analysis is limited in its ability to model some of the failure modes associated with digital systems, especially those that incorporate fault tolerance. Markov methods are generally accepted as an appropriate method for analysing fault-tolerant digital systems. Dynamic Fault Trees (DFTs) are useful for reliability analysis of embedded computer systems. DFTs together with Markov method depicting 'chain of states' can be useful to assess reliability of any computer based system. DFTs are a superset of traditional (static) FTs in that additional gates such as the Sequence Enforcing gate (SEQ), the Functional Dependency gate (FDEP), the Priority And gate (PAND) and the Cold, Hot and Warm Spare gates (CSP, HSP and WSP) are used. SEQ gates only allow component failures in the order specified by its inputs. FDEP gates fail their dependent inputs based on whether their trigger input is failed or not. The FDEP has no output and hence it is connected to FT with dashed line. PAND gates output a failure if their inputs fail in order, and the CSP, HSP and WSP gates model primary-spare relationships. In CSP, HSP and WSP gates, output occurs when primary and all spares have failed (or otherwise unavailable). In CSP gate, spare components have zero failure rates before being switched into active use. In HSP gate, spare components have same failure rates before and after being switched into active use. In WSP gate, spare components have reduced failure rates before being switched into active use. This gate represents events happening in order. The output occurs if and only if the events listed below the gate happens from left to right. For any other sequence gate output is zero.

Using all these special gates and traditional FT gates such as AND, OR, K/M gates system, model is developed. Static gates are solved using simple Boolean algebra. In order to solve DFT gates, it is necessary to use Markov chains, which contains all the information regarding component failures, sequence of component failures, and information on spare allocations. The Markov Chains map into a set of equivalent ordinary differential equations (ODEs) with variables corresponding to state probabilities. These equations are solved using an ODE solver. The probability of being in any failed state during the mission time gives an estimate of the system unreliability.

Fig. V-2 and V-3 [84] of Appendix-V gives the FT representation for a computer based reactor regulating system (Dual Processor Hot Stand-by process control System for an Indian PHWR).

IV-2.2 Issues Related to Quantification of Software Reliability

The software reliability concept has been adopted from electronic hardware reliability. However, it differs in its behavioural characteristics. If it is compared with the 'bath-tub' curve of electronic hardware components, software error rate will be only in decreasing order of magnitude from the beginning to the end of useful life of computer based C & I system. There is no wearout phenomenon in software, and once the software errors are corrected (some times called as 'bug-fixing'), the same error is not likely to occur at the particular location in the software structure. Adequate verification and validation needs to be carried out during design phase and system integration phase. Tools like 'Static Analysers' are commercially available to detect errors in software.

Although, there are limitations to accurately assess the software reliability, USNRC recommends [85] use of PRA techniques to quantify software reliability. Standard methods for quantification of the software are not reported and are still in developmental stage. However, the analyst should make efforts to represent the event in FT at basic event levels. A study sponsored by Rome laboratories, publisher of MI-HDBK-217 made some effort to quantify software failure rate for the use of FT analysis [82]. It is mentioned that similar to hardware reliability, the analysis starts with determination of initial failure rate l0 that is an estimate of fault content at the beginning of the formal system testing (in other words, when software developer finishes his/her job).

$$\lambda_0 = f \times K \times \omega_0 \qquad \text{(IV.1)}$$

Where,

f = linear execution frequency

K = fault exposure ratio, (average value considered 4.2E-07)

ω_0 = number of faults in the program = wf X Is, where

ω_f = Fault density (re commended value based on experience is 6 faults per 10000 source instructions or line of code).

I_s = Number of source instructions

$f = \frac{r}{I_s \times C_{ex}}$, Where r = processor speed expressed in Mega Instructions per seconds (MIPS)

and C_{ex} = language expansion ratio (2.5 for C language)

There are also several adjustments to be made. First, software can fail only when it is running, and there are times when the microprocessor is not executing the code, such as during data acquisition from an A/D converter. Hence, system operating failure rate λ_s can be given as

$$\lambda_S = \lambda_0 \times U_{es} \qquad \text{(IV.2)}$$

where $U_{es} = \frac{t_C - t_N}{t_C}$, t_C = Software cycle time and t_N = data acquisition time

With all these values λ_s can be calculated. One can also express the cumulative effect of the software testing and fixing, on the failure rate reduction. This is expressed as $V_0 = \frac{\omega_0}{B}$

where B is a fault reduction factor (<1). Usually B = 0.995 should be used.

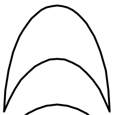
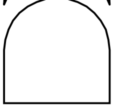
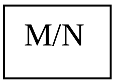
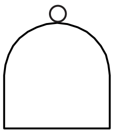
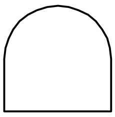
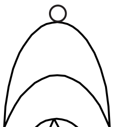
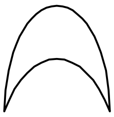
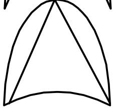
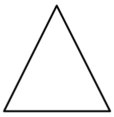
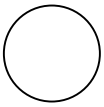
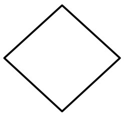
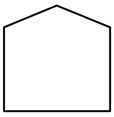
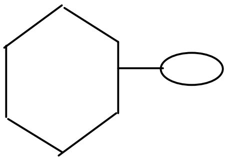
Assigning variable t as a cumulative execution time since the start of the system testing, the fault density as one continues to test is expressed as, $\lambda(t) = \lambda_s \times e^{-\frac{\lambda_s}{V_0}t}$.

This failure rate value can be plugged into a FT analysis as a basic event for 'software failure'.

APPENDIX-V

BASIC FAULT TREE SYMBOLS AND SAMPLE FAULT TREE

V-1 Fault Tree Symbols

Symbols	Names	Gate is TRUE if
	OR gate	At least one input event TRUE
	AND gate	All input events TRUE
	M/N gate	At least M of the N input events TRUE
 	NAND gate	Not all input events TRUE (at least one input event FALSE)
 	NOR gate	None of the input events TRUE (all input events FALSE)
	Exclusive OR gate	Exactly one input event TRUE
	Transfer	
	Basic event	
	Undeveloped event	
	House event	
	Inhibit gate	Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate), FT model converts it to an AND gate with two inputs.

House Events : A house event can be included in the fault tree logic like a basic event but it operates as a ‘logical switch’, which can have only one of the Boolean values TRUE or FALSE (ON/OFF). House events are used to change the FT structure. Different variations of one basic FT can be obtained by defining house events as TRUE or FALSE. This is very useful when system logics could be different for a set of components to meet functional requirements under different situations. The house event ‘settings’ can be defined in two ways.

(i) By setting the house event to TRUE or FALSE in the database (“hard” setting). This means it is always TRUE or FALSE in all analyses, which include this house event.

(ii) By including it in a Boundary Condition Set (BC Set), where a list of house events can be specified, along with a TRUE/FALSE setting. The BC Set can then be used in Analysis Cases, in IEs or in Function Events.

House events affect the logic for different gate types. Gates that become TRUE or FALSE due to house events will themselves operate as house events, and the impact of house events can propagate up through the FT structure. In all cases, the house events (and gates that become TRUE or FALSE) are removed from the tree structure after their effect on the logic have been determined. The impact of a house event for some gates is given in the following table and illustrated with a FT in Fig.V-1 below:

OR-gate	1 or more inputs TRUE ==> TRUE output
	ALL inputs FALSE ==> FALSE output
	1 or more (but less than ALL) inputs FALSE ==> No effect
AND-gate	1 or more inputs FALSE ==> FALSE output
	ALL inputs TRUE ==> TRUE output
	1 or more (but less than ALL) inputs TRUE ==> No effect

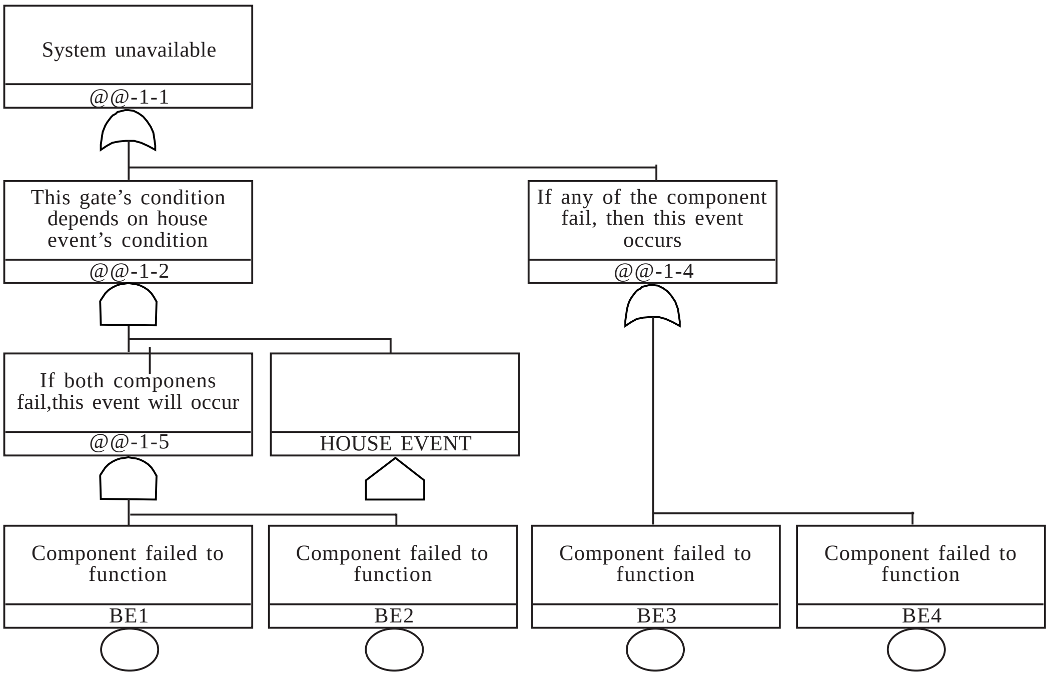

System unavailable
@@-1-1
This gate’s condition depends on house event’s condition
@@-1-2
If any of the component fail, then this event occurs
@@-1-4
If both componens fail,this event will occur
@@-1-5
HOUSE EVENT
Component failed to function
BE1
Component failed to function
BE2
Component failed to function
BE3
Component failed to function
BE4

FIGURE V-1 : AN ILLUSTRATION FOR HOUSE EVENT INCORPORATION IN THE FAULT TREE

RESULTS WITH COMPONENT FAILURE MODEL TAKEN AS 'CONSTANT PROBABILITY MODEL'

Failure Probabilities for BE1 & BE2 = 1E-2 BE3 & BE4 = 1E-3	**House Event State**	**Number of MCS**	**Top Event Unavailability (Q)**
	True (q=1)	3	2.1E-3
	False (q=0)	2	2.0E-3

V-2 Fault tree for dual processor hot standby (DPHS) - Process control system (PCS) [84]

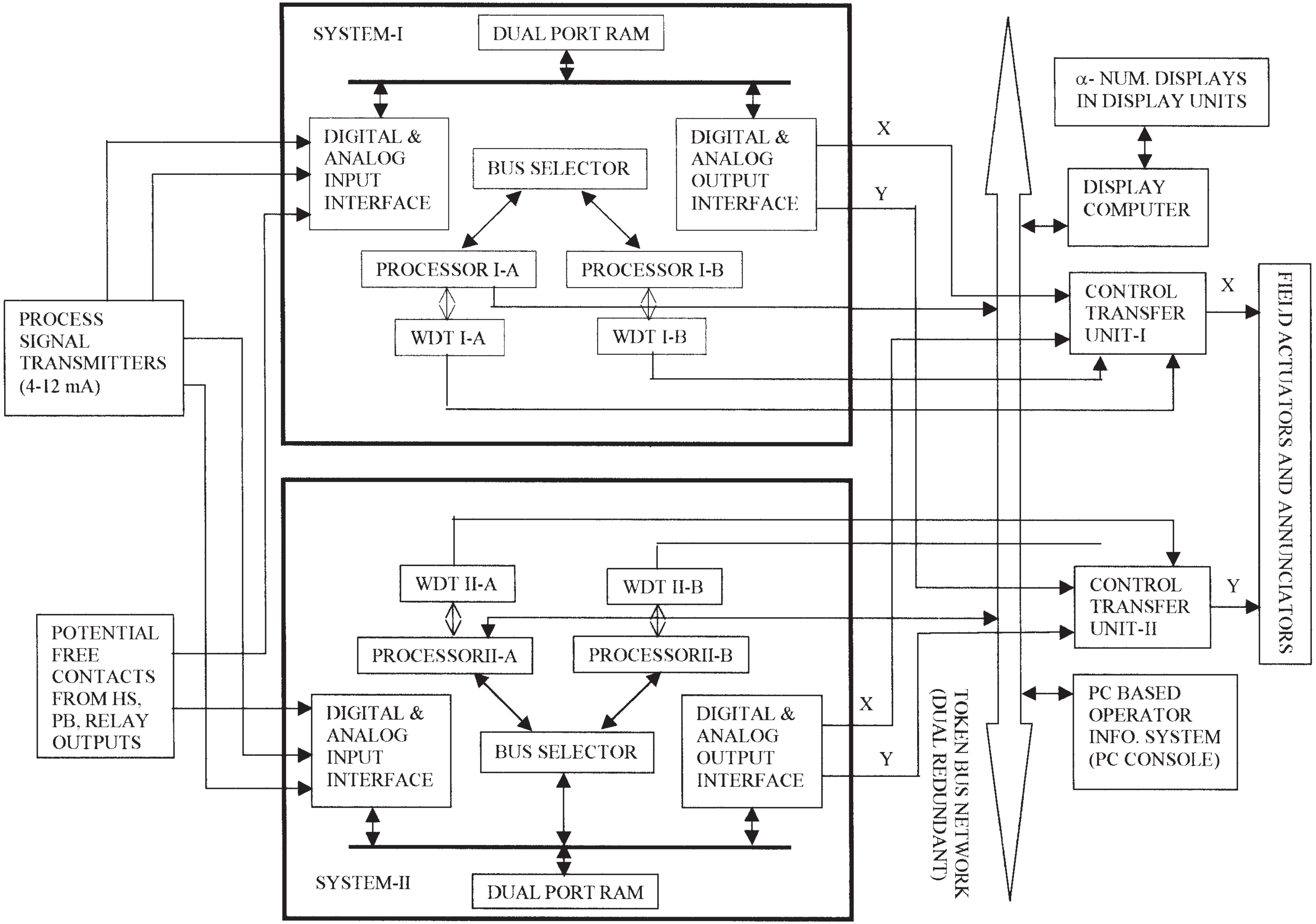

SYSTEM-I
DUAL PORT RAM
DIGITAL & ANALOG INPUT INTERFACE
BUS SELECTOR
DIGITAL & ANALOG OUTPUT INTERFACE
PROCESSOR I-A
PROCESSOR I-B
WDT I-A
WDT I-B
X
Y
PROCESS SIGNAL TRANSMITTERS (4-12 mA)
α- NUM. DISPLAYS IN DISPLAY UNITS
DISPLAY COMPUTER
CONTROL TRANSFER UNIT-I
X
FIELD ACTUATORS AND ANNUNCIATORS
WDT II-A
WDT II-B
PROCESSORII-A
PROCESSORII-B
CONTROL TRANSFER UNIT-II
Y
POTENTIAL FREE CONTACTS FROM HS, PB, RELAY OUTPUTS
DIGITAL & ANALOG INPUT INTERFACE
BUS SELECTOR
DIGITAL & ANALOG OUTPUT INTERFACE
X
Y
TOKEN BUS NETWORK (DUAL REDUNDANT)
PC BASED OPERATOR INFO. SYSTEM (PC CONSOLE)
SYSTEM-II
DUAL PORT RAM

FIGURE V-2 : DUAL PROCESSOR HOT STANDBY - PROCESS CONTROL SYSTEM CONFIGURATION [84]

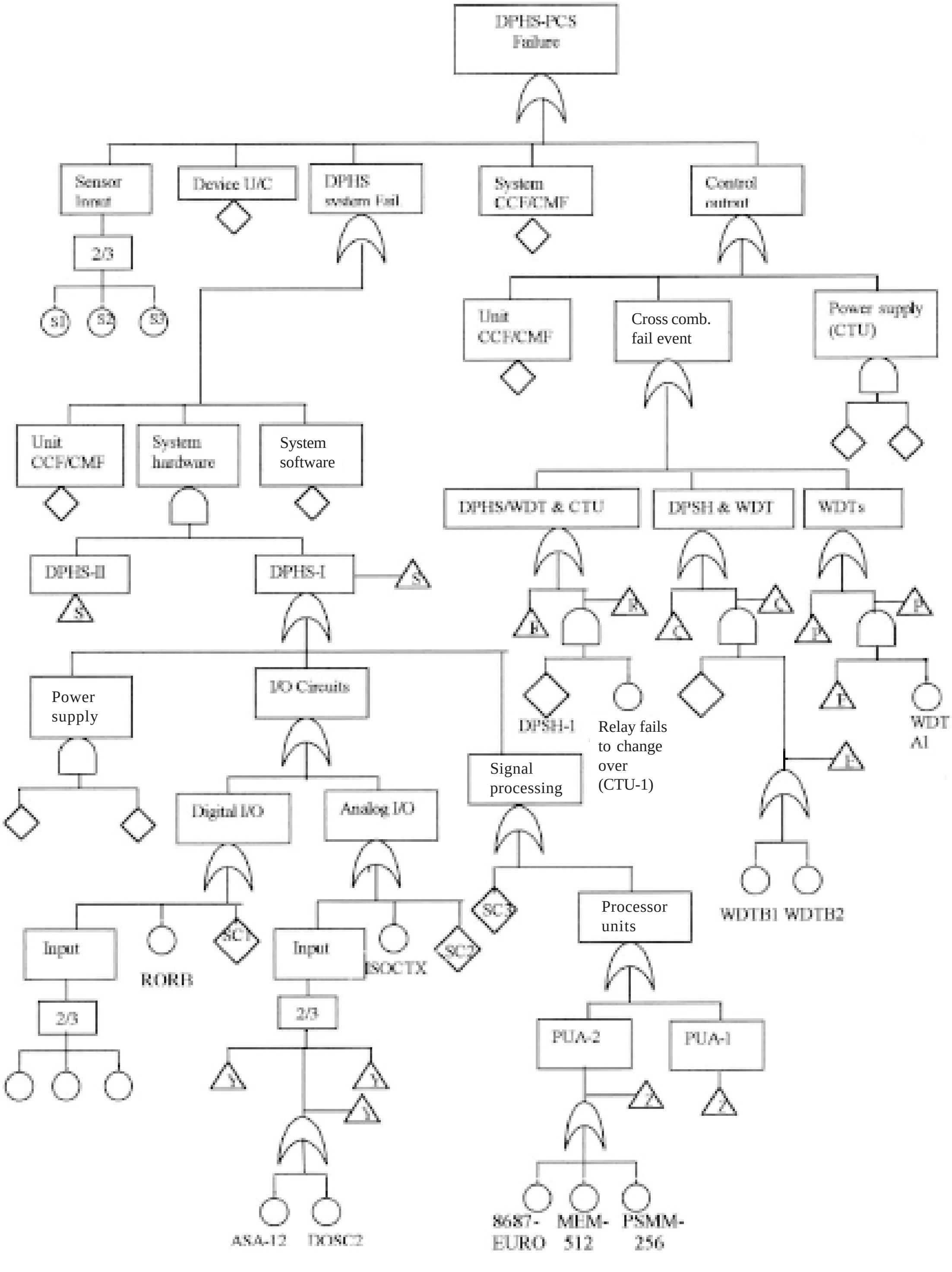


FIGURE V-3 : FAULTY TREE FOR DPHS-PCS [84]

APPENDIX-VI

HUMAN RELIABILITY ANALYSIS (HRA) IN PSA FOR NPPs

VI-1 Introduction

Worldwide, it is found that human error caused events constitute about 70 % of all events occurring in a plant. Therefore, human reliability plays an important role in nuclear safety. The main objective of treating human reliability in a PSA is to ensure, that the key human interactions (HIs) of plant staff are systematically incorporated into the assessment, in order to find which of these actions are dominant risk contributors that should be carefully attended to, to reduce HEP in operator actions. To make the analysis more meaningful and reliable, the input to PSA from HRA should be of quality. This requires systematic data collection and classification, and modelling and quantification of human error. This should take into consideration emergency procedures, Man-Machine Interface (MMI), training programmes and knowledge and experience of plant operators. Here the term ‘plant operator’ refers commonly to all operation, maintenance and other staff involved in plant operation. This section covers all the key issues involved in the incorporation of HRA into PSA, including the requirements and limitations of HRA, categories of human interactions, modelling, assessment and quantification of each interaction, outputs and documentation of the overall HRA process. It does not include external HIs such as sabotage. The management and organisational issues, which have recently been receiving increased attention under the safety culture umbrella, have also not been addressed. Human error events are incorporated in the FT/ET and recovery actions in event sequences. HRA can be done for both internal and external events. While there is an increase in the occurrence of error in HIs during some external events, e.g., seismic, flood, as compared to cases of internal events, they may be difficult to model and quantify because of scanty data.

VI-2 Human Behaviour, Rasmussen’s Model and Human Error

A person makes an error if he/she does something incorrectly, fails to do something, or fails to do something in time. An error of omission occurs when an operator omits a step in a task or the entire task, amounting to an unintended or unnoticed action. An error of commission occurs when the person does the task, but does it incorrectly, amounting to an unintended action excluding inaction. It is a broad category, encompassing selection errors, sequence errors, time errors and qualification errors. Any factor that influences human performance is termed as a Performance Shaping Factor (PSF). PSFs could be categorised broadly as external, stressors and internal. The external PSFs include situational characteristics (e.g. quality of environment - noise and vibration), task, equipment characteristics (e.g. MMI factors) and job task instructions (e.g. written or oral communications). The stressor PSFs include psychological stressors (e.g. monotonous work) and physiological stressors (e.g. fatigue). The internal PSFs are organismic factors that include characteristics of operator resulting from internal and external influences (e.g., cultural background, personality variables, motivation, etc.). Human actions in a plant can be grouped into following types based on work complexities.

(i) Skill based : Highly practiced activities that can be performed with little apparent thought.

(ii) Rule based : Performance of tasks, as per the procedures, within the normal experience and ability of the particular individual.

(iii) Knowledge based : Performance of tasks in unforeseen situations where familiar patterns and rules cannot be applied directly as symptoms could be ambiguous, state of plant is complicated by multiple failures, instrument does not give true representation of situation, etc. A high level of cognitive processing is necessary.

These three types of human behaviour can be represented by Rasmussen’s model, which provides an acceptable framework to identify the type of human behaviour and associated error mechanism as shown in Fig. VI-1.

This model is based on the assumption that humans will generally perform tasks at the lowest level possible to minimise the amount of decision-making or cognitive thought required. Skill based tasks require little or no decision-making and hence a task proceeds directly from initial stimuli, i.e. activation to the execution stage. Rule based tasks require some decision making and hence move first from the initial stimuli to the 'integration' phase where information is processed and only then an appropriate 'procedure' or 'rule' is selected. Finally, the selected 'procedure' or 'rule' is executed. Knowledge based tasks require the highest degree of decision making and this leads to interpretation of information and then to its evaluation, before appropriate 'procedures' can be selected and tasks executed.

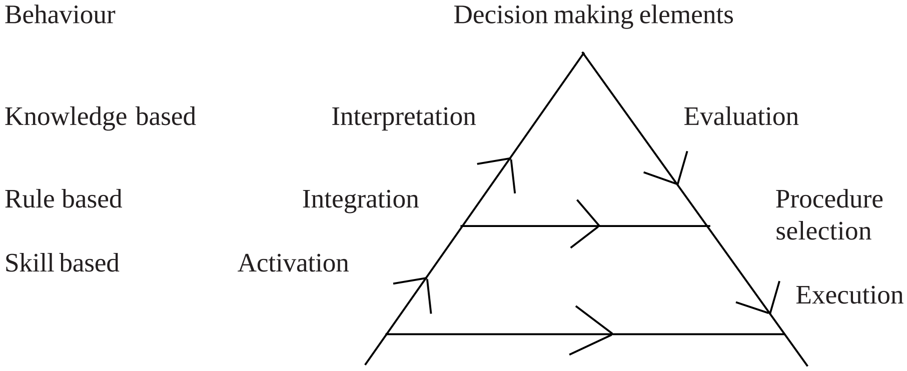


FIGURE VI-1 : RASMUSSEN'S DECISION MAKING MODEL

The error categories, that are associated with Rasmussen's model of human behaviour, for consideration in HRA for PSA, are:

- Slips/Lapses : These are more likely to be caused during skill-based actions. Slips are inadvertent selection of wrong items while attempting to execute a set of planned actions. Lapses are omissions to perform actions during a planned sequence of activities.
- Mistakes : These are associated with rule and knowledge based actions. Mistakes are more serious errors as they arise from an incorrect understanding of a situation, followed by selection of an inappropriate plan of resulting actions (sequence of actions).

For PSA, it is important to be aware of the different potentials for error recovery for the different error categories. Slips and lapses can generally be recovered from, fairly quickly, provided there are appropriate feedback mechanisms and the plant behaviour is reversible. Mistakes are less easily recovered in the short term; 'mindset' problems can occur and operators can persist in attempting to implement an inappropriate plan even when faced with much contradictory information. Recovery actions have to be very positive and powerful to be reliable, e.g., based on key alarms and backed up by adequate training. The Human Reliability analyst should ensure that potential mistakes are identified in the PSA structure and that these are carefully addressed.

There are many ways of classifying human errors. One way is to classify them into errors in action response and errors in cognitive response. The former (also called external error mode) comprises error of omission, error of commission and extraneous act. The latter (also called internal error mode) comprises misdetection, misinterpretation, misdiagnosis and error in decision-making.

VI-2.1 Steps in HRA

The stepwise structured process of HRA based on SHARP methodology is presented below [86].

(a) Definition

The task needs to be defined is to ensure that all relevant human actions are adequately considered in the study. This would also clarify the boundaries for the study and the interface with other assessments being performed. The scope and objective will determine the tasks and analysis of tasks will help in identifying potential human errors. For completeness of coverage and modelling, HIs identified are grouped into following three categories for appropriate modelling in HRA, depending on timing and impact on the plant operation.

(i) Category A, pre-initiators

These are pre-initiators, e.g., maintenance/test/repair actions. Error in this type of interaction can cause equipment or systems to be unavailable when required post-fault. Pre-initiators consist of those actions associated with maintenance and testing that degrade system availability. They may cause failures of a component or component group or may leave components in an inoperable condition. Particularly important are actions or errors that result in concurrent failure of multiple trains of safety related systems. This unavailability is added to other failure contributions for components or system at the FT level. Recovery action for such human errors could be error alarm, post-maintenance testing and post-maintenance inspection checklist, which may be modelled as applicable in quantification stage.

(ii) Category B, initiators

These are initiators, e.g., control room actions, maintenance/test actions during normal operations. The errors in this type of interaction, either by themselves or in combination with other failures (other than due to human error) can cause IEs. Most important are errors that not only precipitate an accident sequence but which also concurrently cause failure of systems related to safety, either front-line safety systems or support systems. There should be particular emphasis on such ‘common cause initiators’, which are caused by human error.

(iii) Category C, post-initiators

These are post-initiators. The errors in this type of interaction can occur in the performance of safety actions or there can be actions/errors that exacerbate the fault sequence. These HIs can be separated into three different types.

Type 1. Procedural safety actions

These actions involve success or failure in following established procedures in response to an accident sequence and is incorporated explicitly into fault and event trees.

Type 2. Aggravating actions/errors

These actions are a special set of commission errors that occur post-fault following an IE and significantly exacerbate the accident progression. They are the most difficult to identify and model. A type of such action occurs when the operator’s mental image of the plant differs from the actual plant state, leading the operator to perform the “Right” action for the “Wrong” event. Another form of Type 2 action or error occurs when the operator correctly diagnoses the event, but chooses a non-optimal strategy for dealing with it. Once the actions and their significant consequences are identified, they can be incorporated into an ET/FT.

Type 3. Improvising recovery/repair action

These consist of recovery actions, which are generally only included in accident sequences that dominate risk profiles. They may include the recovery of previously unavailable equipment or the use of non-standard procedures to ameliorate the accident conditions. They can be incorporated into the PSA as recovery actions in the accident sequence event trees.

Some diagnosis is required for Type 1, 2 and 3 actions and time is a limiting factor, The general approach for dealing with Type 1 and 3 actions is the same and this guideline will treat them as one category. For convenience Type 2 actions are also included in this category although specific measures are outlined for dealing with them.

(b) Screening

Screening is to identify the human actions that are significant to the operation and safety of the plant. Screening can be carried out by a combination of qualitative and quantitative approaches by the analyst, with appropriate justification.

(c) Qualitative analysis

This is to develop a detailed description of important human actions by defining the key influence factors necessary to complete the modelling. The potential for errors and mechanism for recovery from the identified errors should be determined or estimated. Recovery actions identified in EOPs and also cut-sets not in approved procedure should be included. The specific treatment for recovery analysis is given in Appendix-X. This will often require information additional to that collected during the initial task analysis. The above steps should have identified most of the specific constraints and PSFs associated with the overall task (e.g. time available, sequence of steps, specific context of the task). But there may be other factors that need to be considered, particularly relating to the individuals performing the tasks, e.g., experience, level of training, stress levels, etc.

(d) Representation and model integration

Once HIs are selected after screening, and broken down into elements with detailed descriptions, the next task is to select and apply techniques for depicting important human actions in logic structures. There are various models advocated by experts, such as time independent model-Technique for Human Error Rate Prediction (THERP), time dependent model- Human Cognitive Reliability (HCR), and Operator Action Tree (OAT), etc. Some of these HRA models are discussed below.

(i) Time independent models

THERP

In time independent models, time available to the operator is not a major constraint on action, i.e., the probability of the operator taking the action is not significantly altered by reducing or increasing the time available for action. Errors related to such cases usually (but not always) occur before the IE. The models are therefore also referred to as Latent Error Models. For modelling of such errors, THERP is used.

THERP is somewhat analogous to hardware reliability analysis with human actions substituted for component outputs. In THERP, tasks and task steps are identified along with PSFs that influence the steps. The task failure event is modelled in what is called an HRA ET (to distinguish it from a PRA ET). The HRA ET (Fig. VI-2) structures the activities, potential failures and dependences (redundancies) in HIs, in failure logic and includes a failure probability at the end of failure paths. Diagnosis in THERP is considered to be a holistic process and is assigned a single HEP value. HEP data are taken from the THERP Handbook.

Accident sequence evaluation programme (ASEP) HRA procedure

In complex systems like NPPs, HRA can be an involved and time-consuming process. THERP was therefore expanded to cover a more cost effective three-stage HRA procedure called ASEP for application to PSA. The three stages are:

- Screening HRA using the screening HEP assignment methodology of ASEP.
- Nominal HRA using the nominal HEP assignment methodology of ASEP for those tasks whose estimated HEPs are greater than the screening limit.
- THERP HRA methodology applied to those tasks whose HEPs are greater than screening HRA as well as nominal HRA limit values.

The ASEP-HRA procedure includes both screening model and nominal diagnosis model time reliability curves. The details of the ASEP HRA procedure are given in reference [87].

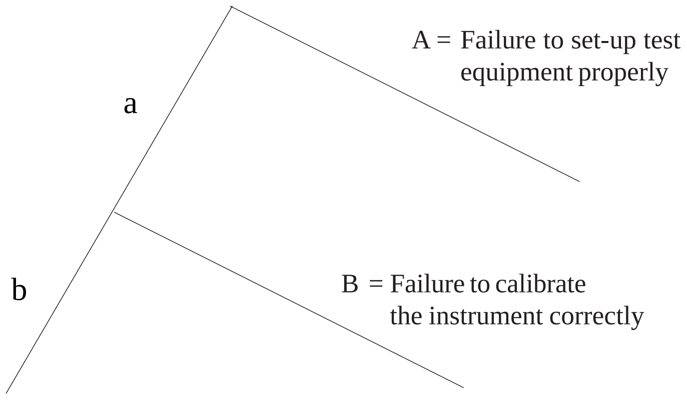
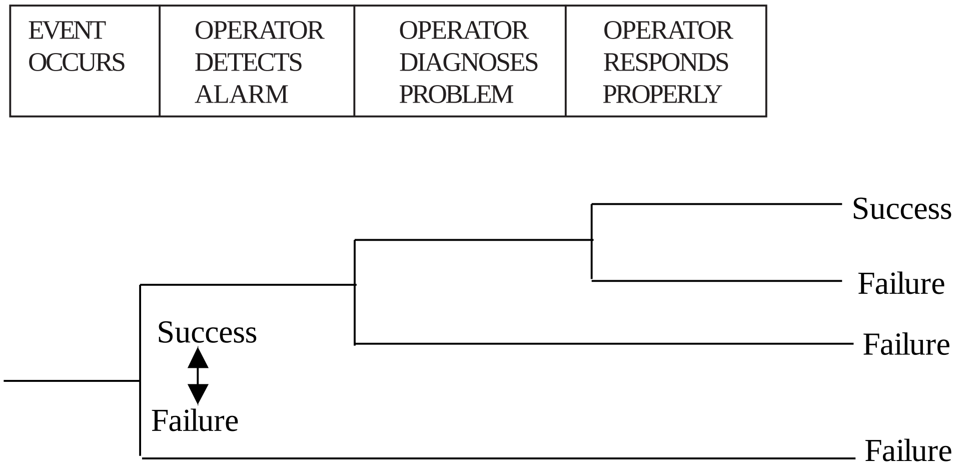

A = Failure to set-up test equipment properly
a
b
B = Failure to calibrate the instrument correctly

FIGURE VI-2 : HIRA EVENT TREE FOR CALIBRATION TASK

(ii) Time dependent models

In these models, time available to the operator for action is, in many cases, a major constraint on the operator's ability to act. Most of the time dependent models are based on a Time Reliability Correlation (TRC), which allows an engineering oriented quantification of human reliability in terms of HEPs. Examples of such models are HCR and OAT models. HCR, which allows practical handling of significant HIs, uses a normalised three parameter Weibull distribution to represent the correlation between time available for response and the probability of failure to respond. OAT (Fig. VI-3) is a representation that identifies alternative actions on the basis of operator interpretations associated with observation, diagnosis and selection of response. The analyst can display the potential of different decision strategies to affect the accident sequence.



EVENT OCCURS	OPERATOR DETECTS ALARM	OPERATOR DIAGNOSES PROBLEM	OPERATOR RESPONDS PROPERLY

FIGURE VI-3 : OPERATOR ACTION TREE (OAT) MODEL

The human cognitive reliability (HCR) model

This is one of the models used in the SHARP technique. The HCR model has been developed for quantification of control room crew success/failure probability as a function of time allowing for skill, rule and knowledge type behaviour that can result in different probabilities. The model also allows for selected PSFs that can influence crew response times. An assumption made is that the probability distribution for crews responding to a plant event is a function of normalised time (actual crew response time to the event/median response time for a number of crews). It depends on the behaviour involved (skill, rule or knowledge). PSFs affect response probability by changing the median response time. PSFs considered in the use of the HCR model are operating experience, stress and quality of the MMI.

