CLASSICAL AND DYNAMIC APPROACHES TO PROBABILISTIC SAFETY ANALYSIS OF FAST REACTORS

By

M. RAMAKRISHNAN

Enrolment Number: PHYS02 2010 04020

Indira Gandhi Centre for Atomic Research, Kalpakkam, India

A thesis submitted to the

Board of Studies in Physical Sciences

In partial fulfillment of requirements

for the degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

(October, 2015)

Homi Bhabha National Institute

Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by **Mr. M. Ramakrishnan** entitled **"Classical and Dynamic Approaches to Probabilistic Safety Analysis of Fast Reactors"** and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

_____ **Date:**

Chairman – Dr. B. Venkatraman

_____ **Date:** 26/10/16

Convener/Guide – Dr. S.Sivakumar

_____ **Date:** 26/10/16

External Examiner - Dr.N.K.Goyal

_____ **Date:** 26/10/16

Member – Dr. K. Velusamy

_____ **Date:** 26/10/2016

Member – Dr. K. Devan 26/10/16

_____ **Date:** 26/10/16

Technology Adviser - Dr. A. John Arul

Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to HBNI.

I hereby certify that I have read this thesis prepared under my direction and recommend that it may be accepted as fulfilling the thesis requirement.

Date: 26/10/16

Place: Kalpakkam

(S.Sivakumar)

Guide

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

M. Ramakrishnan

(M. Ramakrishnan)

DECLARATION

I, hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

M. Ramakrishnan

(M. Ramakrishnan)

List of Publications Arising from the Thesis

Journal Papers

1. M. Ramakrishnan, Pramod Kumar Sharma, V.Bhuvana, A.John Arul, P. Mohanakrishnan and S.C.Chetal, "Insights from Level-1 Probabilistic Safety Analysis of Prototype Fast Breeder Reactor", Nuclear Engineering and Design 250, 2012, pp 664-670.

2. M.Ramakrishnan, A. John Arul, V.Bhuvana, P.PuthiyaVinayagam and P. Chellapandi, "Accident Sequence Modeling Methodology for External Flood Probabilistic Safety Analysis of Prototype Fast Breeder Reactor", Applied Mechanics and Materials, Vols. 592-594 (2014), pp 2460-2464.

3. M. Ramakrishnan, "Unavailability Estimation of Shutdown System of a fast reactor by Monte Carlo Simulation", Annals of Nuclear Energy 90, 2016, pp 264-274.

4. M. Ramakrishnan, "Integration of Functional Reliability Analysis and System Hardware Reliability through Monte Carlo Simulation", Annals of Nuclear Energy 95, 2016, pp 54-63.

Conference Papers

1. M. Ramakrishnan, Pramod Kumar Sharma, A. John Arul, V. Bhuvana, P. Mohanakrishnan and S.C.Chetal, "Level-1 Probabilistic Safety Analysis of Prototype Fast Breeder Reactor", 2nd International conference on Reliability, Safety & Hazard, ICRESH- 2010, Dec 14-16, 2010, Conference Proceedings pp 239-241.

2. M.Ramakrishnan, A. John Arul, V.Bhuvana, P.PuthiyaVinayagam and P. Chellapandi, "Accident Sequence Modeling Methodology for External Flood Probabilistic Safety Analysis of Prototype Fast Breeder Reactor"- Presented in International Mechanical Engineering Congress (IMEC-2014) held at NIT, Trichy, June 13-15, 2014.

3. M.Ramakrishnan and A. John Arul, "Preliminary Tsunami Hazard Analysis for a Power Plant Site on East Coast of India", Presented at 2nd SRESA National Conference on Reliability and Safety Engineering (NCRS-15) held at Anna University, October 8-10, 2015.

M. Ramakrishnan

(M. Ramakrishnan)

DEDICATED TO MY PARENTS

ACKNOWLEDGEMENTS

I thank the almighty for his continued blessings throughout my life. I would like to thank my mother, wife, son and daughter for their support and encouragement during the course of my PhD work.

I express my sincere gratitude to my guide Dr.S.Sivakumar and Dr.A. John Arul for their guidance and encouragement. My sincere thanks to my doctoral committee members, Dr. B. Venkatraman, Dr. K. Velusamy, Dr. K. Devan for their encouragement and interest throughout my PhD. I convey my gratitude to my earlier doctoral committee members Dr.P. Mohanakrishnan, Dr.R.S.Keshavamurthy, Dr.C.P.Reddy and Dr. Mohankumar. I am thankful to Director-IGCAR, Director-RDG and Associate Director-CDG for allowing me to pursue my PhD. I am thankful to Dr. B.V.R. Tata, Ex-Dean Academic-Physics and Dr.Chandrasekar, Dean Academic-Physics for their valuable suggestions in this endeavour.

I acknowledge the help and support received from my friends Dr. Sunil Kumar, Dr. Pandi Kumar, Shri. D.V Subramanian, Shri. Alagan, Shri. Pramod Kumar Sharma, Smt.V. Bhuvana, Shri.Sujoy Sen, Dr. Riyas, Shri. Ashok Kumar and my other friends and well wishers in RND and RSDD. PSA requires input from many disciplines and I am thankful to all those with whom I interacted with, either directly or indirectly for the completion of my PhD. I am thankful to all faculty members, staff and my fellow students at IGCAR training school for helping me in successfully completing my course work.

This acknowledgement is incomplete without mentioning the role played by Smt. Janaki and Shri.Ravi. I am thankful to them for their help and support. I am thankful to IGCAR library for getting me the required papers from other libraries. I am also thankful to the Dean academic-Physics office for their help in submitting my thesis.

CONTENTS

SYNOPSIS

The Fukushima accident in Japan changed to a great extent the public perception about nuclear power. This accident has increased the fear in the minds of people about nuclear power. The future of nuclear power depends on the safe operation of nuclear power plants. This can be achieved by reducing the risk to the public from a nuclear power plant from the present levels. This leads to the innovative reactor design concepts which employ advanced safety features. These new reactor design concepts work on the principle of inherent safety features and passive safety features. These safety features challenge the traditional safety analysis approaches. Improved methods for safety analysis of reactors and the proper utilization of outcome from safety analysis in design and operation of nuclear power plant will reduce the occurrence of such events.

Traditionally safety analysis of reactors was divided into two categories namely deterministic and probabilistic safety analysis. Deterministic safety analysis deals with process dynamics for a specific initiating event which is usually associated with a hardware failure (example: pump trip etc.). Probabilistic safety analysis focuses on hardware components of a safety system with success / failure criteria derived from process analysis. The process and system hardware are decoupled with respect to time evolution. This decoupling between process and hardware components is acceptable under two conditions. The first condition is that the changes in system hardware do not affect the process evolution. The second condition is the changes in process conditions do not affect the system hardware. These two conditions are generally not satisfied in the case of reactor safety systems. A change in system hardware is going to affect the process evolution. Similarly a hardware component may have to change its state either manually or automatically when the process parameters cross some threshold values. Also the process parameters evolution can alter the failure rates of components. A reactor safety system may satisfy either of the two conditions

or both the conditions. Probabilistic Safety Analysis of critical reactor safety systems should consider the time dependent interaction between process and system hardware states. Under such circumstances an integrated model is required which can model the uncertainties in process and stochastic changes in system hardware.

Dynamic reliability models are developed to model process and system hardware interactions for scenarios in which timing of sequences are important [1]. These models can be applied to reliability analysis of critical reactor safety systems like shutdown system and decay heat removal systems. However it is to be mentioned that dynamic reliability models give additional information such as timing of sequences as compared to classical reliability analysis. This thesis is organised into two parts. The first part of this thesis explains the results obtained from probabilistic safety analysis of PFBR based on classical approaches. The second part of the thesis explains the different aspects of dynamic reliability approaches. The significance of using dynamic reliability approach is illustrated with a typical passive decay heat removal system of a FBR as an example. The thesis is organized into seven chapters. Chapters-1 and 2 are common to both parts of the thesis. Chapters-3 and 4 forms the first part while chapters 5 and 6 forms the second part. The chapter wise summary is given below.

Chapter 1: Overview of PSA - This chapter gives an overview of Probabilistic Safety Analysis. The safety analysis of reactors is carried out by both deterministic and probabilistic approaches. The deterministic safety analysis prescribes a set of conservative rules which when satisfied gives the confidence that the level of risk to the public is acceptably low. Defence in depth, single failure criterion and sufficient safety margins are some of the outcomes of deterministic safety analysis [2]. Deterministic safety analysis models the physical evolution of the process for a bounding initiating condition. The likelihood of this initiating condition is not quantified in deterministic safety analysis. Probabilistic Safety

Analysis (PSA) considers a comprehensive list of initiating events with its likelihood and quantifies the risk to the public. The advantages of PSA over deterministic safety analysis are the comprehensive consideration of initiating events, use of multiple failure criteria, better uncertainty modelling capabilities and identification of important components / systems which contribute to risk.

PSA of nuclear power plants becomes popular with the release of the Reactor Safety Study [3]. The importance of PSA for nuclear power plants was highlighted by the Three Mile Island Accident. The level of detail of a PSA study depends on the requirements. The details vary from a gross quantification during the conceptual design stage to the level of Living PSA. Living PSA is a detailed PSA modelling of the plant which incorporates the component details of the plant, operation and maintenance policies of different components etc. Living PSA gives the core damage frequency of a plant as a function of the status of different safety systems at any time. Now PSA has become mandatory in many regulatory frameworks. Recent regulatory practices use inputs from both deterministic and probabilistic approaches. Risk informed regulatory process is followed in India. Regulatory decisions are taken using deterministic safety analysis with appropriate inputs from PSA. The objective of quantifying the risk to general public due to a nuclear power plant is conveniently split into three different levels. These levels are designated as level-1 PSA, level-2 PSA and level-3 PSA. Level-1 PSA calculates the Core Damage Frequency (CDF) and the outcome of level-2 PSA is Radiation Release frequency (RRF). Level-3 PSA quantifies the risk to public.

Chapter 2: Description of a Fast Breeder Reactor - The type of safety systems and nature of initiating events depend on a specific reactor design. The PSA study which is performed for one particular reactor type may not be applicable to other reactor types. The PSA of a sodium cooled fast breeder reactor which is under construction is the subject of this thesis. This chapter describes the Prototype Fast Breeder Reactor (PFBR) which is considered for

this study. PFBR is a 500 MWe pool type sodium cooled fast reactor which is under construction at Kalpakkam [4]. The various safety systems of PFBR are described in this chapter [5]. Shutdown System and decay heat removal system are the frontline safety systems of this reactor. Reactivity control and emergency shutdown following a Design Basis Event (DBE) are the primary functions of shutdown system. PFBR has two independent and diverse shutdown systems namely SDS-1 and SDS-2. The decay heat produced in the core needs to be removed to maintain core integrity. This is achieved by decay heat removal systems subsequent to reactor shutdown. Operation Grade Decay Heat Removal System (OGDHRS) and Safety Grade Decay Heat Removal System (SGDHRS) are the two decay heat removal systems in PFBR. SGDHRS is a passive safety system. The front line safety systems are supported by various support systems like power supply systems, service water system and compressed air system. Power Supply system itself consists of different categories namely Class-IV, Class-III, Class-II and Class-I power supplies depending on the loads connected to them. Service Water System is essential for cooling various loads connected to it like diesel generators, air compressors etc thereby ensuring proper functioning of these equipments. Service water system also cools important structural components like reactor vault and roof slab. Compressed air system supplies air at specified pressure for various pneumatic operated equipments in different safety systems. The modelling of the dependence between front line and support systems and the dependence of various systems among themselves is one of the important features of PSA. The success criteria for modelling various safety systems are derived from process analysis. The safety systems of PFBR have been designed with sufficient redundancy, diversity and fail safe features wherever possible. Ten safety systems of PFBR have been considered. They are ShutDown System (SDS), Operation Grade Decay Heat Removal System (OGDHRS), Safety Grade Decay Heat Removal System (SGDHRS), Class-III Power Supply System, Class-II Power Supply System, Class-I Power Supply

system, Safety Related Service Water System (SRSWS), Compressed Air System (CAS), Roof Slab Cooling System and Bio-Shield Cooling System. This chapter gives a brief description of the above mentioned safety systems.

Chapter 3: Level-1 Internal Events PSA- The level-1 PSA is divided into two categories namely level-1 internal events PSA and level-1 external events PSA. As the name implies, the events which originate within the plant and which has the potential to lead to core damage are considered in level-1 internal events PSA. Level-1 internal events PSA of Prototype Fast Breeder Reactor (PFBR) is presented in this chapter. The level-1 PSA of PFBR was carried out as per the established procedure [6]. The various elements of level-1 PSA like initiating event analysis, success criteria analysis, accident sequence analysis, Systems analysis, human reliability, common cause failures and sensitivity/uncertainty analysis are explained [7]. This study has the following objectives. The first objective is to identify the design modifications if required, to keep the core damage frequency below certain level. The second objective is to identify the dominant contributors to core damage frequency which when reduced will lead to reduction in core damage frequency of future FBR designs. Diversity is introduced between two shut down systems and different loops of decay heat removal system based on this study. This helps in keeping the core damage frequency to around ~1.0E-06 / y. The contribution to core damage frequency is dominated by Loss of Offsite Power (LOSP) and Loss of Steam Water System (LSWS). If the core damage frequency of future FBRs is to be reduced further, design modifications are needed to reduce the contribution from above events. One of the important features of this study, is the introduction of functional reliability analysis in the accident sequence models. This helps in identifying additional accident sequences which would have been otherwise not considered in the accident sequence models. The role of common cause failures and balance in the plant design are inferred from this study. The core damage frequency of PFBR is estimated to be ~0.9 E-06 /y.

Chapter 4: Level-1 External Events PSA - Events which originate outside the plant and which have the potential to damage the core are known as external events. Natural phenomena like earth quakes, flood, fire and tornadoes are some of the external events which can affect a nuclear plant. External events PSA quantify the Core Damage Frequency contribution from these events. The main difference between internal events PSA and external events PSA is the failure of multiple systems / components due to a single external event. The reliability of safety systems is increased by using redundancy in internal events PSA. Redundancy may not increase the reliability of safety systems in external events PSA unless diverse features in design are used for the hazard under consideration. Any external events PSA consist of three elements. They are Hazard analysis, Fragility Analysis of Systems / Structures / Components and accident sequence quantification. Hazard analysis is one of the important steps in quantifying the safety of the plant due to external events. This study is the first application of external events methodology to a pool type fast breeder reactor.

The seismic PSA of PFBR was completed as per the procedure outlined in [8]. The objectives of this study are i) validate the seismic ground motion parameters of the site through probabilistic seismic hazard analysis ii) estimate the core damage frequency due to seismic events. The seismic ground motion parameters of the plant are specified by two levels namely Operation Base earthquake (OBE) and Safe Shutdown Earthquake (SSE). These two levels are determined by deterministic seismic hazard analysis for PFBR site. The deterministic seismic hazard analysis is carried out by considering a few seismic sources close to the site. The earthquake magnitudes for these seismic sources are judgement based. The detailed site specific probabilistic seismic hazard analysis carried out in this study validates the ground motion parameters from deterministic seismic hazard analysis. The ground motion parameters estimated from both the studies matches at 50% exceedence

probability level. Plant specific fragility data is used for some components and for other components generic fragility data from literature [9] is used. The test data from seismic qualification experiments of instrumentation panels of PFBR are used to compute fragility values for instrumentation panels. The core damage frequency due to seismic events is estimated.

PFBR is located on the east coast of India. External flood is one of the important phenomena which can affect PFBR site. Three natural phenomena, Tsunami, storm surge and rainfall have the potential to cause flood at PFBR site. Of the three phenomena, Tsunami wave run up height governs the flood risk at PFBR site. The PFBR site was affected by the December 26th, 2004 tsunami event. The previous study on tsunami hazard analysis was improved by including the local bathymetry in to the tsunami wave run up height model. The previous model under predicts the observed tsunami wave run up height at plant site. The present study significantly increases the tsunami wave run up height predictions [10]. The results from the present study are consistent with the observed run up heights at the plant. From the tsunami hazard analysis, it is inferred that the possibility of core damage due to flooding event is very small for PFBR. This is due to the elevated design of PFBR. Two different approaches to model the accident sequences for EFPSA are compared and a particular methodology is recommended to model the accident sequences [11]. This study enables the use of accident sequences developed for level-1 internal events PSA with appropriate modifications, thereby reducing considerable time and effort.

Chapter 5: Overview of Dynamic Reliability Analysis - This chapter gives a comparison between classical and dynamic reliability approaches. Classical reliability analysis estimates the system reliability in terms of the reliability of its constituent components. The process information is used to arrive at the hardware configuration (failure criteria) for which the process variables will be crossing their safety limits. It is assumed that the process evolution

is independent of system hardware states and failure occurs in a specific hardware configuration in classical reliability. Fault tree and event tree are static in nature. Fault tree and event tree techniques are widely used in classical reliability analysis because of their easiness to review and adaptability to large systems. There are several drawbacks in classical fault tree approach. The formation of logical loops while modelling interconnected systems is one of the drawbacks. It is very difficult to model various types of dependencies between components like dependence in testing, repair / maintenance and increased stress on one component due to the degraded performance of the other component. The fault tree approach requires subjective assumptions. The uncertainties in physical process and stochastic changes in system hardware are not addressed in a systematic manner in classical approaches. The classical approaches neglect the time dependent interaction between the physical process and system hardware.