The HCR correlation is given below and is represented in Fig. VI-4. The model relates the non-response probability P(t) to normalised time $t/T_{1/2}$

$$P(t) = \exp - \left[\frac{\left({}^{t}\!/\!{}_{T_{1/2}} - B_i \right)}{A_i} \right]^{C_i} \qquad \text{(VI-1)}$$

where, t = time available to complete the action or set of actions following a stimulus

$T_{1/2}$ = estimated median time to complete the task (action or set of actions) as adjusted by specific PSFs. This is arrived at on the basis of an analysis of simulator data for similar plants or on the basis of discussions with crews. A_i , B_i , C_i are the correlation coefficients specified for skill, rule and knowledge based processing.

This model involves the four steps given below.

(i) Determine the cognitive process (skill, rule or knowledge) applicable to the HI involved.

(ii) Estimate the time window by thermal hydraulics/transient analysis.

(iii) Estimate the median time reflecting key plant and task specific PSFs

(iv) Estimate the crew response probability using the HCR correlation.

Simulator data have been used to examine the validity of the HCR model. EPRI's Operator Reliability Experiment (ORE) Project also examined the validity of the HCR model and arrived at the conclusion that the operator response time can be well represented by a lognormal probability distribution, which provides as good a fit as the Weibull and is easier to use.

HCR INTERIM PARAMETERS

Cognitive Processing Type	Ai	Bi	Ci
Skill	0.407	0.7	1.2
Rule	0.601	0.6	0.9
Knowledge	0.791	0.5	0.8

Analyst should use his/her judgement in applicability of any model for the specific tasks in the plant. Model integration is done to describe how the significant human actions are integrated into the plant and system models of the PSA, either in FT or ET stages. The analysis pathways for this step are depicted in Fig. VI-5.

(e) Quantification

This step involves use of appropriate data or quantification methods to assign probabilities for the various actions examined, determining sensitivities and establishing uncertainty ranges [88]. The human error data collection and analysis is an important aspect in assuring quality in quantification. The following gives data collection and analysis methodologies.

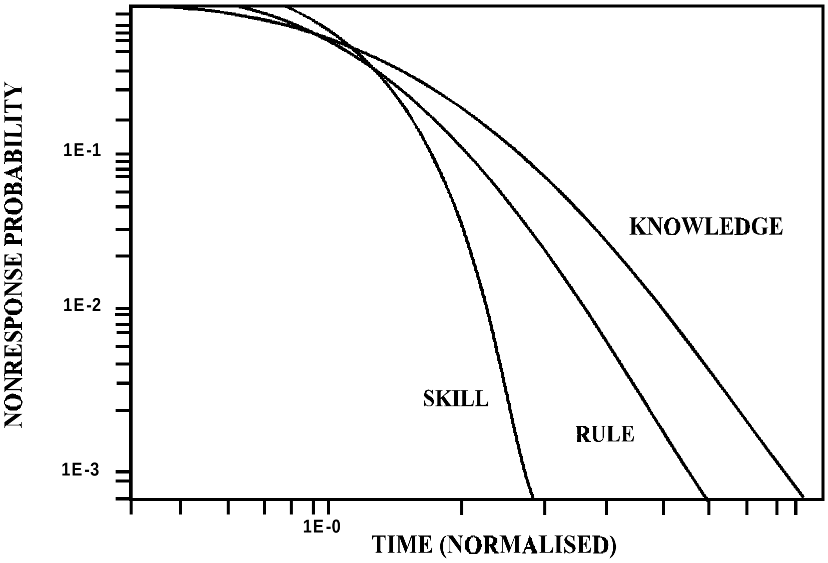


FIGURE VI-4 : HCR CORRELATION

Human reliability analysis data

An HEP is measured by observation. It is the ratio of the number of observed errors to the total number of chances for error to occur. In other words, , Where n = number of errors that occurred and N= number of opportunities for the errors to occur. While this appears simple enough, a good deal of effort is in fact required to estimate an HEP. It is necessary to consider data probability distribution, data dependence and data uncertainty aspects when estimating HEPs.

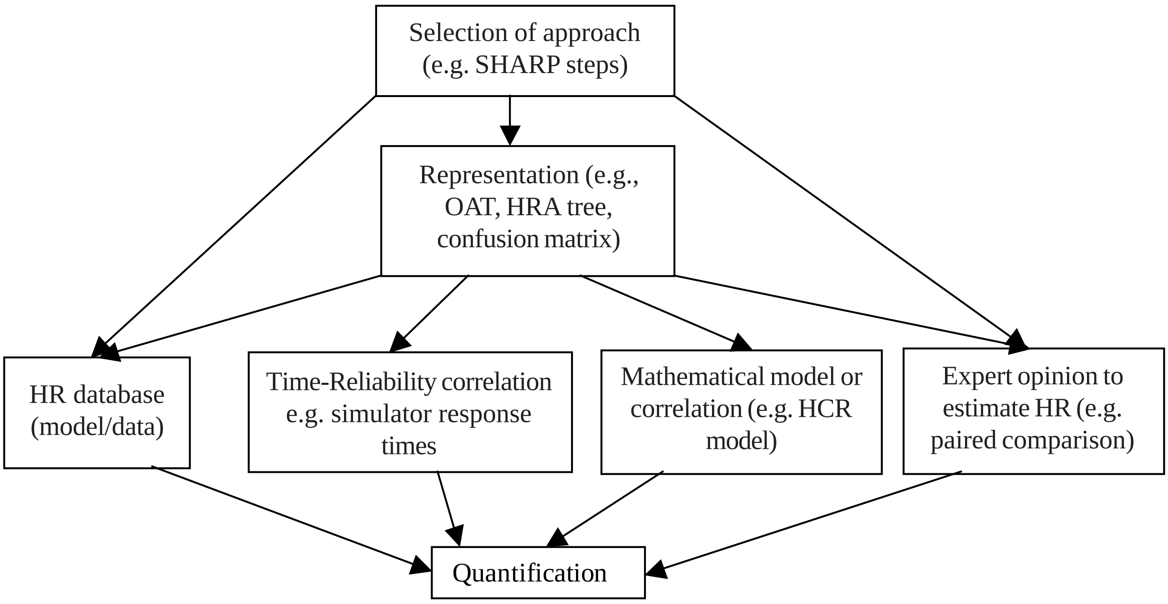

Selection of approach (e.g. SHARP steps)
Representation (e.g., OAT, HRA tree, confusion matrix)
HR database (model/data)
Time-Reliability correlation e.g. simulator response times
Mathematical model or correlation (e.g. HCR model)
Expert opinion to estimate HR (e.g. paired comparison)
Quantification

FIGURE VI-5 : ANALYSIS PATHWAYS

Data collection for HRA [89, 90]

HEPs can be obtained by observational and/or experimental methods. Observational data is obtained from some regular activity being carried out for a different purpose (e.g. a simulator training session). Experimental data are data that are obtained by carrying out activities, the prime intention of which is the generation of error probability data. The main data collection methods are: (i) Observation methods, (ii) Direct observation, (iii) Photo, video and audio recordings, (iv) Experimental Methods, and (v) Part/full scope simulator experiments including simulator training and interview of personnel.

Data are of three main kinds. These are as given below:

(i) Empirical information : The sources of empirical information are reports on plant outages/ power changes and their causes, plant trips and post-trip investigations, maintenance reports and operator logs which indicate unsuccessful activities with no hardware cause present. A typical Human Error Reporting Form (HERF) used for collection of data is given in Table VI-1[90].

(ii) Generic information : When using non plant-specific information, attention has to be paid to plant differences that can affect the applicability of data and assumptions made (if any) in modifying the data before use. Both empirical and generic information are scarce. The scarcity of published information that is readily accessible is by and large due to national or other constraints.

(iii) Subjective information : This consists of information from subjective non-empirical sources like experts and experienced operators. The information can include direct estimates of HEPs and information needed to modify the HEPs in order to make them applicable to a particular situation. Some important issues to be addressed in use of subjective information for a HRA are relevance of the information, biases of subject matter experts, their experience base, chosen sample size and inter-shift differences.

TABLE VI-1 : TYPICAL FORMAT USED FOR COLLECTION OF DATA

PLANT HUMAN ERROR REPORTING FORM			
Atomic power station			
Unit		Form serial No.	
A. Problem Description			
Brief details	Plant status		
	Prior		After
		Shutdown	
		Start-up	
		Power operation	
		Reduced power	
		Off normal	
Number of times the problem has occurred previously Personnel involved (Nos. from personnel list) Continuous duty hours put in (Prior to event occurrences)			
Date		Time of occurrence	

B. Human Error Data			
Relevant indications prior to human action			
1. Audio/visual alarm		2. Visual display	a) Other (specify)
Window CRT		Indicating meter DPM Status indicator Lamp/LED CRT recorder	
Types of activity (Nos. from activity list)			
Location of activity (Nos. from location list)			
Time available for activity (Nos. from time list)			

TABLE VI-1 : TYPICAL FORMAT USED FOR COLLECTION OF DATA (CONTD.)

Type of human error (Nos. from error type list)		
Mode of human error (Nos. from error mode list)		
Cause of human error (Nos. from error cause list)		
Effect of human error	Immediate	
	Delayed	
Space for additional information, if any		

Systems affected USI			
Type of Recovery			
1. Error alarmed			
2. Supervisory check			
3. Regular check			
4. Post maintenance test			
Recommendations for improvement			
Filled by Tech. Engr.		Checked by senior Tech. Engr.	
Issued by TSS		Approved by SORC	
C. Analysis of human error (not to be filled by the station)			
Human error probability			
Performance shaping factor			
Recovery Factor			

Personnel List

Code	Personnel
1CM	Control Operator-Main
1AM	Area Operator-Main
1CF	Control Operator-Fuel
1AF	Area Operator-Fuel
2M	Control Engineer-Main
2F	Control Engineer-Fuel
3M	Area Engineer-Main
3F	Area Engineer-Fuel
4M	Assistant Shift Charge Engineer (ASCE)-Main
4F	Assistant Shift Charge Engineer (ASCE)-Fuel
5	Shift Charge Engineer (SCE)-Main
6MCM	Maintenance Control-Main
6MCF	Maintenance Control-Fuel
6MMM	Maintenance Mechanical-Main
6MMF	Maintenance Mechanical-Fuel
6ME	Maintenance Electrical
6MS	Maintenance Services
7	Other (Explain)

Activity List

Code	Activity
1	Observation/Monitoring
2	Opearation/Execution/Control
3	Maintenance
4	Testing
5	Checking
6	Incident/Accident Response
7	Other (Explain)

Error Type List

Code	Error Type
1	Omission
2	Transposition
3	Inappropriate action
4	Advanced action
5	Delayed action
6	Other (explain)

Error Mode List

Code	Error type
1	Detection
2	Interpretation, diagnosis
3	Decision
4	Action
5	Communication
6	Other (explain)

Time List

Code	Time
1	< 1 Minute
2	< 5 Minutes
3	< 10 Minutes
4	< 30 Minutes
5	< 60 Minutes
6	> 60 Minutes

TABLE VI-1 : TYPICAL FORMAT USED FOR COLLECTION OF DATA (CONTD.)

Error Cause List

Code	Error Cause
1	Complexity of work
2	Work organisation
3	Work station design
4	Procedure content (inadequate procedure)
5	Process format
6	Procedure not followed
7	Unclear task criteria
8	Inadequate supervision or inspection
9	Improper or unauthorised operation or maintenance
10	Poor skill, inexperience, inadequate training or education
11	Hardware problems
12	Personal (physiological or psychological causes)
13	Communication
14	Other (explain)

Location List

Code	Location
1	Control room
2	Control equipment room
3	Turbine building
4	Reactor building (RB) accessible area
5	RB shutdown accessible area
6	Service building
7	Fuelling Machine Vault
8	MCC and switchgear area
9	Switch yard
10	Pump house
11	Upgrading plant
12	DM plant
13	Other (explain)

VI-3 Dependence [88]

For cases where more than two HEPs exist in a MCS of failures in the core damage sequences, dependence must be considered. The level of dependence that will be used, with equations for the conditional probability HEP of failure, given failure of the previous task with P_0 as the independent HEP value [3] is given as:

Zero dependence	$HEP = P_0$
Low dependence	$HEP = \frac{1 + 19\,P_0}{20}$
Moderate dependence	$HEP = \frac{1 + 6\,P_0}{7}$
High dependence	$HEP = \frac{1 + P_0}{2}$
Total dependence	$HEP = 1$

For the case of HCR model, the HEP actions are treated in an integral fashion and thus include intra-crew dependences. The system dependences are included in the construction of the representation and the way they are integrated into the event trees.

VI-4 Human Error Analysis

Estimation of HEP for the human error under consideration, wherever possible, can be done as follows.

$$\text{Actual HEP} = \text{Basic HEP x PSFs x RF} \qquad \text{(VI-2)}$$

where Basic HEP (i.e., the probability of human error for the task considered as an isolated activity/entity) is modified or weighted by the PSFs and the Recovery Factor (RF). The PSF multiplier would depend on the values assigned to applicable PSFs (external and internal to the operator) and stressors. The RF multiplier takes into account a recovery (if any) effected by the operator on detection of error; by way of suitably reducing the Basic HEP.

Examples of modelling and quantification

The details of modelling and quantification with regard to the different categories of HIs and also with HCR and THERP models are illustrated with some examples below.

(1a) Category A, pre-initiator tasks

The basic methodology that can be applied here is the ASEP -HRA procedure and the original THERP Handbook methodology. Data used and recommended in the ASEP-HRA procedure are largely judgemental, but seems to have a reasonable justification based on everyday life experience. Other methods of quantification could be used based on judgemental values. Such methods as Paired Comparisons or the Success Likelihood Index Methodology (SLIM) could be used to consolidate expert opinion.

In finalising the quantification of dependent errors it is essential to exclude from the generic CCF database, those events that are accounted for by the plant specific human reliability analysis.

Example: The following typical example presents a method for determining the mean unavailability for a manual valve in the wrong position. This is typical for a two-train system consisting of two similar manual valves, e.g., MVs 3LP - 40 and 41 in the low-pressure injection/recirculation system shown in Fig. VI-6.

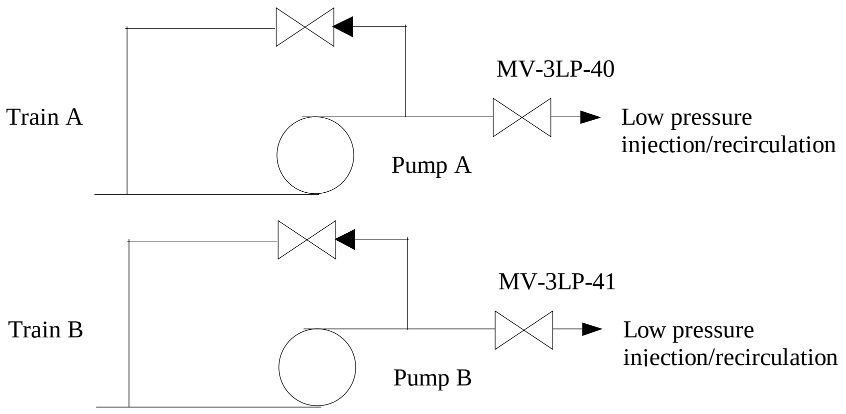

MV-3LP-40
Train A
Low pressure injection/recirculation
Pump A
MV-3LP-41
Train B
Low pressure injection/recirculation
Pump B

FIGURE VI-6 : SIMPLIFIED SYSTEM DIAGRAM

A success criterion is valves are restored to the open position after test or maintenance activity.

Initial conditions

Opportunity to close the manual valve MV 3LP-40 will come from:

(1) Monthly system functional test

(2) Unscheduled mechanical maintenance

The frequency of unscheduled maintenance is determined from pump failure data and is about 0.09 per month. This results in a total frequency of 1.09 per month to change the status of the valve MV 3LP-40 (or 41).

Quantification:

It is assumed that the only error that can fail the LPI/recirculation train is failing to re-open the manual valve MV 3LP-40 (41) in the pump delivery path after maintenance or monthly tests. A probability of failure to restore the value to ‘open’ of 0.01 is recommended. Quality Control (QC) personnel check the completion of the procedure. Given that an independent HEP for QC personnel’s failure to detect the fault is 0.1 and using dependency equations for a low dependence interaction [91] between two groups the conditional HEP is:

$$HEP_c = \frac{1+19n}{20} = \frac{1+19\times 0.1}{20} = 0.15$$

Thus, the probability of MV 3LP-40 being in the wrong configuration immediately following test/maintenance is then estimated as 0.01 x 0.15 =1.5 x 10^{-3}.

Since tests for the two loops may be performed by the same shift of QC personnel, a high dependence will be assumed between the two loop tests. The dependent probability for MV 3LP - 41 in the wrong configuration given that the probability for valve MV 3LP - 40 in the wrong configuration is 1.5 x 10^{-3} is,

$$HEP_c = \frac{1+n}{2} = \frac{1+1.5\times 10^{-3}}{2} \approx 0.5$$

This results in a mean unavailability for common error of both valves in the wrong configuration of (1.5 x 10^{-3}) x 0.5 = 7.5 x 10^{-4}

Incorporation of category A errors into the PSA is straightforward and is generally made via basic events in a fault tree. Assigning an independent unavailability of 1.5 x 10^{-3} to both MV 3LP- 40 and 41 assuming no dependency, an unavailability of the two trains of 7.5 x 10^{-4} can be assigned to the CCF basic event.

(1b) Category B, incident initiating tasks

The purpose in quantification is to determine the frequencies of category B errors. This means that any probability per opportunity numbers must be multiplied by frequencies of the opportunities.

The character of category B errors is such that the same methods as mentioned for category A errors in section 4.1 can be used as a basis for quantification. ASEP-HRA and other simplified versions of THERP may not be sensitive enough to account for all aspects of the layout, readings and procedures. They may be only good enough for conservative screening purposes.

(1c) Category C, post incident tasks

As human performance is very context dependent, any PSF may have a strong impact on human reliability. Quantification is uncertain because this impact cannot presently be modelled with high confidence because no fully validated model is available. Therefore, the best method is to use data, which has been collected in a similar context. This means that one should use plant specific simulator data, which includes

- Probabilities of errors of omissions and commissions, including misdiagnosis as well as execution phase errors.
- Time Reliability Curve (TRC)- A curve representing the probability of not carrying out the required action in a given time.

It is clear that one cannot possibly obtain extensive plant specific simulator data for all plants. In particular, misdiagnosis and commission errors in general may be so rare that no quantification is possible with a reasonable number of experimental runs. Some methods can be used that are based on judgements.

Misdiagnosis : The confusion matrix concept can be used to assess the probability of confusing a transient i with a transient j, possibly leading to erroneous actions. The probabilities Pij of such confusions depend mostly on the similarity of symptoms such as alarms, annunciations and the duration and rate of change of various signals. Another factor influencing the confusion probability is the degree of training and simulator practice given to the operator with respect to each transient. Further, it is also possible to recover from a misdiagnosis if unexpected new symptoms appear and alert the operators and if there is enough time available to normalise and correct the error. Recovery factor Rij may be defined to account for the alerting symptoms and the time available for action.

Slow diagnosis : Time reliability curves/correlations (TRCs) [3] can be used to assess the probability that a correct diagnosis is not done within the time available.

Execution errors : For slips and omissions associated with the execution phase of the action, one may use THERP Handbook data [3].

Recovering from execution errors: If enough time is available and excution error is alarmed one can use the following methods based on expert judgement.

- Paired comparisons : It is a psychological scaling technique in which experts judge whether a human error is more likely in task ‘A’ or task ‘B’. Paired comparison judgements are required between all pairs of a set of tasks. To convert the interval scale of tasks' error likelihood to a ratio scale of HEPs, at least two (or preferably more) of the tasks must have known HEPs for calibrating the interval scale.

- Success likelihood index methodology (SLIM) : SLIM is a HRA technique that uses expert judgement to develop HEP estimates. It is a systematic method that scales task error likelihood as a function of the conditions (PSFs) influencing successful completion of the task. An absolute measure of success probability for the scaled tasks can be calculated after calibrating the scale with reference tasks of known reliability. Multiple judges assess relative importance (weight) of each PSF with respect to its impact on the task. A second independent assessment is made of how good or how bad each PSF is. These are called the ratings of the PSFs. The sum of the products of the weights and ratings of the PSFs considered is the SLI. SLI represents the judges' belief regarding positive and negative effects of PSFs in task success. SLIM assumes that the SLI is logarithmically related to the probability of success Pr(S) of the task, i.e. log (Success Probability) = a $*$ SLI + b where a and b are empirically derived constants. At least two tasks of known reliability are required to calibrate the relationship empirically. Direct Numerical Estimation (DNE) or Absolute Probability Judgement (APJ) as it is also called, is recommended if two tasks of known reliability cannot be obtained.

- Absolute probability judgement: APJ/DNE requires experts to provide HEP estimates for each task. An advantage is that it can be used to obtain estimates of the uncertainity bounds. The experts do not have to make as many judgements as in 'paired comparisons'. Individual estimates are aggregated by arithmetic or geometric average.

The uncertainties of the probabilities obtained from these various methods are high. This is also true for plant specific simulator data as the operator behaviour may or may not be the same during real and simulated accidents. However, these data are the one most recommended.

Example on Post Incident Task : Small Break LOCA (Oconee PSA)

The example illustrates the modelling of Type-C human actions and presents a case of the human error quantification. The event is modelled in the ET is depicted in Fig. VI-8. The events depicted are:

S	:	Small break LOCA
K	:	Failure of the RPS to trip the reactor
Us	:	Failure of core heat removal by high-pressure injection (HPI)

Ys : Failure to maintain reactor coolant system (RCS) makeup supply

Xs : Failure to maintain long-term heat removal.

Further modelling is developed in the support logic and system FTs. There is no support logic for event K as this event is not evaluated further. Event Us corresponds to the top gate of FT for high pressure injection and so has no support logic. The support logic for event Ys is presented in Fig.VI-7. One operator action that features in the dominant accident sequence is YRBSH in Fig.VI-7. The errors appear in the dominant accident sequences and the quantification is briefly outlined here.

Event 1, YRBSH : Operator fails to terminate RB spray operation during a SBLOCA.

Situation : The RB sprays are automatically actuated after a small break LOCA. They may not be needed for extended operation, depending on the operability of the RB cooling units. The operator could terminate spray operation to conserve the Borated Water Storage Tank (BWST) supply for HPI.

Factors : Once spray operation is initiated, there is no procedure that requires its termination (in fact, this would violate a general caution not to defeat a safety system)

Analysis : The conditions stated suggest an HEP of 1.0. However, some credit was given for an operator to respond, after the sprays have reduced the RB pressure, by turning off the spray pumps, thus also conserving the BWST supply. Thus, the HEP assessed for this event is 0.5.

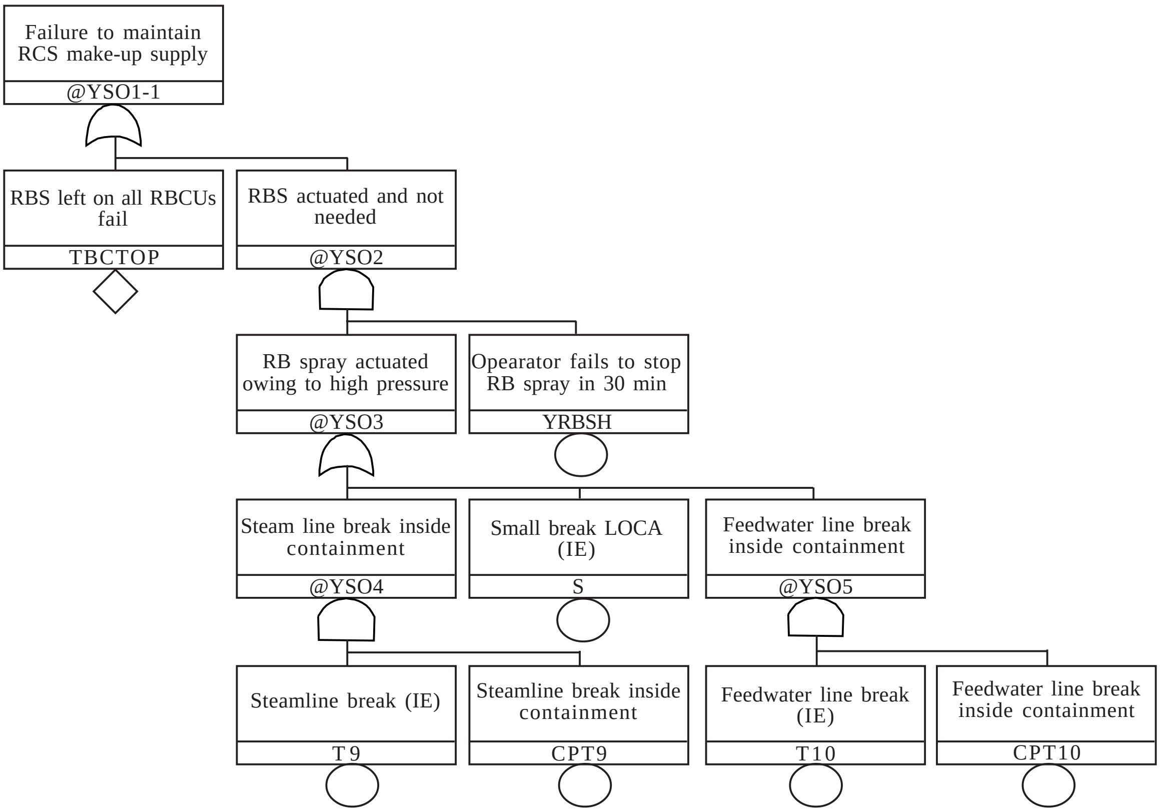

Failure to maintain RCS make-up supply
@YSO1-1
RBS left on all RBCUs fail
TBCTOP
RBS actuated and not needed
@YSO2
RB spray actuated owing to high pressure
@YSO3
Opearator fails to stop RB spray in 30 min
YRBSH
Steam line break inside containment
@YSO4
Small break LOCA (IE)
S
Feedwater line break inside containment
@YSO5
Steamline break (IE)
T9
Steamline break inside containment
CPT9
Feedwater line break (IE)
T10
Feedwater line break inside containment
CPT10

FIGURE VI-7 : SUPPORT LOGIC FOR SMALL BREAK LOCA ET TOP EVENT Y_S, FAILURE TO MAINTAIN RCS MAKE-UP SUPPLY

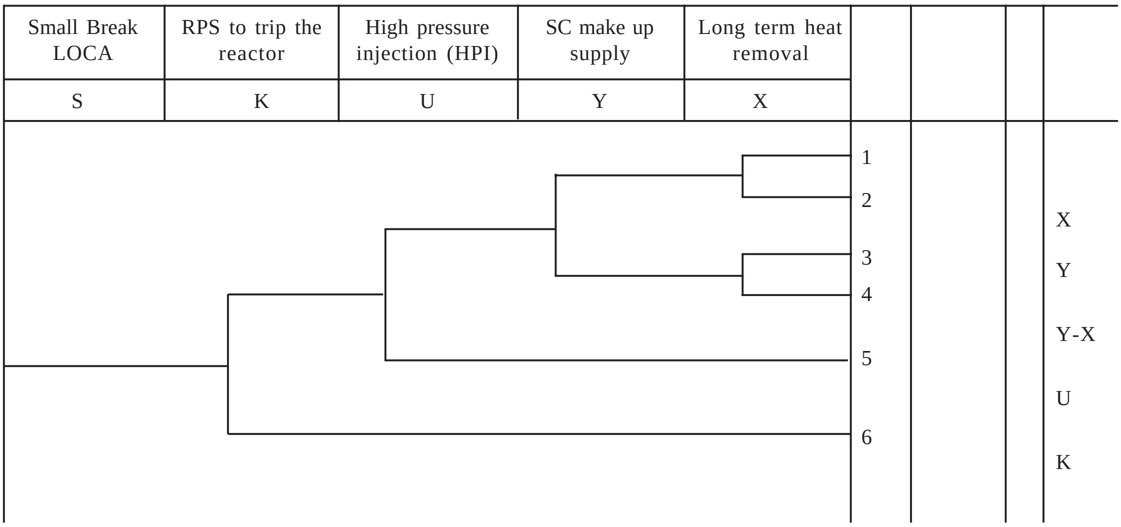


FIGURE VI-8 : OCONEE: EVENT TREE FOR SMALL BREAK LOCA EVENTS

Example for Quantification of Human Reliability using the HCR and THERP Models

The objective of treating human reliability in a PSA study is to ensure that the key HIs of typical operating crews are systematically incorporated into the study. In doing this, factors like MMI, training, procedures, knowledge as well as experience of the operators are also considered. This exercise helps in formulating/modifying the accident management procedures to reduce the chances of human error, thereby minimising the CDF. The example given here [92] considers HRA of the scenario during the total power failure due to fire incident that occurred in NAPS. The occurrence of fire in the turbine building and explosive sound were cues to the operator regarding the seriousness of the situation. These cues led him to trip the reactor and initiate crash cool down. Subsequent occurrence of total power failure at around 8 minutes into the incident was an additional cue that Station Blackout event has occurred.

Station blackout actions

The actions required to be taken in this situation are:

To start diesel engine driven fire fighting pumps

To open Fire Water (FW) injection valves (2 Nos.) to Steam Generators (SGs)

To ensure PHT system integrity for assuring continued core cooling

To ensure sub-criticality status of the reactor

The time available (t) for injecting FW into SGs is about 60 minutes and this is based on the inventory in the SGs. Hence, all the above actions are needed to be taken within an hour.

Quantification for crew non-response probability using HCR model

The nominal time for starting two diesel driven pumps and opening two valves is assessed as 20 minutes. This is the median time.

(i) Performance shaping factors (PSFs)

In Indian PHWRs, the operator is well trained. Hence the PSF for operator experience, K1= - 0.22. Considering the situation to be one of grave emergency, the PSF for stress level, K2 = 0.44. MMI is considered not applicable here, as the situation is one of total power supply failure. Hence, the PSF for quality of operator/plant interface K3 = 0.

Hence, the median time adjusted for the PSFs,

$T_{1/2}$ = 20 x (1- 0.22) (1+ 0.44) (1+ 0) = 22.46 minutes

The normalised time = $t/T_{1/2}$ = 60 / 22.46 = 2.67

The actions are rule based. Hence the HCR correlation coefficients are:

$A_i = 0.601$, $B_i = 0.6$, $C_i = 0.9$.

P(t) the crew non-response probability in time *t* is given by Eq. (VI-1). For this situation P(t) = 0.048

(ii) HEP for actions using THERP handbook data

Starting of diesel driven pumps:

The subtasks involved are listed below. The associated HEPs are given in brackets.

(i) Starting the diesel engine (0.001)

(ii) Observing whether the rated speed has been attained (0.001)

(iii) Opening the pump discharge valves (0.001)

(iv) Checking downstream pressure gauge (0.001)

(v) Informing the control room.

As the fire fighting water pumps are tested weekly, the operator is experienced in carrying out this task. The stress level is considered to be moderately high. Hence a stress factor of 2 is considered. The non-recovery factor is taken to be 0.1, as the action is supervised. Hence, the HEP = 0.004 x 2 x 0.1 = 8 x 10^{-4}. For two pumps, the HEP contribution for starting of the pumps, HEP (pumps) is 1.6x10^{-3}.

Operation of the fire water injection valves to SGs:

Probability of failure to open one valve is 1E-03. Since the action is not frequently carried out, a stress factor of 5 is considered. Hence HEP for a valve is 5E-03. For two valves, the HEP contribution for operation of the valves, HEP (valves) is 1E-02. For ensuring PHT system integrity and core sub-criticality, the time available is sufficiently large. Hence the associated HEPs are negligible. The overall HEP is therefore:

P(t) + HEP (Pumps) + HEP (Valves) = 4.8E - 02 + 1.6E - 03 + 1.0E - 02 = 5.96E - 02

(f) Integration of HEPs into overall PSA quantification

HEPs arrived at based on above quantification processes are included in FT/ET modelling for accident sequence/core damage quantification (Level 1 analysis), for release frequency (level 2 analysis) estimation and also for consequence to public domain (level 3 analysis), as required with the consistent established scope of PSA work.

(g) Sensitivity/Uncertainty analysis [88]

Each HEP is an estimate derived by using models, more basic (task oriented) data and judgement. To assign a distribution to an estimated HEP depends on expert judgement, since background data for HEP is scanty. For each specific HEP, a best estimate and an upper and lower bound can be provided. It is suggested that log normal distribution be used with the upper and lower bounds as the 5th and 95th percentiles. A simplistic method of assessing uncertainty in the quantitative value (rather than identifying precisely the underlying cause of HE) could be as follows.

The HEP results using best estimate, can be divided into two regimes, 0.1 to 1 and < 0.1; A beta distribution can represent HEP in the regime 0.1 to 1.

$$P(x) = \frac{1}{B(\mathrm{r}, \mathrm{s})} \; \mathrm{x}^{y-1} \, (1- x)^{s-1} \quad (0 < \mathrm{x} < 1) \qquad \text{(VI-3)}$$

B(r, s) : normalisation factor; r and s >1,

For the regime < 0.1 assign log normal distribution

$$P(x) = 2\pi\alpha \, (x)^{-1/2} \exp\left(\frac{1\mathrm{n}(\mathrm{x} - \mu)^2}{2\,\sigma^2} \right) \qquad (\mathrm{x} > 0) \qquad \text{(VI-4)}$$

$$\mu = \frac{r}{r+s}\,, \text{ where the mean is } \alpha = \exp(\mu + 0.5)^2, \text{ median } x_{50} = \exp(\mu) \qquad \text{(VI-5)}$$

For sensitivity analysis, changes in the assumption regarding PSFs and the assumptions in HRA can be made to identify the range of the quantification that could be expected.

(h) Documentation

The purpose of documentation is to provide, at all stages of the HRA, a traceable account of the analysis and the results, to facilitate additional analysis at a later date and subsequent applications of the results, and to communicate a clear perception of the impact of the human element on plant safety. The documentation may best be organised in relation to the tasks in the HRA framework making clear what the inputs and outputs were for each task leading to the final quantification. Results should address numerical impacts on CDF and other risk measures, key sensitivities and the major qualitative findings and the insights derived from them. These may include recommendations for improvements to procedures, training or MMI and the influence of human error on the relative ranking of dominant sequences. All significant documents should be referenced and supporting information such as those on task analyses, operator interviews and expert opinion studies should be documented to provide a basis for judgements made. Although the approach is presented in terms of discrete tasks it is acknowledged that at all times, the process should be iterative between tasks.

VI-2.2 HRA in PSA for Events in Non-full Power Operation

In order to consider plant safety more comprehensively, PSA must include the assessment of operation other than high power (low power and shutdown), accident management, BDBA situations, and external events. The nature of operations in such phases, as well as their differences from high power places new requirements on HRA methods. The aspects to be considered in such situations are given below.

(a) Ex-control room actions/operations

These involve command delivery, movement to gain access, local execution and possibility of local feedback not being provided, which is an opportunity for error.

(b) Coordination and communication within teams and between teams

In general, there are many more persons involved in shutdown/accident management who make decisions at various levels. Coordination and control, conflicts, unforeseen consequences of actions, possible lack of written procedures and the availability/flow of information from/to the person in the plant and persons in remote locations all become very important. HRA needs to consider/model group coordinated behaviour. Data needed would relate to failure of coordination and communication, failure of command delivery, i.e. transactions between control room and field, and failure of information delivery. In HRA, factors like communication procedures and protocols (e.g. receiver to repeat a command confirming that it has been understood) and the type of communication equipment used, are to be considered.

(c) Actions without procedure

The number of configurations possible in shutdown is too many. If clear written procedures are not there for all such states, then operator response would have to be strongly based on knowledge and training. Uncertainty about plant configuration would lead to error. Also, mistakes are possible while considering potential consequences during response planning. In accident management, EOPs include Accident Management (AM) guidance. The possible lack of procedures may bring out unconstrained possibilities of plant state, due to actions that include situations not identified by procedure or misrepresentation of instrument readings. Furthermore, there could be a change of persons executing the job. The situation in case of external events is similar to the AM case for internal events. The data needs are dictated by the actions to be improvised.

(d) Decision burden

Decision burden arises in 'real' situations when operators have to consider the consequence of a real action. When there are uncertainties about plant states, with the appearance of unexpected alarms/'values' of parameters or when actions foreseen and/or addressed in the operating procedures, are not in accordance with plant safety vis-à-vis the real situation involving probability-consequence tradeoffs between two or more actions, decision burden results HEPs would then also be related to chances of recovery. While the approach to quantification of human reliability would remain essentially the same as for events in full power operation, there is a need to explicitly consider the factors arising out of the issues in the particular context or environment in which the operations are to take place. The risk associated with events in non-full power operations is in general seen to be somewhat higher.

VI-2.3 Additional Points to Consider in HRA

While selecting the reliability model for quantifying human error, one should be careful that human tasks considered, fit into the model; otherwise, quantification results could be different from reality. Uncertainties in modelling play a significant role in such assessment and hence in the overall PSA results.

In Indian NPPs operators are qualified, trained/retrained (presently on simulators too) and licensed. They follow procedures to execute an action and it may be difficult to draw a distinct line and label an operator action (in particular one from the control room) as skill, rule or knowledge based. (Jens Rasmussen, the originator of these terms himself acknowledged that the dividing lines among them can be fuzzy at times). The HEPs themselves may be more influenced by PSFs relating to personality traits like stress, motivation and culture. In the absence of adequate plant specific data, as a first order analysis, a HEP of likely value say 3E-3 [3] may be used and modified by PSFs using the analysts judgement; Alternately a simplistic approach based on a, adequacy of time available, quality of indication and type of task, matrix could be used, giving HEP values from expert judgement/generic data. Such a matrix is given in the table below. Once specific human actions have been identified to be dominant or recurring in safety significant event occurrences, detailed modelling of HE should be done after careful review of various available models and discussions with plant personnel. Table VI-2 gives preliminary post-IE HEP quantification [84].

TABLE VI-2 : QUANTIFICATION OF POST IE-HEP

Task Type	Quality of Indication	Time			
		T1	**T2**	**T3**	**T4**
Type-1 (Straightforward and/or familiar)	I1	0.003	0.003	0.006	1.0
	I2	0.027	0.027	0.054	1.0
	I3	0.15	0.15	0.30	1.0
	I4	1.0	1.0	1.0	1.0
Type-2 (Average complexity and familiarity)	I1	0.007	0.007	0.014	1.0
	I2	0.05	0.05	0.10	1.0
	I3				1.0
	I4	1.0	1.0	1.0	1.0
Type-3 (Very complex or unfamiliar)	I1	0.007	0.007	0.035	1.0
	I2	0.05	0.05	0.25	1.0
	I3				1.0
	I4	1.0	1.0	1.0	1.0

I1	Unambiguous indication	T1	Time available is unrestricted.
I2	Interpretation required	T2	Time available is more than required.
I3	Unclear indication	T3	Time available is about equal to time required.
I4	No indication	T4	Time available is less than time required.

APPENDIX-VII

PARAMETER ESTIMATION FROM PLANT DATA SOURCE

VII-1 Component Failure Rate Estimation [5]

The parameter to be estimated is either the standby failure rate l_s or the operating failure rate l_0 of the exponential distribution. The steps for estimating both these parameters are as follows.

- Identify the component population whose failure history is to be used to estimate the assumed common component failure rate (i.e. components assumed to have the same failure rates).
- Identify the time period during which the component failures are to be counted.
- In the component population, count the total number of failures N and the total component standby time T (or total operating time for operating components) for the time period.
- Estimate the plant specific mean failure rate λ, as $\lambda = N / T$
- For an assessment of the uncertainties, Bayesian approach can be used in which an appropriate prior distribution is updated using the ‘sufficient’ information to provide a posterior distribution.

VII-2 Repair Time Estimation [5]

The average repair time T_R is estimated as the sum of the observed repair times divided by the number of repair actions. The repair times should include detection plus waiting times. It is important to identify any delay time during which repair is unlikely to be performed, because of the time required for detection and repair initiation.

VII-3 Test Frequency Estimation [5]

The estimation of actual test frequency, or equivalently the actual average time between surveillance tests, can be made, if testing is more frequent than specified in the technical specifications and it is desired that credit be taken for the extra testing. Some of the tests do not contribute to the component (system) unavailability, because during tests the component is in a safe state (e.g. operational) or test override, if a demand on the operation of the component arises, as permitted by design. Tests that occur during a reactor state for which the system is not required to operate should not be taken into account in assessing the unavailability due to testing.

VII-4 Estimation of the Average Test Duration [5]

The test duration time needs to be estimated when the test causes the component to be unavailable. The average test duration time t is estimated as the sum of the total test duration in a certain time period, divided by the number of test operations. The test duration time is the time period from the moment the component was taken out of service to the moment it was returned to service.

VII-5 Estimation Of Maintenance Parameters [5]

The estimations of maintenance frequency and maintenance duration are similar to those for test frequency and test duration.

APPENDIX-VIII

RECOVERY ANALYSIS

Each accident sequence minimal cutset represents one possible way the sequence may occur. The information available to the operator and the recovery action to be taken generally depend on the combination of events that have occurred and hence on the particular minimal cutset. Therefore, recovery actions are generally established considering at the minimal cutset level rather than at the accident sequence level. Since there may be a large number of minimal cut sets for an accident sequence, it may be necessary to consider recovery for only the most significant minimal cutset. A probability of non-recovery is estimated for each minimal cutset which is recoverable by some operator recovery action. The frequency of the minimal cutset is then multiplied by its probability of non-recovery to estimate the final minimal cut set frequency. The final estimated frequency for an accident sequence is computed using these minimal cut set frequencies with recovery. In general, recovery actions can be separated into those which can be accomplished from the control room, and those which can only be performed locally. If recovery can only be performed locally and the local site is inaccessible, the primary event is considered non-recoverable [5]. The recovery actions considered here are primarily the responses beyond EOPs taken to mitigate the consequences of an accident. Some analysts may also include responses identified in EOPs, but for which deterministic accident analysis has not taken credit.

Once a primary event is deemed recoverable and the location of the recovery action is determined, a critical time for the recovery action is estimated. Two types of critical times are considered when determining the critical time for a recovery action.

The primary event itself can have a critical recovery period, which is independent of the accident sequence or of the state of the core or containment in an accident sequence. An example of this type of primary event critical time is that associated with the lubricating oil cooling for a pump. If the primary event is the loss of such cooling, there is a definite time interval during which the pump can operate without the cooling, and this time interval defines the critical time for the recovery of the primary event.

For the second case, the time in which a mitigatory action can be carried out is considered. In general, the accident sequences can be combined into groups with each group having its own set of critical times. For example, sequences initiated by large LOCAs have different time constraint for recovery than do sequences initiated by small LOCAs. In this second type of critical time examination, the questions asked in determining the critical time for recovery are phenomenological in nature. For example, if none of the containment spray pumps receives an actuation signal, the critical time during which they can be manually actuated is determined by how long it takes for the containment to be pressurised to the point of failure. When both types of critical times are in application for a particular recovery action, the shortest critical time is used. Table VIII-1 gives probabilities of recovery and non-recovery based on generic recovery model.

TABLE VIII-1 : PROBABILITY OF RECOVERY AND NON-RECOVERY BASED ON GENERIC RECOVERY MODEL [5]

P(R)	P(NR)	Critical Time for Recovery Action	
		In control room (min.)	Locally (min.)
0.00	1.00	< 5	< 5
0.75	0.25	5 - 10	15 - 20
0.90	0.10	10 - 20	20 - 30
0.95	0.05	20 - 30	30 - 40
0.97	0.03	30 - 60	40 - 70
0.99	0.01	> 60	> 70

APPENDIX-IX

FIRE PSA

IX-1 Introduction

The impact of fire would be extensive in terms of common mode failure of redundant and diverse safety systems. Deterministic and probabilistic techniques are used to assess a fire hazard. Deterministic analysis is typically, carried out first as a regulatory requirement. It is usually developed early in the design of new plants and updated as and when required. Fire risk analysis, i.e. Fire PSA, may not be practical before construction stage since there could be significant changes in layout and construction and materials involved. Fire PSA is to supplement the deterministic Fire Hazard Analysis (FHA) and is recognised as a tool that can provide valuable insights into plant design and operation. Fires are generally treated as external events, although these may be covered, under this section are generated by plant equipment and personnel.

Fire PSA requires information on several important aspects of fire (e.g. ignition, progression, detection and suppression, characteristics of materials under fire conditions) as well as plant safety functions and their behavior under accident conditions. The fire PSA can be divided into 5 major parts: data collection , hazard analysis, propagation analysis, which is analogous to component-fragility analysis, plant system and event sequence analysis and release frequency analysis. The hazard analysis develops the frequency and magnitude of the ‘externally imposed stress’ where ‘stress’ is in terms of potential fire induced accident sequences. The propagation analysis investigates the resistance of the plant to fire damage by studying the propagation of the fire and the effectiveness and timing of suppression. Plant system and event sequence analysis evaluates the response of plant systems to the accident sequence triggered by fire leading to core damage and the release frequency analysis evaluates, taking input from preceding analyses, the response with respect to release of radioactive material from the containment.

The availability of a plant PSA model for internal initiators that represents the contributions to core damage (Level 1 PSA), is a prerequisite for fire PSA. Expanding internal events PSA to fire PSA requires other plant specific data, like cable locations, grouping, and routes. Where plant specific data are not available, generic or other sources could be used with justification for conservatism.

The expertise needed to conduct Fire PSA must combine several disciplines. Thorough knowledge is required of plant design and operation, PSA techniques, fire science, as well as the design and operational aspects of the fire protection systems, including their interaction with the nuclear safety systems. It is essential that the fire PSA team includes specialists who are capable of evaluating the fire damage effects on the SSCs important to safety, and of assessing fire induced failures of power and C&I circuits. The ability to evaluate the adequacy and the likely performance of the installed fire detection and suppression system is also of importance, especially regarding the timing of system actuation compared with timing of component failures, where such timing is used in the analysis.

IX-2 Interface with Internal Events PSA

This task covers examination and interpretation of the existing internal events PSA to determine the plant systems and components as well as those related items of the model that are important to fire PSA.

Each IE of the internal PSA has to be reviewed in order to determine whether it can be induced by fire. Based on low probability consideration, some IEs could have been excluded from the internal events PSA. In such cases the analyst must also consider the possibility of more severe faults that are induced by fire than which have been previously analysed. For such situations a new set of event sequences may have to be developed. For each IE that has potential to be caused by a fire event, it is necessary to determine the systems required for mitigation.

The failure probabilities of the components may have to be adjusted to take into account the unusual environmental conditions imposed by the fire event. The values of HEP before occurrence of fire IE need not be altered.

For the components identified for fire hazard, it is necessary to determine the cables and circuits required to perform its safety-related function. Each such cable should be evaluated to determine the effect of its failure on the operation of the components. It is important that all possible failure modes are identified. The following failure modes or a combination of these may be considered for cables

(1) Open circuit

(2) Short to ground

(3) Short circuit

(4) Hot short

  (1) Intra cable hot short

  (2) Inter cable hot short

These faults may lead to false readings on a sensor circuit, actuation of non-energised systems, or application of high and destructive voltages to low voltage systems. Depending on the plant and the fire scenarios these may lead to serious IEs, or to the additional contributors of system unavailability. Also, credit should not be taken for proper functioning of any electrical or I&C circuit for which detailed analysis could not be done.

IX-3 Methodology [94-97]

The analysis is carried out in five steps, (i) Data Collection, (ii) Hazard Analysis, (iii) Propagation Analysis, (iv) Plant and System Analysis and (v) Release Frequency Analysis

IX-3.1 Data Collection

Fire PSA relies on availability of plant information, both qualitative and quantitative. It concentrates on collection of the plant specific data required for fire risk modelling. The information required for FHA can be summarised as follows:

(1) Description of plant systems, including the location of components and systems within structures. Especially important are routings of safety-related power and control cables.

(2) Fire-protection report, which contains information on temporary and permanent combustible material loading, suppression systems, ventilation systems, and safety equipment inventories for each fire zone, as well as a simplified FMEA for some zones.

(3) Reports on the fire qualification of components with physical data for electrical cables and trays.

(4) Results of the plant-system analysis for internal IEs, especially accident sequences descriptions. Accident sequence frequencies are also useful for screening purposes.

(5) A compilation of plant event reports of safety significance involving fires at NPPs.

Two types of plant specific data are to be obtained; internal events PSA data and fire related data. The information that is needed from the internal event PSA data is the list of IEs, PSA logic models, basic events of the model, CCF events, and human actions. Fire related data can be classified as physical characteristics of the fire compartments, and their inventory, fire occurrence data, reliability estimates of the fire detection and suppression system, human actions and HEPs, and fire induced equipment failure modes and damage criteria. The data for the physical characteristics of the fire compartments may be readily available from the deterministic analysis.

The required plant specific information can be acquired from various design sources, as well as from plant walk downs, where in-situ information is gathered and verified. The recommended sources of plant specific information include design manuals/design basis reports of systems, equipment lists, design drawings and plant procedures and safety reports. All information obtained from plant documentation has to be verified by visually inspecting each fire compartment throughout the plant. Information on any modifications made to the SSCs during the maintenance, etc. should also be collected.

Plant specific fire occurrence data are collected for the source of ignition, the materials involved in the fire, and the damage to the equipment and cables. It is advisable that, in addition to the fire events, the analyst collects generic data on the fire initiation frequencies which are available in the literature and which are drawn from the NPP operating experience. Reliability data for fire protection features include data for active fire protection equipment and for inter-compartment fire barriers. These data can be derived from plant operational experience or using the available plant specific data, extrapolated from generic sources of information. A number of operator actions in the internal events PSA model, including certain important recovery actions will have to be reviewed and, in some cases, re-quantified because of fire effects like smoke, heat, etc. The analyst will also have to establish a list of equipment types within the plant and to specify their damage mechanisms (e.g. heat, flame, smoke, water, etc.) and failure modes.

IX-3.2 Hazard Analysis

Under this, frequency and magnitude of the event-generated impact are evaluated. This is done as a first step by identification of critical areas and assessment of fire frequencies.

IX-3.2.1 Identification of Critical Areas

The plant has to be divided into distinct fire zones/areas, which include compartments or fire cells depending upon the fire containment capabilities. If the location is surrounded completely by walls, ceilings, doors that are fire rated, then the location may be called a ‘Fire compartment’. If the separation of the location from others is not by fire barriers but by methods like spatial separation, so that the fire in one location doesn’t affect in the other, then the location may be called a ‘fire cell’. Where a fire rating cannot be established and justified, it is necessary to consider larger areas of the plant as a single fire compartment. In such a situation fire compartments may be divided into fire cells. The division of all plant buildings and structures into fire compartments and cells, which are scrutinised individually in the analysis, is an important task that permits systematic evaluation of fire events. Use of comprehensive and flexible numbering system for fire compartment and cell identification is advisable. The fire resistance ratings of the walls and ceilings may be determined analytically or be evaluated by engineering judgement according to simplified state-of-the-art methodology that involves the thickness and material of the wall (from graphs or tables published in the literature). The fire resistance rating of each fire compartment barrier is determined by the lowest fire rated element of that barrier.

IX-3.2.2 Location Screening

The purpose is to identify the locations important to the fire risk analysis. The information about the location of safety related equipment, combustible material quantity, frequency of fires and availability of detection and suppression systems are to be obtained and analysed for identifying the areas with significant fire risk. The methods available for identifying the important and critical areas are described below.

(1) The first method considers only the presence of fire vulnerable safety components. The location of interest is considered important if it contains enough safety components so that a severe fire could fail one or more safety systems, which may or may not be in same train. The loss of only one division of safety equipment means a loss of redundancy and does not necessarily lead to core damage and a release of radionuclides; nevertheless, the analyst may decide that this is an event to be quantified.

(2) Failure modes and effects analysis (FMEA)

The locations containing fire-vulnerable safety equipment are identified as in method 1.

Assuming the loss of all equipment at the location, if there is no IE to occur, the area is screened out. Given a LOCA or a transient, a number of safety functions are required for safe shutdown. If the loss of all equipment in the location of interest prohibits the performance of any or all required functions, the location is tabbed for further analysis. The fire-induced loss of control systems is judged to dominate fire induced hardware losses. The event may be screened out if fire causes an IE that will not cause any harm to the safety functions such as safe shutdown of reactor and maintaining in safe shutdown state, decay heat removal and prevention/monitoring of radioactive release.

Where inter zone fire propagation (within fire compartment due to some damage caused during maintenance) may be considered to be important, a more complicated screening approach considering fire loads, effectiveness of fire barriers in the compartment and importance of equipment in adjacent locations may be employed.

(3) In addition to the consideration of a fire in the safety significant component and loss of functions as in method 1 and 2 above, this method takes into account the inventories of combustible materials, the nature of adjacent locations, fire brigade access, ventilation systems, and qualitative judgements on the likelihood of fire initiation and progression. Since the characteristics of adjacent compartments are explicitly considered, the possibility of fire spread from the rooms containing large inventories of combustible materials to compartments containing safety equipment is not overlooked. Fleming et al. discuss a method where the frequency of occurrence of a particular release category, due to all IEs except fire, divided by conditional frequency of that release category, given the loss of all components in the zone of interest, is compared with a rough estimate of the frequency of fires for that zone. If the release category frequency ratio is greater than fire frequency, the location is judged to be an insignificant contributor. This method requires a prior or concurrent assessment of other IEs.

IX-3.2.3 Fire Occurrence Frequency Analysis

The frequency of occurrence can be established from the historical records. Unavailability of this data leads to large uncertainties. Kazarians and Apostolakis (1980) model the frequency of fires for various compartments, using a probability-of frequency framework to consistently treat uncertainties. The fire frequencies are derived by Bayes’ theorem using statistical data (as relevant to plant under study) on number of fire incidents in the specific areas. NUREG CR/2300, Section 11.3.3.1.2 gives the procedure and relevant data applicable to US light water reactors for working out fire frequency probability density function. For the places where there is insufficient data available, relevant generic data may be used with cautious judgement.

IX-3.3 Propagation Analysis

The purpose is to determine the likelihood and extent of various levels of damage in the fire compartment given that a fire has occurred. The methods that can be used for fire propagation analysis are as follows.

IX-3.3.1 Using Multi Stage ET Model

This method uses event trees to separate fire model into 4 elements; (i) ignition, (ii) detection, (iii) suppression, and (iv) propagation. Each element heads a column of the ET. The fire is assumed to start in one component and potentially propagate to the next one. The use of these elements is illustrated in Fig. IX.1 by a two-stage ET for 2 redundant components in the location (more stages may be required for more components). Sub-models as necessary are used by FT methodology to quantify conditional branching probabilities of ETs.

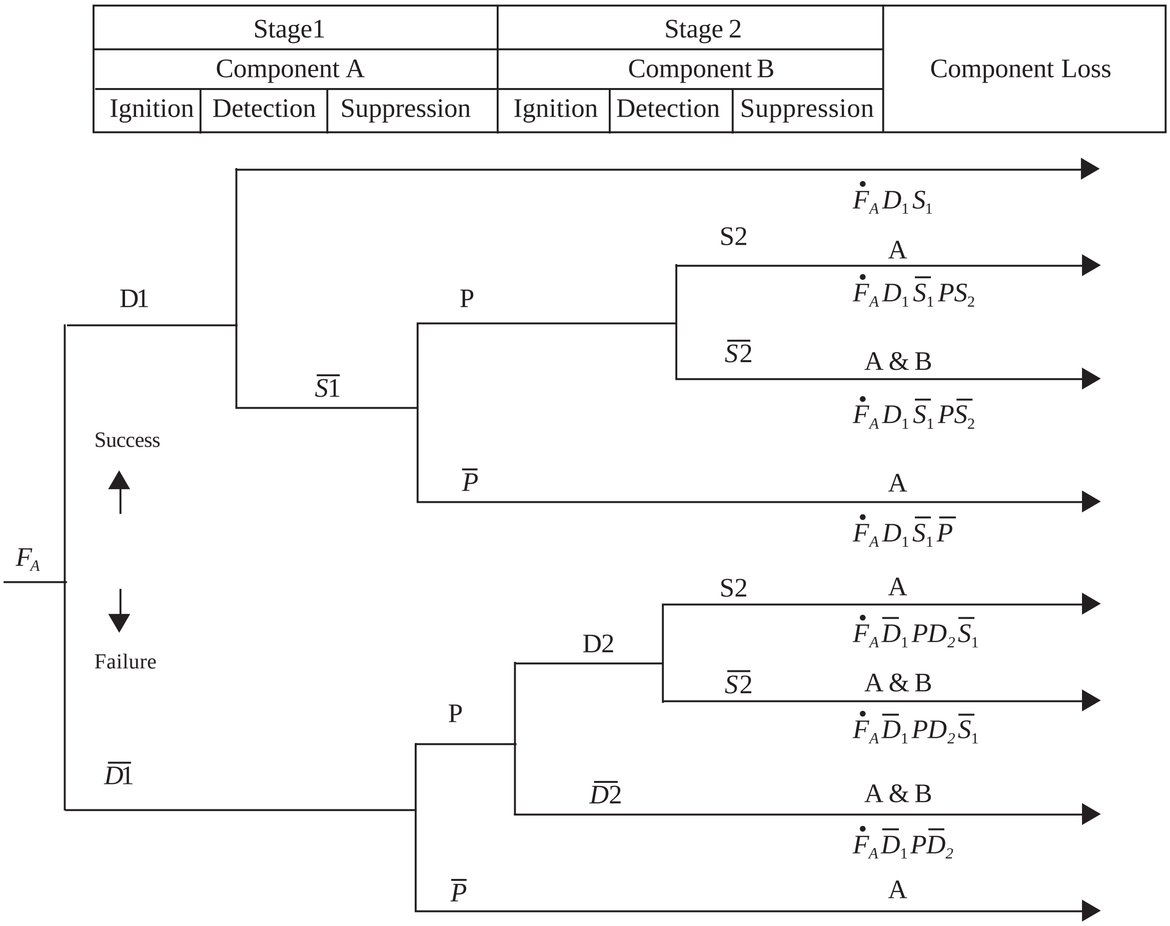


FIGURE IX-1 : ILLUSTRATIVE TWO-STAGE ET FOR TWO REDUNDANT COMPONENTS

IX-3.3.2 Construction of Physical Models

In this approach, fire growth and suppression are viewed as competing time dependent processes. One or more representative fire growth scenarios are developed for each location depending on the physical configuration of the area. The distribution for the analyst-defined characteristic spread time is then compared against the distribution for suppression time to obtain the conditional frequency of fire growth, given the fire scenario. For example, assume the two horizontal cable trays, one stacked over the other, contain critical power and control cables. In the representative fire scenario, a fire initiated in lower tray spreads to upper tray in t_g minutes. The mean fire suppression time is t_s minutes. Note that t_s includes the time to detect fire, which often requires human response. Therefore, the distribution of the fire-spread frequency is the distribution of frequency with which t_s exceeds t_g. The fire-spread time is computed by using physical models, while t_s is estimated from statistical data

The key to this approach is the explicit use of simple physical models for fire, which enables the analyst to properly account for the extremely strong dependence of fire behavior on physical configuration of the fuel and its surroundings, and the consistent treatment of large uncertainties in the model outputs. With these physical models, using a simple ignition- or damage-threshold temperature criterion, the impact of fire on its surroundings is then computed as function of time.

Various computer models like Available Safe Egress Time (ASET-B), CFAST, and COMPBRN, etc. can be used. ASET-B is used for calculating the temperature and position of hot layer in a single room with closed doors and windows. The unavailability of a provision for accounting for ventilation, forms a major limitation of this code. CFAST (Consolidated model of Fire growth And Smoke Transport) is a multi-room fire model that predicts the conditions within a structure resulting from user specified fire. An important limitation of this model is the absence of a fire growth model. COMPBRN III has been generally used in conjunction with PSA in nuclear industry. This model assumes a relatively small fire in a large space or fire involving large fuel loads early during pre-flash-over fire growth period. The model emphasis is on the thermal response of elements within the enclosure to a fire and on modelling simplicity. The temperature profile within each element is computed and an element is considered ignited or damaged when its surface temperature exceeds the user-specified ignition temperature or damage temperature. This has been used successfully for small experimental fires with good results but for very large room fires approaching flash over, may be subject to greater uncertainties.

Details of other codes available and their origin can be found in Chapter 11[94]. Because the behaviour and effects of fire do depend strongly on the layout of location of interest, the physical modelling approach is better compared to others.

IX-3.4 Plant and System Analysis

Once the frequencies of fire induced component losses are assessed, it is possible to estimate the frequency of fire-initiated accident sequences leading to core damage. As with other IEs, separate ETs may be constructed for fires because the operator, rather than the automatic actions, may be responsible for shutting down the plant in response to fire. Often the analyst simply modifies the front end of existing ET for other IEs to model fire in the PSA. The conditional branching probabilities would be altered to reflect the dependence on fire. However, if fires are to be treated as a separate event, care should be taken that data from which basic component failure rates are determined, don’t double count these failures from fires.

The operators may extinguish the fire or operate the equipment manually and prevent fire or they may be misled by the faulty information generated by the effect of fire and may exacerbate/aggravate the situation. Some other issues that have to be addressed in the analysis of fire induced accident sequences are smoke propagation, effects of fire-suppression activities, fires outside the plant and failures of fire barriers. Particular attention must be paid to the inter-system dependencies introduced by fire. Fire as cause of component failures may be included as “house events” directly in the system FTs as function of location and size.

Once the sequences involving fires are delineated and frequency distributions are quantified, the assessment of plant system response and event sequences proceeds as with other IEs. Besides direct impact on system components, fires have other secondary effects like the flooding that results from fire fighting agents; smoke, which may hinder personnel access; the generation of ignition sources for other inflammable products; the possible boiling of water inside pipe passing through the fire, etc. The dependencies of fire as secondary event to some other external event (e.g. fire initiated by an earthquake) should be evaluated in the other external initiator event.

IX-3.5 Release Frequency Analysis

The purpose of this analysis is to derive the frequencies of accident sequences leading to radioactive material release using the results of previous analysis. The distributions for the various categories of radioactivity release from containment should take into account that the same fire that would lead to damage of the core may as well damage the containment ESFs also.

IX-3.6 Special Issues

The steps described above need to be supplemented with additional considerations based on specific features associated with the locations or additional aspects. These include the following.

IX-3.6.1 Analysis of Control Room

In the event of fire in the main control room, the potential impact on safety systems is higher than that of any other area. The potential also exists for the operator to receive contradictory information and for an impact on operator habitability and performance. The potential for any physical dependence between control room and remote shutdown capability and core cooling (e.g., from supplementary control room) are also to be considered in analysis.

IX-3.6.2 Cable Spreading Room and Other Sensitive Areas

The cable spreading rooms, switchgear rooms and other control equipment rooms are centres of convergence for equipment and wiring. These compartments contain electrical equipment and cables that may belong to more than one safety system train. So the impact of fire would be relatively high in these areas. Fire in these locations may also result in spurious actuation because of hot shorts, etc. Since these areas are very significant to fire risk, they have to be handled thoroughly.

IX-3.6.3 Environmental Survival of Component

The combustion products or the fire suppression agents have potential to damage some safety-related component. The data available for impact of these materials is scarce, so the analyst may treat the issue with his expertise and data from other plants. It should be ensured that the effect of actuation of fire suppression system is taken care of in the analysis.

IX-3.6.4 Fire Induced Explosions

During the screening process or the detailed analysis, the potential for fire sequences that lead to a consequential explosion may be identified. It may be outside the scope of a fire PSA to provide a best estimate assessment of the consequences of explosions arising from fire sequences because the damage spread mechanisms from fire explosions (blast effects, missiles, etc) require that different methodologies be applied. It is important that these potential hazards are listed and attached to the report for completeness of the analysis. This list provides input to plant's overall fault schedule, for inclusion under relevant analysis topics.

IX-3.6.5 Integrity of Containment

The factors to be emphasised in fire analysis of containment integrity include the following.

- Prevention of containment bypass sequences via high pressure - low pressure interfaces, together with the potential degradation in the redundancy related to isolation via hot shorts.
- Failure of the containment isolation provisions that may be required to operate, prevent or mitigate the release of radioactivity from the containment; In some plants it may be necessary to critically examine the ability of containment seals and penetrations to withstand the postulated fire.
- Fire induced degradation in the active systems used to sustain containment performance during DBA and BDBA, like decay heat removal, containment spray systems, etc..

APPENDIX-X

SEISMIC PSA

X-1 Introduction

Seismic PSA combines knowledge of earthquake engineering, plant systems and risk analysis. Earthquake engineering is a broad field drawing on aspects of geology, seismology, geotechnical engineering, and structural engineering. Hazards associated with earthquake for a specified exposure time include ground shaking, structural hazard, liquefaction, landslides, lifeline hazards, tsunamis and seiches. The probability that social, economic casualties will exceed a specified value at a site in earthquake (seismic event) is called earthquake risk. The terms earthquakes or seismic events although used interchangeably, are not exactly the same. Seismic events include earthquake. Any disturbances in the interior of the earth, which sends elastic waves in different directions, are called seismic events. The seismic events, depending on sources, can be categorised into natural seismic events (i.e. tectonic, volcanic, collapse and oceanic microseisms) and man-made seismic sources i.e. industrial or military explosions, quarying/mining operations, construction work, nuclear explosions, traffic and reservoir induced earthquakes. This section addresses seismic PSA considering only earthquake event, as significant for a NPP site.

The phenomenon of sudden internal movements in the earth's crust setting up the tremors (ground vibrations) is called an earthquakes. These are caused mostly by faulting and some by volcanic eruptions. The earth's surface (crust) consists of a large number of blocks/rocks called planes (plate tectonics), which may extend deep down to outer layer of mantle. These plates move with respect to each other (the underlying blocks/rocks which are less brittle allow such movement). The differential movement between these two blocks in the earth's crust along new or pre-existing lines is called a fault. Fault may range in length up to a few hundred kilometres and extend to a depth of several tens of kilometres. Based on the type of movement there are different kinds of faults. The slow (typically 2-10 cm/year) and continuous displacements of plates set up deformation and elastic strain with neighbouring plates. When the energy that accumulates due to deformation becomes greater than the rocks can endure, the rock fractures along a plane of the weakness (fault plane), gets displaced/rebounds into a new position (elastic rebound theory) relieving strain energy totally or partially and earthquake originates. The rock fracture usually starts from a point (called focus) close to one edge of the fault plane and propagates along the plane (with a typical velocity 3 km/sec.). The point on the earth's surface vertically above the focus is called the epicentre. The oldest measure of size of earthquake is intensity relating to destruction potential of ground motion upon structure and living beings. Maps of isoseismal curves are drawn for equal values of intensity for different locations on the earth's surface. The most widely adopted scale to measure intensity is Modified Mercali Intensity (MMI) Scale. It has twelve grades (I-X), which can be related to ground acceleration. The magnitude M is the measure of energy release (during an earthquake) derived from the recorded amplitude on a seismograph. The Ritcher magnitude is the logarithm to the base 10 of the maximum amplitude expressed in microns with which a Wood-Anderson standard short period torsion seismometer (characterised with a period of 0.8 second, magnification 2800 and damping nearly critical) would register the earthquakes at an epicentral distance of 100 km. Different magnitude scales saturate at different sizes of earthquakes because of the saturation and non-linear effects in ground motion and wave propagation. Moment magnitude, which depends on the energy released during an earthquake, shows a linear behaviour.

The parameters used to describe characteristics of ground motion from earthquake are as given below:

- Based on amplitude of motion: Peak Ground Acceleration (PGA), Peak Ground Displacement (PGD) and Peak Ground Velocity (PGV). These are based on amplitude of motion.
- Based on frequency content of motion: Ground Motion Spectra and Response Spectra. These are based on frequency content of motion. Response Spectra, which is most widely used, describes the maximum response of a single degree of freedom (SDOF) of structure to a particular

input ground motion as a function of frequency (or natural period) and damping ratio of the SDOF system. It is usually normalised with respect to PGA. The shape of the response spectrum changes according to the site conditions.

Current NPP requires design of SSCs based on ground motion for two levels of severity;

- S1 level corresponding to Operating Basis Earthquake (OBE) considering regional, local geology and seismology and characterisation of subsurface materials by either a probabilistic or a combination of probabilistic and seismotectonic approaches. The magnitude for this earthquake could be reasonably expected to affect the plant during its operating life and has a minimum recurrence interval of 100 years. The SSCs, which need to be functional to continue plant operation, are to be designed for OBE.
- S2 level corresponding to Safe Shutdown Earthquake (SSE) level, which is the maximum earthquake potential and is to be evaluated for magnitude based on seismotectonic approach and history of earthquake in the region with a minimum recurrence of 10,000 years. All SSCs necessary to assure integrity of primary coolant system pressure boundary, safe reactor shutdown, decay heat removal and for Anticipated Operational Occurrence preventing AOC leading to accident condition and mitigating accident consequences, are designed for SSE magnitude of earthquake.

Earthquake motion can initiate accident sequences and has the potential for simultaneously damaging several components in NPP. The main objectives of seismic PSA are as follows:

(i) To identify the most likely accident sequences leading to core damage in the event of an earthquake.

(ii) To identify major seismic risk contributors inside the plant.

(iii) To calculate the overall CDF and overall consequences.