Dynamic reliability approach is an integrated model in which the process and system hardware are evolving as a function of time. The mathematical framework for this model is given by the Chapman-Kolmogorov equation. The different techniques for dynamic reliability approach are continuous time methods and discrete time methods [12]. Continuous time methods attempt to solve the Chapman-Kolmogorov equation. Direct solution of this equation is difficult for typical reactor safety systems. Discrete time methods are widely used as compared to continuous methods. Dynamic Event Trees (DETs) is the most popular discrete time method. A process model is combined with DET in dynamic reliability approaches and the branching times are decided by the process conditions. The implementation of these methods requires a process model, identification of normal and abnormal hardware configurations and branching probabilities between different hardware states. The drawback of this approach is repairs have not been considered as transitions in these models. The branching times are deterministic in DET. Simulating the underlying

physical process and stochastic changes in system hardware through Monte Carlo simulation is a straight forward approach to dynamic reliability analysis. This is one of the approaches in discrete time methods and it is followed in this study. The basic idea of Monte Carlo simulation involves modelling the stochastic changes of system hardware with time. The process evolves deterministically in that hardware configuration until the next change in hardware configuration. Unlike in DET, the branching times are sampled from appropriate distributions. The advantage of Monte Carlo simulation is that component repairs can be modelled. Following are the objectives of the present study. i) Applying a few simulation techniques on a typical reactor safety system and compare the performance of different simulation techniques. ii) Identifying an efficient simulation tool to model the system hardware changes with time. The Monte Carlo simulation schemes in literature are tested mostly on example systems. Reactor safety systems are characterised by rarity of system failures and common cause failure between components. Three Monte Carlo simulation schemes are applied on the typical shutdown system of a fast reactor and the performance of these schemes are compared in terms of variance reduction for fixed computational effort. It is found that the balanced failure biasing Monte Carlo simulation scheme gives better performance in terms of variance reduction. The results obtained from this analysis are comparable with fault tree results. Balanced failure biasing Monte Carlo simulation scheme is chosen to model system hardware evolution with time.

Chapter 6: Dynamic Reliability Analysis of a Passive Safety System - The simulation scheme identified in the previous chapter is used to combine the physical process and system hardware for a simple example system. The example is chosen such that it is possible to compare the simulation results with analytical integration with appropriate time limits [13].

This example demonstrates that in the absence of significant interaction between the physical process and system hardware, classical approaches with appropriate time models are

sufficient. The results obtained from dynamic reliability analysis and other classical approaches like Time Dependent Cut set Evaluation (TDCE) and fault tree with non-recovery of components are comparable in this example system.

Dynamic reliability analysis of an example passive decay heat removal system of a FBR is presented in this chapter. The interaction between system hardware and process can be of three types. The first type of interaction is the one in which changes in system hardware affects the process evolution. The change in transition rates of system hardware as a function of process parameters is the second type of interaction. The third type of interaction involves changes in system hardware induced by the process variables crossing some threshold limit. The process considered in this study is sodium hot pool temperature evolution. Only the first type of interaction is assumed to be present in this example. The objective is i) to develop a method to combine process uncertainty quantification in functional reliability analysis with system hardware Monte Carlo simulation which will be helpful in the absence of full featured dynamic PSA tools ii) to estimate the probability of crossing the various categories of design safety limits on temperature and iii) to make an attempt to address one of the open issues in dynamic PSA that is to understand the conditions for which the classical and dynamic PSA approaches give significantly different results. The process uncertainty quantified in functional reliability analysis is combined with system hardware Monte Carlo simulation for passive decay heat removal system of a FBR. The probabilities of crossing the different categories of design safety limits on hot pool temperature are evaluated. From this analysis it is found that the contribution of process uncertainty to the total failure probability determines whether comparable or different results occur from classical and dynamic approaches. The classical approach here refers to the combination of process uncertainty quantified through functional reliability analysis [14] and system hardware reliability through fault tree. The total failure probability of the system consists of two parts [15]. The first part is the

contribution from the combined effect of process uncertainty and stochastic changes in system hardware. The second part is the contribution from process uncertainty alone. The results from classical and dynamic reliability approaches are significantly different when the contribution from second part is comparable or less than the contribution from the first part. The results from classical and dynamic approaches are comparable when the second part is much greater than the first part. This result is applicable at least for the example system under consideration having the specified type of process and system hardware interaction. This study attempts to gain an insight on the applicability of different methods based on process uncertainties. The use of dynamic PSA reduces the conservatism introduced by classical approaches in the region where the results are significantly different.

Chapter 7: Summary and Future Directions - Classical approaches are used for level-1 internal events PSA and level-1 external events PSA of PFBR. The Core Damage Frequency (CDF) is estimated. The CDF contribution from internal events PSA is dominated by Loss of Offsite Power (LOSP) and Loss of Steam Water System (LSWS). This study leads to the introduction of diversity in the design of front line safety systems. Seismic PSA of PFBR is completed. The seismic hazard analysis validates the design basis ground motion parameters of the plant. Two studies carried out as part of External Flood PSA (EFPSA) of PFBR are presented. Dynamic reliability analysis is a better tool as compared to classical approaches when there is a time dependent interaction between process and system hardware. There is scope for improving process models as compared to the simplified models in this study. The efforts are in the direction of integrating the process codes with system hardware reliability through Monte Carlo simulation. The objective will be to develop a full featured dynamic reliability analysis tool for future fast reactor safety analysis.

References

[1] Devooght. J and Smidts.C , "Probabilistic Reactor Dynamics-I: The Theory of continuous Event Trees", Nuclear Science and Engineering, 111, 1992, pp 229-240.

[2] IAEA-TECDOC-1436, Risk Informed Regulation of Nuclear Facilities: Overview of Current Status, February, 2005.

[3] WASH-1400 (NUREG-75/014), Reactor Safety Study: An assessment of accident risks in U.S. commercial nuclear power plants, USNRC, October-1975.

[4] Chetal, S.C., Balasubramaniyan, V., Chellapandi, P., Mohanakrishnan, P., Puthiyavinayagam, P., Pillai, C.P., Raghupathy, S., Shanmugham, T.K., and Sivathanu Pillai, C., "The design of prototype fast breeder reactor", Nuclear Engineering and Design **236** (7–8), 2006, pp.852–860.

[5] PFBR Final Safety Analysis Report (FSAR), Revision-0, March-2010

[6] IAEA Safety Series 50-P-4, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants, 1992.

[7] Ramakrishnan.M, Pramod Kumar Sharma, Bhuvana V, John Arul A, Mohankrishnan P, and Chetal S.C, "Insights from Level-1 Probabilistic Safety Analysis of Prototype Fast Breeder Reactor", Nuclear Engineering and Design, Vol-250, 2012, pp.664-670.

[8] IAEA-TECDOC-724, Probabilistic Safety Assessment for Seismic Events, IAEA, 1993.

[9] Ramakrishnan.M, John Arul.A, Bhuvana.V, Sajish.S.D, Preliminary Level-1 Seismic Probabilistic Safety Analysis of PFBR, Internal Report, February 2012.

[10] M.Ramakrishnan and A. John Arul, "Preliminary Tsunami Hazard Analysis for a Power Plant Site on East Coast of India", Presented at 2nd SRESA National Conference on Reliability and Safety Engineering (NCRS-15) held at Anna University, October 8-10, 2015.

[11] Ramakrishnan.M, John Arul.A, Bhuvana.V, PuthiyaVinayagam.P and Chellapandi.P, "Accident Sequence Modelling Methodology for External Flood Probabilistic Safety

Analysis of Prototype Fast Breeder Reactor", Applied Mechanics and Materials, Vols. 592-594, 2014, pp 2460-2464.

[12] Tunc Aldemir, "A Survey of Dynamic Methodologies for Probabilistic Safety Assessment of Nuclear Power Plants", Annals of Nuclear Energy, 52, 2013, 113-124.

[13] Ramakrishnan. M , "Unavailability Estimation of Shutdown System of a fast reactor by Monte Carlo Simulation", Annals of Nuclear Energy 90, 2016, pp 264-274.

[14] Sajith Mathews.T, Ramakrishnan. M., Parthasarathy. U, John Arul. A and Senthil Kumar. C., "Functional Reliability Analysis of Safety Grade Decay Heat Removal System of Indian 500MWe PFBR", Nuclear Engineering and Design, 238 (9), 2008, pp. 2369-2376.

[15] Ramakrishnan. M, "Integration of Functional Reliability Analysis and System Hardware Reliability through Monte Carlo Simulation", Annals of Nuclear Energy 95, 2016, pp 54-63.

This page is left blank

LIST OF FIGURES

LIST OF TABLES

This page is left blank

LIST OF ABBREVIATIONS

No.	Abbreviation	Expanded Form
1.	AC	Alternating Current
2.	AHX	Sodium Air Heat Exchanger
3.	AR	Absorber Rod
4.	AS	Actuation System
5.	ASEP	Accident Sequence Evaluation Program
6.	BFB	Balanced Failure Biasing
7.	BRE	Bounded Relative Error
8.	BSC	Biological Shield Cooling
9.	CCCMT	Continuous Cell to Cell Mapping Technique
10.	CCF	Common Cause Failures
11.	CD	Core Damage
12.	CDF	Core Damage Frequency / Cumulative Damage Fraction
13.	CET	Continuous Event Tree
14.	CPLD	Complex Programmable Logic Device
15.	CSR	Control Safety Rod
16.	CSRDM	Control Safety Rod Drive Mechanism
17.	CTMC	Continuous Time Markov Chain
18.	DBE	Design Basis Events
19.	DC	Direct Current
20.	DDET	Discrete Dynamic Event Tree
21.	DG	Diesel Generator
22.	DHDP	Decay Heat Drain Pump
23.	DHR	Decay Heat Removal
24.	DHRS	Decay Heat Removal System
25.	DHX	Sodium-Sodium Heat Exchanger
26.	DIS	Dynamic Importance Sampling
27.	DND	Delayed Neutron Detection
28.	DSL	Design Safety Limit
29.	DSR	Diverse Safety Rod
30.	DSRDM	Diverse Safety Rod Drive Mechanism

No.	Abbreviation	Expanded Form
31.	DTMC	Discrete Time Markov Chain
32.	EFPSA	External Flood Probabilistic Safety Analysis
33.	FBR	Fast Breeder Reactor
34.	FBTR	Fast Breeder Test Reactor
35.	FMEA	Failure Mode Effects Analysis
36.	FPGA	Field Programmable Gate Array
37.	FREDI	Fast REactor Database Information
38.	HCLPF	High Confidence Low Probability Failure
39.	HEP	Human Error Probability
40.	HPT	Hot Pool Temperature
41.	HX	Heat Exchanger
42.	IDPSA	Integrated Deterministic Probabilistic Safety Assessment
43.	IE	Initiating Event
44.	IFB	Inverse Failure Biasing
45.	IHX	Intermediate Heat Exchanger
46.	iid	independent identically distributed
47.	LERF	Large Early Release Frequency
48.	LOCA	Loss of Coolant Accident
49.	LOCC	Loss of Core Configuration
50.	LOPI	Loss of Piping Integrity
51.	LOSP	Loss of OffSite Power
52.	LSWS	Loss of Steam Water System
53.	MT	Mission Time
54.	MTTF	Mean Time To Failure
55.	MTTR	Mean Time To Repair
56.	NPP	Nuclear Power Plant
57.	NRC	Nuclear Regulatory Commission
58.	OBE	Operation Base Earthquake
59.	OGDHRS	Operation Grade Decay Heat Removal System
60.	PFBR	Prototype Fast Breeder Reactor
61.	PGA	Peak Ground Acceleration

No.	Abbreviation	Expanded Form
62.	PGD	Peak Ground Displacement
63.	PGV	Peak Ground velocity
64.	PLOHR	Protected Loss of Heat Removal
65.	PRA	Probabilistic Risk Assessment
66.	PSA	Probabilistic Safety Analysis
67.	PSP	Primary Sodium Pump
68.	PWR	Pressurised Water Reactor
69.	RCB	Reactor Containment Building
70.	RiSSA	Reliability information System for Safety Analysis
71.	RPS	Reactor Protection System
72.	RSS	Reactor Safety Study
73.	RWCS	Raw Water Cooling System
74.	ry	reactor year
75.	SDF	Spent fuel Damage Frequency
76.	SDS	ShutDown System
77.	SG	Steam Generator
78.	SGDHRS	Safety Grade Decay Heat Removal System
79.	SLFIT	Safety Logic with Finite Impulse Testing
80.	SNETP	Sustainable Nuclear Energy Technology Platform
81.	SRA	Strategic Research Agenda
82.	SRSWS	Safety Related Service Water System
83.	SSE	Safe Shutdown Earthquake
84.	SSMRP	Seismic Safety Margins Research Program
85.	SSP	Secondary Sodium Pump
86.	SSUC	Safety Service Unit Coolers
87.	SVS	Safety Vessel Support
88.	SWS	Steam Water System
89.	TDCE	Time Dependent Cut set Evaluation
90.	TG	Turbine Generator
91.	ULOF	Unprotected Loss of Flow
92.	UPS	Uninterrupted Power Supply

This page is left blank

Chapter-1 Overview of PSA

1.0 Introduction

The reactor safety analysis is vital to understand and ensure that the risk to public is acceptably low. This objective can be achieved by two ways. The first approach is conservative safety assessment methods. This approach uses a set of conservative rules for design and operation of a nuclear facility. If these rules and requirements are met they give a high degree of confidence that the risk is acceptably low. This approach enables the use of deterministic safety analysis [1-1, 1-2]. Deterministic safety analysis ensures sufficient safety margins in design, defence in depth, single failure criteria etc. Defence in depth is a hierarchical deployment of equipments and procedures to make multiple physical barriers effective. Single failure criteria ensure that a particular safety action is carried out even during the failure of single safety equipment. This approach was followed during the initial days of reactor operation. The second approach is the probabilistic approach. This approach tries to quantify the uncertainties systematically and will help to understand the degree to which the safety measures in nuclear power plants protect safety and public health. The advantages and disadvantages of both the methods are compared in table-1.

One of the important draw backs of deterministic approach is that it focuses more on less frequent bounding fault conditions rather than on the more frequent lesser fault conditions which contribute more to the plant risk. The probabilistic approach has drawbacks in terms of its scope, modelling difficulties in certain contexts and availability of plant specific data. Certain safety issues can be better understood if the results from both deterministic and probabilistic approaches are combined. The results from probabilistic approach complement the results from deterministic approach. This helps in regulatory decision making. This approach is called Risk Informed Regulation which is followed in many countries worldwide.

Table-1: Comparison of Deterministic and Probabilistic Approaches

Sl. No	Deterministic Approach	Probabilistic Approach
1.	Conservative assumptions are used to address uncertainties in different aspects.	A best estimate approach is followed in most aspects.
2.	A limited set of initiating events and fault sequences are considered and they are assumed to be bounding one.	A comprehensive list of initiating events including beyond design basis events are included in the analysis.
3.	Accident conditions are addressed by assuming the failure of certain safety systems	The initiating events and safety systems are integrated in the PSA models.
4.	Initiating event frequencies and failure probabilities are considered in an approximate way.	Initiating event frequencies and failure probabilities are explicitly modelled in PSA models.
5.	Relative importance of systems / components is given in an approximate manner.	PSA models give a wide range of importance measures for systems and components.

1.1 Historical Development of PSA

Deterministic approach was followed in the initial years of reactor safety analysis. As the safety systems of reactors grew in size and complexity, new methods were needed to reasonably predict the risk estimates. The first comprehensive study on the consequences of a nuclear accident was carried out in 1957 (WASH-740). Two papers [1-3, 1-4] which were published in 1967 and 1969 brought the Probabilistic Risk Assessment (PRA) to the

forefront. PSA was gaining ground in aero space industry along with nuclear industry. Fault tree analysis was in use in the aerospace industry to analyse different safety systems of an aircraft. Subsequently probabilistic risk assessment methods were used for space projects. Reactor safety became an important public policy issue as the number and size of nuclear reactors increased. The Reactor Safety Study (RSS) was initiated by United States Atomic Energy Commission in the year 1972. Fault trees are used to model various safety systems in a reactor. It was realized that integrating over all fault tree for a nuclear power plant was too complex. Event tree model was developed to overcome this difficulty. From then on, Fault trees and event trees have become important tools in PSA. The final report of RSS was published in the year 1975 which is the now famous WASH-1400 [1-5] report. The RSS produced more realistic results compared to previous efforts. The inclusion of common cause failures and human reliability are some of the salient features of this study. The earlier perception of large Loss of Coolant Accident (LOCA) in Pressurised Water Reactor (PWR) contributes significantly to risk was altered by this study. This study found that small LOCA made the highest contribution to risk. The risk from the operation of nuclear power plants was compared with the risks from other causes like accidents, diseases etc. Later this comparison became controversial. The WASH-1400 report was reviewed by the Lewis Committee which found several good qualities of the study. Some of the shortcomings identified were [1-2] the lack of verification of the calculation / analysis process, lack of accurate data for component reliability estimates, the finding that some external events contribute negligibly to the overall risk and the reporting on the health impacts of radiation release. The Unites States Nuclear Regulatory Commission advised its members to use Probabilistic Risk Assessment techniques in general. But the staffs of Nuclear Regulatory Commission (NRC) were familiar with deterministic approaches and there was some reluctance to follow the new approach.

Around that time in March, 1979 half of the core of Three Mile Island (TMI) Unit-2 melted. This accident confirmed a major RSS insight that small LOCAs contribute significantly to risk as compared to large LOCAs. Also the human factor highlighted by RSS study is a highly significant factor in TMI accident. After this accident, PRA played a key role in licensing of reactors.

1.2 Scope and Different Levels of PSA

PSA can be performed at many levels of scope depending on the objective of the analysis. Generally PSA is carried out at three levels of scope [1-6]. These three levels of scope are

a) Systems analysis.

b) Systems and Containment analysis.

c) Systems, Containment and Consequence analysis.

A level-1 PSA analyses the plant design and operation. The objective of this analysis is to identify the accident sequences that lead to a core melt, the basic causes and quantifying the frequencies. The final outcome of this analysis is a list of most probable core melt sequences and insight into their causes. Core Damage Frequency (CDF) is quantified at this level. External events like fire, flood and earthquakes may be included at this level. This level provides an assessment of plant safety, design and procedural adequacy in preventing core melt. A level-2 PSA analyses the physical processes of the accident and response of the containment in addition to the details covered in level-1 PSA. This level attempts to predict the mode of containment failure and the inventories of radio nuclides released into the environment. The core melt sequences can be categorized by the severity of the release. This level of PSA quantifies different categories of release and their frequencies. A level-3 PSA analyses the transport of radio nuclides through the environment and assesses the public health and economic consequences of an accident. Plant risk is estimated in this level. The

results are presented in the form of a risk curve which gives the frequency of various consequences.