The calculation of seismic risk requires detailed information about seismotectonic characteristics of the region, capacities of SSCs to withstand the earthquake motion, different failure modes of the structures and interactions between failures of various SSCs of a NPP. But in many cases, the details available are not adequate. Though sophisticated analytical tools to calculate the real inelastic capabilities of structures and components and high speed computers are available, many a time, engineering judgement based on expert opinion will be required to supplement sparse data and limitations in analyses.

The major steps in the seismic PSA are: (i) seismic hazard analysis for plant site; (ii) calculation of response of SSC; (iii) computation of component fragilities; (iv) modelling plant systems and accident sequences including for new IEs not considered in the internal IEs earlier, integration of events into the existing FTs and accident sequences and quantifications of end states, and (iv) consequence analysis. Some of the factors which may have significant contribution to overall risk, but are difficult to be considered in the analysis are:

(1) Increased probability of human error subsequent to occurrence of a destructive earthquake.

(2) Increased probability of damage to lifelines (air, fluid commanded equipment and instrumentation needed for mitigating and control off-site emergency measures) and other infrastructure, which is used during the emergency evacuation procedures.

(3) Increased probability of delayed response by the authorities and public to nuclear accident due to interference from another catastrophic event (e.g. bridge collapse).

This section covers Level 1 PSA and performance assessment of containment during the seismic event. Because of inherent difficulties in assessment of events, which includes (2) and (3) above, off-site consequences (Level 3 analysis) related to seismic events are not addressed here.

X-2 Probabilistic Seismic Hazard Analysis (PSHA)

Seismic hazard is the frequency of occurrence of earthquake parameter. It is usually expressed in the form of a hazard curve, which is a distribution of frequency of exceedence of the seismic parameter to that parameter, usually PGA. Since there may be a great deal of uncertainty in the parameter values and in the mathematical model of the hazard, the effects of uncertainty are represented through a family of hazard curves. Each curve is plotted for a postulated set of the parameter values and a selected hazard model and a probability value. In contrast to the typical deterministic analysis, which makes use of discrete, single valued events to arrive at the description of seismic hazard, probabilistic analysis allows the use of multi valued or continuous events and models. The basic steps in PSHA are as follows:

(a) Definition of earthquake sources

This involves the identification and characterisation of individual, or groups of, capable/ identified earthquake generating faults and their location. This also includes identification of seismotectonic provinces (a region where there are no identifiable active faults but are having diffused seismic activity). This also includes characterisation of the probability distribution of the potential rupture location. It is assumed to have similar earthquake potential throughout the region. The sources are represented by different earthquake source models as given in Fig. X-1 (e.g. reservoir induced seismic event may be considered as a point source model).

(b) Calculation of recurrence relationships for each source

It involves evaluation of average rate at which the earthquake of some size will be exceeded. It is derived as the best-fit curve between annual frequency of exceedence of magnitude and corresponding magnitudes. The ordinate of the plot represents the logarithm of a number of earthquakes having their sizes greater than or equal to a particular earthquake magnitude, and the abscissa contains increasing earthquake magnitude. The recurrence relationships are usually represented by straight lines.

The recurrence relationship can be represented by Gutenberg-Richter recurrence law, Bounded Gutenberg-Richter recurrence laws or with characteristic earthquake recurrence laws [98]. A study has concluded that while available data sets are not sufficient to disprove the Gutenberg-Ritcher recurrence law, the characteristic earthquake model better represents the observed distribution of earthquake magnitudes [98]. Gutenberg Ritcher recurrence law is represented as given below and shown in Fig.X-4.

$$\text{Log } N = A - Bm \tag{X-1}$$

where, N is the cumulative number of earthquakes of a given magnitude or larger that are expected to occur during the study period of time and m is the magnitude of the earthquake.

For calculation of the seismic hazard that occurs within a time period of study (temporal occurrence), the distribution of the occurrence of earthquake with respect to time should be considered. It is generally assumed that the earthquakes occur at random (after the removal of aftershocks from the data set, which also simplifies the occurrence models used). The Poisson model also assumes that events of a Poisson process occur randomly, with no memory of the time, size, or location of any preceding event. But, it is to be noted that this assumption is inconsistent with elastic rebound theory. If the earthquakes are triggered when the stress on the fault reaches some limiting value, the chances of occurrence should depend on the time, size and location of preceding events. A number of models (time predictable, slip predictable models, Markov models, non-homogenous Poisson models, etc.) have been proposed to account for the past seismicity. Many of these models require additional parameters whose values must be evaluated from historical and instrument based seismicity records that are in many cases too sparse to permit accurate evaluation. A discussion on the different types of models used to represent temporal uncertainty and their applicability is given in Ref. [98]. The temporal occurrence of earthquakes is generally described with the help of a Poisson model. Investigation on the applicability of Poisson and non-Poissonian models have shown that Poisson model is useful for practical seismic risk analysis except when seismic hazard is dominated by a single source for which the time interval since the previous significant event is greater than the average interval time and when the source displays strong 'characteristic time' behaviour.

(c) Calculation of the range of earthquake magnitudes and distances to be considered in the analysis.

Since the earthquakes are assumed to occur anywhere from the earthquake source, distances from all possible locations within that source to the site should be considered. A probable distribution of the source to site distance for an arbitrary site is given in Fig. X-2. In order to estimate the earthquake effect at site, suitable attenuation relationships representing the seismotectonic characteristics of the site should be identified.

(d) Determination of seismic hazard at site

During the determination of seismic hazard at site, the effects of all the earthquakes of different magnitudes occurring at different locations due to different earthquake sources at different probabilities of occurrence (to account for uncertainties in earthquake location, size, ground motion parameter values) are integrated into one curve which depicts the probability values for exceeding different earthquake parameter levels at the site during a specified period of time.

This can be expressed as

$$E(z) = \sum_{i=1}^{N} \alpha_i \int_{m_0}^{m_u} \int_{r=0}^{r=\infty} f_i(m)\, f_i(r)\, P(Z > z \mid m, r)\, dr dm \qquad \text{(X-2)}$$

Where, E(z) is the expected number of exceedences of ground motion level z during a specified time period t (usually taken as one year),   is the mean rate of occurrence of earthquakes between the lower and upper bound magnitudes ( ) considered for the ith source,   is the probability distribution of magnitude (i.e., recurrence relationship) for the ith source, N is total number of sources, is the probability distribution of the distance to the source for the various locations within the source i, and   is the probability that a given earthquake of magnitude m and epicentral distance r will exceed the ground motion level z [98].

Assuming earthquakes are Poisson events, the annual frequency of earthquakes, which will produce the ground motion parameters Z smaller than z is given by

$$H(z) = e^{-E(z)} \qquad \text{(X -3)}$$

and annual frequency of earthquakes in which the value of the ground motion parameter Z is between   and   is given by

$$h(z) = H(z + \Delta z) - H(z) \qquad \text{(X -4)}$$

The annual frequencies for exceeding the specified values are plotted to form a family of curves with different non-exceedence probability levels. The overall flowchart of PSHA is given in Fig. X-3[98] and analytical task flow of seismic hazard analysis is given in Fig. X-4 [98].

Main factors, which contribute to the uncertainty of the hazard curve, are:

(i) geometrical parameters of seismic sources,

(ii) the specification of seismic activity of seismic sources,

(iii) the choice of attenuation relationships, and

(iv) the calculation of earthquake magnitude from records based on intensity

For inclusion of the uncertainties of the parameters in the hazard analysis, a set of hypotheses can be postulated, with each hypothesis consisting of a specified configuration of seismic sources, a value of Gutenberg-Richter slope parameter, a value of upper bound magnitude for each source, etc. A seismic hazard curve representing the annual frequency of exceedence of a specified earthquake parameter is generated for each hypothesis. This exercise can be repeated for all hypotheses resulting in a family of hazard curves. From these, curves corresponding to different levels of exceedence of the earthquake parameter can be generated.

Fig. X-5 shows a family of curves corresponding to different seismic hazard studies conducted for a particular region. The composite best estimate and a measure of uncertainty about this estimate are obtained by assigning, subjectively, relative weights to each estimate. For any level of acceleration, it can be seen from that there are five estimates with corresponding relative weights. This discrete distribution can be converted to a convenient analytical probability distribution such as lognormal and uncertainty can be calculated and plotted (Fig. X-6). The plots obtained are in terms of annual frequency of exceedence, where as for calculation of annual frequency of release, annual frequency of occurrence is needed. This is obtained by taking the differential with respect to the ground motion parameter, for which the hazard curve has been prepared.

The hazard curves are defined in terms of a single parameter. But, for calculation of response of structures, hazard curve has to be translated into engineering quantities. Additional information like response spectrum or a set of time histories is to be defined for calculating the same. This can be done based on experience with similar tectonic and geological regimes and the uncertainties introduced due to these additional parameters also have to be estimated. The variability in response spectra will be pronounced when different source mechanisms and focal distances have to be considered. For example, the duration and long period accelerations will be considerably larger for the larger magnitude earthquake, whereas short period motions will be higher in the moderate magnitude earthquake.

X-3 Computer Codes

(1) EQRISK : EQRISK is a computer program for the evaluation of earthquake hazard at chosen sites. Seismic events are considered as point sources; their occurrence in space is defined by the user. A variety of parameters may be used to quantify ground shaking, such as peak ground acceleration, velocity, displacement, modified Mercalli intensity, spectral velocity, etc. An attenuation function must be specified by the user, and may be in analytical form or (with slight reprogramming) in tabular form. Output gives annual hazard (probabilities of equalling or exceeding) for chosen values of the parameter values for pre-selected hazard levels. The hazard from each seismic source may be output, if desired, by the user. Also, if particular hazard levels have been input, the parameter values associated with these hazard levels are calculated and printed.

(2). EZ-FRISK : This is a software package for both probabilistic and deterministic seismic hazard analyses at a single site. It is targeted for use by structural engineers and earth scientists who want to evaluate ground motions at a site due to the expected seismic activity. Three primary sets of input data needed to execute a study are site location, the seismic sources (faults and areas), and the attenuation equations. The software includes a database of 66 faults for California, and has some attenuation equations built-in.

Both these codes are available from National Information Service for Earthquake Engineering, University of California, Berkeley.

X-4 Responses and Analysis of Plant SSCs

For the calculation of failure frequencies of SSCs, it is necessary to calculate the responses of these components to various levels of seismic excitation, thus translating the hazard input into responses acting on a component (e.g. displacement, shear moments, etc). This generally involves an analysis of the structures, piping systems and other components. The responses of interest could be spectral acceleration, moment, stress and deflection at selected structural, piping and equipment locations. The depth and coverage of analysis will depend on the type of analysis, which was carried out during the design stage of the plant and the applicability of the seismic design procedures and criteria used at the time of design. Although the failures may result in inelastic responses, the analysis can be limited to linear dynamic analysis of structures and subsystems. The variability in the ground motion is incorporated by simulating a set of time histories compatible with a particular peak ground acceleration and spectral shape. The sub-systems are analysed by using multi-support time history analysis. The output of the structure response analysis is the probability density function of the peak response of the structure in terms of moment, stress, deformation etc. of each SSC and the correlation between them. Uncertainties related to the input parameters like damping values of the systems/soil, structure/sub system frequencies could be incorporated with the help of a suitable sampling technique (e.g., Latin hypercube) [4]

X-5 Fragility Evaluation

The fragility of a component is defined as the conditional frequency of its failure for a given value of response parameter like moment, stress, deformation or spectral acceleration.

The objective of fragility evaluation is to estimate the ground motion parameter value for which the seismic response of a given component located at a specified location in the structure exceeds its capacity. Due to many sources of variability in the estimation of capacity, developing a single fragility curve is not appropriate, although a single curve may sometimes be used as shown in Fig. X-8 [99]. Instead the component fragilities are usually described by means of a family of curves with a probability value assigned to each curve to reflect the uncertainty in fragility estimation.

Three major steps in the development of seismic fragilities are selection of components, identification of failure modes and evaluation of ground acceleration capacity. Structures can be considered to fail functionally when the operation of the safety related equipment is potentially interfered with due to seismically induced inelastic deformations or when the failure of their attachments to the structure occurs. If a structural collapse occurs resulting in the failure of many safety related equipment (common cause failure), the event and FTs should be modified to account for this aspect.

(a) Selection of components for fragility evaluation, walk down and screening

Selection of SSC for the fragility evaluation is an iterative process including system analysis. and structural analysis. The system analyst based on the knowledge of plant systems, identifies the SSCs whose failure would lead to core damage and subsequently to radiological consequences. A walk down by the structural analyst is required to add and/or delete certain components from this list.

A detailed walk down of a NPP uncovers seismic vulnerabilities of safety related equipment and identifies spatial seismic interactions between systems. This identifies the components that require a detailed fragility assessment. The walk downs should be conducted by experienced engineers who can make engineering judgement decisions on the relative seismic capacity of equipment. The objectives of plant walkdown are:

1. To confirm that no weakness exist in the plant structures and equipment due to abnormal aging and poor maintenance, which will render the use of generic failure values unacceptable.
2. To confirm the accuracy of system descriptions found in plant design documents
3. To identify any spatial system interactions and system dependencies
4. To gather information on certain potentially weak components.

In general, rigid equipment that is well anchored are not vulnerable to seismic events. Such equipments are pumps, valves, compressors, diesel generators, chillers and heat exchangers.

Some times, there may be a potentially vulnerable ancillary item that governs the failure mode of rigid equipment. Other items, which have been demonstrated to be seismically rugged are piping, cable trays and electrical conduits, provided the support systems do not fail in a brittle manner. The major concern with distributive systems is seismic anchor movement due to differential building motions, or at a flexible anchor point.

Most of the emphasis during a walk down is to judgementally rank the structural capacity of essential equipment based upon its anchorage and its ancillary equipment, identify potential system interaction as discussed earlier and look for other seismic issues that could affect the function of essential equipment. Detailed procedures for plant walk down may be found in [100].

(b) Failure modes

The first step in generation of fragility curves is to develop a clear definition of what constitutes a failure of a safety related SSC. The structural and system response analyst should define the various failure modes of each SSC and the possible interactions between them, including the failure of non-safety related systems, which could lead to failure of safety related systems. It may be necessary to consider several modes of failure of a component (each with different consequences) and fragility curves are required to be generated for each mode of failure. It may be also possible to identify the most likely failure mode by reviewing the equipment design, thereby reducing number of failure modes to be considered. Identification of credible mode of failure is largely based on the experience and judgement of analyst, results from earlier studies and reported failure modes of SSC.

Structures may be considered to fail when they cannot perform the designated functions, i.e., when inelastic deformations are beyond the available values, for the systems supported by the structure and of loss of safety related functions like leak tightness. A structural failure might also result in common cause failures of other systems it houses. For piping, the failure of anchorages and pressure boundary constitute dominant failure modes. Failure of buried structures may also have to be considered. Consideration should be given to potential failure of soil (e.g., liquefaction, toe bearing pressure failure, base slab uplift, etc.)

(c) Calculation of component fragilities

Component fragility is computed by developing the frequency distribution of the seismic capacity of a component and finding the probability of the capacity being less than the response value. Information required for this includes the material strength data of concrete, steel reinforcement, as -built dimensions of the structural members, qualification procedures/test reports for the equipment. Failure of equipment may also consist of failure of function or failure of pressure boundary, with each failure mode having totally different effect upon the plant systems. For most of the mechanical and electrical equipment the fragility data is based on the design analysis data and equipment qualification data. The capacity of a component is evaluated based on its ultimate strength and its capacity for inelastic deformation/energy absorption. A flowchart of response analysis and fragility evaluation is given in Fig. X-7 [99].

(d) Sources of randomness and uncertainty

Two distinct sources of variability contributing to overall variability (uncertainty) can be identified as random/ statistical/frequency and systematic/probabilistic/uncertainty. The random variables represent underlying randomness of variables and events. This variability may arise in part from the stochastic nature of underlying physical processes and in part from the inability to measure precisely the parameters, which characterise those processes. Examples of these are variability in material properties (structure, soil and component) such as strength, inelastic energy absorption and damping, the variability in earthquake time history and that in structural response when earthquake is defined in terms of PGA. The variability from uncertainty arises mainly from modelling uncertainty and represents the current level of ignorance concerning the variables and events. Sources of such uncertainties include variability due to an insufficient understanding of structural material properties, errors in the calculated response that result from using inappropriate modelling for the structure and inaccuracies in mass and stiffness representation, inaccurate representation of attenuation laws, generic configuration of seismic sources and also the use of engineering judgement in view of in complete plant specific data on the fragility levels of component and on response. It is distinguished from randomness because it originates with the methods used to model the seismic hazard and the plant response rather than as the result of inherent variability in the physical processes being modelled. All the variables that attribute to the response or strength of a component has some randomness and uncertainty associated with it and this results in uncertainty and randomness in response and strength. Tables X-1 and X-2 able gives some guidance on the dominant source of uncertainty/ randomness of some important variables [99].

TABLE X-1 : CAPACITY VARIABLE

Material strength	Uncertainty
Ductility	Uncertainty + Randomness
Load combination (normal + seismic)	Uncertainty

TABLE X-2 : RESPONSE VARIABLE

Peak to peak variation in input motion	Randomness
Phase difference of earthquake components	Randomness
Phase difference of modal responses	Randomness
Vertical/horizontal acceleration ratio	Randomness
Soil stiffness	Uncertainty + Randomness
Soil damping	Randomness
Structural stiffness	Uncertainty + Randomness
Structural damping	Randomness
Non-linearities	Uncertainty
Soil-structure interaction	Randomness

The fragility analyst may often assign both randomness and uncertainty to some parameters whose variability is affected by both the input motion time history and lack of knowledge in the modelling of the phenomenon. Damping and ductility are examples where the variability is usually defined as a combination of randomness and uncertainty.

The fragility of a particular component for a particular failure mode can be expressed as the best estimate of a median input parameter and two random variables. When the capacity is expressed in terms of PGA, it can be expressed as,

$$A = A_m \varepsilon_R \varepsilon_U \tag{X-5}$$

where, is the median capacity and are the random variables with unit medians representing inherent randomness about the median and uncertainty in the median value [99]. It is typically assumed that both these random variables are lognormally distributed with standard deviations respectively.

The lognormal distribution can be justified as a reasonable distribution since the statistical variation of many material properties and seismic response variables may be well represented by this distribution, provided one is not interested with the extreme tails of the distribution [101, 102]. Also, the central limit theorem states that the products and quotient of random variables tend to be lognormally distributed regardless of the distribution of individual variables. The use of lognormal distribution for estimating very low failure probabilities of components or structures associated with tails of distribution is considered to be conservative since the low probability tails of the distribution generally extend further from the median than actual structural resistance or response data might extend.

With perfect knowledge (i.e. only accounting for the random variability), the conditional frequency of failure f_0 for a given peak ground acceleration level, a, is given by,

$$f_0 = \Phi\left[\frac{\text{In}(a/A_\text{m})}{\beta_\text{R}}\right] \tag{X-6}$$

where $\Phi[\ ]$ is the standard Gaussian cumulative distribution. The frequency of failure f^1at any non-exceedence probability level Q can be derived as

$$f^1 = \Phi\left[\frac{\text{In}(a/A_m) + \beta_U\Phi^{-1}(Q)}{\beta_r}\right] \tag{X-7}$$

where $Q = P\left[f < f^1 \mid a\right]$ = probability that the conditional frequency of failure, f, is less than f^1 for a peak ground acceleration 'a'. For the purpose of displaying fragility curves, the non-exceedence probability level Q is utilised. Subsequent computations are made easier by discretising the probability 'a' into values 'q' associated with different values of failure frequency f^1. A family of fragility curves each with an associated probability 'q', is developed. In some applications, the composite variability β_C is used which is defined by,

$$\beta_C = \sqrt{\left(\beta_R^2 + \beta_U^2\right)} \tag{X-8}$$

As an example, let the fragility parameters for a component be $A_m = 0.7$ g , $\beta_R =$ 0.35 and $\beta_U = 0.25$. Using Eq. (X-6), the best estimate of the conditional failure frequency for a peak ground acceleration of 0.60 g is calculated as 0.33; the conditional failure frequency at 95 % non-exceedence probability for a ground acceleration of 0.50 g using Eq. (X-7) is calculated as 0.77. Using similar calculations, fragility curves are developed.

The following two methods are generally used to develop fragility curves for use in seismic PSA-Scaling method and Simulation method. In either method, the hazard definition and the system models are the same. The difference lies in the details of development of the fragility description for structures and components as shown in Fig. X-7. In either case though, the final fragility description is a conditional probability of failure relative to a hazard parameter defined at ground. In the scaling method, existing structural analysis are utilised and the fragility curves are referenced to a ground motion parameter. In the simulation method [90], new structural and equipment analyses are conducted and the fragility curves are referenced to the component/structure interface response parameter, but must ultimately be scaled to reference a ground motion input parameter.

Scaling Method

In this method an overall factor of scaling is developed to represent best estimate of actual response and capacity as opposed to the design response and capacity. In estimating fragility parameters, it is convenient to work in terms of an intermediate random variable called factor of safety. This is defined as the ratio of the ground acceleration capacity to the safe shut down earthquake acceleration A_SSE used in plant design. The median factor of safety F_m can be directly related to the median ground acceleration capacity as

$$F_m = \frac{A_m}{A_{SSE}} \tag{X-9}$$

The standard deviations $\beta_{F,R}$ and $B_{F,U}$ are identical to that of A_m. For structures, the factor of safety is modelled as a product of three random variables

$$F = F_S F_\mu \, F_{RS} \tag{X-10}$$

Where F_S represents the ratio of ultimate strength (or strength to loss of function) to the stress calculated for A_{SSE}. In calculating the value of F_S, the non-seismic portion of the total load acting on the structure is subtracted from the strength as follows

$$F_S = \frac{S - P_N}{P_T - P_N} \tag{X-11}$$

where S is the strength of the element for the specific failure mode, P_N is the normal operating load and P_T is the total load on the structure (i.e., sum of the seismic load for A_{SSE} and normal operating load). F_μ is the inelastic energy absorption factor and F_{RS} is the load response factor, which accounts for the conservatism in the calculation of deterministic response parameters. Many factors like spectral shape factor, damping factor, modelling factor, mode combination factor, earthquake component combination factor, factor to account for effect of soil-structure interaction, influence the value of F_{RS}

For equipment and other components, the factor of safety is modelled as

$$F = F_S F_\mu F_{RE} F_{RS} \tag{X-12}$$

The factors $F_S \, F_\mu$ together represent the capacity factor of safety for the equipment relative to the floor acceleration used for equipment design. The equipment response factor F_{RE} is the ratio of equipment response calculated in the design to the realistic equipment response, with both the responses being calculated for floor response spectra. Important variables that influence the equipment response and its variability are spectral shape, modelling, damping, combination of modal responses, combination of earthquake components and qualification method.

The total failure probability of a component can be calculated as

$$P_f = \sum\nolimits_a \phi(a) f(c \mid a) \tag{X-13}$$

Where, $\phi(\alpha)$ is the annual rate of occurrence of the ground motion parameter and $f(c \mid \alpha)$ is the fragility of the particular component associated with the value of ground motion parameter α.

Simulation Method [99]

In the simulation method, multiple response analyses are conducted from the ground up for structures and selected equipment and piping. The equipment and piping models may be coupled or uncoupled from the structural models. Multiple time history analyses are conducted in combination with variations of the important variables contributing to response. The resulting response, whether load in a structural or equipment element, or a floor response spectrum, is defined probabilistically so that factors associated with the response are not required. The capacity of the structure or component is then computed and a capacity factor relative to the local input motion parameter is derived. The randomness and uncertainties associated with the capacity is estimated and a fragility curve relative to the local input motion parameter is developed. Since the hazard is defined at the ground, this fragility description must be translated to the ground by dividing by the ratio of the local response parameter used as a response for fragility curve development to the ground input parameter used to define the hazard. The randomness and uncertainty is computed for the capacity, to quantify the randomness and uncertainty relative to the ground motion input.

Apart from these, various other methods (from simple calculation procedures to detailed analytical studies), which can be used for the derivation of the fragility curves are elaborated in Ref.[4]. Often, generic fragility curves are used directly. Ref [103] contains a compilation of seismic fragilities developed in PSAs of numerous nuclear plants. These may be used when results of the walk down and a review of the design basis suggest that they are appropriate. Some of these generic fragilities may be used in conjunction with earthquake experience data using Bayesian methods [104]. Fragility description for components qualified by testing may be approximated from the test results but, unfortunately, the true capacity is unknown. Usually, the test level represents appropriately a 95% confidence of less than 5%

probability of failure, commonly termed as High Confidence Low-probability of Failure (HCLPF) value. There is usually conservatism in the structural response and in the testing input so that the HCLPF relative to ground is substantially greater than the SSE. This conservatism defines the structural response factor and an over testing factor. If the test data are used to develop the fragility curve, the randomness β_R and β_U on the capacity must be estimated. They are usually estimated to be of the same magnitude as the β_R and β_U developed for the capacity of the other components. The fragility curve is initially defined relative to the floor response of the structure and then translated to ground by incorporating the structural response factor and its randomness and uncertainty. A schematic picture of combination of structural responses and system capacity is given in Fig. X-8 [99].

X-6 Plant System and Event Sequence Analysis

The frequency of core damage and radioactivity releases to the environment are calculated by using plant logic combined with component fragilities and seismic hazard estimates. Event trees are constructed considering all initiated events for the seismic initiator(s) and FTs are developed incorporating additional (failure) basic events to account for seismic mode of failure probability to random failures for the components, in particular to safety significant components as identified by well established methods like importance measures and FMECA and keeping in view all possible dependencies and secondary effects of seismic initiator. The analyses are done, integrating failure probabilities due to seismic event evaluated from component response and fragility analysis both at FT and ET levels (including CET) to arrive at core damage frequency (Level 1 PSA) and/or frequency of release to environment in Level 2 PSA. Fig. X-9 gives an overview of Seismic PSA for Level 1 PSA analysis. If internal event PSA already exists, then this only need to be modified by seismic failure related inputs. However, there are various aspects that should be kept in view while performing plant system and event sequence analysis. The major differences between seismic and internal events are:

- Identification of initiated events from seismic initiator
- Increased likelihood of multiple failures of safety systems requiring a more detailed ET
- Secondary seismic effects
- More pronounced dependencies between component failures as a result of correlation between component responses and between capacities

Initiating events

Some IEs, which are considered improbable for an internal event PSA, may not be negligible in the seismic PSA. An example of this could be reactor vessel rupture. For large earthquake, multiple initiated events may occur at the same time with markedly different effects on problematic ESFs. The effect of a seismically induced flood may be quite different from those of other external floods because the plant may be subjected to more problems than one threat to safety, and effects may be greater than that arising from either separately. Perhaps more than the associated external initiated events are internal initiated events such as fire and flood. The seismic initiator may fail the barriers and fire detection/ mitigating systems and the combination of fire and structural motion may together produce more damage in this safety systems than if these had occurred separately. These aspects of indirect (seismic failures) are quite complex to model besides other PIEs in ETs.

Dependent failures

The potential in seismic PSA for additional CCF/dependent failure should be considered in ET/FT. Most secondary effects are termed as system interactions i.e. failure of a safety and more likely non-safety systems or components affecting the performance/functioning of a safety-related system/ component. These interactions may be spatial (location) or systematic. Spatial interaction is failure of un-reinforced, masonry walls impacting safety component. System interactions include such scenarios as failure of a non-safety heat exchanger or cooling line affecting decay heat removal capacity or associated system in ultimate heat sink.

Seismic-fire interaction

Other types of secondary effects include fire following an earthquake, inadvertent actuation of fire protection systems and plant specific secondary effects such as flooding due to outside dam failures. Fire protection system is typically not designed for earthquakes. Fire protection system (FPS) failures on earthquake though are reviewed as spatial system interaction sources of spray or failure in the event of a fire; the unavailability then becomes an even more serious concern. Another issue with fire protection systems is (spurious) unintended actuation resulting from earthquake. This is often a source of damage to equipment. Other consequences, which could result from inadvertent activation of FPS, are inhabitability of the control room and shutdown of emergency diesel generators upon a fire signal.

However, in some cases seismically induced secondary events may not constitute an immediate input into seismic PSA. For example, for an earthquake causing failure of a dam and consequently flooding a NPP site, additional risk can be accounted for within the framework of 'Flood PSA'. It may be necessary to produce a new seismic hazard curve for some secondary effects if they take place some distance away from the site; for example, the loss of offsite power may be initiated at a switching station remote from the NPP. The time aspects of secondary effects should not be forgotten, the most obvious example is impact due to aftershocks. It is possible that in performing PSA, it may be discovered that secondary effects have not been excluded when siting/constructing the plant. Some of the reasons could be discovery of a new fault in the site vicinity, new constructional features in the site vicinity such as pipeline, petrochemical facility or a dam. Also, new understanding and/or interpretation of safety concept/regulations may also require considerations of earthquake levels beyond design basis.

Treatment of simultaneous occurrence of external events

The consideration of effects from simultaneous external events in the context of seismic initiator becomes an issue, treatment of which brings in complexity. One may calculate the probability of sustaining severe external events simultaneously and assume some maximum damage state to result. The frequency of such damage states arising from this simultaneous occurrence would then be simply equal to the expected frequency of simultaneous occurrence to the two external events. This frequency may be well within whatever is deemed to be an acceptable risk for the facility. If so, then no further analysis would be necessary. If not, then it might be necessary to re-evaluate the situation to reduce conservatism and possibly resort to rigorous analysis dealing with the effect of two simultaneous events.

System response

System response for seismic PSA need to be modelled as in internal event PSA considering additionally seismic mode of failure. If operating procedure and equipment are designed to respond differently to seismic initiated failures, these could be appropriately modelled in FT/ET. Operator error could be enhanced due to seismic event, this should be difficult to quantify due to lack of data and unless specifically called for is usually ignored in a seismic PSA.

Fault tree

There are two major modifications to internal initiator FTs, which must be made for seismic PSA. First it is necessary to incorporate failures, which because of their extreme improbability are not included in the internal event FTs for example, wall or roof collapse, severe concrete spallation, basemat uplift, tilting, relay chattering etc. The second major modification involves those failures, which are considered in the internal initiator analysis, which may have a second mode of failure that should be included in FTs. For example, internal initiator PSA might include as a primary failure, random failure of a MOV to 'close on demand'. The seismic PSA FT could be modified to change the MOV failure to close from a primary failure to a gate failure having two primary failures as inputs, the random failure of the valve and the seismically induced failure of the valve. This has the potential for increasing the size of the FTs. However, this can be kept to a manageable size by impacting seismically induced failures only to components which have significant risk contribution as identified by internal initiator PSA or FMEA. Some failures such as maintenance errors or electrical cabling might be considered so highly resistant to seismically induced failures that their probability for seismically induced failures can be neglected. Also operator errors need not to be modelled with two separate failures modes- random and seismic, as it would be difficult to impact separately such earthquake induced failures. However, in general, these earthquake dependent failures need to be quantified assigning probabilities which vary with earthquake level but which are estimated without necessarily employing explicit response/fragility model.

The seismic unavailability analysis and ET quantification are done in the similar manner as with internal initiator PSA after incorporating seismic related failure probabilities as evaluated from component response and fragility analyses.

X-7 Consequence Analysis

The consequence model (radioactivity release consequence to public domain) developed for external events may be employed to analyse the consequence of seismic events. The impacts of huge earthquake affecting the parameters of consequence models such as evacuation time, disturbing communication network, damaging roads, population distribution, public response, etc need to be incorporated for refinement in analysis. Also seismic event may invalidate the consequence modelling assumptions that people will seek shelter in nearby buildings from external radiation. In the presence of the multiple hazards (i.e., earthquake itself and reactor accident) people may react differently than they would if faced only with a reactor accident. For such reasons, the spectral distribution of population exposed to radiation effects in a seismically induced reactor accident may be different from that for internal events. Similarly, there are some differences in the expected property damage for the two events. These differences may be difficult to incorporate in modelling. However, large uncertainties assigned to the parameters of consequence model may cover the variation due to seismic events. The final output of the consequence analysis is a family of risk curves (e.g. no. of fatalities vs. frequency of occurrence per reactor year, for different confidence levels to give non-exceedence probabilities)[4].

X-8 Documentation and Presentation of Results

These should be done as per the general guidelines given in Appendix-I. Special care should be taken for external events. Documentation for seismic PSA should include the following:

(a) List of external events identified as potential hazards,

(b) The site specific screening criteria used,

(c) Detailed description of hazard analysis for each selected external event,

(d) Development of plant response, component fragility, IEs, ETs, and FTs, APET/CETs, probability distribution of CDF, frequencies of various release categories and risk curves.

Results should include the following:

(a) Identification of external events appropriate to the site and plant,

(b) Selection of events with detailed assessment,

(c) Hazard analysis, plant response as applicable, component fragilities, modifications to the ETs/FTs and APET/CETs drawn for internal PSA and modification to consequence model, as appropriate,

(d) Probability distribution of CDF, frequencies of various release categories, risk curves on consequences as appropriate,

(e) Conclusion or recommendation including areas needing more studies.

X-9 Interpretation/Review of Results

The seismic PSA results can be represented as median or mean value of the frequency of occurrence and the fragility curves (lower and upper) defining a range of frequencies within 90 % (or any other desired fraction) of the frequency contained. The central value (median or mean) can be roughly thought to reflect the contribution to the risk due to intrinsic randomness while the confidence interval gives the measure of uncertainty with which CDF, release to environment (Level 2) or consequence (Level 3) is obtained. Final results of a seismic PSA are typically compared to results from internal events and other external events. If there are significant differences, unique vulnerabilities of one plant from the other are not apparent, then there may be some modelling differences that may warrant further examination. The Table X-3 [105] shows a comparison of mean core melt frequencies. It may be kept in view that the radiological risk associated with external events should not exceed the range of radiological risks associated with internal events. Also it should be kept in mind while comparing seismic results that uncertainty is much greater than that obtained for internal or other external events. Once PSA results for internal and external events are available, it is customary to conduct sensitivity analysis and cost benefit studies (without compromising risk) before making decisions on backfit measures. If the seismic PSA includes a containment performance evaluation, useful information should be obtained on the potential sources of seismic induced containment failure or containment bypass. This information along with sensitivity studies may be important findings useful for risk informed decisions. It can be concluded that the events that lead to core damage, also result into loss of mitigating systems and containment failures, and the supporting systems that are common for core cooling and containment cooling may have more importance from a risk viewpoint than systems dedicated to one or the other.