PSA can be performed at any stage of the plant life. The PSA analysis performed after initial plant design but before construction is useful in identifying design weaknesses and improving the designer's understanding of the safety significance of plant design features. A PSA study performed just before plant start up will be useful in identifying the procedural inadequacies. PSA of an operating plant can use plant specific component data and this analysis is most complete with applicable results. Even in the operating plants many changes will take place due to the availability / unavailability of a safety system, components under maintenance etc. These details of the operating plant are captured in 'living PSA' which at any time gives the risk from the nuclear power plant under consideration. A brief literature survey on the different methods used in PSA is given in section 1.3.

1.3 Literature Survey on Different Methods Used in PSA

There are several methods available to estimate the reliability measures of a safety system. Some of them are reliability block diagram, fault tree and Markov state space models to name a few. Reliability block diagram (RBD) [1-7] provides the functional relationship between different components in a series–parallel configuration. RBD is the pictorial representation of a Boolean expression. RBDs are helpful to get preliminary estimates of reliability based on the initial understanding of the system. RBD can be developed for simple systems with few components. It is difficult to develop a RBD for a complex nuclear safety system due to the large number of components. Also it is difficult to systematically account for the various failure modes of components. The fault tree technique is suitable to model the large safety systems of nuclear reactors. Fault tree [1-8] technique is a deductive methodology. Top down approach is followed in fault tree. The top event of the fault tree is usually a system failure. The causes for the occurrence of the top event are systematically

analysed in terms of the failure of sub systems or components. Fault trees are relatively simple to develop and convenient for review. Fault tree techniques are suitable for modelling independent failures and repairs. It is difficult to account for various types of dependencies in failure and repair using a fault tree. There is a possibility of logical loop formation in a fault tree. The dependent failures and repairs can be modelled in a better way with Markov state space models. However the state space of the system grows exponentially with number of components in the system. Therefore Markov state space method requires large memory to store huge transition matrix. This method is suitable for systems with small number of components. This method requires enumeration of all the 2^n possible states of a system assuming two states for each of the n components in the system.

More recent techniques for system reliability evaluation are Binary Decision Diagram (BDD) and Stochastic Petri Nets. The Binary Decision Diagram method [1-9] has been formulated over the last decade. Normally BDDs are generated from fault trees. Its advantages include increased efficiency in determining the qualitative characteristics of a failure mode represented using a fault tree, and improved accuracy when calculating the corresponding quantitative performance measures. The disadvantage of the approach however, is that the conversion from the fault tree cannot be guaranteed to be optimal, reducing the advantages of using the method. This is because the ordering of the basic events can have a crucial effect on the size of the final BDD [1-10].

Stochastic Petri Nets [1-11] are a modelling formalism that can be conveniently used for the analysis of complex models of Discrete Event Dynamic Systems (DEDS) and for their performance and reliability evaluation. However, these models also have disadvantages. The main disadvantage is that the basic Stochastic Petri Nets are quite primitive. So there is a significant burden placed on the analyst in order to specify complex models. In addition to

that, the graphical representation may become too complex to be useful. Another disadvantage is that the representation of priorities or ordering is difficult to manage.

Monte Carlo simulation techniques are suitable to overcome the draw backs of BDD and Stochastic Petri Nets. An overview of Monte Carlo simulation techniques is presented in chapter-5. Of the several methods, Fault tree technique is widely used for system reliability analysis. Event tree technique is used to model the accident sequences starting from an initiator event. Event tree technique is an inductive methodology which is used to model accident progressions. In nuclear industry both fault tree and event trees are widely used in Probabilistic Safety Analysis. There are several software tools available to carry out the Boolean algebra in fault tree / event tree techniques like RISK SPECTRUM, ISOGRAPH, PSA PACK etc. to name a few. These software tools give information on cut sets, probability of their occurrence and different importance measures. Uncertainty analysis is carried out by simple Monte Carlo simulation and most of these software tools have this capability. Availability of software tools with the above mentioned capabilities make fault tree/ event tree techniques as standard tools for carrying out PSA.

1.4 Thesis Organization

The PSA overview was discussed in the previous sections. The PSA of a fast reactor is the subject of this thesis. Chapter-2 describes the fast reactor. This thesis consists of two parts namely classical approaches to PSA and dynamic approaches to PSA.Chapters-3 and 4 forms the first part. The studies reported in these chapters are based on classical reliability approaches. Chapters-5 and 6 constitutes the second part. The second part is based on dynamic approaches to reliability. Chapter wise organization of the thesis is as follows.

Chapter-2 describes the fast reactor which is considered for this study and explains the various safety systems of the reactor. The different safety systems are categorised as front line systems and support systems. The dependence between different systems is brought out.

Chapter-3 explains the level-1 full power internal events PSA carried out for the reactor described in chapter-2. The various elements of carrying out level-1 internal events PSA and the implementation aspects are discussed in this chapter. The important results from this study are also presented.

Chapter-4 presents the level-1 external events PSA. Seismic events and flood are the two external events considered. The various steps involved in external events PSA are briefly explained here. Seismic PSA results are presented. Two different accident sequence modelling approaches for external flood PSA are compared. Tsunami hazard analysis carried out as part of External Flood PSA of PFBR is explained.

Chapter-5 presents the drawbacks of classical reliability approaches and the necessity for dynamic reliability approaches in which process and system hardware evolves with time. As a first step literature survey of different Monte Carlo simulation approaches for system hardware reliability is carried out. The performance of these approaches for a typical shutdown system of a fast reactor is presented. A particular simulation approach is identified which gives better performance in terms of computational effort and variance reduction. The results obtained from simulation are compared with the results from fault tree analysis.

Chapter-6 uses the identified simulation approach in chapter 5 and combines it with the process evolution with time. First a very simple example in which it is possible to compare the results obtained from simulation with analytical integration is presented. This approach is subsequently extended to the passive decay heat removal system of a FBR. The probabilities of crossing the various safety limits on temperature are estimated. The results obtained from the present approach are compared with two different approaches. It is found that the results match closely for certain conditions of process uncertainty.

Chapter-7 presents the summary and future directions for this study. It is required to integrate detailed process models with improved models of system hardware simulation. This will enable better reliability quantification and additional insights on process and system hardware interaction.

This Page is left blank

Chapter-2 Description of a Fast Breeder Reactor

2.0 Introduction

Fast Breeder Reactors (FBR) came to prominence because of its ability to effectively use fuel and breed fuel. Fast Breeder Reactors form the second stage of India's three stage nuclear energy programme [2-1]. The Fast Breeder Test Reactor (FBTR) is an experimental and test reactor which is in operation from 1985. This is the first fast reactor in India. The Prototype Fast Breeder Reactor (PFBR) is a 500MWe, sodium cooled, pool type, mixed oxide fuelled reactor. This reactor is under construction at Kalpakkam. The objective of this reactor is to demonstrate the viability of FBRs both technically and economically. The Probabilistic Safety Analysis (PSA) of this reactor is the subject of this thesis. The design features of a nuclear reactor are one of the inputs to PSA. The objective of the present chapter is to give an overall picture of PFBR and the various safety systems considered for PSA.

2.1 PFBR Description

The overall flow diagram of PFBR comprising primary circuit housed in reactor vessel, secondary sodium circuit and balance of plant is shown in fig.1. The primary circuit consists of two Primary Sodium Pumps (PSP). They maintain the sodium flow in primary circuit. The heat from primary sodium is transported from Intermediate Heat Exchangers (IHX) to steam generators (SG) by two secondary sodium loops. Each secondary sodium loop is provided with one Secondary Sodium Pump (SSP). Each secondary sodium loop is connected to four steam generators. Totally eight steam generators produce steam to run the turbine. The turbine is provided with 60% steam bypass capacity. The various safety systems of PFBR are explained in the subsequent sections. Reactivity control and decay heat removal are the important safety functions in any reactor. The reactivity control in PFBR is carried out by two independent fast acting diverse ShutDown Systems (SDS). There are two decay heat

removal systems in PFBR namely Operation Grade Decay Heat Removal System (OGDHRS) and Safety Grade Decay Heat Removal System (SGDHRS). The shutdown system and

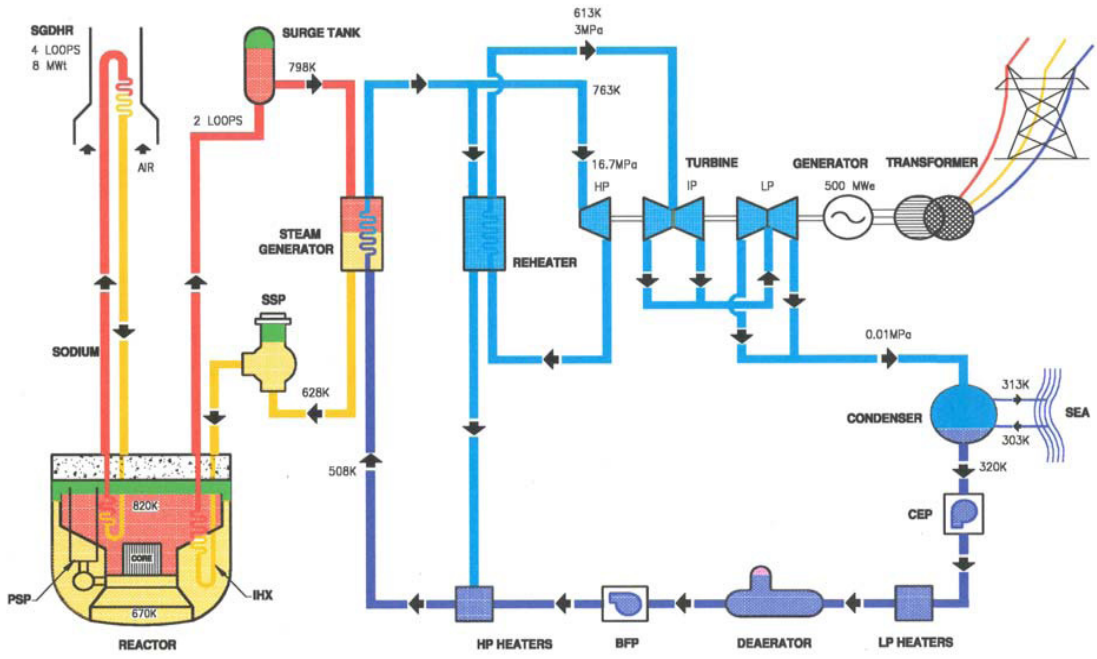

Fig.1. Flow Diagram of Prototype Fast Breeder Reactor

decay heat removal systems are the frontline safety systems in PFBR. The frontline safety systems depend on several support systems like power supply systems, service water system and compressed air system. The front line systems in PFBR are designed with fail safe features under certain conditions. The shutdown system is fail safe against loss of power. The pneumatically operated dampers of SGDHRS are fail safe on loss of instrument air. A brief description of various safety systems of PFBR [2-2] are given in subsequent sections.

2.1.1 ShutDown System (SDS)

PFBR has two independent and diverse shutdown systems namely Shut Down System-1(SDS-1) and Shut Down System-2 (SDS-2). The purpose of reactor shutdown system (SDS) is to promptly terminate the fission chain reaction and thereby ensure safety during the Design Basis Events (DBE). SDS-1 is also used for power regulation, power raising and setback without affecting the safety functions on demand. Power raising and setback is change of power to desired levels when required. Each system is capable of

shutting down the reactor into cold sub-critical state and maintaining it. Each shutdown system consists of Reactor Protection System (RPS), Actuation System (AS) and safety support systems. RPS consists of sensors to monitor plant parameters, analogue signal processing circuits, SCRAM logic, SCRAM switches (power gates) and power supply. AS consists of Absorber Rods (AR), electromagnets and drive mechanisms to drop or drive the absorber rods into the core. The overall structure of both the shutdown systems is shown in fig.2. Optical inter-link enables both sets of SCRAM parameters (from RPS1 and RPS2) to trigger both the actuation systems while maintaining electrical isolation. The Delayed Neutron Detection (DND) is common to both the systems. Safety logic receives trip signals from neutron flux monitoring, temperature monitoring, failed fuel element detection, flow monitoring, pump speed etc and processes them in a logical fashion and gives command for initiating reactor shutdown. The analog output signals of these systems are converted into binary signal in a comparator, which form the inputs to the safety logic. SDS-1 consists of 9 Control Safety Rods (CSR). Each absorber rod is having individual Control Safety Rod Drive Mechanism (CSRDM). The safety logic with finite impulse testing (SLFIT) is used in SDS-1. Field-Programmable Gate Array (FPGA) is used to build SLFIT. SDS-2 consists of 3 Diverse Safety Rods (DSR) with each rod having individual Diverse Safety Rod Drive Mechanism (DSRDM). SDS-2 has a dynamic pulse coded safety logic built with Complex Programmable Logic Device (CPLD) technology. The safety logic circuits are designed such that loss of power in any of the instrument channels or malfunction at various stages will lead to reactor trip. The absorber rods are held by electromagnets in both SDS-1 and SDS-2. When there is a demand on shutdown system, the electromagnets are de-energised and the rods fall inside the core due to gravity. The success criterion for SDS-1 is eight out of nine rods dropping inside the core. For SDS-2, two out of three rods dropping inside the core is a success. The shutdown function will be achieved if either SDS-1 or SDS-2 actuate on demand. Physical

diversity between the two shutdown systems is achieved by using two safety logics working on diverse design principles. Functional diversity is achieved by choosing diverse SCRAM parameters for the same event. The reliability target for shutdown system as established by

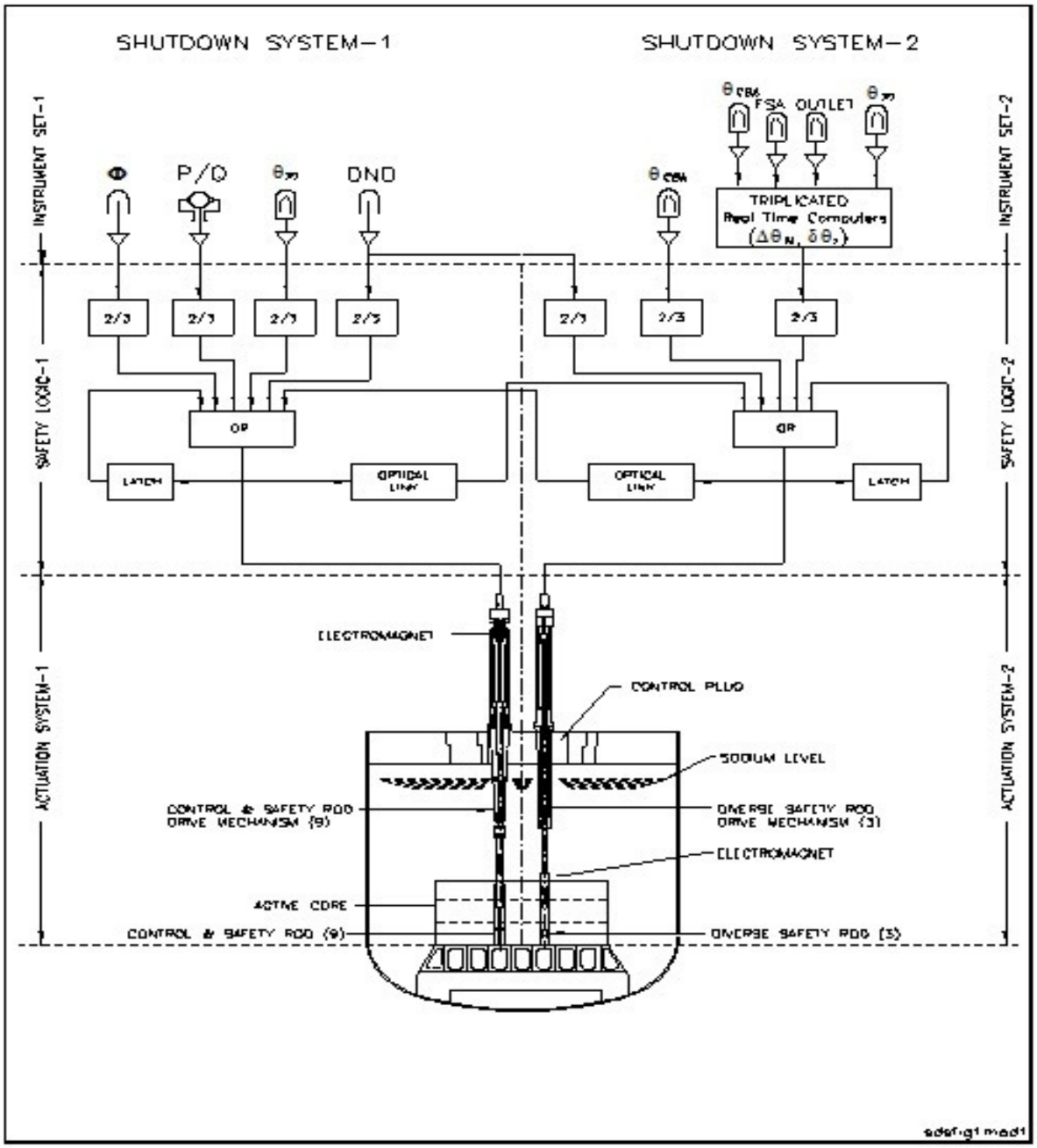

Fig.2: Schematic Diagram of ShutDown System

the safety criteria of PFBR [2-3] are as follows. The failure frequency of each shutdown system shall be less than 10^{-3} /ry. The overall failure frequency of shutdown system shall be less than 10^{-6} /ry.

2.1.2 Operation Grade Decay Heat Removal System (OGDHRS)

Decay heat removal through the steam water system is one of the two diverse decay heat removal paths in PFBR. This is called the Operation Grade Decay Heat Removal System (OGDHRS). The OGDHRS consists of four small variable pressure steam condensers, Decay Heat Drain pumps (DHDP), Steam water separator and condenser fans. Each condenser is provided with two forced draft type condenser fans. There are two Decay Heat Drain Pumps (DHDP) each having 100% capacity. Decay heat removal through OGDHRS is envisaged under the following conditions. If at least one secondary sodium loop and Steam Water System (SWS) are functional following any Design Basis Event (DBE), then decay heat removal through OGDHRS is possible. The operating strategy involves the transfer of the DHR function from the normal steam water system components to the OGDHR specific system. This is achieved by isolating the turbine through valve action. Subsequently the OGDHRS condensers start condensing steam and the water is collected in steam water separator. Following a DBE, it takes approximately ~25 minutes to collect 40 m^3 of water in steam water separator. This time and quantity of water is arrived based on detailed analysis [2-4]. Feed water from steam water system should be available for these 25 minutes following a DBE. Once sufficient water is collected in steam water separator, the feed water supply from steam water system can be switched off and water from separator will be fed to steam generator through decay heat drain pumps. The secondary sodium pumps are provided with class-III power. Decay heat drain pumps and condenser fans are on class-IV power. During Loss of Off Site Power (LOSP) OGDHRS is unavailable. The success criteria for this system is as follows: a) Availability of at least one primary sodium pump b) Availability of at least one secondary sodium circuit c) Availability of at least two out of four steam generators in each secondary sodium loop d) Availability of feed water circuit in steam water system for initial one hour e) Availability of at least one decay heat drain pump f) Availability of all the

four decay heat removal condensers g) Availability of both the condenser fans in the respective condenser.

2.1.3 Safety Grade Decay Heat Removal System (SGDHRS)

The second decay heat removal system is called Safety Grade Decay Heat Removal System (SGDHRS). This circuit consists of four independent loops. Each SGDHR loop consists of i) one sodium-sodium heat exchanger (DHX) dipped in the hot pool ii) one sodium-air heat exchanger (AHX) iii) one expansion tank iv) one storage tank v) associated sodium piping and valves vi) argon supply and vent system for expansion tank and storage tank vii) nitrogen flooding circuit for AHX casing viii) air circuit for AHX with casing, inlet ducts, dampers and stack. The DHX transfers heat from radioactive primary sodium (hot pool) to intermediate sodium. The AHX dissipates heat from intermediate sodium to atmospheric air. SGDHRS is a passive system. The only active element in the system is the air dampers (at the inlet and at the outlet) in the air circuit which have to be opened on demand. The air dampers at the inlet and outlet are divided into two halves and one half is motor operated and the other half is pneumatically operated for ensuring diversity. Provision is also there to open the dampers manually at damper site. Diversity in the design of DHX and AHX is adopted in SGDHR system to obtain the required reliability values. The two loops of SGDHRS are located in one building and the other two loops are located in another building. The intermediate sodium flow by natural circulation is obtained by placing the thermal centre of AHX ~ 41 m above the thermal centre of DHX. The drive force for the flow of air over the finned tubes of AHX is obtained by providing a stack of height 30 m. During normal plant operation, pneumatic and electrical motor operated air dampers provided at the inlet and outlet of AHX are kept in crack open position. This permits certain amount of natural circulation in the SGDHRS to enable smooth change over to decay heat removal mode when required. The air dampers are opened on auto mode when the SGDHR system is

required for decay heat removal. If the dampers fail to open on auto, then the dampers can be opened manually. After reactor scram SGDHRS will be initiated automatically from the SCRAM signal. If OGDHRS is removing decay heat, the operator shall bring the SGDHRS into poised state manually and decay heat is removed through OGDHRS. The success criterion for SGDHRS is the availability of one loop for the entire mission. A schematic diagram of SGDHRS is shown in fig.3.

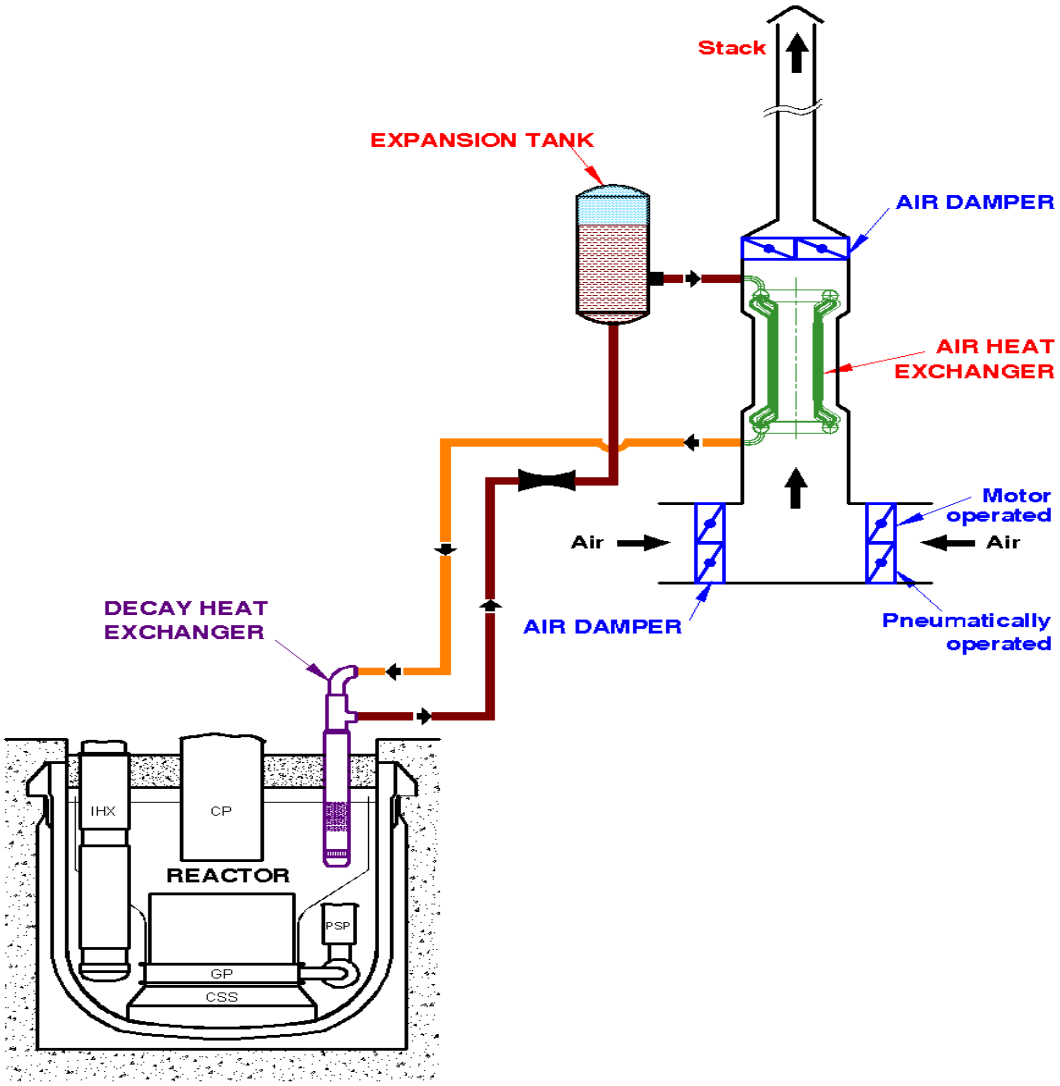

Fig.3. Schematic Diagram of SGDHRS

2.1.4 Class-IV and Class-III Power Supply Systems

The grid power supply at the station is normally called the class-IV power. The class-IV power to PFBR is from one of the following paths. a) From the grid through the station

transformer. b) From the grid through the generator transformer and two numbers of unit auxiliary transformers with generator circuit breaker kept in open position. c) From the terminals of the Turbine Generator (TG) through the two numbers of unit auxiliary transformers when the generator circuit breaker is closed during power generation. The availability of power from any one of the above three sources is sufficient to meet the station services. The AC supply voltages (Class IV and III) selected for the station auxiliary loads are 6.6 kV for high voltage loads and 415V for medium voltage loads. The unavailability and frequency of loss of Offsite Power are calculated by collecting loss of offsite power data for Kalpakkam site.

Normally the 6.6 kV buses in PFBR site are supplied by the grid supply. 415V buses derive power from 6.6 kV buses through step down transformers. 6.6 kV buses receive supply from the grid through Unit bus and Station bus. Either unit bus or station bus will connect the grid and 6.6 kV bus at any given time. Standby emergency Diesel Generators (DG) are provided as onsite sources of AC power. Class-IV power supply with Diesel Generator backup is called Class-III power supply. Class-III power supply is given to essential loads which cannot tolerate AC power supply interruption beyond three minutes. PFBR consists of two 6.6 kV divisions with two sections per each division. There are four Diesel Generators and each DG is rated to supply 50% of the total emergency power supply demand. These four Diesel Generators are located in two different buildings with two DG in each building. The two DG units housed in one building are physically segregated from one another by fire barrier wall and each DG is also functionally independent from the other. The important loads on class-III buses are primary sodium pump, secondary sodium pump, safety related service water pumps, biological shield cooling water pumps, compressors of compressed air system and blowers of roof slab cooling system. The success criterion for this system is the availability of two out of four diesel generators. All the four DGs would start

automatically on loss of class-IV power. Each DG would feed its associated 6.6 kV bus section. The cooling for DG is provided by the safety related service water system.

2.1.5 Class-II Power Supply System

No-break AC power supply is called Class-II power supply. This is derived from Class-III buses through a rectifier/charger and inverter. Battery backup is provided at the input of inverter to provide no break AC supply during the unavailability of Class III supply. The important loads on this system are motors associated with Control and Safety Rod Drive Mechanism (CSRDM) / Diverse Safety Rod Drive Mechanism (DSRDM) and motors associated with SGDHRS dampers. There are four independent divisions of class-II power supply. Each division is having its own Uninterrupted Power Supply (UPS) systems, battery and main distribution board. Each class-II division and main distribution board is rated for 50% of the total class-II loads of the plant. In each UPS system there are two UPS units each rated for 50% of the total class-II loads. When one UPS unit fails the other UPS unit will continue to supply the loads of the division without interruption. The loads will be transferred only when both the UPS units in a division fails. Two divisions of class-II electrical power supply are located in electrical building-1 and the other two divisions are located in electrical building-2. The rectifiers, chargers and inverters of class-II power supply are of solid state type. Electrical independence and physical independence are maintained between the four divisions right from buses to local distribution boards. The class-II power supply system is ungrounded. This will facilitate independent earth fault location and detection for each division. The loads connected to particular division are assumed to be failed when a class-II division fails. This is a conservative assumption because the loads can be transferred from one division to another in case of failure of a division.

2.1.6 Class-I Power Supply System

No-break DC power supply is called Class-I power supply. This is derived from Class-III buses through a rectifier/charger. Battery backup is provided at the output of rectifier/charger to provide no break DC supply during the unavailability of Class III supply. There are four independent divisions of class-I 48V DC power supply. Each division is having its own battery, charger and main distribution board. Each division is receiving independent input power supply from the class III, 415V buses. A standby battery charger common to divisions 1 and 2 and another charger common to divisions 3 and 4 are provided. When a main charger fails the standby charger is connected to the affected bus automatically. The output of the standby charger is interlocked such that any one division out of two divisions can be fed from the standby charger. There are no bus couplers between the divisions. Two divisions of class-I 48V DC are located in one building with their respective chargers, batteries and main distribution boards. The other two divisions and their batteries, chargers and main distribution boards are located in another building. The rectifiers and chargers are of solid state type. Electrical independence and physical independence are maintained between the four divisions of class-I power supply. Redundant class-I loads are supplied from redundant class-I divisions. The loads of class-I bus can be fed from the buses of non-safety related systems class-I power supply in case of failure of one division. Separate feeders are provided for that purpose. The loads connected to a particular division are assumed to have failed when a class-I division fails. This is a conservative assumption.

2.1.7 Safety Related Service Water System

Safety Related Service Water System removes heat from specified loads and dissipates the heat to raw water cooling circuit through Safety Service Unit Coolers (SSUC). The demineralised water is used as coolant. The loads of Safety Related Service Water System are DG coolers, Biological shield cooling Heat Exchangers (HX), Roof slab cooling

HX, Spent Fuel Cooling HX, Safety related chillers, Drain coolers, Gas compressors and Nitrogen to Water HX for Primary Cold Trap. Safety Related Service Water System consists of two identical redundant trains. Each train is capable of meeting the safety load requirements independently. Each train has 2×100% pumps, 2×50% unit coolers, one expansion tank and one chemical feed tank in each train. One train is run continuously to meet the heat loads. The power supply to redundant trains is from redundant divisions. The pumps of this system are connected with class-III supply. Tie line with valves is provided between the two trains. The pumps and unit coolers of the two trains are located in two different rooms. Expansion tanks are provided in both the trains to take care of any volume changes and pressure surges. Makeup for demineralised water is available for seven days of operation. This demineralised water makeup is supplied at the expansion tanks which are located at an elevation on the suction side of the pumps. The reactor will not be operated in the case of unavailability of safety related service water system. The Safety Service Unit Coolers are located on the discharge side of the service water pumps. The demineralised water is slightly at a higher pressure than raw water in SSUC to reduce the ingress of raw water into demineralised water. The success criteria for safety related service water system is the availability of at least one pump and two unit coolers.

2.1.7.1 Raw Water Cooling System

Raw Water Cooling System (RWCS) is the heat sink to safety related service water system. This system is an open re-circulation system. It receives heat from safety related service water and rejects heat to the atmosphere in a cooling tower and returning to unit coolers. RWCS also consists of two trains with each train comprising two pumps. At least one pump is required for the operation of this system. The cooling tower consists of four cells. Each cell is having a cooling tower fan which is on class-III power supply. A flow control valve is provided for each cell. The success criterion for cooling tower fans is three

out of four fans should be operating with their corresponding flow control valves available. Provision is made for makeup of raw water to compensate for different losses. Raw water make up is provided from the raw and firewater storage tank. The tank has storage for supplying make up to RWCS for 7 days.

2.1.8 Biological Shield Cooling System

The function of the Biological Shield Cooling (BSC) system is to cool the lateral and bottom shield concrete. This is done to maintain concrete temperature within permissible limits. BSC system removes the radiant heat passed on to concrete shield from the main vessel and heat generated in the concrete due to gamma radiation from sodium. Biological shield concrete consists of lateral concrete shield around the safety vessel and bottom shield below the safety vessel. Lateral concrete shield is further divided into upper lateral, Safety Vessel Support (SVS) and lower lateral for ease of cooling. Carbon steel liners are provided at the inner face of concrete in the upper lateral, SVS, lower lateral and bottom parts. Cooling pipes in the concrete are welded to the liner. The system consists of circulating pumps, plate type heat exchangers (BSC water to Service water), filters, expansion tank, chemical dosing tank, supply and return headers and embedded piping. BSC system consists of two loops and normally both loops are in operation. There are two pumps with one working and the other on standby. Two plate type heat exchangers are provided with one working and the other on standby. The success criteria are availability of one out of two pumps and one out of two plate type heat exchangers. The loss of cooling to the reactor vault concrete requires manual reactor SCRAM. This is one of the initiating events in event tree analysis. The initiating event frequency is computed from fault tree analysis for this system.

2.1.9 Roof Slab Cooling System

The top shield cooling system maintains the required temperature levels in the top shield by removing the heat transferred to it from the sodium pool. It also maintains the

temperature difference between top and bottom plates of top shield to limit the tilt of components supported on top shield like primary pump, IHX, CSRDM, DSRDM etc. to design values. The heating of the top shield is due to heat transfer from the sodium pool and the contribution due to nuclear heat generation in concrete is negligible.

The top shield is cooled using air in a closed loop during normal operation and the air in turn, is cooled by service water. Inlet and outlet ducts are provided on the periphery of roof slab. The inlet and outlet ducts run to the cell provided for top shield cooling system outside Reactor Containment Building (RCB). This cell contains 4 redundant blowers each of 50% capacity. Two blowers are in operation at a given time. Manually operated butterfly valves are provided at inlet & outlet of each blower to isolate the blower if required, and to control flow through the blower in operation. Non return valves are provided at the discharge of each of the blowers to avoid reverse flow. Two heat exchangers each of 100% capacity are provided. At a given time, one will be used and the other is kept in standby mode. Butterfly valves are provided at the inlet and outlet of the heat exchangers for isolation, if required. In case of non-availability of service water system, the heat exchangers are isolated and the cooling system is operated in once through mode with air drawn from outside RCB. The success criteria for this system is the availability of two out of four blowers (with associated pipes and valves) and availability of one out of two heat exchangers. The loss of cooling to roof slab requires manual SCRAM of the reactor and it is one of the initiating events considered in event tree analysis.

2.1.10 Compressed Air System

The system provides supply and distribution of compressed air of three categories namely instrument air, mask air and service air. Instrument air is used in pneumatic instruments, valves and dampers. Mask air is used in areas of high particulate activity or where the atmosphere is contaminated. Service air is used for air drying and cleaning the

components. Of the three categories, instrument air is directly connected with the operation of safety equipments. A set of four compressors of oil free, rotary screw type is provided. The compressors, receivers and air drying plant are located in Service Building. There are two air receivers. Two air drying plants are provided. Normally two compressors are operating and one compressor will be in auto standby mode. The other compressor will be in manual standby mode. The compressors are connected to class-IV power supply during normal operation. Provision exists to connect all the four compressors to class-III power supply. However one compressor will be connected to class-III power supply during LOSP. Separate air bottles are provided for operation of important safety equipments like SGDHRS dampers. These bottles are always full and sufficient for three actuations. The success criteria are the availability of at least one compressor, one air receiver and one air dryer.

2.2 Summary

A brief description of various safety systems of PFBR is presented in this chapter. The level-1 full power internal events PSA described in chapter-3 is based on the description of the systems and success criteria given in this chapter.

Chapter-3 Level-1 Internal Events PSA

3.0 Objective

This chapter presents an advanced application of level-1 PSA for PFBR. The objectives of this study [3-1] are (i) to gain insights into the design of various safety systems and suggest design modifications to achieve the safety targets (ii) identification of core damage categories and (iii) obtain design inputs for future FBRs in the country by identifying dominant contributors. The scope of the present analysis is limited to risk at full power operating state due to internal events including offsite power failure events. The existing procedure for carrying out level-1 internal events PSA is applied to a pool type FBR for the first time to the author's knowledge. Since the plant is under construction, the outcomes obtained from such an analysis are used to make different design changes in the plant for different safety systems. The design changes are in the form of introducing diversity in redundant safety systems. Certain special class of internal events like load falling, missiles as well as internal fire and flood are not considered. The metric obtained will be Core Damage Frequency, and it is compared with other reactors to understand where the new design stands with respect to this safety parameter. An attempt is made to infer the balance of design through the relative contribution of different initiating event groups to the core damage frequency.