TABLE X-3 : CONTRIBUTION OF IES TO CDF/CMF FOR PUBLISHED PSAS WITH COMPLETE SEISMIC ANALYSIS [105]

Plant	Year	Contribution (%)					
		Seismic	Internal	Fire	Wind	Other external	CDF
Zion	1981	8	85	7	-	-	6.7E-05
IP2	1983	6	58	10	26	-	1.4E-04
IP3	1983	2	88	9	1	-	1.4E-04
Seabrook	1983	13	75	11	-	1	2.3E-04
Limerick	1983	13	34	53	-	-	4.4E-05
Milstone 3	1984	15	77	8	-	-	5.9E-05
Oconee 3	1984	25	56	4	5	10	2.5E-04

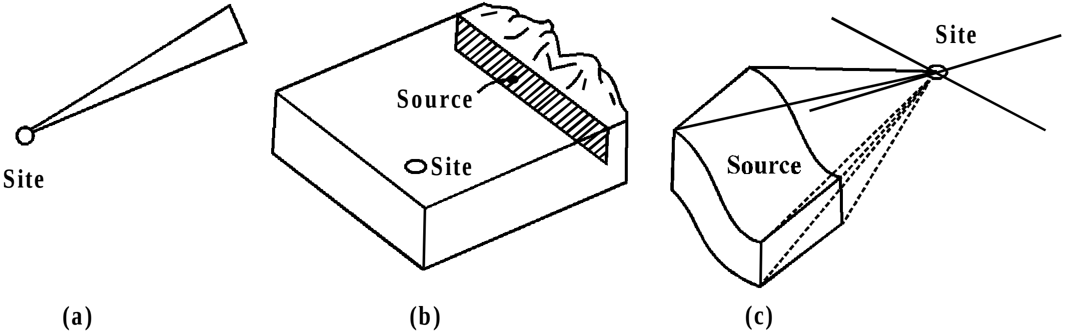


FIGURE X-1 : DIFFERENT TYPES OF EARTHQUAKE SOURCE MODELS CONSIDERED IN THE ANALYSIS

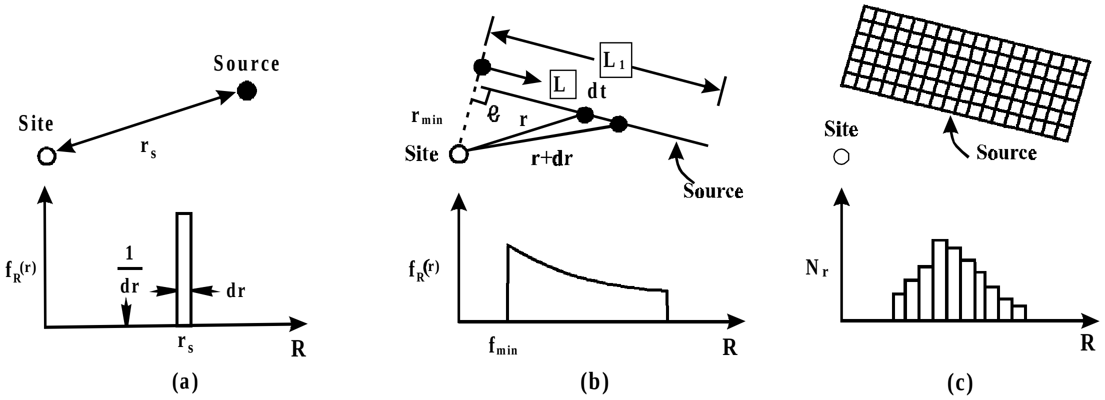


FIGURE X-2 : A PROBABLE DISTRIBUTION OF THE SOURCE TO SITE DISTANCE FOR AN ARBITRARY SITE

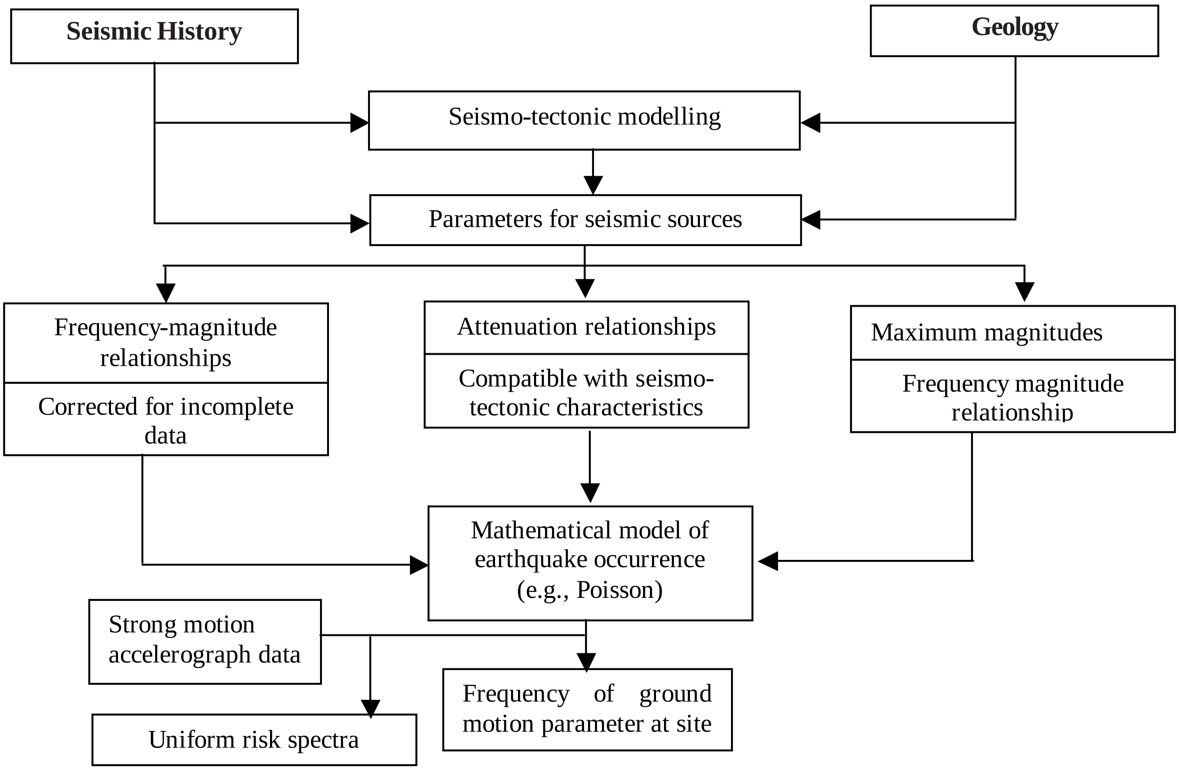

Seismic History
Geology
Seismo-tectonic modelling
Parameters for seismic sources
Frequency-magnitude relationships
Corrected for incomplete data
Attenuation relationships
Compatible with seismo-tectonic characteristics
Maximum magnitudes
Frequency magnitude relationship
Mathematical model of earthquake occurrence (e.g., Poisson)
Strong motion accelerograph data
Uniform risk spectra
Frequency of ground motion parameter at site

FIGURE X-3 : FLOWCHART OF PSHA [99]

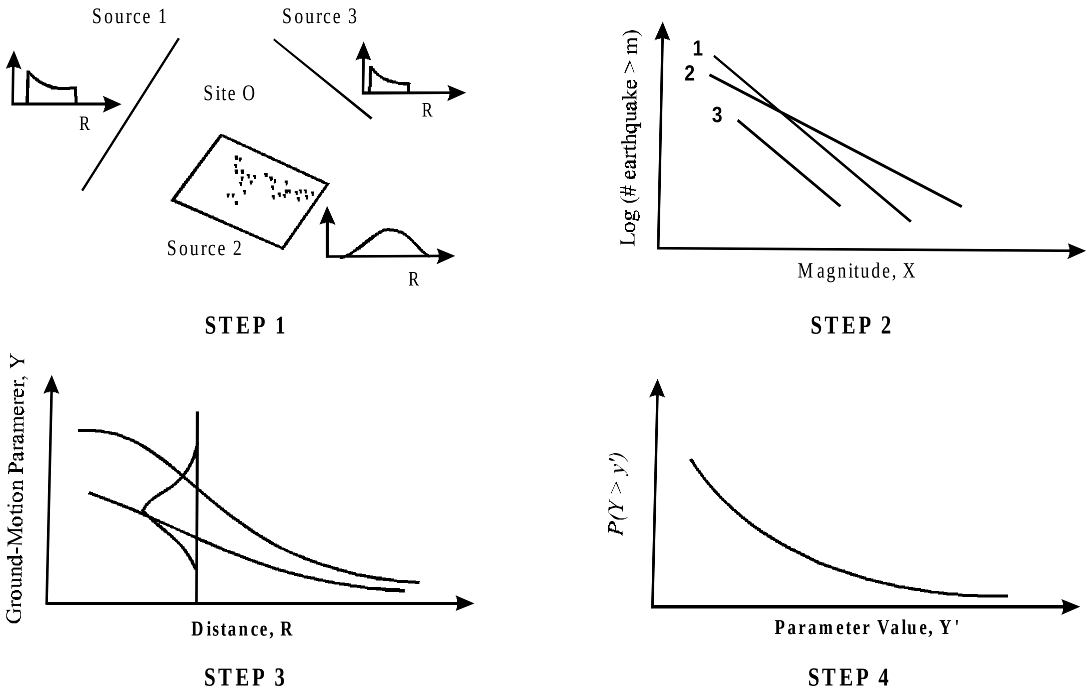
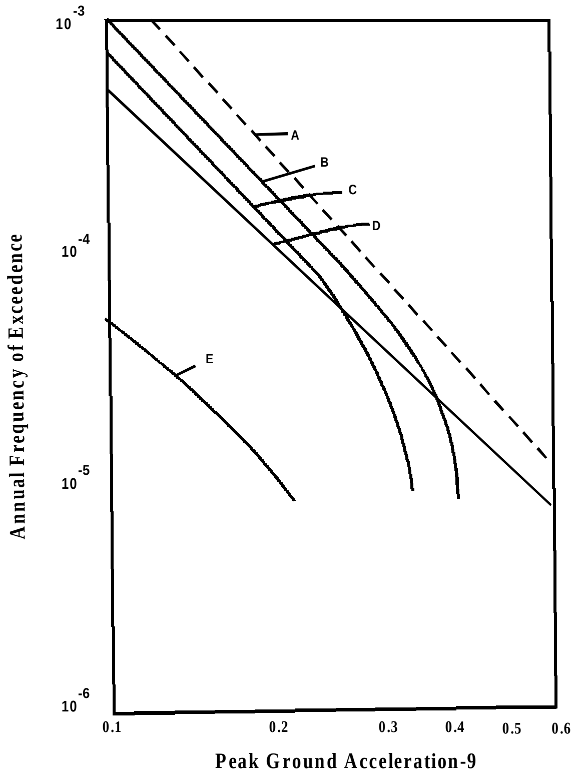


FIGURE X-4 : STEPS IN SEISMIC HAZARD ANALYSIS [98]



Based on Source	Weighting Factor Acceleration Range-9		
	0.1 - 0.2	0.3	≥ 0.5
A	0.09	0.07	0.05
B	0.37	0.42	0.46
C	0.18	0.21	0.23
D	0.27	0.20	0.15
E	0.09	0.10	0.11
Σ	1.00	1.00	1.00

FIGURE X-5 : SEISMIC HAZARD ESTIMATES FOR A PLANT SITE BASED ON RESULTS FROM DIFFERENT STUDIES [101]

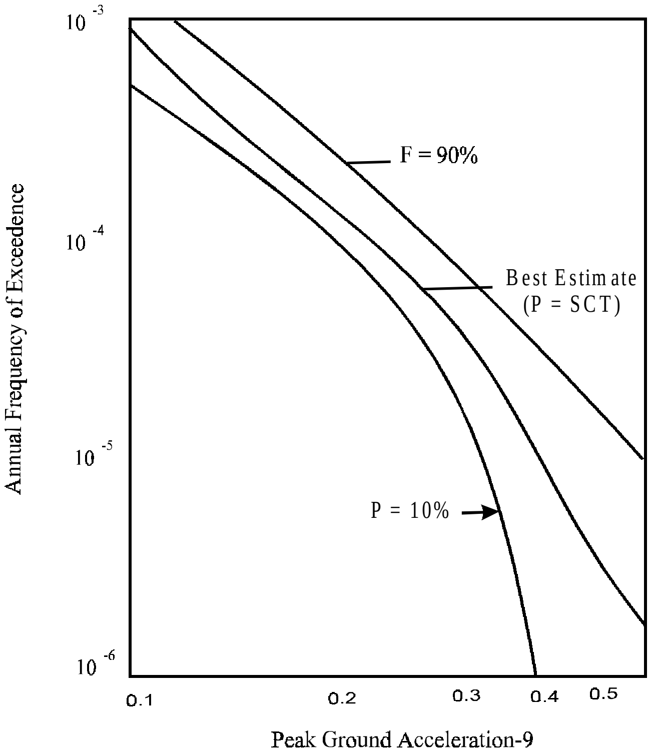


FIGURE X-6 : UNCERTAINTY BANDS ON SEISMIC HAZARD ESTIMATES [101]

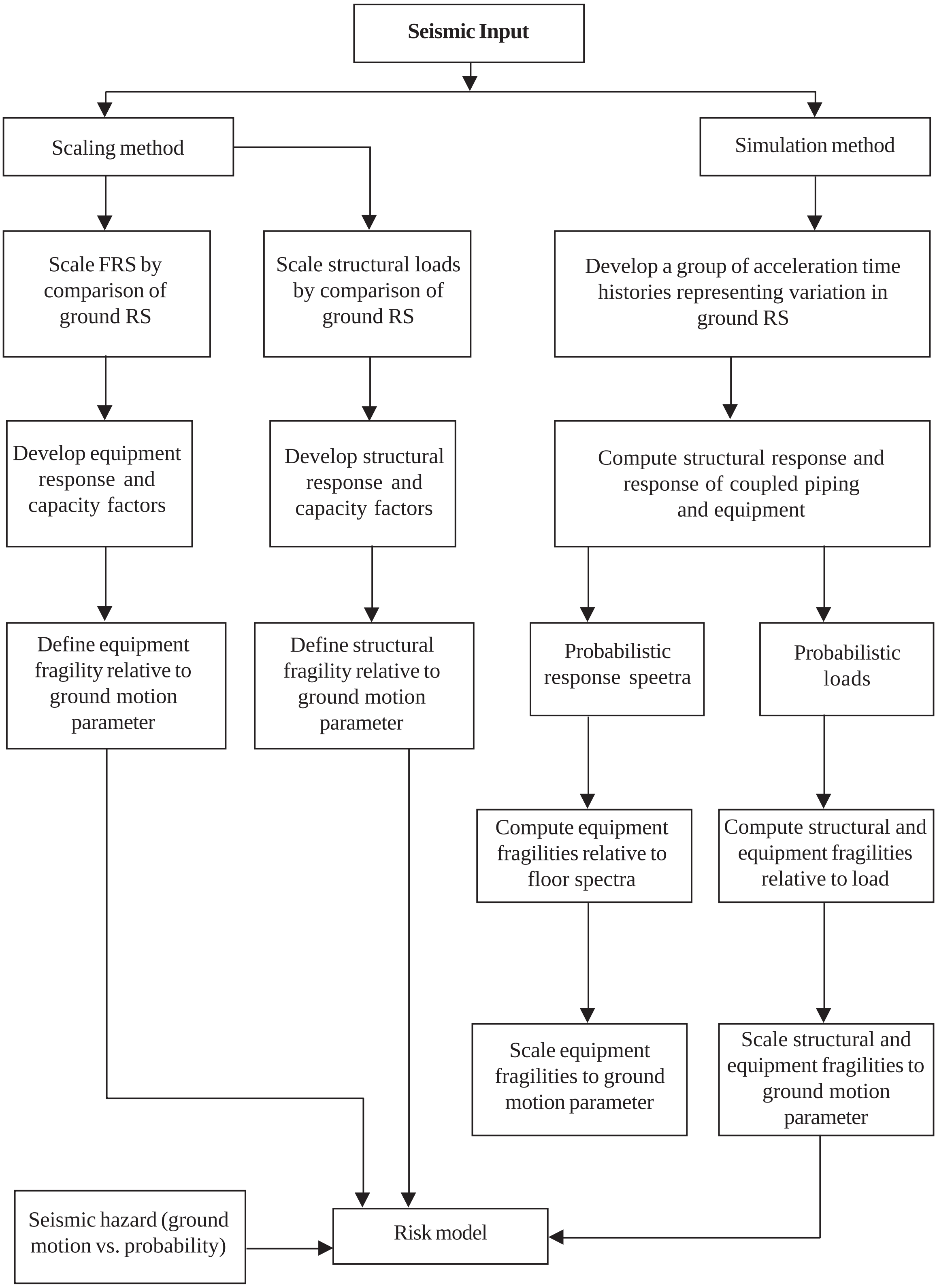

Seismic Input
Scaling method
Simulation method
Scale FRS by comparison of ground RS
Scale structural loads by comparison of ground RS
Develop a group of acceleration time histories representing variation in ground RS
Develop equipment response and capacity factors
Develop structural response and capacity factors
Compute structural response and response of coupled piping and equipment
Define equipment fragility relative to ground motion parameter
Define structural fragility relative to ground motion parameter
Probabilistic response speetra
Probabilistic loads
Compute equipment fragilities relative to floor spectra
Compute structural and equipment fragilities relative to load
Scale equipment fragilities to ground motion parameter
Scale structural and equipment fragilities to ground motion parameter
Seismic hazard (ground motion vs. probability)
Risk model

FIGURE X-7 : FLOWCHART FOR SEISMIC FRAGILITY DEVELOPMENT [99]

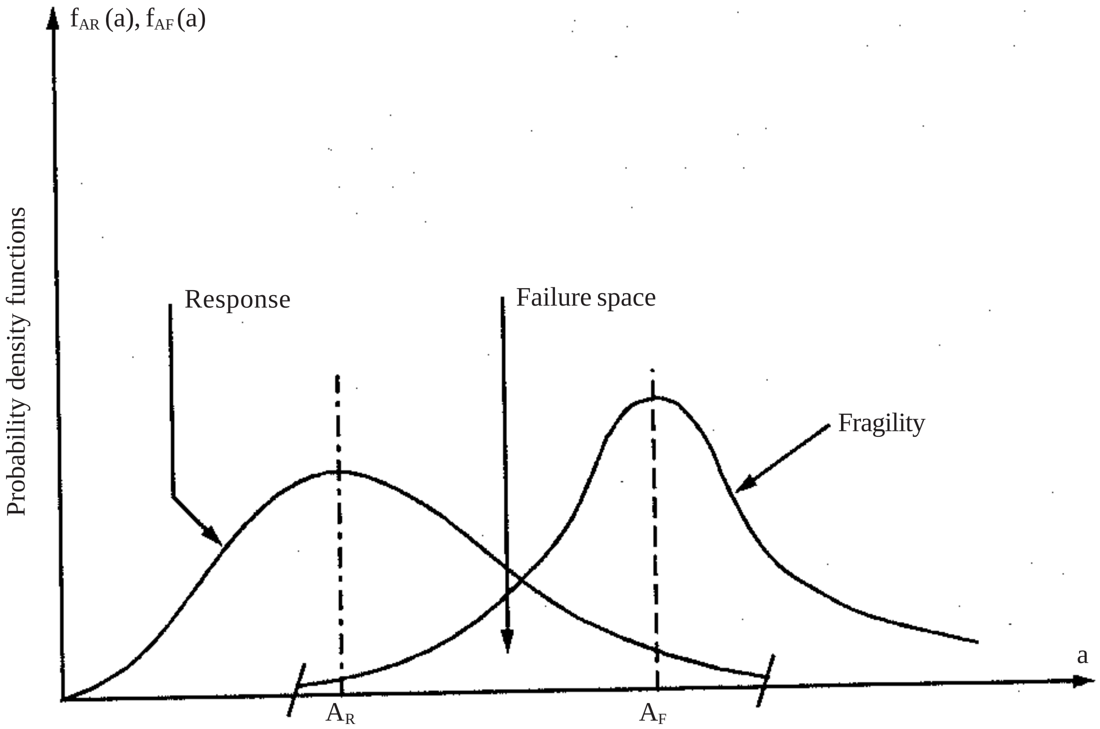


FIGURE X-8 : COMBINATION OF RESPONSE AND FRAGILITY VALUES [99]

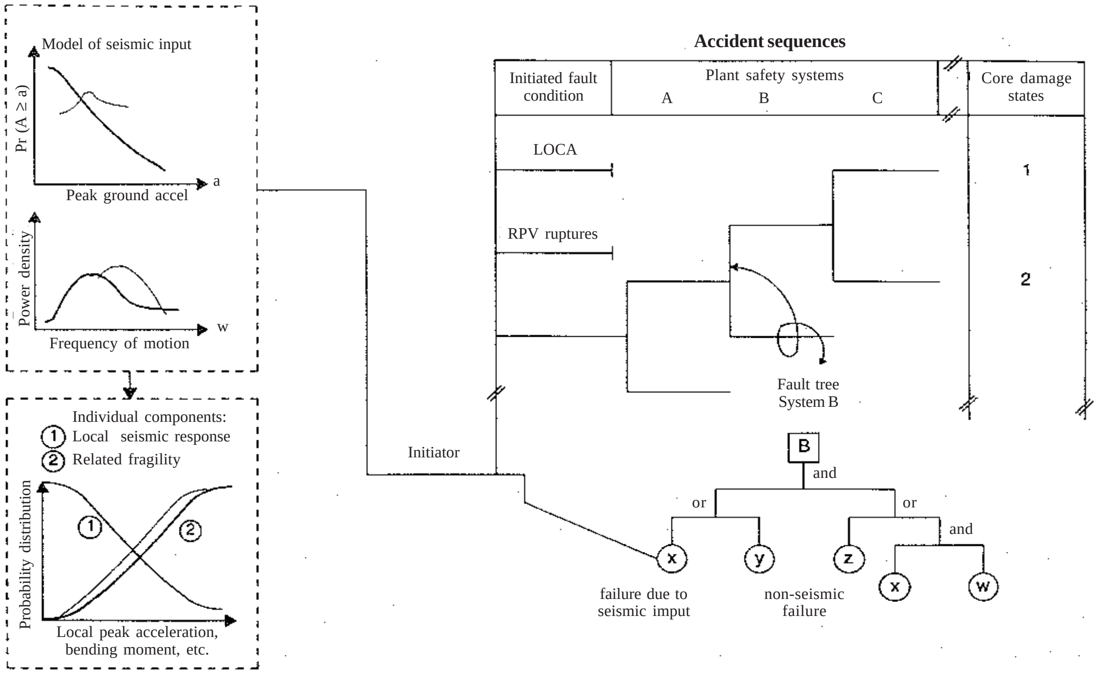


FIGURE X-9 : SCHEMATIC OVERVIEW OF SEISMIC PSA AND INTEGRATION OF FAILURE PROBABILITIES DUE TO SEISMIC EVENT [99]

APPENDIX-XI

FLOOD PSA

The risk analysis from flooding is performed along similar lines to those followed for other external events like earthquakes and fires. The method includes flood hazard analysis, fragility and vulnerability evaluation, plant and system analysis and release frequency analysis.

The first step in flood hazard analysis is the identification and selection of the initiator(s), which can cause hazard to the plant and next step, is to perform flooding hazard analysis, i.e., to establish the relation between the frequency and magnitude of flood parameter.

XI-1 Selection of IEs [7]

Two types of flood phenomena; River floods and Coastal floods are identified for contribution of risk to NPPs. These floods could arise as a result of dam failure, heavy rainfall, snowmelt, tsunami, seiches and high waves.

XI-2 Parameter Definition for Each Initiator [7]

Usually, the most important characteristics of this analysis are those parameters that are related to size (meaning damage potential). Parameterisation of an initiator by size is relatively easy, e.g., for river floods, in which the key issue is elevation of the river compared with elevation of the plant structures, equipment, dykes and embankments.

An extreme river flood may result from one or more of the following causes; precipitation, snowmelt, failure of the water flow control structures, either from seismic or hydrological causes or because of faulty operation of the structures, and channel obstruction as a result of landslides, ice effects, log or debris jams. Rivers and river floods are usually subject to significant changes over time due to natural or man made causes. Water level data at a specific site are, therefore, usually inhomogeneous over time. The size of a river flood can be measured in terms of discharge, velocity, water level, duration and the contribution of wave action.

Extreme floods from the sea can be of the following types, or a combination thereof: storm surge, tide, tsunami, seiches and waves. An extreme draw down condition resulting from a combination of wind, tsunami and an extremely low tide, may also affect the site. Alongside the extreme water levels, wave action is also a major contributor to hazard. Wind speed, direction and duration; which can occur simultaneously with the flood, should be taken into account, along with a probabilistic assessment of wave action at lower levels, which can be more serious, depending on the site conditions.

XI-3 Approximate Screening by Impact [7]

In this task, the objective is to perform an approximate screening in order to eliminate those initiators on the initial list whose impact cannot initiate an event sequence that could lead to core damage. The main screening rationale is to examine the immediate consequences of the event. For a screening process the following points are important.

The available warning time: This can be sufficiently long to shut off the operation for river sites (e.g. more than 1 day in advance). For coastal sites, in general the warning time is shorter, sometimes only a matter of hours. The warning time is the period needed for a possible flood to travel from the main source (river, basin upstream, dams, earthquake, etc.) to the site, and is therefore also directly related to the accuracy of prediction.

The type of water retaining structure: For sites with a dyke system, there is more urgency to shut down the plant even when floods lower than the design basis occur, because any dyke burst will cause severe flooding of the plant.

The adjacent areas: It is possible that other areas will be flooded as the design basis flood occurs, so that the level will be lower than expected. A plant at the edge of a narrow flood plain is more likely to be flooded than one in a wide delta area, where additional/adjacent flooding is possible.

XI-4 Detailed Screening by Frequency [7]

In this task, the analyst should perform a careful and detailed analysis to screen out those classes of initiators whose frequency is so low that elimination of the hazard source will not modify the risk profile. To provide the means for appropriate review at a later stage it is important that the analyst carefully records the reasons for using a particular screening criterion. In case of floods if the site is in an area in which there is a danger of flooding, only those sources relevant to flooding need to be considered.

XI-5 Detailed Parameterisation of Each Initiator [7]

It is necessary to select the parameter(s) to be used to characterise the initiator's damage potential. Of course, the damage potential may depend on the location in the plant, etc. The damage potential may also depend on the co-location of equipment and structures in close proximity, selection of the parameters to characterise the initiators damage potential cannot be accomplished without careful interaction with the plant response. The commonly used parameter to determine the risk of flood is flood height since little flood-induced damage can be postulated unless flood exceeds some minimum level.

For floods, the following parameters are commonly in use

Rivers: The water level, water discharge/velocity and duration.

Sea/lake: The water level, duration and velocity.

Waves: The height, length, period, wind speed and direction.

Wave run up: The height, overtopping and quantity per second.

Seiche: The wave oscillation and height.

Ice: The thickness and stream velocity.

After screening, once the initiators to be considered for flood risk analysis and the parameter(s) associated with them are decided upon, the next step of flood hazard analysis is performed.

XI-6 Flood Hazard Analysis [7]

This task is the full hazard analysis that should be performed for each initiator, which has not been screened out or bounded in earlier tasks. The objective is to generate a curve that relates the frequency (or the frequency of exceedance, or the probability) to the size of the parameter selected for that particular initiator.

The frequency of occurrence of Probable Maximum Flood (PMF) for a magnitude of parameter (flood height, flood intensity, flood rate, etc.) can be derived from statistical data, fitting available data with historical or theoretical distribution like lognormal. In fact a family of hazard curves should be drawn for non-exceedence probability levels (e.g. 5 to 95 % probability values) to represent uncertainties in developing the curve.

XI-7 Plant Vulnerability/ Fragility Evaluation [7]

The objective of a fragility evaluation is to estimate the frequency of producing certain flood damage states as a function of flood intensity. Therefore, the first step in fragility evaluation is to define the flood damage states. These could be expressed as specific contributions of structural failures that might result from external floods or the occurrence of flooding for various combinations of important impact locations resulting in functional disability of SSCs important to safety.

The failure mechanisms that should be considered for the fragility evaluation include loss of structural integrity through collapse, sliding, overturning, water run up and ponding, excessive impact and hydrostatic loads, missile strikes, flooding/submergence of component, seepage through walls and roofs, flow through openings, sprays and thermal shocks and blockage of cooling-water intakes, etc. The methodology to estimate fragility follows a line similar to that given for seismic fragility evaluation of components in terms of safety factors incorporated into design.

XI-9 Plant and System Analysis [7]

The plant analysis covers analyses of the full spectrum of possible undesirable plant consequences, including analysis of the probability of core degradation for each of the initiator and flood damage states and integrated. This step of analysis uses the basic event and fault tree methodology. The phrase plant and system analysis, encompasses not only how the physical equipment behaves after an external initiator has occurred, but also how the operating staff and other utility personnel respond, as well as common mode failures. However, in common mode failure modelling, the situation is not as well developed as that for internal initiators and the analyst must use judgement as to the best approach. The information required for the plant and system analysis includes information on the plant site, the plant design, the as-built condition of the plant and the operational aspects.

Treatment of human failures will also need some judgement as stress levels and conditions under which the operators will have to work may differ considerably.

XI-10 Release Frequency Evaluation [7]

This covers evaluation of the conditional frequencies of source term and off-site consequences given the occurrence of initiator and damage state. The methods described for Level 2 (sec. 3.3) for analysing CET and off-site impact (sec. 3.4) for Level 3 for internal events would be applicable, with the difference that dependences between the cause of the flood and certain factors that might affect off-site consequences must be taken into account. These dependences include weather conditions, the effect of the flood on emergency plans and evacuation, and liquid pathways for radionuclides.

APPENDIX-XII

ACCIDENT SEQUENCE AND PHENOMENA TO BE ADDRESSED IN THE ACCIDENT PROGRESSION MODELS

(The following list is only indicative but not exhaustive)

Main Manifestation	Phenomena Involved
Changes in core thermal hydraulics, failure of the RCS pressure boundary	Depletion of coolant inventory, change in core power, core heatup
Reactor vessel failure*	Core heatup
Core degradation	• Fuel heatup and heat transfer to neighbouring structures • Metal-water reaction and hydrogen generation • Clad ballooning, failure • Pressure tube sagging; pressure tube contacting calandria tube (PHWR) • Melting of fuel, and relocation with molten metals • Structural collapse of fuel rods • Relocation of molten material into lower plenum of the reactor vessel (for PWR and BWR)
Energetic phenomena	• High pressure melt ejection, debris fragmentation and dispersal in the containment atmosphere (for vessel type of reactor) • Steam explosion • Hydrogen generation, ignition and combustion • Direct containment heating
Containment response	• Core-catcher*/core-concrete reaction • Steam and non-condensable gas accumulation and resulting changes in containment pressure • Hydrogen stratification or mixing • Thermodynamics effect of containment coolers, suppression pool • Ignition and burning of combustible gases (deflagrations and detonations) • Containment failure due to over-pressure and temperature conditions

* For PWR/BWRs

APPENDIX-XIII

CONTAINMENT FAILURE MODES AND BINNING ATTRIBUTES FOR APET/CET

TABLE XIII-1 : TYPICAL CONTAINMENT FAILURE MODES AND MECHANISMS

Mode of Failure	Mechanism of failure
Direct bypass	Interfacing systems LOCA, steam generator tube rupture, externally initiated
Isolation failure	System failure, operating mode, leak path higher than normal
Vapour explosion	Rapid pressurisation, blast loads
Combustion	Detonation, deflagration
Over temperature	Core-concrete interactions, penetrations failure
Over pressurisation	Direct energy transfer, steam spike (explosion)
Concrete penetration	Base mat penetration

TABLE XIII-2 : TYPICAL BINNING ATTRIBUTES FOR APET/CET END STATES

Binning Attributes	Variations
Timing of release	Very early, early, intermediate, late
Containment bypass/ isolation	Interface LOCA, steam generator tubes ruptures, other initiators
Mode/mechanisms of release	DBA leakage, beyond DBA leakage, rupture
Fission product removal mechanisms	Suppression pool, filtered vents, secondary containment, others
Location of release	Ground level, stack level
Energy of release	Low, high
Duration release	Rapid, protracted

APPENDIX-XIV

CORE INVENTORIES FOR DIFFERENT TYPES OF REACTORS

XIV-1 Core Inventory for PHWR (220 MWe)

The total noble gas activity comprises about 8.01 % of the gross activity present in the core. The halogens together comprise about 8.6 % of the core activity. Alkali metals contribute about 8.6 % of the PHWR core activity. The tellurium activity is about 4.7% of the gross activity in the PHWR. It may be noted here that noble gases, halogens, alkali metals and tellurium together comprise the volatiles, which together constitute 29.9 % of the core activity at reactor shutdown. The alkaline earth metals contribute about 11.8 % of the core activity. Noble metals together contribute 15.6 % of the core activity. Rare earths together contribute about 23.5% of the core activity. Refractory Oxides contribute 14.4 % of core activity.

TABLE XIV-1 : CORE INVENTORIES (3700 MWD/T U) [107]

Radionuclides	Core Inventory (Bq)	Core Inventory (g)
Noble gases	2.922×10^{8}	2.750×10^{4}
Halogens	3.153×10^{8}	1.305×10^{3}
Alkali metals	3.127×10^{8}	1.368×10^{4}
Tellurium	1.718×10^{8}	2.196×10^{3}
Alkaline earth metals	4.296×10^{8}	1.208×10^{4}
Noble metals	5.691×10^{8}	3.036×10^{4}
Refractory oxides	5.269×10^{8}	1.853×10^{4}
Rare earths	8.572×10^{8}	4.862×10^{4}

TABLE XIV-2 : CORE INVENTORIES OF IMPORTANT RADIONUCLIDES (3700 MWD/T U) [107]

Noble Gases	Radionuclide	Half-life	Core Inventory (Bq)	Core Inventory (g)
	^{85}Kr	10.7 y	5.065×10^{4}	129.0
	^{85m}Kr	4.48 h	6.144×10^{6}	0.746
	^{87}Kr	1.27 h	1.184×10^{7}	0.418
	^{88}Kr	2.80 h	1.670×10^{7}	1.330
	^{133}Xe	5.29 d	4.430×10^{7}	236.6
	^{133m}Xe	2.23 d	1.398×10^{6}	3.118
	^{135}Xe	9.17 h	2.965×10^{6}	1.160
Halogens	^{131}I	8.04 d	2.158×10^{7}	174.0
	^{132}I	2.28 h*	3.129×10^{7}	3.030
	^{133}I	20.8 h	4.472×10^{7}	39.46
	^{134}I	52.6 m	4.867×10^{7}	1.824
	^{135}I	6.68 h	4.145×10^{7}	11.80

TABLE XIV-2 : CORE INVENTORIES OF IMPORTANT RADIONUCLIDES (3700 MWD/T U) [107] (CONTD.)