3.1 Approach

The approach followed for analysis is small event tree-large fault tree approach. The standards IAEA-SG-50-p4 and ASME RAS-2002 are referred [3-2, 3-3]. The fault trees are developed as far as possible by following immediate cause approach. Failure Mode Effects Analysis (FMEA) is done for limited important systems like shutdown system and Safety Grade Decay Heat Removal System to gain insight into failure modes and its impact on

safety. The following necessary technical elements of PSA as per ASME Standard [3-3] have been addressed and considered for analysis.

1. Initiating events analysis
2. Success criteria analysis
3. Systems analysis
4. Accident sequence analysis
5. Parameter estimation
6. Human reliability
7. Common Cause Failures
8. Quantification
9. Sensitivity and Uncertainty analysis

3.1.1 Initiating Events Analysis

The objective of the initiating events analysis is to identify and quantify events that could lead to core damage. An initiating event is an event that creates a disturbance in the plant and has the potential to lead to core damage, depending on the successful operation of the various mitigating systems in the plant. A judgment is required that any initiating event not identified in the analysis would make only a small contribution to the total risk. The initiating events whose frequency of occurrence is greater than 1.0 E−6 / ry are considered for this analysis. These events are grouped into 16 event groups as indicated in table-2. Grouping has been done in such a way that events in the same group have similar mitigation requirements [3-3]. The grouping of initiating events also takes into consideration the availability of different safety systems for different initiating events and their respective mission times. The frequencies of initiating events are based on reactor operating experience [3-4, 3-5]. The applicability of these initiating events to PFBR design is studied [3-6]. Some of the initiating events are specific to a particular type of plant. For such events, the initiating

event frequencies from similar plant designs are preferable. In the absence of such data, the initiating event frequency was calculated based on detailed fault tree modelling of individual systems as in the case of Roof Slab Cooling System and bio shield cooling system.

Table-2: Initiating Event Groups

No.	IE Group	IE Group Label	IE Freq (/yr)
1	Transients 1 (e-g: Withdrawal of one control rod)	TR1	0.3
2	Transients 2 (e-g: Unanticipated Reactivity Transients)	TR2	2.38
3	Global Loss of Flow 1 (e-g: Primary Sodium Pump Trip)	GLF1	2.1
4	Global Loss of Flow 2 (e-g: Secondary Sodium Pump Trip)	GLF2	2.5
5	Local Loss of Flow	LLF	0.01
6	Loss of Steam Water System 1	LSWS 1 (with OGDHRS)	1.67
7	Loss of Steam Water System 2	LSWS 2	1.8
8	Off-site power failure	PSS1	2
9	Failure of one Diesel Generator set during mandatory testing (with reactor on power)	PSS2	0.5
10	Loss of one division of class-I power supply	PSS3	0.01
11	Loss of one division of class-II power supply	PSS4	0.01
12	Total loss of cooling system of reactor vault concrete	OTH1	0.18
13	Loss of safety related service water system	OTH2	0.2
14	Loss of one SGDHR circuit during reactor on power	OTH3	0.25
15	Loss of compressed air system	OTH4	0.08
16	Planned shutdown	PSD	1.5
		Total	**15.49**

3.1.2. Success Criteria Analysis

The success criteria element defines the minimum number of working parts required for the successful performance of safety functions. For critical safety systems, support systems and operator action success criteria are defined with firm technical basis. For shutdown system the success criteria are arrived at after a detailed neutronic calculation for shutdown rod worth. For SGDHRS, the success criteria are arrived at after a detailed thermal hydraulic analysis. The success criteria of different systems mentioned in chapter-2 are derived based on detailed engineering analysis. The success criteria are based on electrical

load criterion for electrical systems and heat load criterion for heat removal systems like OGDHRS, Safety Related Service Water System, Roof Slab Cooling System and Biological Shield Cooling System. The success criteria for compressed air system are based on capacity and pressure requirements.

3.1.3. Systems Analysis

The systems analysis element identify the causes of failure and failure modes for each plant safety system in terms of the constituting parts in such a way that system-level success criteria, mission times, time windows for operator action and basis for the system logic model are obtained. The inter-system and intra system dependencies including Common Cause Failures (CCF) that could influence the system unavailability are identified in this exercise [3-3]. For PFBR, the important safety functions and the associated safety systems and safety related systems were identified and detailed fault tree modelling of these systems were carried out. Totally ten systems were identified which have safety and safety support functions. While modelling each system the support systems were also modelled along with human errors. A brief description of each of these systems and its function is explained in sections 2.1.1–2.1.10 in chapter-2.

3.1.4 Accident Sequence Analysis

The accident sequence analysis models the event sequence following an initiating event. For example, if the secondary sodium pump trips, there will be a flow reduction in secondary sodium circuit. The reduced flow in the secondary side leads to rise in primary sodium temperatures which are monitored by the respective sensors. Based on these sensor signal, reactor SCRAM action takes place. Once the reactor SCRAM takes place, the decay heat removal function is initiated. Event trees model this sequence of events. For each of the initiating event groups identified in Table-2, event trees were developed. The fault trees developed for each of the safety systems were attached with the event trees. The primary

sodium system is common to both OGDHRS and SGDHRS. The primary sodium system is modelled separately in event tree and unavailability values of OGDHRS and SGDHRS excluding primary sodium system were used in event tree. Since SGDHRS is a passive decay Heat Removal System, system failure due to inadequate performance needs to be considered. So its functional failure probability was calculated as a function of number of loops available [3-7] and these values are used in event tree. A typical event tree which includes the functional failure of SGDHRS is shown in Fig. 4. The inclusion of functional reliability analysis identifies additional accident sequences which can lead to core damage. The traditional event tree without including functional failures identifies branches B-4 and B-8 which can lead to core damage. The branches B-2, B-3, B-5, B-6 and B-7 are the additional branches which can lead to core damage due to process uncertainties.

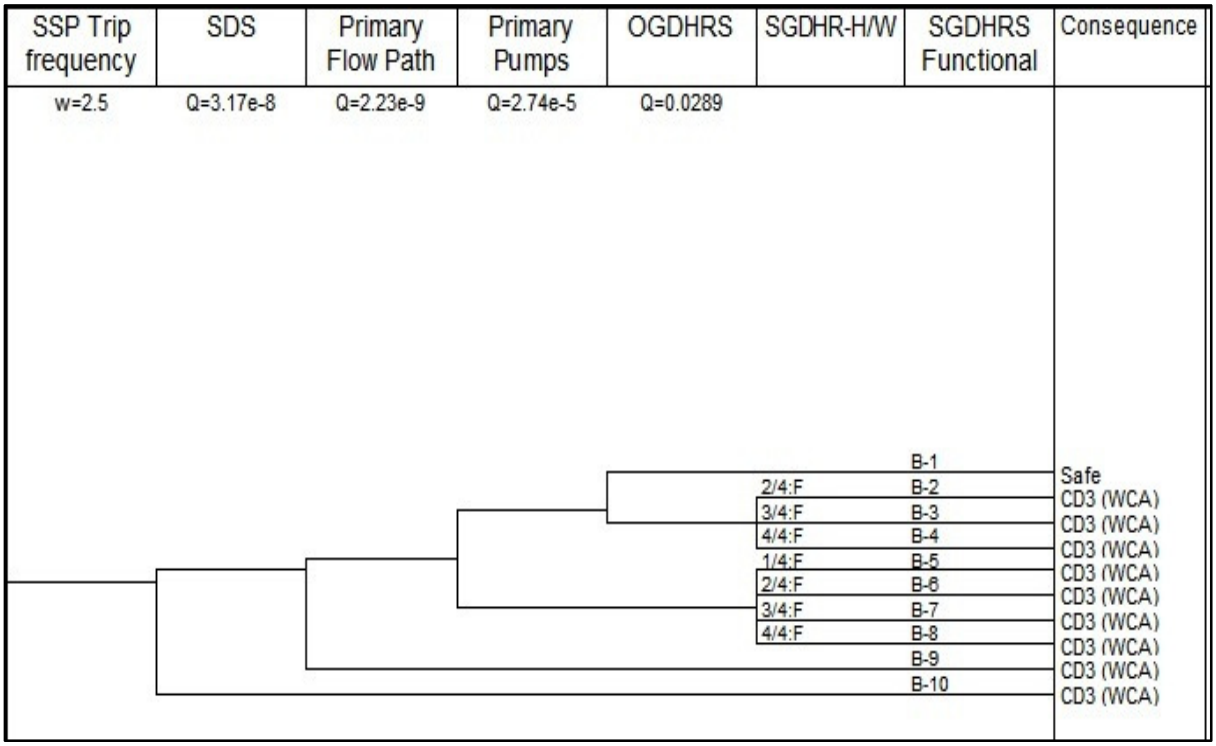

Fig.4: Event Tree with Functional Failures

Depending on the event sequence progression the end states of the event tree branches can be either safe or any one of the core damage categories namely few pin failures (CD1), Sub-assembly failure (CD2) and Whole Core Accident (CD3). The core damage categories

CD1 and CD2 appear in Local loss of flow event trees. Local loss of flow event tree has the maximum uncertainty associated with it because of the absence of credible initiating event frequency and lack of data on how the event progression will be and the time scale involved with it.

3.1.5 Parameter Estimation

The objective of the parameters estimation is to provide estimates of the data used to determine the probabilities of the basic events representing equipments failure and unavailability. Data, generic or plant-specific, should reflect the configuration and operation of plant. Unavailability of Components or systems due to maintenance or repair should be considered. Data uncertainties should be appropriately accounted for. Data used in this analysis is based on international reactor operating experience and Fast Breeder Test Reactor (FBTR) operating experience. For important safety systems like SDS, data from international operating experience reported in literature [3-8] and FBTR operating experience are combined with Bayesian update procedure. A relational database called FREDI (Fast reactor REliability Database-IGCAR) and an user interface called RiSSA (Reliability information System for Safety Analysis) was developed [3-9]. RiSSA has the capability to carry out Bayesian updating also.

3.1.6 Human Reliability

Human actions can affect the event sequence in a number of ways. Plant personnel can affect the availability and safety by inadvertently disabling equipment during testing, maintenance or calibration. The action taken by plant personnel after the occurrence of an initiating event can mitigate or increase the severity of the initiating event. The analysis of human reliability is important in the safe operation of a nuclear power plant. The objective of human reliability analysis is to ensure that the impacts of plant personnel are reflected in the assessment of overall risk. For PFBR level-1 PSA study Accident Sequence Evaluation

Program (ASEP) Human reliability analysis procedure has been selected [3-10] for important safety systems like SDS. The human error in threshold setting of SDS1 and SDS2 are considered independent as threshold setting of one system is hardware based and the other one is software based. Also threshold setting is done by different set of persons. For other systems a screening value of 1.0 E−3 is used for human error probability [3-11].

3.1.7 Common Cause Failures

Common Cause Failures analysis is for those groups of components that may be subject to coupled failures. Common cause events are a subset of the class of dependent events whose causes are not normally explicitly modelled as basic events in the system logic models. In principle, the logic models can be developed further to include a large number of basic events that corresponds to common cause events. Each common cause basic event in such a logic model would be indicated as resulting failure of two or more components. In this analysis of Level-1 PSA of PFBR beta factor and alpha factor model [3-12] has been used to perform CCF. CCF group has been identified by having similar components in similar environmental condition. The beta factor model is used when the level of redundancy is two. Alpha factor model is used when the level of redundancy is greater than two. In some cases, when failure data is not available to estimate alpha factors, beta factor model is used as a conservative estimate. In this study, beta factor model is used in shutdown system, Safety Grade Decay Heat Removal System, etc. Alpha factor model is used in Safety Related Service Water System. The beta factors are arrived at after a detailed procedure considering the design features, operation and maintenance procedures of the individual safety systems. This method is applied to shutdown system and Safety Grade Decay Heat Removal System.

3.1.8 Quantification

The fault trees developed during systems analysis stage are quantified using the data collected in parameter estimation. The unavailability estimated for different safety systems

of PFBR are given in table-3.

The fault trees are connected with the accident sequence models developed using event tree. The initiating events identified in section 3.1.1 and their frequencies are used for event tree quantification. The frequencies of different core damage categories are quantified. The Core Damage Frequency (CDF) is calculated as a sum of contributions from core damage categories CD2 and CD3. Significant contributors to CDF are identified such as initiating events, accident sequence and basic events. These results reflect the design, operation and maintenance of the plant.

Table-3: System Analysis Results

No.	System	Unavailability
1	Shut Down System (Global Fault / Local Fault)	3.2 E-8 / 3.3 E-8
2	Operation Grade Decay Heat Removal System (OGDHRS)	3.0 E-2
3	Safety Grade Decay Heat Removal System (SGDHRS)	1.0 E-7 *
4	Class III Power Supply System-6.6 kV Bus Section level	2.5 E-6
5	Safety Related Service Water System (SRSWS)	4.8 E-4
6	Class I Power Supply System -48 V division level	1.2 E-6
7	Class II Power Supply System- Division Level	9.0 E-7
8	Compressed Air System	6.0 E-5**
9	Biological Shield Cooling System	7.6E-4
10	Roof Slab Cooling System	5.7E-4

* - Calculated for a mission time of 720 h ** - Calculated for a mission time of 24 h

The low unavailability values for shutdown system and safety grade decay heat removal system are achieved mainly by the introduction of diverse features between two shutdown systems and the different loops of SGDHRS. The unavailability values without diverse features are greater than the present values.

3.1.9 Sensitivity and Uncertainty Analysis

The purpose of sensitivity analysis is to determine the sensitivity of the Core Damage Frequency to component failures and human errors and to address those modelling assumptions suspected of having a potentially significant impact on the results. These

assumptions are generally in areas where information is lacking and heavy reliance must be placed on the analyst's judgment.

The objective of uncertainty analysis is to provide quantitative measures of uncertainties in the results of PSA, namely the frequency of core damage, the frequency of accident sequence categories and unavailability of various safety systems.

3.2 Salient Feature of the Study

The salient feature of the study is the inclusion of functional reliability analysis of SGDHRS in accident sequence analysis. SGDHRS is nearly a passive decay Heat Removal System which is sensitive to uncertainties in its governing parameters. So functional reliability analysis of SGDHRS is carried out for various loop configurations and included in the event tree. The method of functional reliability [3-7] involves (i) identification and quantification of the sources of uncertainties, (ii) propagation of the uncertainties through thermal hydraulic models and (iii) estimation of functional failure probability. Functional Reliability Analysis is further explained in section 6.4 of chapter-6.

3.3 Insights from this study

3.3.1 Common Cause Failure (CCF) Modelling

When the minimal cut sets of various safety systems are analyzed, it is observed that invariably the unavailability of CCF events dominate the system unavailability. This can be inferred from Table-4. This suggests a simplified but quicker analysis considering only CCF and this has been performed for three example systems namely (1) Shut Down System (SDS), (2) Safety Grade Decay Heat Removal System (SGDHRS) and (3) Class III Power Supply System (DG) and results checked with detailed analysis. For shutdown system the dominant cut sets are Common Cause Failure of Control Safety Rods (CSR) and Diverse Safety Rods (DSR). The unavailability of SGDHRS is dominated by Common Cause Failure of

intermediate circuit pipe line leak and CCF of stack. CCF of DG fail to start and fail to run dominate the unavailability of Class III power supply system.

Assuming that the CCF of redundant components in the above systems can be represented by Beta factor Model [3-12], a sensitivity study on the parameter beta was carried out for highly dependent components in redundancy (β = 10%) and completely independent components (β= 0%). The unavailability of the example systems (i) for the case used in Level-1 PSA, (ii) with highly dependent components and (iii) with completely independent components in redundancy are listed in Table-5. As expected from CCF theory, this study makes it clear that in safety systems employing high level of redundancy as in nuclear power plants, the modelling of CCF plays a crucial role in safety system unavailability calculations. A careful choice of CCF model parameters based on plant specific design, operation and environment inputs are the best way out to prevent over/under prediction of Core Damage Frequency (CDF). A resource saving method of reliability analysis will be to calculate CCF only.

Table-4: CCF Contribution to Total Unavailability

No.	System	Unavailability	Unavailability Due to CCF	CCF % in Total Unavailability of The System
1	SGDHR	7.27E-8	5.85E-8	80.46 %
2	SDS	3.17E-8	3.10E-8	97.79 %
3	DGSPLY	3.20E-3	2.33E-3	72.81 %

Table-5: Sensitivity of System Unavailability to β

No.	System	Unavailability (in Level1 PSA)	Unavailability With β = 10%	Unavailability With β = 0%
1	SGDHR	7.27E-8	1.48 E-4	9.70 E-12
2	SDS	3.17E-8	3.02 E-7	7.13 E-10
3	DGSPLY	3.20E-3	5.91 E-3	1.24 E-3

3.3.2 Plant Design

The relative contribution of various event groups to CDF is more or less balanced as shown in Fig. 5, implying that the major design features are balanced. The contribution from

Loss of OffSite Power (LOSP) is ~23% and from Loss of Steam Water System equipment is about 22%. The likelihood of CDF to have been caused by any of the other events like loss of flow in primary, transients etc. is about 55%. The examination of dominant cut sets indicates that further reduction in CDF, especially due to loss of offsite power event, is possible by use of fully diverse shutdown systems and further enhancing the reliability of SGDHRS. The CDF contribution due to LOSP event and shutdown system failure is given by the expression $\lambda_{LOSP} \times P_{SDS.}$ λ_{LOSP} is the initiating event frequency for OffSite Power events and P_{SDS} is the failure probability of Shutdown system. P_{SDS} can be reduced by using diverse or independent shutdown devices. The remaining contributors are in the residual risk category, which require further data / operating experience for making a definite case.

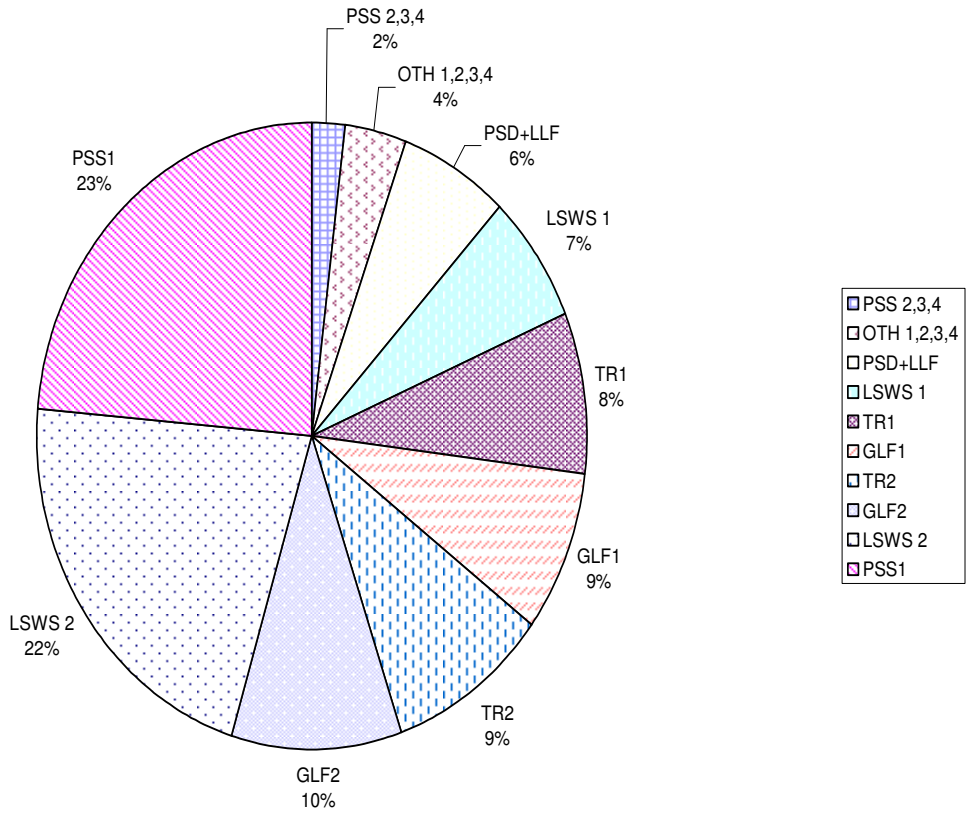

Fig. 5: CDF Contribution from Initiating Event Groups

3.4 Results and Discussion

The estimated Core Damage Frequency of PFBR is ~0.9 E–06 / ry. The contribution to CDF from Loss of Offsite Power (PSS1 event group) is ~23% while Loss of Steam Water System (LSWS2) contributes ~22%. The CDF estimate is compared with CDF estimates of other reactors and is presented in Table-6 [3-13, 3-14, 3-15]. The system reliability results are given in Table-3. The initiating event groups and contribution to CDF from each of the initiating event groups are given in Table-7.

Table-6: CDF estimates of Other Reactors

Reactor	Internal Events CDF (/y)	Dominant Factor
EBR- II	1.6E-6 (Ext 3.6E-6)	LOSP, Long Term DHR
CRBRP	3.7E-6 (Ext 3.2E-5)	-
UK EPR	0.6E-6	20% LOCA, 20%ATWS 15% LOSP, 20% secondary transients.
AP-1000	0.24E-6	-

Level-1 Probabilistic Safety Analysis of PFBR has been carried out and the estimated CDF is ~0.9E–06 / ry. One of the major contributions from this study is the introduction of diversity in the two shutdown systems of PFBR and introduction of diversity in the different loops of SGDHRS. A CDF of the order of 1.0E-06 /y is achieved mainly due to the introduction of these diverse features in design. Another significant contribution of this study is the inputs obtained for future FBR designs. The results are dominated by the contribution from the initiating event groups PSS1 (Loss of Off Site Power events) and LSWS2 (Loss of Steam Water System). A significant reduction in these contributions will reduce the CDF estimate and hence reduced risk from the plant. The process uncertainties quantified through functional reliability analysis is combined with system hardware reliability using event tree. This leads to the identification of additional accident sequences which can lead to core damage. These sequences might have been missed out if the event tree is developed in

Table-7: CDF Contribution from Initiating Event Groups

IE Group	SGDHR MT (Hrs)	CD3 Frequency (/yr)	CD2 Frequency (/yr)
TR1	168	7.36E-08	
TR2	168	8.28E-08	
GLF1	720	7.58E-08	
GLF2	720	9.02E-08	
LLF	NA	2.02E-09	1.97E-09
LSWS 1 (with OGDHRS)	720	6.02E-08	
LSWS 2	720	1.92E-07	
PSS1	24	2.10E-07	
PSS2	24	1.73E-08	
PSS3	24	3.45E-10	
PSS4	24	3.45E-10	
OTH1	720	6.48E-09	
OTH2	168	6.98E-09	
OTH3	168	9.42E-09	
OTH4	72	8.42E-09	
PSD	720	5.40E-08	
Total		**8.90E-07**	**1.97E-09**

traditional success / failure branches. The maximum relative contribution to the total CDF from an individual initiating event group is less than 25% implying that the major design features are balanced. For high redundant systems approximate reliability estimates or bounds can be obtained very efficiently by modelling only CCF components and first order component failures if any.

This Page is left blank

Chapter-4 Level-1 External Events PSA

4.0 Introduction

A level-1 external event PSA quantifies the Core Damage Frequency due to external causes like earthquakes, flood, fire etc. The external events PSA differ from internal events PSA in the following aspects. Treatment of dependent failures is one of the significant differences from internal events PSA. The operating conditions of the plant are significantly different from internal events PSA due to the increased stress levels on operators and possible lack of accessibility to many important areas of the plant. These factors make the external events PSA a complex one. Any external events PSA consist of three elements. The first element is the hazard analysis which quantifies the frequency of exceedence of different levels of hazard variable. The second element is the fragility quantification of different safety systems, structures and components for different levels of hazard variable. Fragility is the conditional probability of failure of a component / system for a given hazard level. The third element is the integration of hazard and fragility through plant logic models. Seismic PSA and flood PSA of PFBR were carried out. These studies are the first application of external event methodology to a pool type FBR. Hazard analysis is one of the important steps in external event analysis. The plant core damage frequency is estimated with the hazard curve as the basis. This requires the calculation of frequency of exceedence over the range of hazard variable. The ground motion parameters of the plant are specified for two different levels and its associated exceedence frequencies. This is not sufficient for the quantification of core damage frequency. The seismic hazard analysis in this thesis calculates frequencies of exceedence over the range of hazard variable. In this thesis, the seismic hazard analysis is carried out with a new attenuation relationship developed for the region of interest instead of the exponential relationships used in different studies. The probabilistic seismic hazard analysis in this chapter validates the design basis ground motion parameters of the PFBR

plant obtained through deterministic seismic hazard analysis. The study on tsunami hazard analysis is improved by including local bathymetry into the model. The inclusion of bathymetry significantly alters the tsunami wave run up height predictions. This improved model predicts the observed tsunami wave run up height (during Dec 26th 2004) at the site in a better way as compared to an earlier study. Further in this study, two different accident sequence assessment models for external flood PSA are compared with respect to resources and correctness of results. These studies which are carried out as part of external event PSA are explained in this chapter.

4.1 Seismic PSA of PFBR

The objective of this analysis is to estimate the Core Damage Frequency due to seismic events. The general methodology to carry out seismic PSA is explained in [4-1, 4-2]. The scope and level of detail of this study is as per the capability category I in ASME standard [4-2]. This implies the relative importance of contributors can be identified at system or train level. Site specific seismic hazard analysis is carried out using the attenuation relationship for peninsular India. A method to use whatever little data obtained from seismic qualification experiments is identified. Plant specific data for components like main vessel and roof slab are used. Generic data reported in literature are used for components for which plant specific data are not available. This study does not address the secondary events of earthquakes like load falling, quake induced fires and internal flooding due to collapse of tanks etc. The probabilistic seismic hazard analysis, fragility analysis, integration of seismic hazard and fragility and quantification of core damage frequency of PFBR [4-3] are explained in subsequent sections.

4.1.1 Probabilistic Seismic Hazard Analysis

The objective of this analysis is to develop hazard curves which quantify the frequency of exceedence for different levels of hazard variable. Seismic hazard at a site is

represented by different ground motion parameters like Peak Ground Acceleration (PGA), Peak Ground Velocity (PGV) or Peak Ground Displacement (PGD). The damage to structures is known to correlate with PGA for medium magnitude earthquakes and with PGV for high magnitude earthquakes. PGA is not a detailed measure of ground shaking but considered adequate for earth quake engineering purposes. The methods of assessing seismic hazard at a site consist of enumerating potential sources from historical records which are within a distance of less than 300Km. The consideration of 300Km as the radius is the normal practice followed in seismic hazard analysis [4-4]. Earthquake data for the present analysis is for the period 1504-2001 AD [4-5, 4-6]. Earthquakes with moment magnitude greater than or equal to three have been considered for this analysis. Earthquakes less than this magnitude are unlikely to cause structural damage and are not considered in the present analysis. There are a total of 271 earthquakes with moment magnitude greater than three reported in these literatures. Seismic Hazard analysis involves three steps. The first step is the seismic activity characterisation of a region and identification of seismic sources. The second step is the modelling of earthquake occurrence and calculation of mean annual rate of exceedence of ground motion parameter over a reference value for different seismic sources. This step requires modelling of the attenuation. The third step is deriving the hazard curve. These three steps are explained in the subsequent paragraphs briefly.

The seismic activity of a region is characterised by the Gutenberg-Richter earthquake recurrence relation as in equation (4-1) [4-6].

$$Log_{10} N = a - bM \qquad (4\text{-}1)$$

N is the total number of earthquakes of magnitude equal to or greater than M in a year. The parameters a and b in equation (4-1) are the regional seismic parameters. Different values of parameters are reported in literature for Kalpakkam region. The difference is due to the different earthquake catalogues considered for these studies. The parameter b characterises

the seismic activity of a region as it gives the change in number of earthquakes with magnitude. A value of 0.5989 [4-6] is used for the parameter b as it gives a slightly conservative estimates for number of earthquakes on the higher magnitude side. The number of seismic sources considered in this study is 28 within 300Km radius from Kalpakkam. These sources were identified from online seismotectonic atlas available in Geological Survey of India website [4-7]. This atlas is used to calculate the source to site distance. The maximum earthquake magnitude from a specific fault is obtained from [4-8].

The occurrence of an earthquake in a seismic source is assumed to follow a poisson distribution. The probability that a ground motion parameter X at a given site will exceed a specified level x during specified time T is given by equation (4-2).

$$P\ (X > x) = 1 - e^{-\eta(x)T} \qquad (4\text{-}2)$$

η(x) is the mean annual rate of exceedence of ground motion parameter X, with respect to x. The mean annual number of events $\eta_l(x)$, in which a ground motion parameter X (peak ground acceleration in this study) exceeds a value x at the site because of an earthquake on the l^{th} seismic source is given by equation (4-3).

$$\eta_l(x) = \sum_i \eta_l P_l(m_i)\ P_{X|m_i}(x) \qquad (4\text{-}3)$$

η_l in equation (4-3) is the mean annual number of earthquakes on the l^{th} source. $P_l(m_i)$ is the conditional probability of earthquake on the source having a magnitude equal to m_i. $P_{X|mi}(x)$ is the probability with which the ground motion parameter X exceeds a value x given an earthquake of magnitude m_i. Equation (4-3) is applicable to seismic point sources in which the source to site distance is a constant. The general expression with seismic line sources where source to site distance is also a random variable is given in [4-9]. The product $\eta_l P_l(m_i)$ in equation (4-3) represents the number of earthquakes of magnitude m_i per year from the l^{th} seismic source. This is calculated from the magnitude recurrence model [4-3, 4-8].

Estimation of the other term P_{Xlmi} (x) in equation (4-3) needs a model to relate the ground motion parameter with earthquake magnitude and distance. This model is known as the attenuation relationship.

The significant difference of this study from several other studies is the use of attenuation relationship developed for peninsular India [4-10]. Most of the other studies use the exponential attenuation relationship. The attenuation relation for peninsular India is given by equation (4-4).

$$\ln(x) = a_1 + a_2(M-6) + a_3(M-6)^2 - \ln(D) - a_4 D + \ln(\in) \qquad (4\text{-}4)$$

x represents the peak ground acceleration and M is the moment magnitude in equation (4-4). D is the hypo central distance and ϵ is the error associated with regression. a_1,a_2,a_3,a_4 are the coefficients of the attenuation relationship. Equation (4-4) calculates the PGA at bedrock level. Due to variations in local site conditions, the surface level PGA could be different from bedrock level. In the present study it is assumed that the bedrock level PGA is equal to the surface level PGA.

The hazard curves generated for Kalpakkam based on the above mentioned steps are shown in fig.6. The annual frequency of exceedence for different values of PGA is reported. The three curves give the annual frequency of exceedence at three different probabilities of exceedence 5%, 50% and 95%. The PGA values for Operation Base Earthquake (OBE) and Safe Shutdown Earthquake (SSE) values obtained for PFBR plant site through deterministic seismic hazard analysis is 0.078g and 0.156g. The frequencies of occurrence of these levels of earth quake are 10^{-2} /y and 10^{-4} /y respectively. These frequency assignments are judgement based and they are not obtained through rigorous analysis. The basis for the judgement is past seismic events observed in the region. The results obtained from probabilistic seismic hazard analysis in the present study are comparable with the values obtained from deterministic seismic hazard analysis at 50% probability of exceedence level.

The OBE level earthquake occurs with a frequency of ~10^{-2}/y in the present analysis. The SSE level earthquake occurs with a frequency of approximately to 8×10^{-4} /y in the present analysis with a limiting value of 0.17g. The high frequency of exceedence for SSE level is due to the conservative assumptions involved in the analysis as explained in section 4.1.2. SSE level earthquake is important because all safety systems have to be qualified for this earthquake level.

4.1.2 Assumptions used in Seismic Hazard Analysis

The maximum earthquake magnitude considered from each source in the analysis is conservative. Conventionally the maximum magnitude for analysis is taken as 0.5 units more than the maximum magnitude observed from the seismic fault. In the present analysis the maximum magnitude for analysis is taken as 1.0 unit more than the maximum magnitude observed from the fault. The shortest distance from the seismic fault to the site is taken as source to site distance. Conservative parameters of Gutenberg-Richter relationship are used in the present analysis.

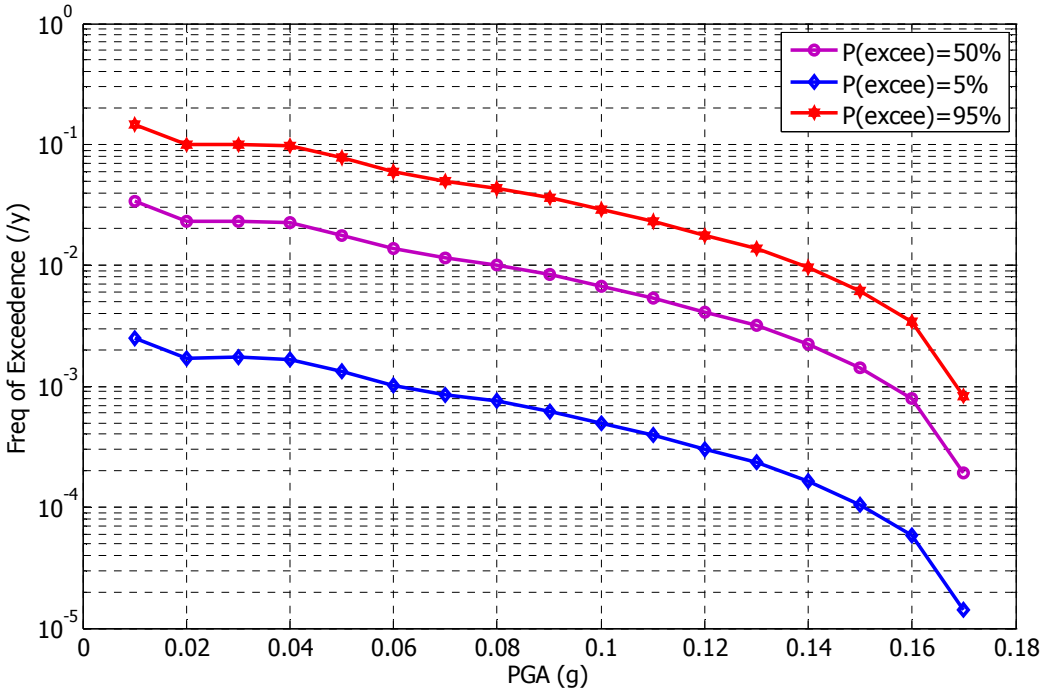

Fig.6: Hazard Curves for Kalpakkam for different exceedence probabilities

4.1.3 Seismic Fragility Analysis

Seismic fragility of a structure or equipment is defined as the conditional probability of its failure for a given value of the seismic response parameter. Seismic fragilities are needed in a Probabilistic Safety Assessment to estimate the failure probabilities of different safety systems. The different safety systems of PFBR are explained in chapter-2. As described in the PRA procedures guide [4-9], there are two approaches for evaluating seismic fragilities : i) the zion method wherein the fragility is expressed as a function of a global ground motion parameter (e-g: peak ground acceleration) and ii) Seismic Safety Margins Research Program (SSMRP) method, which defines the fragility in terms of a local response parameter. Zion method is used in the present study for fragility analysis.

4.1.3.1 Zion Method Fragility Model

The fragility for a component corresponding to a particular failure mode can be expressed in terms of the best estimate of the median ground acceleration capacity A_m and two random variables [4-11]. Thus the ground acceleration capacity, A is given by equation (4-5).

$$A = A_m \Psi_R \Psi_U \qquad (4\text{-}5)$$

In equation (4-5), Ψ_R and Ψ_U are two random variables with unit medians. Ψ_R represents the inherent randomness about the median and Ψ_U represents uncertainty in the median value. In this model it is assumed that both Ψ_R and Ψ_U is log normally distributed with logarithmic standard deviations α_R and α_U respectively. The quantification of fault trees in the plant system and sequence analysis, requires the uncertainty in fragility needs to be expressed in terms of a range of failure probabilities for a given ground acceleration.

The probability of failure P at any non-exceedence probability level S can be derived as,

$$P = \phi\left(\frac{\ln\left(\frac{a}{A_m}\right)+\alpha_U\phi^{-1}(S)}{\alpha_R}\right) \qquad (4\text{-}6)$$

A_m is the median ground acceleration capacity and a is the PGA value at which fragility is to be evaluated. ϕ and $\phi^{-1}(\ )$ are the standard Gaussian cumulative distribution function and its inverse respectively.