Alkali Metals	Radionuclide	Half-life	Core Inventory (Bq)	Core Inventory (g)
	^{134} Cs	2.05 y	2.355 X 10 ^{5}	1.819 x 10^{2}
	^{136} Cs	13.0 d	3.654 X 10 ^{5}	4.984 x 10^{0}
	^{137} Cs	30.1 y	4.980 X 10 ^{5}	5.723 x 10^{3}
Tellurium	^{127m} Te	109.0 d	1.787 X 10 ^{5}	18.93
	^{127} Te	9.35 h	2.037 X 10 ^{6}	0.771
	^{129m} Te	33.4 d	9.512 X 10 ^{5}	31.56
	^{131m} Te	30.0 h	3.218 X 10 ^{6}	4.034
	^{132} Te	3.25 d	3.080 X 10 ^{7}	101.4
	^{133m} Te	55.4 m	1.720 X 10 ^{7}	0.674
	^{134} Te	42.0 m	3.613 X 10 ^{7}	1.076
Alkaline Earths	^{89} Sr	52.0 d	2.253 X 10 ^{7}	7.750 x 10^{2}
	^{90} Sr	28.1 y	3.866 X 10 ^{5}	2.833 x 10^{3}
	^{91} Sr	9.48 h	2.805 X 10 ^{7}	7.735 x 10^{0}
	^{92} Sr	2.71 h	3.007 X 10 ^{7}	2.391 x 10^{0}
	^{140} Ba	12.80 d	3.888 X 10 ^{7}	5.329 x 10^{2}
Noble Metals	^{99} Mo	2.75 d	3.973 X 10 ^{7}	8.281 x 10^{1}
	^{103} Ru	39.6 d	2.954 X 10 ^{7}	9.148 x 10^{2}
	^{105} Ru	4.44 h	2.041 X 10 ^{7}	3.034 x 10^{0}
	^{106} Ru	1.01 y	3.181 X 10 ^{6}	9.502 x 10^{2}
	^{105} Rh	1.48 d	1.598 X 10 ^{7}	1.892 x 10^{1}
Refractory Oxide (Alkaline Earth)	^{95}Zr	65.5 d	3.404 X 10 ^{7}	1.584 x 10^{3}
	^{97}Zr	16.8 h	3.710 X 10 ^{7}	1.940 x 10^{1}
	^{95} Nb	35.1 d	2.969 X 10 ^{7}	7.589 x 10^{2}
Rare Earths	^{91} Y	58.6 d	2.758 X 10 ^{7}	1.124 x 10^{3}
	^{93} Y	10.2 h	3.458 X 10 ^{7}	1.036 x 10^{1}
	^{140} La	1.68 d	3.965X 10 ^{7}	7.122x 10^{1}
	^{141}Ce	32.5 d	3.637 X 10 ^{7}	1.276 x 10^{3}
	^{144} Ce	28.5 d	1.222 X 10 ^{7}	3.830 x 10^{3}
	^{143} Pr	13.6 d	3.379 X 10 ^{7}	5.017 x 10^{2}
	^{147} Nd	11.0 d	1.437 X 10 ^{7}	1.788x 10^{2}
	^{147} Pm	2.62 y	1.379 X 10 ^{6}	1.487 x 10^{3}
	^{149} Pm	2.21 d	9.454 X 10 ^{6}	2.385 x 10^{1}
	^{151} Sm	92.9 y	1.000 X 10 ^{3}	3.801 x 10^{1}
	^{156} Eu	15.2 d	1.422 X 10 ^{6}	2.578 x 10^{-1}

XIV-2 Core inventory for Other Reactors

TABLE XIV-3 : TYPICAL CORE INVENTORIES OF IMPORTANT RADIONUCLIDES IN OTHER REACTORS [107]

Group	Nuclide	Half-life	Core Inventory (MCi)			
			Thermal 1100 MWe	LMFBR 1100 MWe	BWR 160 MWe	BWR 530 MWe
Xe	^{133}Xe	5.3 d	185	173	28.89	99.61
I	^{131}I	8.04 d	91	95	14.18	50.52
	^{133}I	20.8 h	184	169	28.83	100.5
Cs	^{134}Cs	8.06 y	10.4	1.7	1.484	1.574
	^{137}Cs	30.0 y	6.2	2.6	1.854	2.012
Te	^{127}Sb	3.9 d	7.9	8.9	1.525	5.692
	^{132}Te	3.2 d	131	125	20.06	71.23
Ba	^{89}Sr	50.5 d	91	48	13.69	44.69
	^{90}Sr	29.1 y	4.7	1.0	1.373	1.385
	^{140}Ba	12.7 d	166	133	24.74	85.43
Ru	^{99}Mo	66.0 h	174	52	25.96	89.24
	^{103}Ru	39.4 d	142	72	21.74	80.56
	^{106}Ru	368 d	35	49	7.831	15.54
	^{105}Rh	1.5 d	86	38	13.96	44.73
La	^{91}Y	58.6 d	122	68	17.64	58.17
	^{95}Zr	65.5 d	159	19	24.02	81.18
	^{95}Nb	35.1 d	157	16	24.61	80.53
	^{140}La	40.3 d	171	136	25.16	88.47
	^{141}Ce	32.5 d	160	143	23.58	81.54
	^{143}Ce	33.0 d	147	118	21.83	73.60
	^{144}Ce	285 d	97	41	19.24	39.76
	^{143}Pr	13.6 d	146	118	21.77	72.13
	^{147}Nd	11.0 d	64	55	9.335	31.88
	^{239}Np	2.36 d	1976	1966	319.5	1409
	^{241}Pu	14.4 y	8.6	24	2.169	1.636
	^{242}Cm	153 d	1.8	5.8	0.3447	0.1393

Note: For reactors with continuous refuelling, the equilibrium core inventory calculated at full power is considered. For other reactors, the end of cycle radionuclide inventory is considered in source term analysis.

TABLE XIV-4 : FBTR MARK II CORE INVENTORY OF IMPORTANT FISSION PRODUCTS (100GWD/T BURNUP AND 40 MW_{th}) AND THEIR RELEASE INTO RCB IN THE EVENT OF CORE DAMAGE ACCIDENT (CDA) [107]

Isotope	Core Inventory (Bq)	Release Fraction to RCB (OECD)	Release into RCB (Bq)
I-131	5.51E16	0.90	4.96E16
Cs-137	2.48E15	0.81	2.01E15
Sr-90	8.14E14	0.11	8.95E13
Kr-85m	8.21E15	0.90	7.39E15
Kr-87	1.45E16	0.90	1.31E16
Kr-88	1.75E16	0.90	1.58E16
Xe-133	9.40E16	0.90	8.47E16
Xe-135	9.84E16	0.90	8.85E16
Pu-239	1.96E14	0.01	1.96E12

TABLE XIV-5 : CORE INVENTORY OF IMPORTANT ISOTOPES (100 GWd/T BURNUP AND 1250MW$_{th}$) AND THEIR RELEASES INTO RCB DURING CDA FOR PROTOTYPE FAST BREEDER REACTOR (PFBR) [107]

Isotope	Core Inventory (Bq)	OECD Release Fraction Into RCB	Release into RCB (Bq) with OECD Fractions	FR Release Fraction into RCB	Release into RCB (Bq) with EFR Fractions
I-131	1.48 E + 18	0.9	1.33 E + 18	0.1	1.48 E + 17
I-132	1.96 E + 18	0.9	1.76 E + 18	0.1	1.96 E + 17
I-133	2.54 E + 18	0.9	2.29 E + 18	0.1	2.54 E + 17
I-134	2.53 E + 18	0.9	2.28 E + 18	0.1	2.53 E + 17
I-135	2.23 E + 18	0.9	2.01 E + 18	0.1	2.23 E + 17
Cs-134	2.82 E + 14	0.81	2.28 E + 14	0.1	2.82 E + 13
Cs-137	8.42 E + 16	0.81	6.82 E + 16	0.1	8.42 E + 15
Rb-88	5.22 E + 17	0.81	4.23 E + 17	0.1	5.22 E + 16
Ru-103	2.41 E + 18	4.00 E - 02	9.64 E + 16	4.00 E - 02	9.64 E + 16
Ru-106	1.06 E + 18	4.00 E - 02	4.24 E + 16	4.00 E - 02	4.24 E + 16
Sr-89	7.12 E + 17	0.11	7.83 E + 16	4.00 E - 02	2.85 E + 16
Sr-90	2.88 E + 16	0.11	3.17 E + 15	4.00 E - 02	1.15 E + 15
Ce-141	2.11 E + 18	4.00 E - 02	8.44 E + 16	4.00 E - 02	8.44 E + 16
Ce-144	1.05 E + 18	4.00 E - 02	4.20 E + 16	4.00 E - 02	4.20 E + 16
Te-131m	1.63 E + 17	0.16	2.61E + 16	0.1	1.63 E + 16
Te-132	1.88 E + 18	0.16	3.01 E + 17	0.1	1.88 E + 17
Ba-140	1.93 E + 18	0.11	2.12 E + 17	4.00 E - 02	7.72 E + 16
Zr-95	1.76 E + 18	4.00 E - 02	7.04 E + 16	4.00 E - 02	7.04 E + 16
La-140	1.96 E + 18	4.00 E - 02	7.84 E + 16	4.00 E - 02	7.84 E + 16
Kr-85m	2.26 E + 17	0.9	2.03 E + 17	1.0	2.26 E + 17
Kr-87	4.08 E + 17	0.9	3.67 E + 17	1.0	4.08 E + 17
Kr-88	4.94 E + 17	0.9	4.45 E + 17	1.0	4.94 E + 17
Kr-85	4.69 E + 15	0.9	4.22 E + 15	1.0	4.69 E + 15
Xe-133	2.55 E + 18	0.9	2.30 E + 18	1.0	2.55 E + 18
Xe-135	2.66 E + 18	0.9	2.39 E + 18	1.0	2.66 E + 18
Pu-239	4.51 E + 15	1.00 E - 02	4.51 E + 13	1.00 E - 04	4.51 E + 11

TABLE XIV-6 : EQUILIBRIUM ACTIVITY OF MAIN DOSE CONTRIBUTING FP NUCLIDES IN 100 MW_{th} RESEARCH REACTOR CORE [106]

Radionuclide	Half-life	Equilibrium Activity (Ci)
Noble Gases		
Kr-85m	4.4 h	1.055E+6
Kr-87	78 m	2.140E+6
Kr-88	2.8 h	3.013E+6
Xe-133	5.17 d	5.609E+6
Xe-135	9 h	2.356E+6
Xe-138	17 m	5.198E+6
Halogens		
Br-83	2.4 h	4.44E+5
I-131	8.05 d	2.359E+6
I-132	2.3 h	3.555E+6
I-133	20.8 h	5.613E+6
I-134	52.5 m	6.332E+6
I-135	6.7 h	5.247E+6
Alkali metals		
Cs-134	2.2 y	3.238E+2
Cs-136	12.90 d	5.872E+3
Cs-137	30 y	2.085E+4
Tellurium		
Te-127	9.3 h	1.088E+5
Te-129m	37 d	5.993E+4
Te-131m	30 h	3.022E+5
Te-132m	77 h	3.540E+6
Sb-127	91 h	1.204E+5
Sb-128	9.3 h	1.091E+4
Sb-129	4.6 h	5.500E+5
Se-81	81.4 m	1.574E+5
Alkaline Earth Metals		
Sr-89	50.5 d	2.358E+6
Sr-90	28 y	2.1019E+4
Sr-91	9.7 y	4.864E+6
Sr-92	2.7 h	4.974E+6
Ba-140	12.8 d	5.040E+6
Noble Metals		
MO-99	66.5 h	5.004E+6
Ru-103	39.7 d	1.794E+6
Ru-105	4.45 h	8.701E+5
Ru-106	1.01 h	3.968E+4
Rh-105	36 h	8.502E+5

TABLE XIV-6 : EQUILIBRIUM ACTIVITY OF MAIN DOSE CONTRIBUTING FP NUCLIDES IN 100 MW$_{th}$ RESEARCH REACTOR CORE [106] (CONTD.)

Radionuclide	Half-life	Equilibrium Activity (Ci)
Metals with Refractory Oxides		
Zr-95	65 d	2.693E+6
Zr-97	17 h	4.872E+6
Nb-95	35 d	1.280E+6
Rare Earths		
Y-90	64.3 h	2.047E+4
Y-91	58 d	2.594E+6
Ce-141	33 d	3.657E+6
Ce-143	33 h	4.926E+6
Ce-144	280 d	6.613E+5
Pr-143	13.7 d	4.612E+6
Nd-147	11.1 d	1.858E+6
Pm-147	2.6 y	6.543E+5
Eu-156	15.4 d	1.500E+4
Sn-123m	136 d	1.267E+4

ANNEXURE-I

OUTLINE OF A PSA PROJECT PLAN

Project Objectives

Contains a short and concise description of the objectives of the PSA project, a description of user requirements and expectations, and a description of the intended safety related applications of the PSA.

Regulatory Requirements and Applicable Technical Standards

Regulatory requirements on PSA and its applications should be in place and should be outlined.

Scope

Contains a short and concise description of the context and extent of the work in the PSA project.

Clients

Identifies the recipients and users of the PSA project.

Quality Assurance Programme

Describes the context and extent of the QA programme for the PSA project. It should be ensured that the PSA project plan is reviewed and approved.

PSA Project Work Process

A detailed delineation of the main steps and tasks of the PSA project. It should include scheduled evaluations, reviews and assessments, presentation of interim and final results.

Schedule and Milestones

A schedule for the main steps and tasks of the PSA project. Special care needs to be devoted to steps and tasks, which require an iterative process with other tasks.

Project Interfaces

Description of project interfaces with groups, organisations or projects not explicitly integrated within the PSA project.

Project Deliverables

Description of the reports, scope of the reports and relationship between the reports and the requirements of the identified recipients.

Resource Allocation

Describes the duration of work and how resources will be planned and allocated. This includes staff, budgets and equipment. There should be a description of facilities for carrying out the work and or required modifications or upgrades.

References

List of references cited in the PSA project plan.

ANNEXURE-II

TECHNICAL INSTRUCTIONS SAMPLE FOR SYSTEM ANALYSIS

Technical Instruction Format

Technical instructions show the level of detail and the kind of controls implemented in the task process [2]. The sample for technical instructions for system analysis is given below.

CONTENTS

1. PURPOSE
   - 1.1 Introduction
   - 1.2 Objectives

2. SCOPE

3. REFERENCE DOCUMENTS

4. RESPONSIBILITIES
   - 4.1 System analyst
   - 4.2 System analysis task leader
   - 4.3 PSA project manager
   - 4.4 Document control manager

5. PROCEDURE
   - 5.1 Justification and authorisation
   - 5.2 Organisation of the report
   - 5.3 Performance of the system analysis
     - Procurement of system documentation
     - System familiarisation
     - Modelling assumptions
     - First stage review
     - Fault tree development and evaluation
     - Second stage review, review of the draft report
     - Preparation of the final report
   - 5.4 Approval process
   - 5.5 Revisions and cancellations
     - Revisions
     - Cancellations
   - 5.6 Distribution

ANNEXURE-III

CONENTS OF WORK SPECIFICATION

Where work specification is to be issued before commencement of work, it should include the following as a minimum [5]

(a) A summary of the work proposed.

(b) An introduction, which should explain the background of the project and give a general description of the plant and the extent of the work, the purpose of the study and the nature of the work to be carried out.

(c) A detailed and clear description of the scope of the work.

(d) A description of the extent of the study, which should clearly specify what will be produced in the PSA and the work to be carried out by the organisation responsible for the analysis. The methodological steps that should be included should also be specified. For example, the specification would include:

- the proposed method
- a list of PIEs to be considered and justification and verification required
- the FTs to be constructed for the plant by an approved method and their review if required
- the database to be developed, if necessary, methods for covering newer plant specific components in the generic database, the justification of additions and/or modifications, and wherever applicable, the extent of intended use of plant specific experience
- analytical work, including the studies to be carried out to determine the consequences of operation, and requirements for the use of real time simulation for fault development

The contents of written reports and the format to be adopted should be detailed. The form of the output may differ depending on the end use envisaged for the PSA. Specifically, the form of a detailed numerical report relevant to the needs of a design or licensing organisation is unlikely to meet the requirements of the operating staff.

(e) Input from the organisation that commissioned the PSA should specify the documentation that it will provide. The commissioning organisation should nominate a representative through whom all communications should be collected, and should call for changes to existing computer software. All this should be clearly specified.

(f) The required time-scale for completion of the project should be specified or the body carrying out the analysis should be required to submit a programme for approval. The project programme should include milestones, which mark completion of significant parts of the work.

(g) The form of the contract, confidentiality and copyright are not covered in the report, but should be taken into consideration if external resources are used.

ANNEXURE-IV

MASTER LOGIC DIAGRAMS FOR BWR AND PHWR

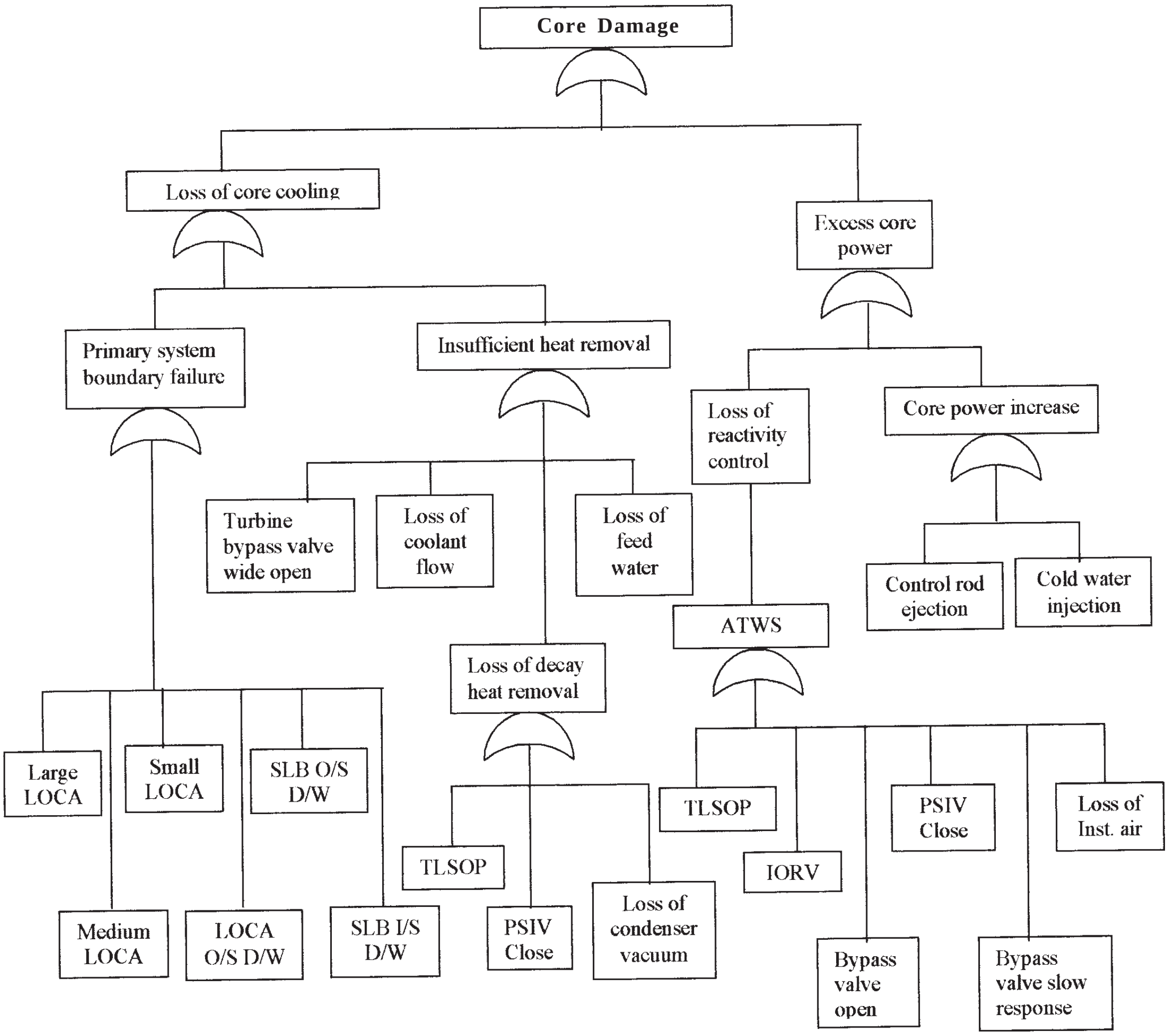


FIGURE AIV-1 : MASTER LOGIC DIAGRAM FOR BWR

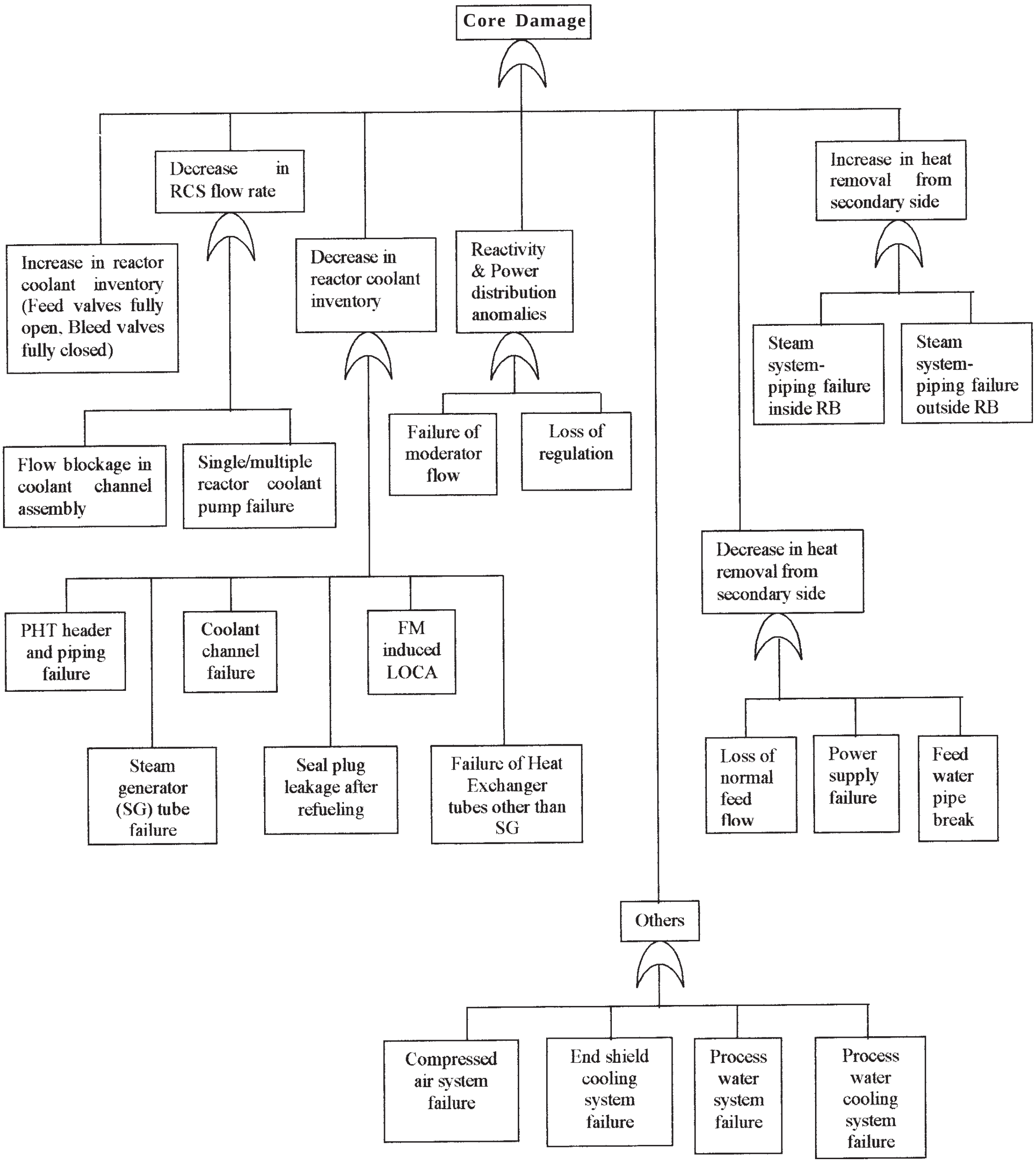

Core Damage
Increase in reactor coolant inventory (Feed valves fully open, Bleed valves fully closed)
Decrease in RCS flow rate
Flow blockage in coolant channel assembly
Single/multiple reactor coolant pump failure
Decrease in reactor coolant inventory
PHT header and piping failure
Steam generator (SG) tube failure
Coolant channel failure
Seal plug leakage after refueling
FM induced LOCA
Failure of Heat Exchanger tubes other than SG
Reactivity & Power distribution anomalies
Failure of moderator flow
Loss of regulation
Others
Compressed air system failure
End shield cooling system failure
Process water system failure
Process water cooling system failure
Decrease in heat removal from secondary side
Loss of normal feed flow
Power supply failure
Feed water pipe break
Increase in heat removal from secondary side
Steam system-piping failure inside RB
Steam system-piping failure outside RB

FIGURE AIV-2 : MASTER LOGIC DIAGRAM FOR TYPICAL PHWR

ANNEXURE-V

FORMAT FOR COMPONENT FAILURE DATA RECORDING

PSA Report I

1. Name :
2. Process :
3. Transaction details : Failure data is generated based on running input DR Step I, VI, IX & X & History feed back.
4. Pre-requisites : History feed back
5. Input : USI, Tag. No., Unit No.
6. Lay-out : As per attached sheet.

USI No.	Tag No.	Unit	Reactor Status		Equipment Run-hours	Failure Detection		Problem Description	Type & Mode of failure/Cause of failure	Component Repair		
			Before failure	After failure		Time	Date			Description	Time taken for repair	Date & Time of Eqpt. Return

ANNEXURE-V (CONTD.)

FORMAT FOR COMPONENT FAILURE DATA RECORDING

PSA Report II

1. Name :
2. Process :
3. Transaction details : Required Maintenance/Test data is generated based on PM job plan.
4. Pre-requisites : History feed back
5. Input : USI, Tag. No., Unit No.
6. Lay-out : As per attached sheet.

USI No.	Tag No.	Unit	Duration of Reactor Critical hours in calendar year	Test Data			Equipment changeover	PM frequency
				Test Frequency	Test Duration	No. of Demands		

ANNEXURE-VI

RULES OF BOOLEAN ALGEBRA

TABLE AVI-1 : RULES OF BOOLEAN ALGEBRA

Mathematical Symbolism	Engineering Symbolism	Designation
1a) $X \cap Y = Y \cap X$ 1b) $X \cup Y = Y \cup X$	$X.Y = Y.X$ $X + Y = Y + X$	Cumulative Law
2a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ 2b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X.(Y.Z) = (X.Y).Z$ $X + (Y + Z) = (X + Y) + Z$	Associative Law
3a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ 3b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X.(Y + Z) = X.Y + X.Z$ $X + (Y.Z) = (X + Y).(X + Z)$	Distributive Law
4a) $X \cap X = X$ 4b) $X \cup X = X$	$X.X = X$ $X + X = X$	Idempotent Law
5a) $X \cap (X \cup Y) = X$ 5b) $X \cup (X \cap Y) = X$	$X.(X + Y) = X$ $X + (X.Y) = X$	Law of Absorption
6a) $X \cap X' = \phi = 0$ 6b) $X \cup X' = \Omega = 1$ 6c) $(X')' = X$	$X.X' = \phi = 0$ $X + X' = \Omega = 1$ $(X')' = X$	Complementation
7a) $(X \cap Y)' = X' \cup Y'$ 7b) $(X \cup Y)' = X' \cap Y'$	$(X.Y)' = X' + Y'$ $(X + Y)' = X'.Y'$	de Morgan's Theorem
8a) $X \cup (X' \cap Y) = X \cup Y$ 8b) $X' \cap (X \cup Y') = X' \cap Y'$	$X + (X.Y) = X + Y$ $X'.(X + Y') = X'.Y' = (X + Y)'$	These relationships are unnamed but are frequently useful in the reduction process

ANNEXURE-VII

PROBABILITY DISTRIBUTIONS AND BAYES THEOREM

The Table AVII-1 below lists the probability distribution types along with the distribution parameters.

TABLE : AVII-1 PROBABILITY DISTRIBUTIONS

Distribution Type	Distribution Parameters
Lognormal	Mean, Error Factor (EF)
Beta	Mean, α (scale parameter)
Gamma	Mean, α (scale parameter)
Normal (Gauss)	Mean, standard deviation
Poisson	Mean, occurrence per unit
Exponential	Mean, occurrence per unit
Discrete	At least two percentile values
Weibull	Mean, δ (scale parameter), β (shape parameter)

The following notations are used:

$E(x)$	The Expected Value (Mean Value)
M	The median value (50th percentile)
μ	The scale parameter of the normal and lognormal distributions, equal to the mean (and median) value for the normal distribution.
σ	The shape parameter of the normal and lognormal distributions, equal to the standard deviation for the normal distribution.
α	The scale parameter of the gamma and beta distributions
β	The shape parameter of the gamma, beta and Weibull distributions
δ	The scale parameter of Weibull distribution
$\Gamma(z)$	The gamma function
λ	Occurrence rate

Probability Density Function (for random variable X, to have value x)

Lognormal Distribution

$$f(x) = \frac{1}{\sigma x\sqrt{2\pi}}\exp\left(-\frac{(\ln x - \mu)^2}{2\sigma^2}\right)$$

$$\sigma = \ln(EF) / 1.6449$$

$$M = \exp(\mu)$$

$$E(x) = \exp(\mu + \tfrac{\sigma^2}{2})$$

Beta Distribution

$$f(x) \ = \ \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}x^{\alpha-1}(1-x)^{\beta-1}$$

$$E(x) = \frac{\alpha}{\alpha+\beta}$$

Gamma Distribution

$$f(x) \ = \ \frac{\beta^{\alpha}}{\Gamma(\alpha)}x^{\alpha-1}e^{-\beta x}$$

$$E(x) = \frac{\alpha}{\beta}$$

Normal Distribution

$$f(x) \ = \ \frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$$

$$E(x) = \ M \ = \ \mu$$

Poisson Distribution

$f(x) = \frac{e^{-\lambda}\lambda^{x}}{x!}$, x = 0, 1, 2, 3, …..

$E(x) = \lambda$, where λ = pn, p = probability of failure of interest and n = sample size

Negative Exponential Distribution

$$f(x,\lambda) = \lambda e^{-\lambda x}$$

$$E(x) = \frac{1}{\lambda}$$

Discrete Distribution

A discrete distribution is defined by specification of at least two percentiles.

Weibull Distribution

$$f(x;\delta,\beta) = \frac{\beta}{\delta}\left(\frac{x}{\delta}\right)^{\beta-1}e^{-\left(x/\delta\right)^{\beta}}$$

$$E(x) = \delta\Gamma\left(1+\frac{1}{\beta}\right)$$

Bayes Theorem

It relates values called a priori (or prior) probabilities, which existed before we guess any information from the outcome itself, and also values called a posteriori (or postrior) probabilities which are determined after the outcomes (results of the experiment) are known. If, H1, H2, …..Hn are mutually exclusive events whose union is the sample space of an experiment, and if E is an arbitrary event deifned on this sample space such that P(E) > 0, Bayes' theorem says that the probability of H1, given by E, is

$$P(H_i \setminus E) = \frac{P(H_i \cap E)}{P(H_1 \cap E) + P(H_2 \cap E) + ... + P(H_n \cap E)}$$

$$= \frac{P(E \setminus H_i)P(H_i)}{\sum_{1}^{n} P(H_i)P(E \setminus H_i)}$$

ANNEXURE-VIII

EXAMPLES OF NODAL QUESTIONS FOR APETS/CETS FOR A PWR [9]

	Top Events	Prior Dependencies	Question Type
Very Early Time Frame (early phase of damage progression)			
1	Is containment isolated ?	None	Based on PDS
2	Fraction of PDS with AC power available ?	None	Based on PDS
3	What is the mechanical status of sprays in this time frame ?	None	Based on PDS
4	What is the mechanical status of fans in very early time frame ?	None	Based on PDS
5	Does RCS depressurise manually in early time frame ?	2	Based on EOPs
6	Does Temperature induced hot leg failure occurs in very early time frame ?	5	Accident progression
7	Does Temperature induced steam generator tube rupture occur in very early time frame ?	5, 6	Accident progression
8	Is AC power restored or maintained in very early time frame ?	2	Based on PDS
9	Are sprays actuated in very early time frame ?	3, 6, 8	Accident progression
10	Does H_2-combustion occur in very early time frame ?	4, 5, 6, 8, 9	Accident progression
11	Does containment fail in very early time frame ?	1, 10	Accident progression
12	Is containment isolation recovered in very early time frame ?	1, 8	Based on PDS
13	Is filtered vent system actuated in very early time frame ?	1, 10, 11	Accident progression
Early Time Frame (late phase of damage progression including vessel breach)			
14	Is core damage arrested in-vessel preventing vessel breach ?	5, 6, 7, 8	Accident progression
15	Does energetic fuel coolant interaction occur and fail RPV and containment ?	5, 6, 7, 14	Accident progression
16	What is the mode of vessel breach and the core debris ejection process ?	5, 6, 7, 14, 15	Accident progression
17	Does vessel rocketting occur and fail containment ?	16	Accident progression
18	Is under-vessel region flooded or dry at vessel breach ?	None	PDS and design
19	What is the mode of under-vessel fuel-coolant interaction following vessel breach ?	16, 18	Accident progression
20	Does hydrogen combustion occur at vessel breach ?	4, 8, 9, 10, 14, 16	Accident progression
21	Does containment fail at vessel breach ?	1, 11, 13, 15, 16, 19, 20	Accident progression
22	Does filter fail at vessel breach ?	1, 11, 13, 15, 16, 19, 20, 21	Accident progression
Late time frame (long after vessel breach)			
23	Is AC power restored or maintained in late time frame ?	8	Based on PDS

ANNEXURE-VIII (CONTD.)

EXAMPLES OF NODAL QUESTIONS FOR APETS/CETS FOR A PWR [9]

	Top Events	Prior Dependencies	Question Type
24	Do sprays actuate or continue to operate in late time frame ?	23, 9	PDS/accident progression
25	Do fan coolers actuate or continue to operate in late time frame ?	4, 8	Based on PDS
26	What is the status of fans/sprays in late time frame ?	24, 25	Summary question
27	Is core debris in a coolable configuration ex-vessel ?	16, 18, 19, 15, 17	Accident progression
28	Does H_2-combustion occur in late time frame?	10, 20, 26	Accident progression
29	Does containment failure in late time frame?	1, 10, 11, 13, 15, 21, 26, 20, 28, 19	Accident progression
30	Does filter vent system actuate in late time frame?	1, 10, 11, 13, 15, 19, 20, 21, 26, 28, 27	Accident progression
31	Is containment basemat integrity maintained ?	11, 12, 21, 22, 27, 29, 31	Accident progression
32	What is the mode of containment failure ?	11, 21, 29	Accident progression

ANNEXURE-IX

HISTORICAL PERSPECTIVE AND CURRENT STATUS OF SOURCE TERM EVALUATION

1. Historical Perspective

The first significant attempt to estimate the source term in LWRs was made as part of the WASH-740 study. The next stage in the development of the Source Term estimation was the publication of Dinunno's TID-14844. WASH-1400, the work of Rasmussen's Reactor Safety Study (RSS) in 1975, which is the first major application of PRA to NPP, includes also the study of estimation of source term. Similar work was followed by the German Risk Study in 1979 [109] for German plants. Source Term estimates were also made in the UK as part of the licensing of the Sizewell B PWR [110]. While WASH-1400 established the methodology for source term estimation, for use in probabilistic analysis, it could not explain the extremely low iodine releases from the degraded TMI-2 core. Another gap in the WASH-1400 study was the behaviour of Fission Products (FPs) in the primary coolant system, and the effect of ESFs on the time-dependent behaviour of FPs in the containment.