4.1.3.2 Fragility Evaluation of Components

A list of components is to be selected for fragility evaluation. Selection of components or systems for fragility evaluation is an iterative process with close interaction between systems analyst and structural analyst. The selection of components for this study is guided by the accident sequences identified for the internal events. There are around 188 components and structures identified for PFBR [4-3]. These 188 components are grouped into groups based on the mountings and supports for these components and its importance in the context of a seismic event based on judgement. For example, electronic components may be mounted on single instrumentation panel and that panel alone is considered in this analysis. Apart from identifying the components for fragility analysis, it is also important to identify the failure modes for each component. A clear definition of what constitutes a failure must be arrived at which is agreeable to both structural analyst and the systems analyst. Several modes of failure may have to be considered and fragility curves may have to be generated for each of these modes. It may be possible to identify the failure mode which is most likely to be caused by the seismic event by reviewing the equipment design and to consider only that mode. Otherwise, fragility curves are developed based on the premise that the component could fail in any one of all potential failure modes. It is assumed that the component could fail in any one of the possible failure modes for most components in this study.

The other part of fragility evaluation is the data requirement. From equation (4-6), it is clear that the parameters required for fragility evaluation of components are A_m, α_R and α_U. The data for the components are generally obtained from analysis and testing. The analysis becomes more plant specific as more fragility data is generated from specific design inputs and analysis results. Site specific structural analyses are more suitable for components such as civil structures, reactor vessel, core assembly, roof slab and structural failure of equipment due to anchorage and support failures. Site specific data is used for main vessel and roof slab which are obtained from detailed structural analysis [4-12]. The factor of safety and margin above the SSE level earthquake were derived from such an analysis. The median acceleration capacities estimated from this analysis for main vessel and roof slab are 0.481g and 1.284g respectively. The qualification tests conducted for instrumentation panels are used to estimate plant specific data of instrumentation panels. The methodology is explained in section 4.1.3.3. In the absence of plant specific data, the generic data from past seismic PSA studies reported in literature are used [4-13]. However the generic data is to be screened for applicability to FBR. The screening is carried out based on component type, size and design aspects to the extent possible. The generic data source reports the range of median acceleration capacity, α_R and α_U for different components. Log normal distribution is fitted to the given median acceleration capacity range and the median of the fitted distribution is used as median acceleration capacity (A_m) of the component.

4.1.3.3 Methodology to Compute Median Acceleration Capacity from Test Data

Some PFBR components like instrumentation panels of shutdown system are subjected to shake table tests. The objective of this test is to qualify the component for Safe Shutdown Earthquake (SSE) level of PFBR. Few components are tested. In the case of PFBR shutdown system, one instrumentation panel is subjected to shake table test [4-14]. The instrumentation panels are mounted at different elevations. Based on the Safe Shutdown

Earthquake (SSE) level of the plant, the spectra at different elevations were derived. The instrumentation panel is subjected to the spectrum (acceleration) at the given elevation. After the test, the panel is subjected to inspection for any potential damage. The Shutdown System panel which is subjected to the test did not fail at the SSE level acceleration of 0.156g. Based on this information median acceleration capacity of the panel is to be derived. Assuming that the tested acceleration level corresponds to High Confidence Low Probability Failure (HCLPF), the median acceleration capacity can be derived. In this calculation the acceleration level 0.156g corresponds to non-exceedence probability of 0.95, and failure probability of 0.05.

HCLPF method assumes that P and S are known in equation (4-6). a is the PGA value at which the test is performed. α_R and α_U are taken from literature. Rearranging equation (4-6), the median acceleration capacity can be calculated from equation (4-7).

$$A_m = a/\exp\left(\alpha_R \phi^{-1}(P) - \alpha_U \phi^{-1}(S)\right) \qquad (4\text{-}7)$$

The median acceleration capacity calculated by the above procedure for shutdown system instrumentation panel is used for the fragility analysis. The calculated median acceleration capacity for shutdown system instrumentation panel is 0.47g.

4.1.3.4 Evaluation of System Fragility from Component Fragilities

The system fragility analysis is the evaluation of system failure probability as a function of Peak Ground Acceleration (PGA) from individual structure and component fragility curves. Fault trees are developed for important safety systems of PFBR. The following assumptions are made in fault tree development.

a. In fault tree, components are modelled up to cabinet/ panel or subsystem levels. The detailed modelling of systems up to the component level is not considered.

b. The redundancy at train or component level is not considered in this analysis as most of the redundant trains or components have identical acceleration capacities. If there is a

seismic specific redundancy then the train or component with highest acceleration capacity will be modelled e-g: DSR of ShutDown System (SDS).

c. The Human Error Probability (HEP) is assumed to be one in a seismic scenario. Also it is assumed that there is loss of offsite power during a seismic event.

The fragility of each component is calculated at different PGA levels and each time fault tree analysis was carried out to quantify the system fragility. The analysis is repeated for various non-exceedence probability values.

4.1.4 Accident sequence Models

The accident sequence models are developed using event trees. Seismic event with specific PGA value is the initiating event. The important safety functions are shutdown and decay heat removal. These safety functions depend on the structural integrity of important structures like core support structure, roof slab etc. The effect of secondary events like load falling on safety critical equipment is not assessed in the present analysis. The accident progression modelled in event tree leads to various end states. The various end states are given below.

i) PLOHR- Protected Loss of Heat Removal - Core Damage due to failure of decay heat removal after shutdown

ii) ULOF - Unprotected Loss of Flow - Core Damage due to failure in shutdown system

iii) LOPI- Loss of piping integrity - Core Damage due to failure in primary circuit

iv) LOCC- Loss of Core Configuration - Core Damage due to either failure of core support or collapse of top shield.

The total Core Damage Frequency (CDF) is the sum of all contributions from the above mentioned end states. The event tree developed for seismic PSA of PFBR is shown in fig.7. The results in fig.7 corresponds to 50% Non-exceedence probability for Safe Shutdown Earthquake (SSE) PGA of 0.156g. The contribution to CDF from each of the end states is

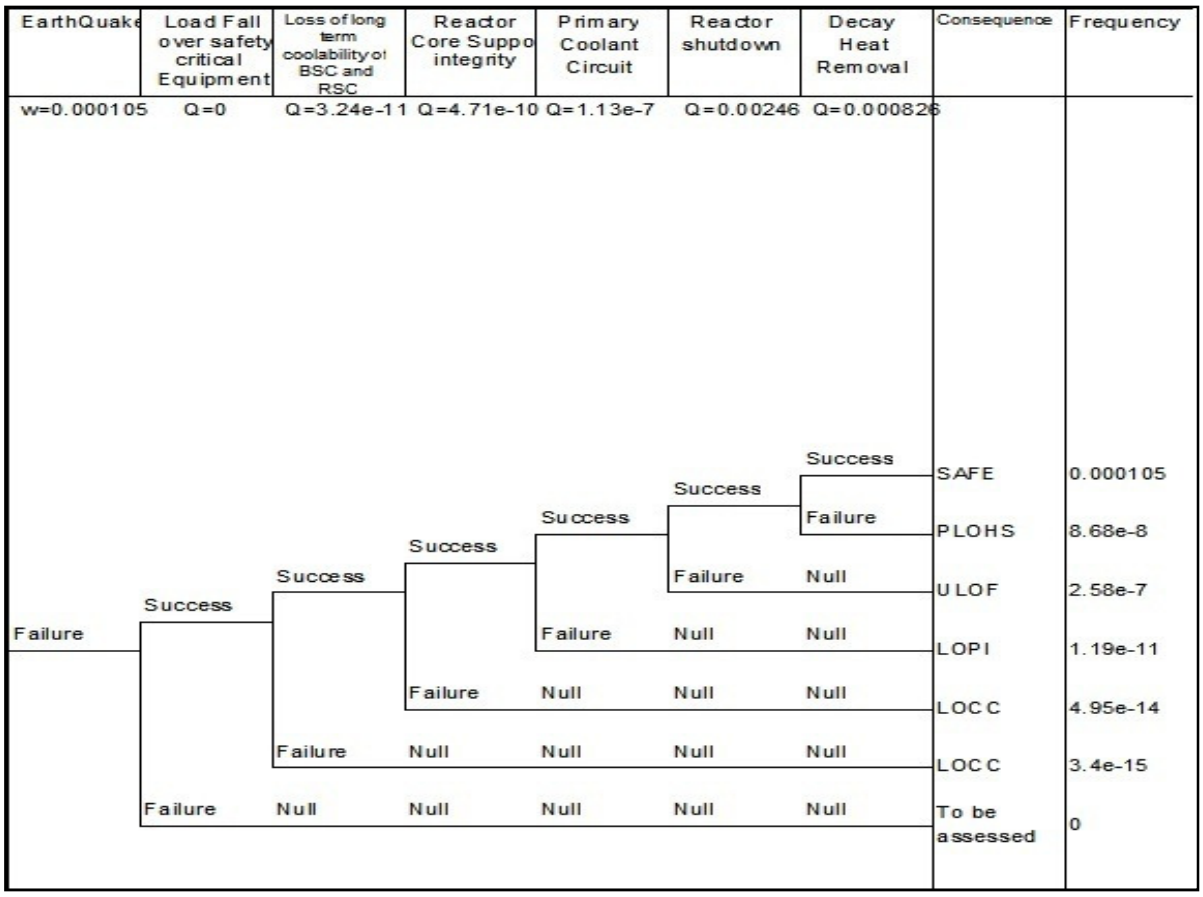

Fig.7: Event Tree for Seismic PSA

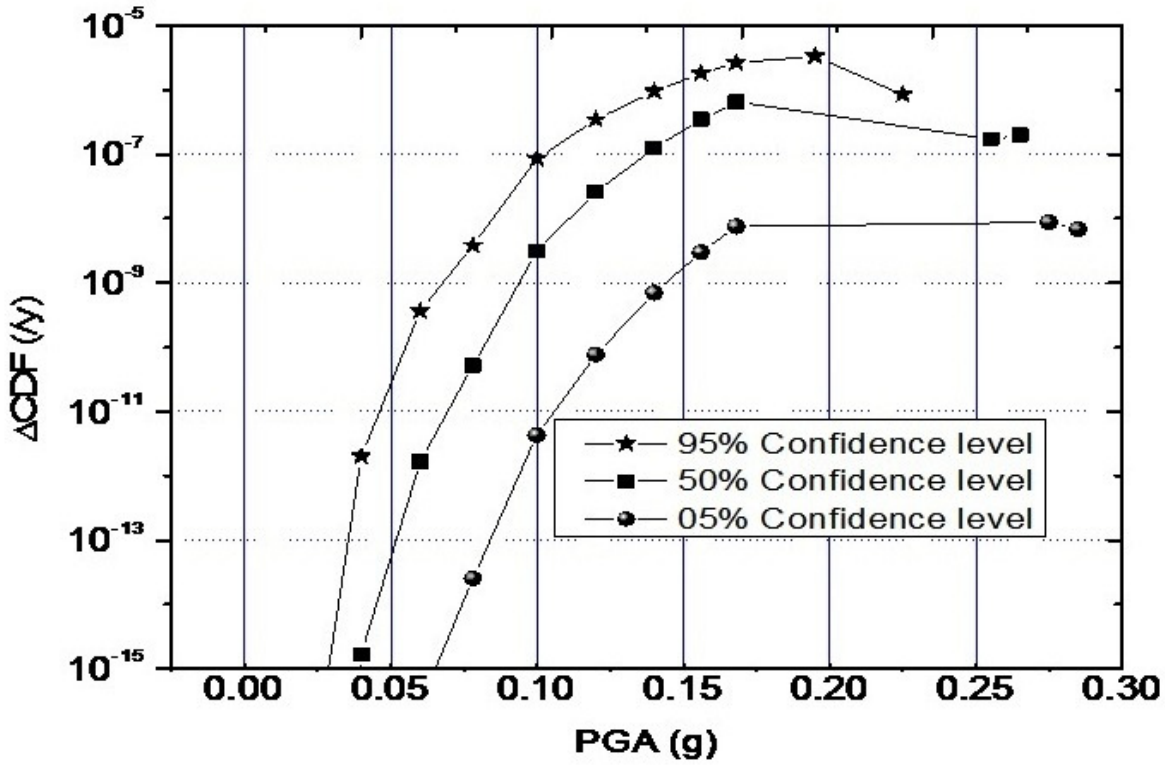

Fig.8: Core Damage Frequency as a Function of Peak Ground Acceleration

shown in fig.7 for the above mentioned case. The major contributor to CDF is the ULOF end state in this case.

4.1.5 Results and Discussion

The results from seismic probabilistic safety analysis are shown in fig.8. The CDF for different PGA values are given for 5%, 50% and 95% confidence levels. The results indicate that the significant contribution to core damage frequency from seismic hazard input is from 0.1 g to 0.25 g and above. The hazard region above 0.2 has large uncertainty. The total CDF values for 5%, 50% and 95% confidence levels are 1.0E-08 /y, 1.5E-06 /y and 1.0E-05 /y respectively. The dominant contributor to CDF at SSE level earth quake of PFBR for 50% confidence level is instrumentation panels. This may be due to the methodology adopted for deriving the median acceleration capacity of instrumentation panels. Detailed engineering analysis is required to assess the median acceleration capacity of instrumentation panels.

4.2 External Flood PSA of PFBR

The Fukushima accidents highlighted the potential of external flooding to cause core damage of a Nuclear Power Plant (NPP). Identifying the weak links of a plant during a flooding event is an important step towards reducing the risk from such flooding events [4-15, 4-16]. The presence of water in many areas of the plant may be a common cause failure for safety related systems. The unavailability of emergency power supply systems, electric switchyard and the possibility of losing the external connection to the electrical power grid may affect the vital safety systems like decay heat removal system. Considerable damage can also be caused to safety related structures, systems and components by the infiltration of water into internal areas of the plant, induced by high flood levels. The External Flood Probabilistic Safety Analysis (EFPSA) for PFBR is carried out with the following objectives.

- Evaluate the plant response of PFBR under different flooding scenario
- Determine the key contributors to

1. Core Damage Frequency (CDF) due to external flooding

2. Spent fuel damage frequency (SDF) due to external flooding

- Understand the accident progression following a flooding event

The EFPSA of PFBR consists of several important steps like hazard analysis, plant walk down, system modeling and identification of essential structures, systems / components, response analysis, fragility analysis, accident sequence modeling and quantification of core damage frequency. Two studies carried out as part of EFPSA of PFBR are reported in this thesis. The first study is the tsunami hazard analysis for PFBR site. The major contributor to flood hazard at PFBR site is tsunami. PFBR site is affected by the December 26th 2004 tsunami event. Hence it is very important to quantify the tsunami hazard. The previous study on tsunami hazard analysis does not consider the local bathymetry. The tsunami wave run up height is under predicted by such a model as compared to the run up heights observed during the 2004 event. The present study combines two different studies to improve the tsunami wave run up height predictions. The second study is the comparison of two different accident sequence modeling methodologies for EFPSA of PFBR. It is shown that both approaches lead to identical expressions for core damage frequency. This study enables the use of existing accident sequence models developed for level-1 internal events PSA with some modifications. It reduces the accident sequence model development effort and time for EFPSA of PFBR. These two studies are explained in the subsequent sections.

4.2.1 Probabilistic Tsunami Hazard Analysis

The flood hazard analysis for Kalpakkam site includes three natural phenomena, i) Tsunami ii) Storm surge and iii) Local precipitation. Hazard curves are to be developed for each of these phenomena. Kalpakkam site specific Tsunami hazard analysis is reported in [4-17]. A brief description of this study and the drawbacks of this study with respect to the observed tsunami event in the year 2004 are explained in section 4.2.1.1. The improved

method by including the local bathymetry of Kalpakkam site is presented in section 4.2.1.2 [4-18].

4.2.1.1 Tsunami Hazard Analysis for Kalpakkam

The study area includes part of Southern Indian Peninsula, the Andaman and Nicobar Islands, Sri Lanka and Indonesia. In the region of study, the nearest fault is the buried ridge in the Indian Ocean about 1100 Km from Kalpakkam. The other faults in the Sumatra and Andaman region lie in the range of about 1400-2000 Km. Earthquake data for a period from 1815 to 2006 were collected. There are twenty tsunami events in this region between the years 1847 and 2006. The Tsunami data includes tsunami source location, magnitude of causative earthquake, run-up heights recorded at various stations for a particular event. There are 718 run-up data reported for 26 December 2004 tsunami event. The number of earthquakes of magnitude greater than or equal to M per year is calculated by the Gutenberg-Richter relation for the study area. The Tsunami run up height (h) as a function of earthquake magnitude (M) and distance (D) is modelled by equation (4-8).

$$h = c_1 \exp(c_2 M)\,(D+\in)^{-c_3} \qquad (4\text{-}8)$$

c_1, c_2 and c_3 are the parameters which are determined by regression analysis. ϵ is the distance correction factor. The probability of earthquake occurrence in a time span of t years is assumed to follow a Poisson process. The probability of exceeding a certain wave height is computed from this Poisson model and using equation (4-8). Two curves are given in [4-17]. The first curve gives the tsunami wave run up height for different return periods and probabilities of exceedence. The second curve gives the tsunami wave run up height as a function of distance from source for the 26th December 2004 event. This second curve is shown in fig.9. The maximum water level observed at PFBR site during December 2004 tsunami is 4.7m above MSL. Following are the observations from the two curves reported in [4-17].

a) There is limiting value of tsunami run up height beyond which it is not increasing. But with the limited data on tsunami run up height, it is better to have some conservative estimate for tsunami run up height.

b) The predicted run up heights using equation (4-8) for the December 26, 2004 tsunami event is shown in fig.9. The predicted run up heights from equation (4-8) agrees well with the observed run up heights for large distances (distances more than 3000 Km). For Kalpakkam site, the under ocean faults are located at a distance of 1000-2000 Km. In this region, many observed run up heights are under predicted by equation (4-8). One of the reasons for this under prediction is the non-inclusion of bathymetry data specific to the site.