The Chernobyl accident source term was undoubtedly the largest accidental release of radioactivity ever recorded. The following table gives accident release sources in some major reactor accidents.

TABLE AIX-1 : ACCIDENT RELEASE SOURCES IN THE HISTORICAL REACTOR ACCIDENTS [112-120]

Reactors	Accident phenomenon/consequences	Radioactivity release
The National Research Experimental (NRX) reactor	Power 'runaway' occurred, reactor core and calandria vessel destroyed	100 % gaseous and volatile release: 8 x 10^{+3} – 3 x 10^{+4} C_i
The Wind scale Pile # 1 reactor	Uncontrolled wigner energy release causing burning of fuel and graphite, Reactor core destroyed	100 % of noble fission gas inventory was released. About 10 % of the volatiles including iodine, tellurium and cesium escaped past the filters. Total polonium release: 180-290 C_i
The Stationary Low-power (SL-1) Reactor	Super-prompt criticality accident occurred. Steam voids and water hammer set up which destroyed reactor core, vessel was thrown away and core material ejected outside	5-15% of total FP inventory escaped 1 x 10^{+4} NGs, 80 C_i of I^{131}, 0.5 % C_i of Cs^{137}, 0.1 C_I of Sr^{90} and 0.01 % of the non-volatiles
The three mile island (TMI-2) reactor	Feed water transient with series of malfunctions involving human errors Complete destruction of core	2.5-13 MC_i of Xe^{133}, 1.6 to 8.4% of NG and 17 C_i of I^{131}, No non-volatiles escaped to atmosphere
The Chernobyl Unit # 4 Reactor	Accident triggered by TG experiment requiring reduced flow in reactor, operation at intermediate prohibited power level, steam bubble formation, insertion of positive reactivity resulting in super-prompt criticality. Reactor exploded, reactor vessel top closure got lifted and destroyed the upper part of the reactor building.	100 % NGs (3.3 x 10^{+16} Bq), 15-20 % volatiles and 3-4% non-volatiles later revised to 50-60 % iodine, 33-43 % for Cs and 25-60 % for tellurium

2. Current Status

The source term estimation has evolved from overly conservative empirical release factors to reasonably sized but still empirical methodology. The methodology set in place by the Reactor Safety Study is here to stay, inspite of the use of unwieldy computer code packages, which it entails; and the several gaps in the knowledge about the phenomenology of severe accidents.

ANNEXURE-X

SOURCE TERM EXAMPLES

1. RSS Study

TABLE AX-1 : ACCIDENT SEQUENCES THAT COULD RESULT IN SIZEABLE RELEASE OF RADIOACTIVE ISOTOPES

Designation	Description
1. RSS PWR large containment	
(i) TMLB' - $\delta, \gamma, \varepsilon$ (2×10^{-6}, 7×10^{-7}, 6×10^{-7} per Rx-y)	Loss of RCS heat removal given loss of all AC power; containment failure due to over-pressurisation, H_2 burning, or melt-through
(ii) S_2C - δ (2×10^{-6} per Rx-y)	Failure of containment spray injection given a small LOCA; containment failure due to over-pressurisation
(iii) S_2D - ε (9×10^{-6} per Rx-y)	Failure of ECCS given a small pipe break; containment failure due to containment melt-through
2. RSS BWR	
(i) TC - γ (1×10^{-5} per Rx-y)	Failure of reactor shutdown system given a transient event; containment failure due to over-pressure, release through RB.
(ii) TW - γ - γ' (1×10^{-5} , 3×10^{-6} per Rx-y)	Failure of decay heat removal system given a transient event; containment failure due to over-pressure, release through reactor building or release direct to atmosphere.

Key to PWR/BWR Accident Sequence Symbols

PWR Accident Sequence Symbols	
B'	Failure to recover either on-site or off-site electric power within 1-3 h following 'loss of off-site power'
C	Failure of the containment spray injection system
D	Failure of the core cooling injection system
L	Failure of the secondary system steam relief valves and the auxiliary feed water system.
M	Failure of the secondary system steam relief valves and the power conversion system.
S_2	A small -small LOCA with an equivalent diameter 1/2 to 2 in.
T	Transient event
t	Containment failure due to hydrogen burning
d	Containment failure due to overpressure
e	Containment vessel melt-through
BWR Accident Sequence Symbols	
C	Failure of reactor protection system
T	Transient event
W	Failure to remove residual core heat
t	Containment failure due to over-pressure: release through containment building
t'	Containment failure due to over-pressure : release direct to atmosphere

2. Examples from the Sizewell B Source Term Study [108]

In the Sizewell B study, the degraded core accidents were divided into 21 categories, each comprising similar states of plant damage. For each category, a CET was drawn and the results were grouped into 12 release categories, each having a similar type of release of radioactive materials. The categories (UK-1 to UK-12) are described briefly in the Table-AX-2. The annual probability of each release category is estimated from the quantification of the branches of the ET. The different categories are distinguished by different amounts of FPs released, the amount of energy in the plume, the height of release and the warning time available prior to the release.

The STs were estimated in two stages. In the 'first estimate' many conservative assumptions were made such as no FP retention in the reactor coolant circuit; as a result, the STs were high. In the 'second estimate', a set of source terms were calculated using the best judgment for the release categories UK-1, UK-2, UK-5 and UK-6, as these categories were the major contributor contributors to risk. The STs for UK-1, UK-2, UK-5, and UK-11 are given in Table AX-3. The Westinghouse analysis estimated that the containment would be breached in only 6 % of the degraded core accidents, corresponding to an annual probability of about 7.5 x 10^{-8}. This low value shows that the containment has an important effect in reducing the risk from beyond DBAs. Of course, the estimated radiological consequences of degraded core accidents without containment failure would be akin to those of a DBA.

TABLE AX-2 : SIZEWELL B RELEASE CATEGORIES

Category	Description
UK-1	This category is used for accident sequences in which a containment bypass pathway exists from the reactor coolant circuit to the environment. The pathway considered in WCAP is the failure of the isolation valves separating the reactor coolant circuit and the low-pressure residual heat removal system. This category is also used for multiple steam generator tube rupture sequences.
UK-2	This category is used for early failure of the containment due to high internal pressures, with a ST reflecting the occurrence of a steam explosion, and in which containment sprays are not functioning. It also includes those sequences where, although there is no over-pressure failure, a failure to close containment penetrations or a small containment bypass occurs.
UK-3	This category is used for early over-pressure failure of the containment where sprays are not functioning. It is also used for sequences where sprays are functional, but where containment failure occurs so soon after most of the FPs are released from the reactor, that the sprays are not effective in removing FPs and, in particular, for small LOCA sequences
UK-4	This category is used for early over-pressure failure of the containment with the assumed occurrence of a steam explosion at a time when the spray system is functioning. It is also used to include isolation failure with sprays functioning and for single SG tube rupture sequences.
UK-5	This category is used for late over-pressure failure of the containment without sprays operating. Failures are as a result of relatively slow pressure build-up due to loss of containment heat removal capability. Cooling of the core debris is lost so that dry-out and vaporisation release occurs. It is pessimistically assumed that containment failure occurs after 4 h.
UK-6	This category is used for late over-pressure failure of the containment without sprays operating. Failures are as a result of relatively slow pressure build-up due to loss of containment heat removal capability. Debris in the cavity from the molten core remains covered by water so that no vaporisation release occurs
UK-7	This category is used for early over-pressure failure of the containment with spray systems functional for a significant period before reactor pressure vessel failure.

TABLE AX-2 : SIZEWELL B RELEASE CATEGORIES (CONTD.)

Category	Description
UK- 8	This category is used for late over-pressure failure of the containment where spray systems are functional and core debris remains covered by water.
UK-9 and UK-10	These categories are used for melt-through of the base of the containment, with and without spray failure, respectively. A release takes place through the surrounding soil to the environment.
UK-11 and UK-12	These categories are used for all core melt accidents in which the containment remains intact or for which cooling is successfully restored to the core while still in the pressure vessel. UK-11 and UK-12 refer to cases with and without spray failure, respectively. Radioactivity released to the environment would be that due to normal rates of containment leakage.

Notes: (i) 'Early failures' may occur in the first few hours of an accident, due, for example, to a coincidence of the containment fans and sprays failing to operate and hydrogen burn or steam spike occurring.

(ii) 'Late failures' may occur up to 10-12 h into an accident.

TABLE AX-3 : SIZEWELL B PRA RESULTS

Release Category	Start	Duration	Fraction of Core Inventory Released						
			Xe	I	Cs	Te	Ba	Ru	La
UK-1	1 h	3 h	0.9	0.7	0.5	0.3	6.0E-2	2.0E-2	4.0E-3
UK-2	1 h	0.5 h	0.9	0.7	0.4	0.35	5.0E-2	0.2	3.0E-3
UK-5	8 h	0.5 h	1.0	0.3	0.3	0.5	4.0E-2	3.0E-2	6.0E-3
UK-11	2 h	> 24 h	6.0E-2	6.0E-5	3.0E-5	3.0E-5	3.0E-6	2.0E-6	4.0E-7
Actual Accidents									
Chernobyl	0 h	10 d	1.0	0.4	0.25	> 0.1	4.0E-2	5.0E-2	3.0E-2
TMI-2	3 h	1 h	< 8.0E-2	2.0E-7	0.0	0.0	0.0	0.0	0.0

ANNEXURE-XI

'RISK COEFFICIENTS' FOR HEALTH EFFECTS CALCULATIONS

TABLE AXI-1 : VALUES OF RISK COEFFICIENT 'S' FOR HEALTH EFFECTS CALCULATIONS [108]

Dose in Organ/Tissue		**Effect**	**Slope Parameter**	**Median does D_{50} (S_v)[1] Upper End of Exposure Interval (days)**							**Threshold for Exposure During Time Interval Ti (Sv)**			
External Irradiation	**Internal Irradiation**		**'S'**	**1**	**7**	**14**	**21**	**30**	**200**	**365**	**1**	**2**	**3**	**4**
		MORTALITY												
lung	lung	pulmonary syndrome	7.0	9.3	-	94.0	-	-	22.0	540.0	5.0	47.0	110.0	270.0
red bone marrow	red bone marrow	haematopoietic syndrome	6.0	4.7	-	8.5	-	17.1	-	-	2.3	4.2	8.5	-
remainder[2]	-	gastrointestinal syndrome	10.0	15.0	35.0	-	-	-	-	-	10.0	23.0	-	-
		skin burns (5%)	4.7	35.0	50.0	-	-	-	-	-	23.0	45.0	-	-
skin	-	pre-and neonatal death[3]	3.0	1.0	-	-	-	-	-	-	0.1	-	-	-
ovaries	uterus													
		MORBIDITY												
lung	lung	lung function impairment	7.0	4.6	-	47.0	-	-	110.0	270.0	2.3	23.0	55.0	135.0
thyroid	thyroid	hypothyroidism	1.3	60.0	-	-	-	external exposure			2.0	-	-	-
				-	-	-	-	300.0 iodine inhalation			10.0	-	-	-
skin	-	skin burns	4.7	35.0	50.0	-	-	-	-	-	23.0	45.0	-	-
skin	-	cataracts	1.5	3.1	-	6.2	-	-	-	9.3	1.0	3.0	4.5	-
ovaries	uterus	mental retardation[3]	1.0	4.1	-	-	-	-	-	-	0.1	-	-	-

TABLE AXI-2 : VALUES OF RISK COEFFICIENTS ‘A’ FOR HEALTH EFFECTS CALCULATIONS [108]

Organ/Tissue	Effect	Model(2)	Fraction of Cancers which are Fatal	Effects (1) per 10^6 Persons and 10^2 Sv
Red bone marrow	Leukemia	A	1.0	52
Bone surface	Cancers	A	1.0	1
Breast	Cancers	R	0.4	80
Lung	Cancers	R	0.75	90
Stomach	Cancers	R	0.85	224(3)
Colon	Cancers	R	0.55	
Liver	Cancers	R	1.0	
Pancreas	Cancers	R	0.9	
Thyroid	Cancers	R	0.1	17
Remainder	Cancers	R	0.6	38
Skin	Cancers		0.0	138(4)
Gonads	Hereditary			200

(1) The numbers given are the numbers of fatal cancers of serious hereditary effects, averaged over males and females (including breast) assuming linear dose risk relationship

(2) A absolute risk model. R: relative risk model

(3) Sum for the GI-tract

(4) Morbidity

ANNEXURE-XII

SHUTDOWN PSA FOR PHWRS

In general the methodology and steps followed for PHWR shutdown PSA is similar to the steps followed for internal initiating events. However, special attention is required with regards to initiating event identification, initiating event, frequency calculation, event tree development and system modeling. A typical PHWR specific shutdown PSA case with regard to various stages is brought out here.

Initiating events : The number of initiating events assessed for shutdown PSA in terms of their safety implications are generally very low. A typical PHWR shutdown PSA identifies seven initiating events mainly related to support systems and regulation actions, i.e., loss of regulation, loss of instrument air, loss of service water, loss of shutdown cooling system, etc.

Initiating event frequencies : To calculate plant specific initiating event frequencies for shutdown PSA of PHWR, all possible shutdown state cases, such as reactor is shutdown with the HTS cold depressurised and full, with HTS depressurised and full, and with HTS drained to the header level, etc. need to be considered.

Event tree development : In the event tree development, special care is required to introduce the operator actions to initiate most of the auto logic linked with reactor power operation state, such as initiation of manual injection of ECCS, etc. Also, for the availability of systems to provide a heat sink, shutdown cooling system and auxiliary boiler feed water system should not be taken out for maintenance together.

System modelling : Due to low decay heat levels, the success criteria for most systems are less stringent at shutdown than at full power such as the number of air supply compressors etc. Also the standby failures are dominated by maintenance unavailability.

Results and discussion : Shutdown State PSA analysis provides insights into the importance of various aspects of design, operating practices, maintenance restrictions, accident procedures and outage management with respect to the prevention of core damage.

ANNEXURE-XIII

AN EXAMPLE OF RISK BASED AGEING MANAGEMENT

Because the ageing contributions were identified to be large, additional test and maintenance actions were evaluated which could better control the ageing contributors. The specific additional activities evaluated involve carrying out scheduled overhauls at given intervals and carrying out improved surveillance tests on the risk dominant ageing contributors. Since the motor operated valves (MOVs) in the ECCS (i.e. the HPI and LPR systems) are dominant contributors to the ageing effects, as was identified in Table AXIII-1 and AXIII-2 [119], additional ageing management is focused on these valves. The additional ageing management, which is considered, consists of overhauling or replacing the valves every 60 months, as well as improving the test efficiency and increasing the test frequency to once every 6 months. A total of 14 valves are involved in this additional ageing management process.

Table AXIII-1 presents the top individual ageing contributors and Table AXIII-2 presents the top two component ageing interactions. Higher order ageing interactions were determined not to be significant for this application. The top 25 contributors with component names are given in each table, representing approximately 99% of the total contributor. The CDF risk importance, S_i or S_{ij} is then given for the contributor. The ageing rate (a) and the Mean Time Between Failures (MTBF) are also shown in the table. The MTBF is used as the replacement time (L). Components whose MTBF is larger than 40 years are indicated by MTBFs of 720 months. For those components, the appropriate non-replacement unavailability equation was used. The other entities in each table are the test intervals (T), the unavailability increase (Δq_i) due to ageing, and the CDF increase (ΔC) for the contributor. The sum of CDF increases from the contributors is given at the upper right hand side of the table. It is interesting to note that the ageing interactions, which arise from the simultaneous ageing of multiple components, are significant contributors.

Tables AXIII-3 and AXIII-4 [121] give single and double interaction contributions to the CDF increase with the modified overhaul and testing schedules. From these tables, these modified activities result in a CDF increase from ageing of $3.8 \times 10^{-5} + 1.9 \times 10^{-5} = 5.7 \times 10^{-5}$ per year. This compares with the base case CDF increase from ageing of $1.8 \times 10^{-4} + 7.6 \times 10^{-4} = 9.4 \times 10^{-4}$ per year from Tables AXIII-1 and AXIII-2. The additional ageing control thus produces a factor of 16 reduction in the CDF increase due to ageing. (From 9.4×10^{-4} to 5.7×10^{-5} per year). The CDF increase due to ageing is now comparable to the baseline CDF without ageing. It is important to note that ageing controls need to be focused not only on the top single MOV contributors (in Table AXIII-3), but also on the MOVs involved in the ageing interactions (Table AXIII-2), since different valves are involved.

The methodology illustrated above is applied to CDF (Level 1 PSA). However, it can be applied to other risk levels (e.g. consequence in public domain) and can include structural as well as component ageing focusing on risk importance contributors, which can be used as additional insights for risk-informed decision on ageing management and life extension programme.

TABLE AXIII-1 : CDF INCREASES FOR PLANT A : BASE CASE, SINGLE CONTRIBUTIONS [121]

Plant A: Single Contributors				**Total ΔC: 1.8E-04 /year**			
Rank	**Component Name**	**Sensitivity Coefficient (S_i)**	**Ageing Rate (a) (/hr/yr)**	**MTBF (L) (months)**	**Test Interval (T) (months)**	**Δq_1**	**ΔC (/year)**
1	LPR-MOV-FT-1862A	1.5E-04	3.6E-06	167	30	2.6E-01	3.9E-05
2	LPR-MOV-FT-1860A	1.5E-04	3.6E-06	167	30	2.6E-01	3.9E-05
3	LPR-MOV-FT-1890A	1.4E-04	3.6E-06	167	30	2.6E-01	3.5E-05
4	HPI-MOV-FT-1350	6.7E-05	3.6E-06	167	30	2.6E-01	1.7E-05
5	LPR-MOV-FT-1862B	2.1E-05	3.6E-06	167	30	2.6E-01	5.4E-06
6	OEP-DGN-FS-DG01	3.8E-04	3.6E-06	72	4	1.4E-02	5.3E-06
7	LPR-MOV-FT-1860B	2.0E-05	3.6E-06	167	30	2.6E-01	5.3E-06
8	OEP-DGN-FR-6HDG1	3.4E-04	3.6E-06	72	4	1.4E-02	4.8E-06
9	OEP-DGN-FS-DG03	2.0E-04	3.6E-06	72	4	1.4E-02	2.8E-06
10	OEP-DGN-FS-DG02	2.0E-04	3.6E-06	72	4	1.4E-02	2.8E-06
11	OEP-DGN-FR-6HDG3	1.9E-04	3.6E-06	72	4	1.4E-02	2.7E-06
12	OEP-DGN-FR-6HDG2	1.7E-04	3.6E-06	72	4	1.4E-02	2.5E-06
13	PPS-MOV-FT-1535	9.5E-06	3.6E-06	167	30	2.6E-01	2.4E-06
14	HPI-CKV-FT-CV225	2.1E-03	4.0E-09	720	11	4.8E-04	1.7E-06
15	HPI-CKV-FT-CV25	2.1E-03	4.0E-09	720	11	4.8E-04	1.7E-06
16	HPI-MOV-FT-CV410	2.1E-03	4.0E-09	720	11	4.8E-04	1.7E-06
17	HPI-MOV-FT-1115C	5.7E-06	3.6E-06	167	30	2.6E-01	1.5E-06
18	HPI-MOV-FT-1115D	5.7E-06	3.6E-06	167	30	2.6E-01	1.5E-06
19	HPI-MOV-FT-1115B	5.7E-06	3.6E-06	167	30	2.6E-01	1.5E-06
20	HPI-MOV-FT-1115E	5.7E-06	3.6E-06	167	30	2.6E-01	1.5E-06
21	LPR-MOV-FT-1890B	4.5E-06	3.6E-06	167	30	2.6E-01	1.2E-06
22	PPS-MOV-FT-1536	3.4E-06	3.6E-06	167	30	2.6E-01	8.8E-07
23	HPI-MOV-FT-1867D	2.9E-06	3.6E-06	167	30	2.6E-01	7.5E-07
24	OEP-DGN-FR-DG01	5.0E-05	3.6E-06	72	4	1.4E-02	7.2E-07
25	SIS-ACT-FA-SISA	1.8E-05	3.0E-07	720	6	1.8E-02	5.4E-07

TABLE AXIII-2 : CDF INCREASES FROM ACTIVE COMPONENTS FOR PLANT A : BASE CASE, DOUBLE CONTRIBUTIONS [121]

Plant A : Double Contributors								Total ΔC : 7.6E-04 /year				
Rank	Component Name	Sensitivity Coefficient (S_i)	Ageing Rate (a) (/hr/yr)	MTBF (L) (months)	Test Interval (months)	Δq1	Component Name	Ageing Rate (a) (/hr/yr)	MTBF (L) (months)	Test Interval (months)	Δq_2	Δ C (/year)
1	HPI-MOV-FT-1115B	1.9E-03	3.6E-06	167	30	2.6E-01	HPI-MOV-FT-1115D	3.6E-06	167	30	2.6E-01	1.3E-04
2	LPR-MOV-FT-1115C	1.9E-03	3.6E-06	167	30	2.6E-01	LPR-MOV-FT-1115E	3.6E-06	167	30	2.6E-01	1.3E-04
3	LPR-MOV-FT-1890A	1.5E-03	3.6E-06	167	30	2.6E-01	LPR-MOV-FT-1890B	3.6E-06	167	30	2.6E-01	1.0E-04
4	LPR-MOV-FT-1860A	1.5E-03	3.6E-06	167	30	2.6E-01	LPR-MOV-FT-1860B	3.6E-06	167	30	2.6E-01	1.0E-04
5	LPR-MOV-FT-1862A	1.5E-03	3.6E-06	167	30	2.6E-01	LPR-MOV-FT-1860B	3.6E-06	167	30	2.6E-01	1.0E-04
6	LPR-MOV-FT-1860A	1.5E-03	3.6E-06	167	30	2.6E-01	LPR-MOV-FT-1862B	3.6E-06	167	30	2.6E-01	1.0E-04
7	LPR-MOV-FT-1862A	1.5E-03	3.6E-06	167	30	2.6E-01	LPR-MOV-FT-1862B	3.6E-06	167	30	2.6E-01	1.0E-04
8	SIS-ACT-FA-SISA	6.5E-03	3.0E-07	720	6	1.8E-02	SIS-ACT-FA-SISA	3.0E-07	720	6	1.8E-02	5.9E-06
9	RMT-ACT-FA-RMTS	1.5E-03	3.0E-07	720	6	1.8E-02	RMT-ACT-FA-RMTS	3.0E-07	720	6	1.8E-02	1.4E-06
10	OEP-DGN-FR-6HDG3	5.6E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-6HDG1	3.6E-06	72	4	1.4E-02	1.1E-06
11	OEP-DGN-FS-DG01	4.9E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FS-DG02	3.6E-06	72	4	1.4E-02	9.9E-07
12	OEP-DGN-FS-DG01	4.9E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FS-DG03	3.6E-06	72	4	1.4E-02	9.9E-07
13	OEP-DGN-FS-DG01	4.0E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FS-6HDG2	3.6E-06	72	4	1.4E-02	8.1E-07
14	OEP-DGN-FS-DG01	4.0E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-6HDG3	3.6E-06	72	4	1.4E-02	8.1E-07
15	OEP-DGN-FS-DG02	4.0E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-6HDG1	3.6E-06	72	4	1.4E-02	8.1E-07
16	OEP-DGN-FR-6HDG1	4.0E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-6HDG2	3.6E-06	72	4	1.4E-02	8.1E-07
17	OEP-DGN-FS-DG03	3.9E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-6HDG1	3.6E-06	72	4	1.4E-02	7.8E-07
18	OEP-DGN-FS-DG01	5.0E-03	3.6E-06	72	4	1.4E-02	MSS-SRV-OO-SGSRV	7.0E-07	22	22	3.4E-03	2.4E-07
19	LPI-MDP-FS-SI1B	1.5E-03	2.0E-07	86	2	5.8E-04	LPR-MOV-FT-1862A	3.6E-06	167	30	2.6E-01	2.3E-07
20	LPI-MDP-FS-SI1A	1.5E-03	2.0E-07	86	2	5.8E-04	LPR-MOV-FT-1860B	3.6E-06	167	30	2.6E-01	2.3E-07
21	LPI-MDP-FS-SI1B	1.5E-03	2.0E-07	86	2	5.8E-04	LPR-MOV-FT-1860A	3.6E-06	167	30	2.6E-01	2.3E-07
22	LPI-MDP-FS-SI1A	1.5E-03	2.0E-07	86	2	5.8E-04	LPR-MOV-FT-1862B	3.6E-06	167	30	2.6E-01	2.3E-07
23	OEP-DGN-FR-6HDG1	4.6E-03	3.6E-06	72	4	1.4E-02	MSS-SRV-OO-SGSRV	7.0E-07	22	22	3.4E-03	2.2E-07
24	PPS-MOV-FC-1536	2.9E-06	3.6E-06	167	30	2.6E-01	PPS-MOV-FC-1535	3.6E-06	167	30	2.6E-01	1.9E-07
25	OEP-DGN-FS-DG03	9.1E-04	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-DG01	3.6E-06	72	4	1.4E-02	1.8E-07

* Control values

TABLE AXIII-3 : CDF INCREASES FOR PLANT A : CONTROL ALTERNATIVE 1, SINGLE CONTRIBUTORS [121]

Plant A: Single Contributors				**Total ΔC: 1.8E-04 /year**			
Rank	**Component Name**	**Sensitivity Coefficient (S_i)**	**Ageing Rate (a) (/hr/yr)**	**MTBF (L) (months)**	**Test Interval (T) (months)**	**Δq_1**	**ΔC (/year)**
1	OEP-DGN-FS-DG01	3.8E-04	3.6E-06	72	4	1.4E-02	5.3E-06
2	OEP-DGN-FR-6HDG1	3.4E-04	3.6E-06	72	4	1.4E-02	4.8E-06
3	LPR-MOV-FT-1862A	1.5E-04	3.6E-06	60*	6*	1.9E-02	2.9E-06
4	LPR-MOV-FT-1860A	1.5E-04	3.6E-06	60*	6*	1.9E-02	2.9E-06
5	OEP-DGN-FS-DG02	2.0E-04	3.6E-06	72	4	1.4E-02	2.8E-06
6	OEP-DGN-FS-DG03	2.0E-04	3.6E-06	72	4	1.4E-02	2.8E-06
7	OEP-DGN-FR-6HDG3	1.9E-04	3.6E-06	72	4	1.4E-02	2.7E-06
8	LPR-MOV-FT-1890A	1.4E-04	3.6E-06	60*	6*	1.9E-02	2.6E-06
9	OEP-DGN-FR-6HDG2	1.7E-04	3.6E-06	72	4	1.4E-02	2.5E-06
10	HPI-CKV-FT-CV225	2.1E-03	4.0E-09	720	11	4.8E-04	1.7E-06
11	HPI-CKV-FT-CV25	2.1E-03	4.0E-09	720	11	4.8E-04	1.7E-06
12	HPI-CVK-FT-CV410	2.1E-03	4.0E-09	720	11	4.8E-04	1.7E-06
13	HPI-MOV-FT-1350	6.7E-05	3.6E-06	60*	6*	1.9E-02	1.3E-06
14	OEP-DGN-FR-DG01	5.0E-05	3.6E-06	72	4	1.4E-02	7.2E-07
15	SIS-ACT-FA-SISA	1.8E-05	3.0E-07	720	6	1.8E-02	5.4E-07
16	LPR-MOV-FT-1862B	2.1E-05	3.6E-06	60*	6*	1.9E-02	4.0E-07
17	LPR-MOV-FT-1860B	2.0E-05	3.6E-06	60*	6*	1.9E-02	3.9E-07
18	PPS-MOV-FT-1535	9.5E-06	3.6E-06	60*	6*	1.9E-02	1.8E-07
19	HPI-MOV-FT-1115B	5.7E-06	3.6E-06	60*	6*	1.9E-02	1.1E-07
20	HPI-MOV-FT-1115D	5.7E-06	3.6E-06	60*	6*	1.9E-02	1.1E-07
21	HPI-MOV-FT-1115C	5.7E-06	3.6E-06	60*	6*	1.9E-02	1.1E-07
22	HPI-MOV-FT-1115E	5.7E-06	3.6E-06	60*	6*	1.9E-02	1.1E-07
23	LPR-MOV-FT-1890B	4.5E-06	3.6E-06	60*	6*	1.9E-02	8.5E-08
24	PPS-MOV-FT-1536	3.4E-06	3.6E-06	60*	6*	1.9E-02	6.5E-08
25	HPI-MOV-FT-1867D	2.9E-06	3.6E-06	60*	6*	1.9E-02	5.6E-08

* Control Values

TABLE AXIII-4 : CDF INCREASES FOR PLANT A : CONTROL ALTERNATIVE 1, DOUBLE CONTRIBUTIONS [121]

Plant A: Double Contributors											**Total ΔC : 1.9E-05 /year**	
Rank	**Component Name**	**Sensitivity Coefficient (S_i)**	**Ageing Rate (a) (/hr/yr)**	**MTBF (L) (months)**	**Test Interval (months)**	**Δq1**	**Component Name**	**Ageing Rate (a) (/hr/yr)**	**MTBF (L) (months)**	**Test Interval (months)**	**Δq_2**	**Δ C (/year)**
1	SIS-ACT-FA-SISA	6.5E-03	3.0E-07	720	6	1.8E-02	SIS-ACT-FA-SISA	3.0E-07	720	6	1.8E-02	5.9E-06
2	RMT-ACT-FA-RMTS	1.5E-03	3.0E-07	720	6	1.8E-02	RMT-ACT-FA-RMTS	3.0E-07	720	6	1.8E-02	1.4E-06
3	OEP-DGN-FR-6HDG3	5.6E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-6HDG1	3.6E-06	72	4	1.4E-02	1.1E-06
4	OEP-DGN-FS-DG01	4.9E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FS-DG02	3.6E-06	72	4	1.4E-02	9.9E-07
5	OEP-DGN-FS-DG01	4.9E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FS-DG03	3.6E-06	72	4	1.4E-02	9.9E-07
6	OEP-DGN-FS-DG01	4.0E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FS-6HDG2	3.6E-06	72	4	1.4E-02	8.1E-07
7	OEP-DGN-FS-DG01	4.0E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-6HDG3	3.6E-06	72	4	1.4E-02	8.1E-07
8	OEP-DGN-FS-DG02	4.0E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-6HDG1	3.6E-06	72	4	1.4E-02	8.1E-07
9	OEP-DGN-FR-6HDG1	4.0E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-6HDG2	3.6E-06	72	4	1.4E-02	8.1E-07
10	OEP-DGN-FS-DG03	3.9E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-6HDG1	3.6E-06	72	4	1.4E-02	7.8E-07
11	HPI-MOV-FT-1115B	1.9E-03	3.6E-06	60*	6*	1.9E-02	HPI-MOV-FT-1115D	3.6E-06	60*	6*	1.9E-02	6.8E-07
12	HPI-MOV-FT-1115C	1.9E-03	3.6E-06	60*	6*	1.9E-02	HPI-MOV-FT-1115E	3.6E-06	60*	6*	1.9E-02	6.8E-07
13	LPR-MOV-FT-1862A	1.5E-03	3.6E-06	60*	6*	1.9E-02	LPR-MOV-FT-1862B	3.6E-06	60*	6*	1.9E-02	5.4E-07
14	LPR-MOV-FT-1862A	1.5E-03	3.6E-06	60*	6*	1.9E-02	LPR-MOV-FT-1860B	3.6E-06	60*	6*	1.9E-02	
15	LPR-MOV-FT-1860A	1.5E-03	3.6E-06	60*	6*	1.9E-02	LPR-MOV-FT-1862B	3.6E-06	60*	6*	1.9E-02	
16	LPR-MOV-FT-1860A	1.5E-03	3.6E-06	60*	6*	1.9E-02	LPR-MOV-FT-1860B	3.6E-06	60*	6*	1.9E-02	
17	LPR-MOV-FT-1890A	1.5E-03	3.6E-06	60*	6*	1.9E-02	LPR-MOV-FT-1890B	3.6E-06	60*	6*	1.9E-02	
18	OEP-DGN-FS-DG01	4.6E-03	3.6E-06	72	4	1.4E-02	MSS-SRV-OO-SGSRV	7.0E-07	22	22	3.4E-03	2.4E-07
19	LPR-MOV-FT-1115C	9.1E-03	3.6E-06	72	4	1.4E-02	MSS-SRV-OO-SGSRV	7.0E-07	22	22	3.4E-03	1.3E-04
20	OEP-DGN-FR-6HDG1	1.5E-03	3.6E-06	72	4	1.4E-02	OEP-DGN-FR-DG01	3.6E-06	72	4	1.4E-02	
21	LPI-MDP-FS-SI1A	1.5E-03	2.0E-07	86	2	5.8E-04	LPR-MOV-FT-1862B	3.6E-06	60*	6*	1.9E-02	2.3E-07
22	LPI-MDP-FS-SI1B	1.5E-03	2.0E-07	86	2	5.8E-04	LPR-MOV-FT-1862A	3.6E-06	60*	6*	1.9E-02	2.3E-07
23	LPI-MDP-FS-SI1B	1.5E-03	2.0E-07	86	2	5.8E-04	LPR-MOV-FT-1860A	3.6E-06	60*	6*	1.9E-02	2.3E-07
24	LPI-MDP-FS-SI1A	1.5E-03	2.0E-07	86	2	5.8E-04	LPR-MOV-FT-1860B	3.6E-06	60*	6*	1.9E-02	2.3E-07
25	PPS-MOV-FC-1536	2.9E-06	3.6E-06	60*	6*	1.9E-02	PPS-MOV-FC-1535	3.6E-06	60*	6*	1.9E-02	1.8E-07

ACRONYMS

ATWS	Anticipated Transients Without Scram
AOO	Anticipated Operational Occurrences
AOT	Allowed Outage Time
APET	Accident Progression Event Tree
ASEP	Accident Sequence Evaluation Programme
BDBA	Beyond Design Basis Accidents
BE	Basic Event
CD	Core Damage
CCF	Common Cause Failure
CCDP	Complementary Cumulative Distribution Functions
CDF	Core Damage Frequency
CET	Containment Event Tree
DBA	Design Basis Accident
DCH	Direct Containment Heating
D/W	Dry Well
ET	Event Tree
FP	Fission Product
FT	Fault Tree
HCR	Human Cognitive Reliability
HEP	Human Error Probability
HRA	Human Reliability Analysis
HI	Human Interaction
IORV	Instrument Operated Relief Valve
LERF	Large Early Release Frequency
LOCA	Loss Of Coolant Accident
LPSA	Living PSA
LCO	Limiting Conditions for Operation
NPP	Nuclear Power Plant
O/S	Outside
PDS	Plant Damage State
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSC	Probabilistic Safety Criteria
PSG	Probabilistic Safety Goals

ACRONYMS (CONTD.)

PSF	Performance Shaping Factors
PSIV	Primary Steam Isolation Valve
RM	Risk Monitor
SER	Significant Event Report
SHARP	Systematic Human Action Reliability Procedure
SLB	Steam Line Break
SLIM	Success Likelihood Index Method.
SPSA	Shutdown PSA
STI	Surveillance Test Interval
Tech. Spec. (TS)	Technical Specifications
THERP	Technique for Human Error Rate Prediction
TLSOP	Total Loss of Power
TRC	Time Reliability Curve

REFERENCES

1. INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations, Codes and Safety Guides QI-Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna, 1996.
2. INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for a Quality Assurance Programme for PSA, TECDOC-1101, IAEA, Vienna, 1999.
3. Handbook of HRA with Emphasis on Nuclear Power Plant Application, Final Report: Swain A.D. and Guttmann H.E. , NUREG-CR/ 1278, Sandia National Laboratories, August, 1989.
4. U.S. NUCLEAR REGULATORY COMMISSION, PRA Procedures Guide, NUREG/CR-2300, 1981 draft.
5. INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety series No. 50-P-4, IAEA, Vienna, 1992.
6. Fullwood Ralph R. and Hall Robert E., Probabilistic Risk Asessment in Nuclear Power Industry - Fundamentals and Applications, Pergamon Press, New York, USA, August 1987.
7. INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-7, IAEA, Vienna, 1995.
8. INTERNATIONAL ATOMIC ENERGY AGENCY, Site Survey for Nuclear Power Plants, Safety Report Series No. 50-SG-S9, IAEA, Vienna, 1984.
9. INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Safety series No. 50-P-8, IAEA, Vienna, 1995.
10. U.S. NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plant, NUREG 1150 (Vols1-2), December 1990**.**
11. M. N. Ozisk and T.S. Kress, ‘Effects of Internal Circulation Velocity and Non-condensable Gas in Vapor Condensation from a Single Rising Hypothetical Core Disruptive Accident’, ANS Transactions, 27, 551, 1997.
12. M. F. Kennedy and R. B. Reynold, ‘Methods of Calculating Vapor and Fuel Transport to the Secondary Containment in an LMFBR Accident’, Nuclear Technology, 20, 149, 1973.
13. G. Berthoud et. al., ‘Experiments on LMFBR Aerosols Source Term After Severe Accident’, Nuclear Technology, 81, 257, 1988.
14. Beonio-Brocchieri et. al., ‘Nuclear aerosol codes’, Nuclear Technology, 81, 1988.
15. ANS, Report of the Special Committee on Source Terms, American Nuclear Society, 1984.
16. P.N. Clough, Source Term and the Chernobyl Accident, in Nuclear Safety after Three Mile Island and Chernobyl, Ed., G.M. Ballard, Elsvier Applied Science, 1990.
17. Croff, A.G., ORIGEN2: A Revised and Updated Version of the Oak Ridge Isotope Generation and Depletion Code, ORNL-5621, ORNL, Oak Ridge, Tenn., 1980.
18. B.R. Bowsher, Fission Product Chemistry and Aerosol Behaviour in the Primary Circuit of a Pressurised Water Reactor under Severe Accident Conditions.
19. F. Balard and B. Carluec, Evaluation of the LMFBR Cover Gas Source Terms and Synthesis of the associated R & D, Technical Committeee Meeting on Evaluation of Radioactive Materials and Sodium Fires, held in O-arai, Japan, IWGFR-92, 1996.
20. Williams, M.M.R. and Loyalka, S.K., Aerosol Science: Theory and Practice, Pergamon Press, 1991.
21. M. A. Morcuwitz, Leakage of Aerosols from Containment Building, Health Analysis, Vol. 42, 195, 1982.

22. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Series No. 50-P-12, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), IAEA, Vienna, 1996.

23. Organisation for Economic Co-operation and Development Report, Probabilistic Consequence Assessment Codes, Second International Comparision, Overview, Paris (1994).

24. INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessments of Nuclear Power Plants for Low Power and Shutdown Modes, TECDOC-1144, Vienna, March 2000.

25. INTERNATIONAL ATOMIC ENERGY AGENCY, PSA for Shutdown Mode for Nuclear Power Plants, TECDOC-751, IAEA, Vienna, 1994.

26. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Analysis of Nuclear Power Plants during Low Power and Shutdown Condition, TECDOC-1042, IAEA Vienna, 1998.

27. INTERNATIONAL ATOMIC ENERGY AGENCY, Living Probabilistic Safety Assessment (LPSA), TECDOC-1106, August 1999.

28. U S NUCLEAR REGULATORY COMMISSION, A Process for Risk-Focused Maintenance, NUREG/CR-5695, Washington, D C 20555, March 1991.

29. U. S. NUCLEAR REGULATORY COMMISSION, An Approach for Plant-specific, Risk-Informed Decision Making: Technical Specifications, RG-1.177, August 1998.

30. Optimisation of Technical Specifications Applications in USA, Lecture 54.4.4, Pranab K. Samanta, IAEA Course: Use of PSA in the Operation of NPPs, 1992.

31. INTERNATIONAL ATOMIC ENERGY AGENCY Doc., Protection Against Internal Hazards Other than Fire and Explosion Draft DS 299, Vienne, Nov, 2001.

32. DPR Package, KK/S-10 on System of Steam and Energy Conversion of PSAR of Kudankulam Project.

33. U. S. NUCLEAR REGULATORY COMMISSION, Safety Evaluation Report Related to the Operation of Hope Creek Generating Rtation, Supplement No. 6, NUREG-1048, July, 1986.

34. Sajjad Ali Khan, PSA for Waste Repositories: An Overview of Reliability Data, Nuclear Plant Journal, 1994.

35. INTERNATIONAL ATOMIC ENERGY AGENCY, Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, TECDOC-1200, Vienna, February 2001.

36. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Aspects of NPP Ageing, TECDOC-540, Vienna, 1990.

37. U. S. NUCLEAR REGULATORY COMMISSION, Risk Evalutions of Aging Phenomena: The Linear Aging Reliability Model and Its Extentions, NUREG-CR-4769, 1987.

38. U. S. NUCLEAR REGULATORY COMMISSION, Data Summaries of Licensee Events Report of Diesel Generators at U S Commercial NPPs, NUREG-1362, 1982.

39. U. S. NUCLEAR REGULATORY COMMISSION, Evaluation of Core Melt Frequency Effects due to Component Ageing and Maintenance, NUREG-CR-5510, 1990.

40. O. Jorge and B. Chaumont, ‘French Regulatory Decision Process for Severe Accident Management and Orientations for Future European Research’, FISA-2001, Symposium on Energy Research in Reactor Safety and Post-Symposium Workshop, Luxembourg 12-15, Nov. 2001.

41. Syed Ali, Bagchi, ‘Risk Informed In-Service Inspection’, Nuclear Engineering Design 181, pp221-224 (1998).

42. Balkey, et.al., ‘ASME Risk-Based In-Service Inspection and Testing: An outlook for the future’, Risk Analysis, Vol.18, (1998), pp. 407-421.

43. Balkey, et.al., 'Developments on US NRC Approved WOG/ASME Research Risk Informed In-Service Inspection Methodology', A Report

44. U. S. NUCLEAR REGULATORY COMMISSION, 'Risk Informed In-Service Inspection Evaluation Procedure', Electric Power Research Institute, TR-112657, July 1999.

45. National Standard of Canada, Canadian Standards Association, Periodic Inspection of CANDU Nuclear Power Plant Components, CAN/CSA-N-285.4, Ontario, 1983.

46. Gosselin, Fleming, 'Evaluation of pipe failure potential via degradation mechanism assessment', ICONE 5, pap 2641, May 26-30, Nice, France (1997).

47. U. S. NUCLEAR REGULATORY COMMISSION, 'An Approach for using Probabilistic Risk Assessment in Risk Informed Decisions on Plant Changes to the Licensing Basis', Regulatory Guide 1.174, July 1998.

48. U. S. Nuclear Regulatory Commission, 'An Approach for Plant Specific Risk Informed Decision-making: In-Service Inspection', Regulatory Guide 1.178, August 1998.

49. Mayfield et.al., 'Risk Informed In-Service Inspection Program', Nuclear Engineering Design 195, pp211-215 (2000).

50. American Society of Mechanical Engineering Code CASE N-560, Alternative Examination Requirements for Class1, Category B-J Piping Welds

51. American Society of Mechanical Engineering Code CASE N-578, Risk Informed Methods for In-Service Inspection of pipe welds

52. T.V.Vo, et.al, 'Probabilistic Risk Assessment based guidance for piping In-service Inspection', Nuclear Technology, Vol.88, pp13-20 (1989).

53. RIBA PROJECT, 'Risk Informed Approach for In-service Inspection of Nuclear Power Plant components', EUR 20164 EN, Project Summary, December 2001.

54. Gopika Vinod, H. S. Kushwaha, A.K. Verma and A. Srividya, 'Importance Measures In Ranking Piping Components For Risk Informed In-Service Inspection', Reliability Engineering and System Safety Vol. 80 (3), May 2003.

55. K.N. Fleming, S. Gosselin, and J. Mitman, 'Application of Markov Models and Service Data to Evaluate the Influence of Inspection on Pipe Rupture Frequencies,' Proceedings of the ASME Pressure Vessels and Piping Conference, Boston August 1-5, 1999

56. James W. Purvis, Sabotage at NPPs, Sandia National Laboratories.

57. INTERNATIONAL ATOMIC ENERGY AGENCY, Risk Management: A Tool for Improving NPP Performance, IAEA, TECDOC-1209, Vienna, April 2001.

58. ELECTRICAL POWER RESEARCH INSTITUTE report, An Approach to Risk-Informed Changes to Physical Security, TR-123787, California, (1999).

59. INTERNATIONAL ATOMIC ENERGY AGENCY, External Man-Induced Events in Relation to Nuclear Power Plant Siting, Safety Series-50-SG-S5, Vienna, 1981.

60. Viktorov A. N., Baranaev Yu. D., Dogov V. V., Probability of External Events with the Aircraft Impact on Nuclear Power Plant, International Meeting, PSA/PRA Severe Accidents' 94, Ljubljana, SLOVENIA, 17-20 April 1994.

61. R5: 'An Assessment Procedure for the High Temperature Response of Structures', Issue 2, Barnwood, Gloucester, Nuclear Electric Ltd. (Now British Energy).

62. R6: 'Assessment of the integrity of Structures Containing Defects', British Energy, R/H/R6-Revision 3, 1998.

63. Rastogi Rohit, Bashin Vivek, Vaze K. K., Kushwaha H. S., 'Assessment of Integrity of Components in Piping of 500 MWe PHWR using R-6 method.', Nuclear Engineering and Design, Vol. 212, pp-99-108, 2002.

64. Rastogi Rohit, Bashin Vivek, Vaze K. K., Kushwaha H. S, and Joshi G.A., 'Estimation of probability of failure of Primary Heat Transport Piping of Indian Presurised Heavy Water Reactors using Advance Monte-Carlo Techniques', International Conference on Modeling, Simulation, Optimisation for Design of Multi disciplinary Engineering systems (MSO-DMES), Paper no. 56, sept., 24-26, 2003, Goa, India.

65. Madsen H. O., Krenk S. and Lind N. C., Methods of structural safety, Englewood Cliffs, NJ, Prentice Hall, Inc., 1986.

66. Ang, A.H-S and Tang, W. H., Probability Concepts in Engineering Planning and Design, Vol. I & II, Wiley, New York.

67. Rangnathan R., 'Structural Reliability: Analysis and Design', Jaico Publication House, Mumbai, 1999.

68. INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Review of Probabilistic Safety Assessment (PSA) Level 1, TECDOC 1135, Vienna, Feb. 2000.

69. INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Review of Probabilistic Safety Assessment (PSA) Level 2, IAEA-J4-CS-25/99, Draft 1, Vienna, 1999.

70. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Codes for Level 1 Probabilistic Safety Assessment, TECDOC-553, Vienna, 1990.

71. A. Gieseke et al., The Source Term Code Package, IAEA-SM-281/49, in Source Term Evaluation for Accident conditions, IAEA Symposium at Columbus, Ohio, 1985.

72. Bunz, H. et. al, NAUA-MOD5 and NAUA-MOD5M- Two Computer Programs for Calculating the Behaviour of Aerosols in a LWR Containment Following a Core-Melt Accident', KfK-4278.

73. Owczarski P.C., Schreck, R. I., Postma, A. K., Techanical Bases and Users Manual for the Prototype of a Suppression Pool Aerosol Removal Code (SPARC): NUREG/CR-3317.

74. U.S. NUCLEAR REGULATORY COMMISSION, MELCOR Home Page, Executive Summary from melcor.sandia.gov/execsum 185.htm, NUREG/CR-6119, NOV. 2001.

75. Haware, S. K., Markandeya, S. G., Ghosh, A. K., Venkat Raj, V.. Assessment of a Multi Compartment Containment Analysis Computer Code CONTRAN with the Experiments on Containment Response during LOCA Conditions, Paper No. HMT-94-118, First ISHMT-ASME Heat and Mass Transfer Conference and 12th National Heat and Mass Transfer Conferene, BARC, Jan. 5-7, 1994.

76. Haware, S. K., Bhartiya, S., Ghosh, A. K., Venkat Raj, V., Analylitical Studies on the Catalytic Oxidation of Hydrogen using the Code HYRECAT, CHEMCON-95, Kalpakkam, India.

77. Nuclear Energy Agency/Organisation for Economic Co-operation and Development, International comparison study on reactor accident consequence modelling, Summary Report to CSNI by an NEA Group of Experts, , Paris 1984.

78. Nuclear Energy Agency/Organisation for Economic Co-operation and Development, International Comparison Exercise on Probabilistic Accident Consequence Assessment Codes, Technical report, Report eur 15109, 1994.

79. U.S. NUCLEAR REGULATORY COMMISSION, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, NUREG/CR-5801, 1993.

80. R. A. Humphreys, Checklist Method for Evaluating the b-Factor, Paper 2c/5, National Reliability Conference, (1987).

81. ELECTRICAL POWER RESEARCH INSTITUTE, Classification and analysis of reactor operating experience involving dependent events, EPRI-NP-3967, California, 1985.

82. MIL-HDBK-217F, Military Handbook: Reliability Prediction of Electronic Equipment, DOD, Washington D.C. (1992).

83. Raghavan Manian., Joanne Betchta Dugan, David Coppit and Kevin J. Sullivan, Combining Various Solution Techniques for Dynamic Fault Tree Analysis of Computer Systems, Proceedings of Third IEEE International High-Assurance Systems Engineering Symposium, 1998.

84. S. K. Khobare, Report on Reliability Analysis of DPHS-PCS', RCnD/3572/BARC/(July 29, 1999).

85. Safety and Reliability Assessment Methods, Digital Instrumentation and Control Systems in NPPs: Safety and Reliability Issues, 1997.

86. Hannaman, G. W., A. J. Spurgin, Systematic Human Action Reliability Procedure (SHARP), EPRI NP-3583, 1984.

87. U.S. NUCLEAR REGULATORY COMMISSION, Swain A.D. Accident Sequence Evaluation Programme HRA Procedure Rep.NUREG/CR-4772, USNRC, Washington, DC, 1987.

88. INTERNATIONAL ATOMIC ENERGY AGENCY, Case Study on the use of PSA Methods Human Reliability Analysis, TECDOC-592 IAEA, Vienna, 1991.

89. INTERNATIONAL ATOMIC ENERGY AGENCY, Collection and classification of human reliability data for use in PSA, TEC DOC-1048, IAEA Vienna, 1998.

90. K. Subramaniam, R.K. Saraf, V.V.S. Sanyasi Rao and V. Venkat Raj, Collection and Classification of Human Error and Human Reliability Data from Indian Nuclear Power Plants for use in PSA. Rep. BARC/1999/E-041, India, 1999.

91. INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in PSA for Nuclear Power Plants, Safety Series No: 50 P-10, IAEA, Vienna, 1995.

92. K. Subramaniam, R.K. Saraf, V.V.S. Sanyasi Rao and V. Venkat Raj, A Perspective on Human Reliability Analysis and Studies on the Application of HRA to Indian Pressurised Heavy Water Reactors. Rep. BARC/2000/E-013.

93. C. W. Gordon, A course in System Reliability using the Fault Tree Method, Bruce A Risk Analysis Fault Tree Guide, December, 1989

94. National Fire Protection Association Fire protection Handbook, 18th ed., Quincy, Massachusetts, 1997

95. INTERNATIONAL ATOMIC ENERY AGENCY, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants SRS 10 IAEA Safety Report Series No. 10, Vienna, 1998.

96. INTERNATIONAL ATOMIC ENERY AGENCY, Preparation of Fire Hazard Analyses for Nuclear Power Plants, Safety Refund Series No. 8, 1998.

97. A User's Guide for FAST: Engineering Tools for Estimating Fire Growth and Smoke Transport, Special Publication 921, 2000 Edition, National Institute of Standards and Technology, USA.

98. Steven L. Kramer, Geo-technical Earthquake Engineering, Prentice-Hall International

99. INTERNATIONAL ATOMIC ENERGY AGENCY, PSA for Seismic event, TECDOC-724, Vienna, 1993.

100. U.S. NUCLEAR REGULATORY COMMISSION, Recommendation to the NRC on Trial Guidelines for Seismic Margin Reviews of Nuclear Power Plants, NUREG/CR-4482.

101. Kennedy, R.P., Cornell, C.A., Campbell, R.D., Kaplan, S., and Perla, H.F., Probabilistic seismic study of an existing nuclear power plant, Nuclear Engineering and Design, 59, 315-338, 1980.

102. Kennedy, R.P. and Ravindra, M.K., Seismic Fragilities for Nuclear Power Plant Risk Studies, Nuclear Engineering and Design, 79, 47-68, 1984.

103. Campbell R. D, Ravindra M. K, Murray R. L., Compilation of Fragility Information from Available PSAs, Lawrence Liremore National Lab. Report, VCID-20571, Rev-1., 1998.

104. A. Yamaguchi, M. K. Ravindra, R. D. Campbell, Bayesian Methodology to Generic Seismic Fragility Evaluation of Component in Nuclear Plants, Paper MO4/3, Structural Mechanics in Reactor Technology, Tokyo, 1991.

105. R. H. Sues, P. J. Amiro, R. D. Campbell, Significance of Earthquake Risk in NPP PSA, Nuclear Engineering Design, p. 27-44, V-123, 1990.

106. Safety Analysis Report, DRUVA, 1994.

107. 'Source Term', V.K.Sharma, Kapil Deo S.Singh and Pradeep Bhargava, Health Physics Division, BARC, Mumbai, India, 2001.

108. 'Level 3 PSA' , V.K.Sharma, Kapil Deo S.Singh and Pradeep Bhargava, Health Physics Division, BARC, 2001.

109. Bayer, A. and Hauser, F.W., Basic Aspects and Results of the German Risk Study, Nuclear Safety 22, pp 605-709, 1981.

110. J.H. Gittus, PWR Degraded Core Analysis, UKAEA, 1982.

111. ATOMIC ENERTY REGULATORY BOARD, Radiation Protection Aspects in Design for Pressurised Heavy Water Reactor Based Nuclear Power Plants, D-12, AERB, Mumbai, India, 2005.

112. HMSO, Accident at Windscale No. 1 Pile on 10th October, 1957, British Report Cmnd 232, London, 1957.

113. Wilson, R., Report to the American Physical Society of the Study Group on Radio-nuclide Release from Severe Accidents at Nuclear Plants, Reviews of Modern Physics, 57 (3), Part II, 1985.

114. USAEC, IDO Report on the Nuclear Incident at the SL-1 Reactor, January3, 1961, at Nuclear Reactor Testing Station, IDO-19302, Idaho, 1962.

115. Kemeny, J. G. et al., Report of the President's Commission on the Accident at Three Mile Island, US Government Printing Office, Washington, 1979.

116. Miller, A., Radioactive Source Terms and Shielding at TMI-2, Trans. ANS, 34,pp683, 1980.

117. Pigford, T.H., The Management of Nuclear Safety: A Review of TMI after two years Nuclear News, March, 1981.

118. INTERNATIONAL ATOMIC ENERGY AGENCY, Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident, Safety Report No 75-INSAG-1, Vienna, 1986.

119. Mourad, R., Source Term of the Chernobyl Accident, OECD (NEA)/CEC Workshop on Recent Advances in Reactor Accident Consequence Assessment, Rome, Italy, January, 1988.

120. Lewis, W.B., The Accident to the NRX Reactor on December 12, 1952, AECL-232, Atomic Energy of Canada Ltd., 1953.

121. W. E. Veroly, M. H. Hassan, Calculations of CDF Increase due to Ageing under a Given Maintenance Programme, IAEA-SM-321/28.

BIBLIOGRAPHY

1. INTERNATIONAL ATOMIC ENERGY AGENCY, Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plant, Technical Report Series No.282, IAEA Vienna, 1998.

2. INTERNATIONAL ATOMIC ENERGY AGENCY, IPERS Guidelines for the International Peer Review Service, Second Addition, Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessments, IAEA-TECDOC-832 Vienna, 1995.

3. PSA for Industrial and Environmental Applications, Volume I, IAEA Regional Training Course, NTC, KAERI, 1995.

4. U S NUCLEAR REGULATORY COMMISSION, PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, Vol. 1, NUREG/CR-2300-V1, USNRC, January, 1983.

5. INTERNATIONAL ATOMIC ENERGY AGENCY, Use of PSA Level 2 Analysis for Improving Containment Performance, IAEA-TECDOC-1002, March, 1998

6. U S NUCLEAR REGULATORY COMMISSION, Gieseke, J. A., et al., Source Term Code Package: A User's Guide, Rep. NUREG/CR-4587, BMI-2138, Battle Columbus Laboratories, Columbus, OH, 1986.

7. Bunz, H. et. al, 'NAUA-MOD5 and NAUA-MOD5M- Two Computer Programs for Calculating the Behaviour of Aerosols in a LWR Containment Following a Core-Melt Accident', KfK-4278.

8. Williams, D. A., OECD International Standard Problem Number 34, FALCON Code Comparison Report, AEA RS 3394, December, 1994.

9. GESELLSCHAFT FUR REAKTORSICHERHEIT, ATHLET Mod 1.0 – Cycle E, Users Manual, Garching, 1990.

10. GRIFFITH, R.O., et al., CONTAIN 1.2 Users Manual, Rep. SAND94-2358, Sandia Natioal Laboratories, NM, 1994.

11. GAUVAIN, J., et al., 'ESCADRE Mod 1.0 – JERICHO: Reactor Containment Thermal Hydraulics During a Severe Accident - Reference Document', Rep. IPSN/DRS/SEMAR/96-06, Fontency-rux-Roses, 1996.

12. DELAVAL, M., et al., 'ESTER 1.0 Manual Vols. 1-4,' Report EUR 16307/(1-4) EN, 1996.

13. GONZALES, R., et al. 'ICARE2 - A Computer Programme for Severe Core Damage Analysis in LWRs,' Rep. IPSN/DRS/SEMAR/93-33, Fontency-rux-Roses, 1993.

14. ELECTRIC POWER RESEARCH INSTITUTE, 'MAAP 3.0B Computer Code Manual,' Vol.1 and 2, EPRI-NP-7071-CCML Palo Alto, CA, November, 1990.

15. U S NUCLEAR REGULATORY COMMISSION, GAUNTT, R.O., et al., 'MELCOR Computer Code Manuals: Version 1.8.4,' NUREG/CR-6119, Vol. 1-2, Rev. 1, SAND97-2398, Sandia National Laboratories, NM, July, 1997.

16. U S NUCLEAR REGULATORY COMMISSION, ALLISON, C.M., et al., 'SCDAP/RELAP5/MOD3.1 Code Manual (Vols 1-5),' NUREG/CR-6150, EGG-2720, Idaho National Engineering Laboratory, IA, October, 1993.

17. KAJIMOTO, M., et al., 'Development of THALES-2, A Computer Code for Coupled Thermal Hydraulics and Fission Product Transport Analysis for Severe Accident at LWRs and its Application to Analysis of Fission Product Revaporisation Phenomena,' paper presented at Internation Topical Meeting on Safety of Thermal Reactors, Portland, OR, 1991.

18. U S NUCLEAR REGULATORY COMMISSION, HEAMES, T.J., et al., VICTORIA: A Mechanistic Model of Radionuclide Behaviour in the Reactor Coolant System Under Severe Accident Conditions, Rep. NUREG/CR-5545, Rev.1, Washington, D. C., December, 1992.

19. BESTION, D., 'CATHARE - General Description of CATHARE2 V1.3,' Rep. CEA/STR/LML/94-265 Paris, 1994.

20. M.W. Jankowski, Introduction to the Source Term, International Training Course on Radiological Accident Consequence Assessment, Dublin, Ireland, July, 1988.

21. INTERNATIONAL ATOMIC ENERGY AGENCY, Techniques and Decision-making in the Assessment of Off-site Consequences of an Accident in a Nuclear Facility, IAEA Safety Series # 86, Vienna, 1987.

22. USAEC, Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants, USAEC, 1957.

23. J.J. Dinnuno, Calculation of Distance Factors for PWR and Test Reactor Sites, TID-14844, USAEC, 1962.

24. INTERNATIONAL ATOMIC ENERGY AGENCY, The International Nuclear Event Scale, Vienna, 1990.

25. Mosey D., Reactor Accidents, Nuclear Engineering International Special Publications, 1990.

26. Atomic Energy of Canada Limited, The Safety of Ontario's Nuclear Power Reactors, a Scientific and Technical Review, A Submission to the Ontario Nuclear Safety Review, Chairman K. Hare, 1987.

27. U S NUCLEAR REGULATORY COMMISSION, M.R. Kuhlman et al., CORSOR User's Manual, NUREG/CR-4173, BMI-2122, Battelle Columbs Laboratories, 1985.

28. U S NUCLEAR REGULATORY COMMISSION, Jordan, H., and Khulman, M.R., TRAP-MELT2 User's Manual, Battelle Columbus Laboratories, NUREG/CR-4205, BMI-2124, 1985.

29. H. Bunz et al., NAUA-MOD 4: A Code for Calculating Aerosol Behaviour in LWR Core-melt Accidents, KfK-3554, 1983.

30. U S NUCLEAR REGULATORY COMMISSION, Powers, D.A. et al., VANESA, A Mechanistic Model of Radionuclide Release and Aerosol Generation During Core Debris Interactions with Concrete, Sandia National Labs., NUREG/CR-4308, June, 1985.

31. M.Khatib-Rahbar et al., QUASAR : A Methodology for Quantification of Uncertainties in Severe Accident Source Terms, Trans. ANS, Vol. 53, 1986.

32. Nuclear Energy Agency, Severe Accident Management, NEA/OECD, 1992.

33. INTERNATIONAL ATOMIC ENERGY AGENCY, Implementation of Defence-in-depth for Current and Future Nuclear Power Plants, Draft Report, Vienna, 1995.

34. NATIONAL RADIOLOGICAL PROTECTION BOARD, COMMISSARIAT A L'ENERGIE ATOMIQUE, A Methodology for Evaluating the Radiological Consequences of Radioactive Effluents Released in Normal Operations, Rep. V/3011/75-EN, Commission of the European Communities, Luxembourg, 1979.

35. KfK and NRPB, 'COSYMA: A New Program Package for Accident Consequence Assessment', A Joint Report by KfK and NRPB, EUR - Report 13028, 1991.

36. COMMISSION OF THE EUROPEAN COMMUNITIES, Methods for Assessing the Off-site Radiological Consequences of Nuclear Accidents, Rep. EUR-10243-EN, CEC, Luxembourg, 1986.

37. Nixon, W., Cooper, P.J., Underwood, B. Y., Peckover, R.S., Accident Consequence Analysis, Nuclear Energy 24, 229-239, 1985.

38. Kelly, G.N., Clarke, R.H., An Assessment of the Radiological Consequences of Releases from Degraded Core Accidents for the Sizewell PWR, Rep. NRPB-R-137, National Radiological Protection Board, Chilton, 1982.

39. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Probabilistic Accident Consequence Assessment Codes -Second International Comparison, Overview Report, OECD, Paris, 1994.

40. Probabilistic Fracture Mechanics by Galerkin Meshless Methods, Part I and II, Reliability Analysis of S. Rahaman and B. N. Rao, College of Engg. The University of Iowa, accepted for publication in 'Compuational Mechanics', December, 2001.

LIST OF PARTICIPANTS

WORKING GROUP FOR PSA GUIDELINES

Dates of meeting	:	July 18 & 19, 2001 August 17, 2001 September 11, 2001 October 23, 2001 December 04, 2001 January 2 & 3, 2002 January 22 & 23, 2002 January 30 & 31, 2002 February 7 & 8, 2002 February 15, 2002 February 20 & 21, 2002 February 28, 2002 March 5, 2002 May 9 & 10, 2002 May 21 & 22, 2002

Members and Invitees of Working Group:

Shri P. Hajra	:	AERB (Former)
Dr. Om Pal Singh	:	AERB
Shri S.K. Khobare	:	BARC
Dr. V.V.S. Sanyasi Rao	:	BARC
Smt. Rajee Guptan	:	NPCIL
Shri U.K. Paul (Member-Secretary)	:	AERB
Shri R.K. Saraf (Co-opted)	:	BARC (Former)
Late Shri P.G. Zende (Co-opted)	:	NPCIL
Shri V.K. Sharma (Co-opted)	:	BARC
K. Subramaniam (Co-opted)	:	BARC
Dr. P.V. Varde (Co-opted)	:	BARC
Shri V.V. Pande (Co-opted)	:	AERB
Shri Vishnu Verma (Co-opted)	:	BARC
Shri Roshan A. D. (Co-opted)	:	AERB
Shri Laxman. V (Co-opted)	:	AERB
Shri Kapil Dev Singh (Co-opted)	:	BARC
Shri Pradeep Bhargava (Co-opted)	:	BARC
Shri R.B. Solanki (Permanent Invitee)	:	AERB
Shri R.S. Rao (Permanent Invitee)	:	AERB

ADVISORY COMMITTEE ON CODES, GUIDES AND ASSOCIATED MANULAS FOR SAFETY IN OPERATION OF NUCLEAR POWER PLANTS (ACCGASO)

Dates of meeting	:	December 5 & 6, 2002 January 2 & 3, 2003 December 5 & 6, 2003 April 3, 2003 February 4 & 5, 2004 October 28, 2004 February 14, 2006

Members and Invitees of ACCGASO:

Shri N. Rajasabai	:	Kaiga NPP, NPCIL (Former)
Shri Subhash Mittal	:	NPCIL (Former)
Shri B. Rajendran	:	IGCAR
Shri S.K. Agarwal	:	BARC (Former)
Shri R. Venkatraman	:	AERB
Shri M.L. Joshi	:	BARC
Shri H.C. Mehta	:	NPCIL
Shri P.R. Krishnamurthy	:	AERB
Shri Y.K. Shah (Member-Secretary)	:	AERB

ADVISORY COMMITTEE ON NUCLEAR SAFETY (ACNS)

Dates of the meeting	:	November 11, 2006 June 15, 2007

Members and Invitees of ACNS:

Shri G.R. Srinivasan	:	AERB (Former)
Shri S.C. Hiremath	:	HWB (Former)
Shri D.S.C. Purushottam	:	BARC (Former)
Shri A.K. Anand	:	BARC (Former)
Shri R.K. Sinha	:	BARC
Shri H.S. Kushwaha	:	BARC
Shri S.S. Bajaj	:	NPCIL (Former)
Prof J.B. Doshi	:	IIT, Bombay
Shri S. Krishnamony	:	BARC (Former)
Dr S.K. Gupta	:	AERB
Shri K. Srivasista (Member-Secretary)	:	AERB
Shri N. Rajasabai (Chairman, ACCGASO), Invitee)	:	NPCIL (Former)
Shri Y.K. Shah (Member-Secretary, ACCGASO), Invitee	:	AERB
Shri P. Hajra (Chairman, WG), Invitee	:	AERB (Former)
Shri U.K. Paul (Member-Secretary, WG), Invitee	:	AERB

PROVISIONAL LIST OF AERB SAFETY CODES, GUIDES, MANUALS AND TECHNICAL DOCUMENTS ON OPERATION OF NUCLEAR POWER PLANTS

Safety Series No.	Title
AERB/SC/O	Code of Practice on Safety In Nuclear Power Plant Operation.
AERB/SG/O-1	Staffing, Recruitment, Training, Qualification and Certification of Operating Personnel of Nuclear Power Plants.
AERB/SG/O-2	In-service Inspection of Nuclear Power Plants
AERB/SG/O-3	Operational Limits and Conditions for Nuclear Power Plants
AERB/SG/O-4	Commissioning Procedures for Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/SG/O-5	Radiation Protection During Operation of Nuclear Power Plants
AERB/SG/O-6	Preparedness of Operating Organisation for Handling Emergencies at Nuclear Power Plants
AERB/SG/O-7	Maintenance of Nuclear Power Plants
AERB/SG/O-8	Surveillance of Items Important to Safety in Nuclear Power Plants
AERB/SG/O-9	Management of Nuclear Power Plants for Safe Operation
AERB/SG/O-10A	Core Management and Fuel Handling of Pressurised Heavy Water Reactors
AERB/SG/O-10B	Core Mangement and Fuel Handling of Boiling Water Reactors
AERB/SG/O-11	Management of Radioactive Waste Arising from Operation of Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/SG/O-12	Renewal of Authorisation for Operation of Nuclear Power Plants
AERB/SG/O-13	Operational Safety Experience Feedback for Nuclear Power Plants
AERB/NPP/SG/O-14	Life Management of Nuclear Power Plants
AERB/NPP/SG/O-15	Proof and Leakage Rate Testing of Reactor Containments
AERB/NPP-PWR/O-16	Commissioning of Pressurised Water Reactors
AERB/NPP&RR/ SM/O-1	Probabilistic Safety Assessment for Nuclear Power Plants and Research Reactors
AERB/NPP/SM/O-2	Radiation Protection for Nuclear facilities
AERB/NPP/TD/O-1	Compendium of Standard Generic Reliability Database for Probablistic Safety Assessment of Nuclear Power Plants
AERB/NPP/TD/O-2	Human Reliability Analysis: A Compendium of Methods, Data and Event Studies for Nuclear Power Plants

AERB SAFETY MANUAL NO. AERB/NPP & RR/SM/O-1

Published by : Atomic Energy Regulatory Board
Niyamak Bhavan, Anushaktinagar
Mumbai - 400 094
INDIA.

BCS