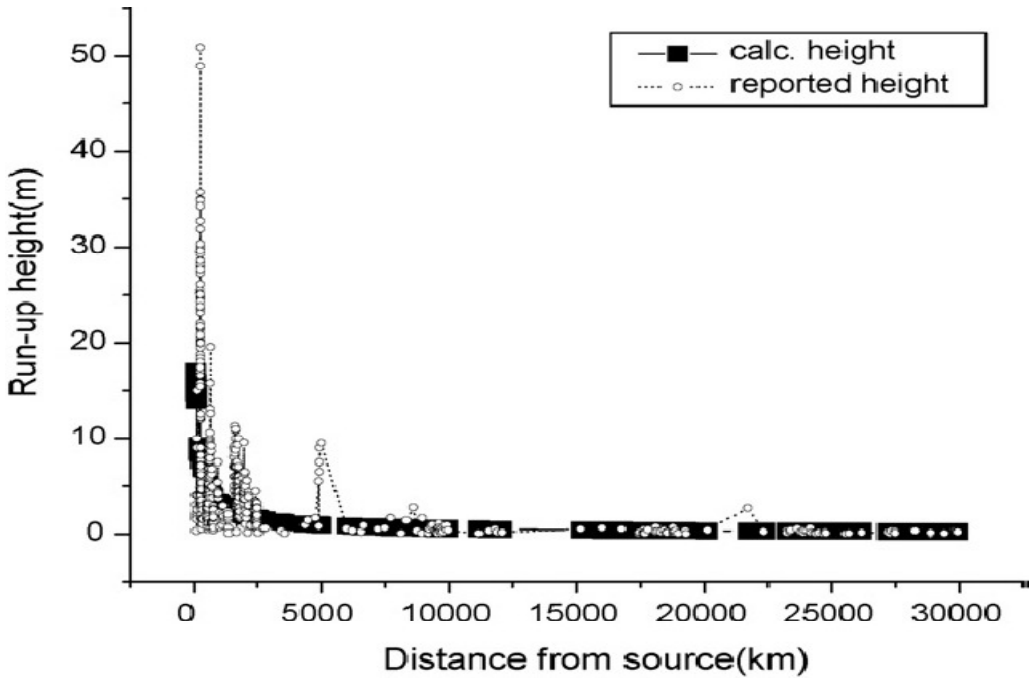

Fig.9. Variation of Tsunami Run up Height with Distance-Observed and Predicted values

4.2.1.2 Improved Method for Tsunami Hazard Analysis

The prediction of tsunami run up heights in the previous section can be improved by including the local bathymetry for Kalpakkam [4-18]. A simplified model to include local

bathymetry is needed. The Work-energy theorem method is identified as a simple model to achieve this objective.

4.2.1.3 Work-Energy Theorem Method

The work-energy theorem method [4-19] attempts to derive the tsunami wave run up heights based on the principle of conservation of energy. The work-energy theorem states that the sum of initial total mechanical energy (E_i) and the work done by the external forces (W_e) is equal to the final total mechanical energy (E_f). The mechanical energy can be potential energy or kinetic energy.

$$E_i + W_e = E_f \qquad (4\text{-}9)$$

A tsunami wave approaching the coast contains both kinetic and potential energy. The external work done by wind (W_e in equation (4-9)) is considered to be negligible. As it advances shallower waters its velocity decreases and height increases. The work is being done by the wave as it climbs the beach and the energy of the wave is gradually dissipated. Ultimately, the volume of water comes to a rest position. The work done reduces the kinetic energy from the wave. An expression is derived for tsunami wave run up height using this principle which is given by equation (4-10). This relationship tries to estimate the beach run up height from the tsunami wave height at zero metre depth and offshore angle.

$$H = \sqrt{\frac{g}{d}}\, H_0 . t_c . \tan(\theta_b) \qquad (4\text{-}10)$$

H is the beach run up height and H_0 is the wave height at zero metre depth. θ_b is the beach slope angle. g is acceleration due to gravity and d is the depth information used to calculate t_c. The depth used to calculate t_c in this study is 1m. t_c is the time tuning coefficient which is defined as the time taken by the wave to travel from 1m depth to 0m depth. The time tuning coefficient t_c follows an empirical relationship with offshore angle which is given by equation (4-11).

$$t_c = 0.6791\ [\tan(\theta_{off})]^{-1.0606} \qquad (4\text{-}11)$$

θ_{off} is the off shore slope angle. Fig.10 gives the geometry of off shore slope, beach slope and wave height at mean sea level. The wave height at zero metre depth (H_0) is denoted by OZ in fig.10.

4.2.1.4 Bathymetry Data for Kalpakkam and Assumptions in this study

The off shore slope of Kalpakkam beach is measured at a distance of 125m from the coast line for four profiles [4-20]. The slope varies from 34^o to 60^o before the 2004 Tsunami event, and it is from 44^o to 65^o after the 2004 tsunami event. Broadly the slope varies from 30^o to 65^o. The following assumptions are made in this study.

a) The beach is having a gentle gradient and the beach angle is equal to the off shore angle ($\theta_b=\theta_{off}$). Equation (4-10) is used to calculate beach run up heights for plain beaches without any obstruction. Equation (4-10) gives the maximum vertical run up height. The run up heights predicted by equation (4-10) are conservative if obstructions like bunds, protection walls etc. are present in the beach.

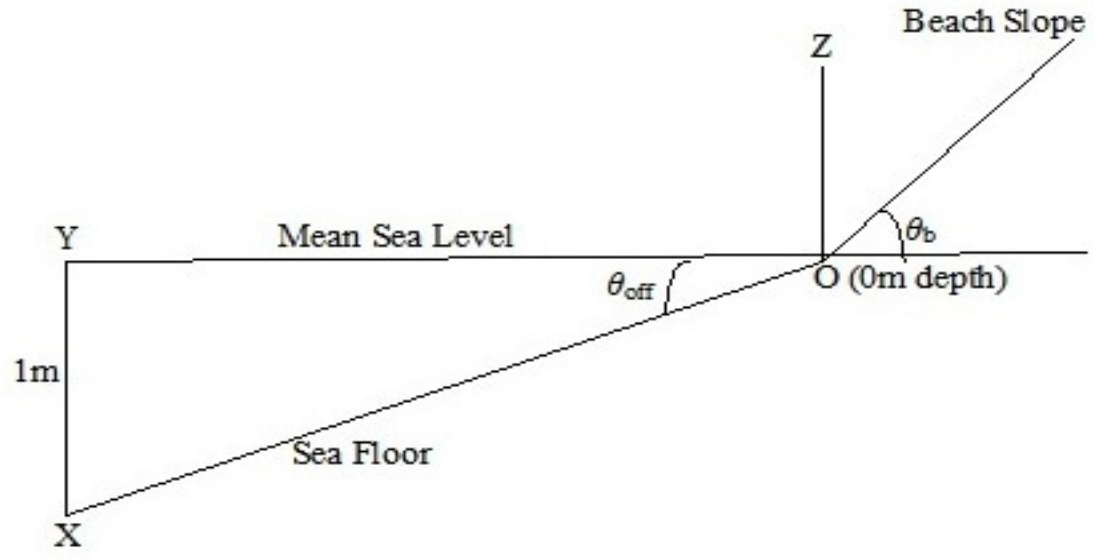

Fig.10: Geometry used in Work Energy Theorem Method

b) It is further assumed that the run up height predicted by equation (4-8) is the wave height at zero metre depth for work-energy theorem method.

c) The beach slope varies from 30^o to 65^o. The beach slope of 30^o is used in this analysis as it gives a conservative estimate of run up heights.

4.2.1.5 Results

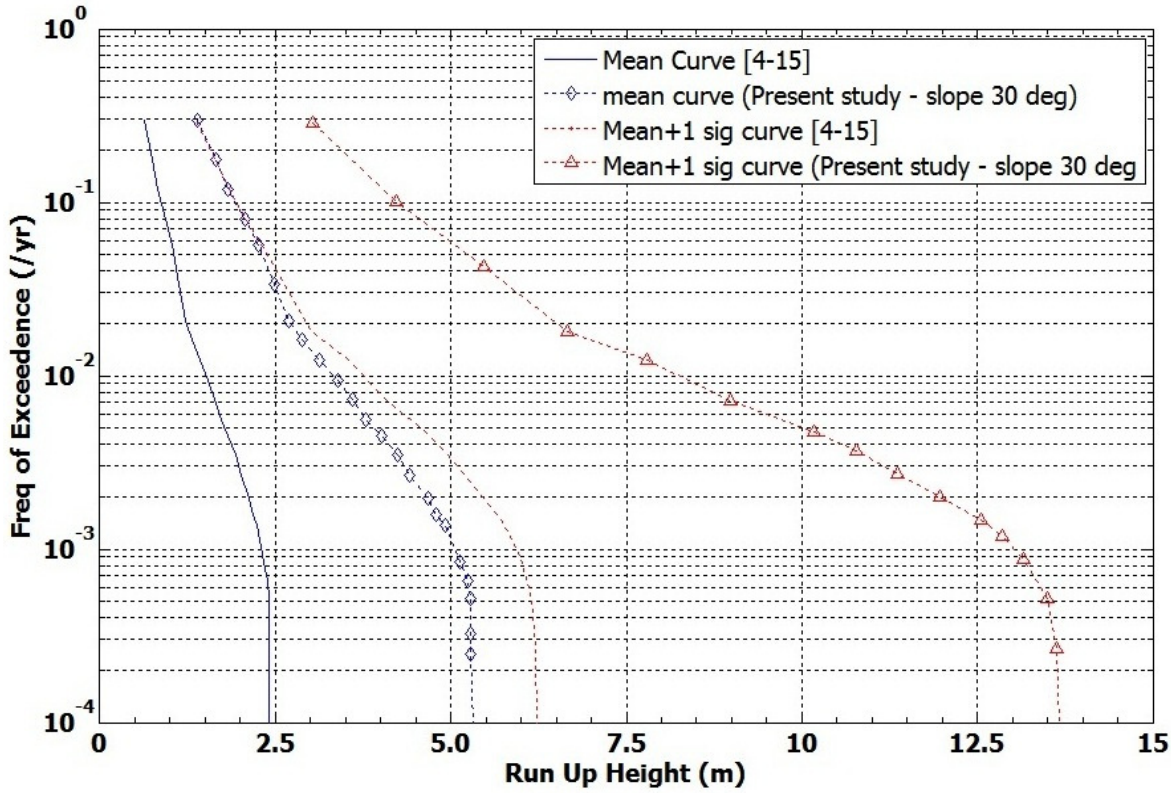

Fig.11: Tsunami Hazard Curves for Kalpakkam Site

The tsunami hazard curves generated for Kalpakkam site are given in fig.11. The hazard curve gives the frequency of exceedence as a function of tsunami run up height. The hazard curves reported in the earlier study and the curves obtained from the present study are shown in fig.11. The inclusion of bathymetry increases the tsunami wave run up height predictions significantly. The mean and one sigma upper bound curves are given in fig.11. The upper bound run up height predicted by the earlier study [4-17] using equation (4-8) for a 100 year return period is ~3.8m above MSL where as the observed run up height at site is ~4.7m above MSL. The observed run up height lies between the mean and upper bound curve in the present study for 100 year return period. This increases the confidence in the present

study as compared to the earlier one. The use of extreme value frechet distribution fit to the data points in [4-17] increases the run up height predictions for low frequency of exceedence or higher returns periods. There is no significant change in run up height predictions for low return periods which can explain the observed run up height at plant. Out of the three methods considered, the inclusion of bathymetry in the model alone explains the observed run up height at site.

Of the three hazards considered for flood PSA of PFBR, tsunami run up height governs the flood height at PFBR site. The nuclear island of PFBR is critically important from the safety point of view. The finished floor level of nuclear island buildings is approximately 9.6m above MSL. Based on the above reported tsunami hazard, it can be stated that the probability of flooding of nuclear island buildings is very small.

4.2.2 Accident Sequence Modelling Methodology for External Flood Probabilistic Safety Analysis of PFBR

The accident sequence models for external flood probabilistic safety analysis can be developed with event trees by two different methods. One method is developing event trees with flooding events as the initiator. The second method is using the event tree developed for level-1 internal events PSA with conditional initiating event frequency. These two approaches are compared quantitatively and it is shown that they are equivalent. This study [4-21] enables the use of accident sequences developed for level-1 internal events PSA with small modifications for EFPSA of PFBR. The accident sequence models development time and effort will be reduced due to the above reason. This study is explained in section 4.2.2.1.

4.2.2.1 Accident Sequence Model

The Core Damage Frequency (CDF) for a particular initiating event k can be written as in equation (4-12).

$$\text{CDF} = \sum_k \lambda_k \text{P}(\text{CD}|\text{k}) \quad (4\text{-}12)$$

CDF in equation (4-12) is the total core damage frequency due to both internal and external causes, λ_k is the event frequency for a specific event k and P (CD ⁞ k) is the conditional probability of core damage given an event k. One method to estimate CDF is to use the event tree developed for level-1 internal events PSA with conditional initiating event frequency. Let E_1 represents the set of internal events and E_2 represents the set of external events. With this splitting of event set into two, equation (4-12) can be written as in equation (4-13).

$$CDF = \sum_{k\in E_1} \lambda_k P(CD|k) + \sum_{k\in E_2} \lambda_k \sum_{j\in E_1} P'(j|k)\, P'(CD|j,k) \quad (4\text{-}13)$$

P'(j|k) is conditional probability of occurrence of internal event initiator j given the occurrence of external event k. P'(CD ⁞ j,k) is the conditional probability of core damage given the occurrence of an internal event j and external event k.

The other method is to develop event tree with external event initiator. But both P'(j ⁞ k) and P '(CD ⁞ j,k) have to be evaluated as fragilities. The CDF estimate based on this approach is given by equation (4-14).

$$CDF = \sum_{k\in E_1} \lambda_k P(CD|k) + \sum_{k\in E_2} \lambda_k P^{(e)}(CD|k) \quad (4\text{-}14)$$

$P^{(e)}$(CD|k) is the probability of core damage given an external event k. If equation (4-13) and (4-14) are equivalent then it leads to equation (4-15).

$$P^{(e)}(CD|k) = \sum_{j\in E_1} P'(j|k) P'(CD|j,k) \quad (4\text{-}15)$$

4.2.2.2 Illustrative Example from PFBR

The equality of equation (4-15) is explained with an example from PFBR. However it is to be noted that, the example is an illustrative one and does not give the exact details such as redundancy and diversity at system level and component level. The block level fault trees for two important safety systems of PFBR namely shutdown system (SDS) and decay heat removal system (DHRS) are given in figures 12 and 13 respectively.

The simplified event trees with conditional initiating event occurrence for a particular external flood level are given in figures 14 and 15. The initiating event for the event tree in Fig. 14 is flood induced Primary Sodium Pump (PSP) trip for a particular external flood level. Flood induced Secondary Sodium Pump (SSP) trip at a particular external flood level is the initiator for the event tree in Fig. 15. The total component failure probabilities denoted by P is a combination of random failures and flood induced failures. This is modelled with a step function and is given as input to basic events of the fault tree. Depending on the accident sequence progression the end state can be either safe or Core Damage (CD) state. The quantification of event tree is to be done for different hazard levels. The CDF estimate based on this approach is given by the second term on the right hand side of equation (4-13).

The event tree based on the second approach with flooding event as the initiator is given in figure 16. In this approach the combination of frequency of external flood occurrence and conditional probability of initiating event occurrence in the first approach is

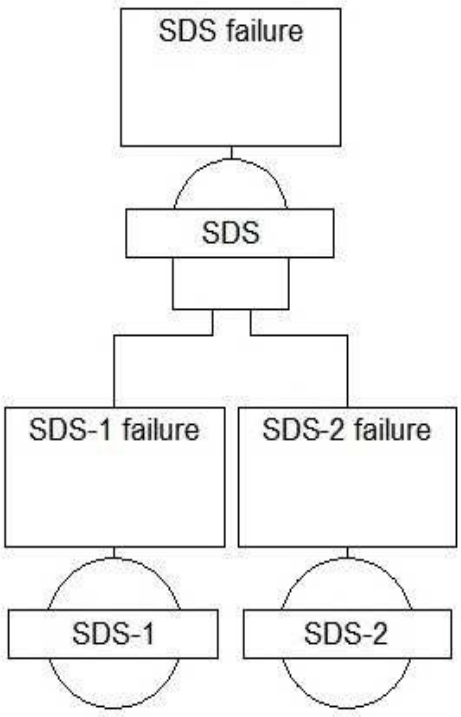

Fig.12: SDS Fault Tree

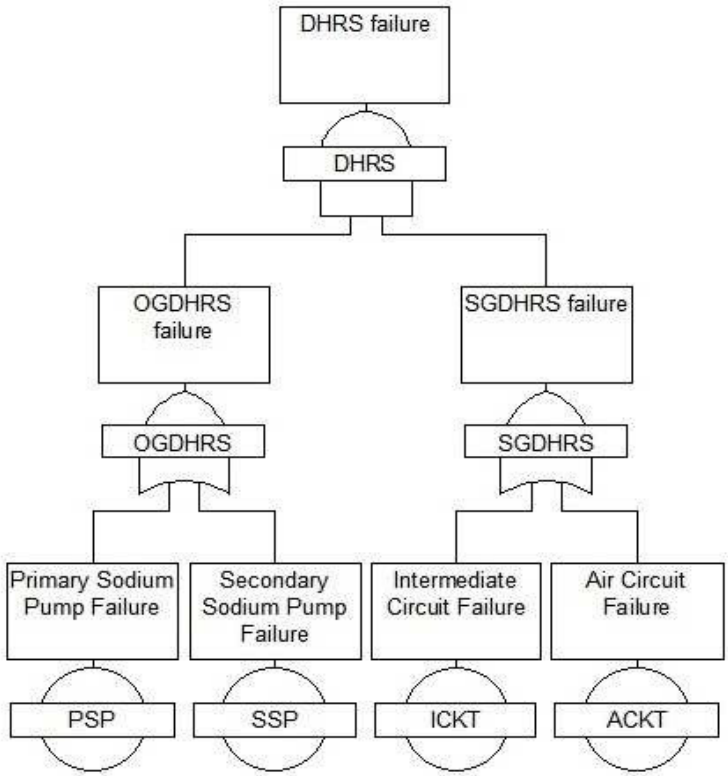

Fig.13: DHRS Fault Tree

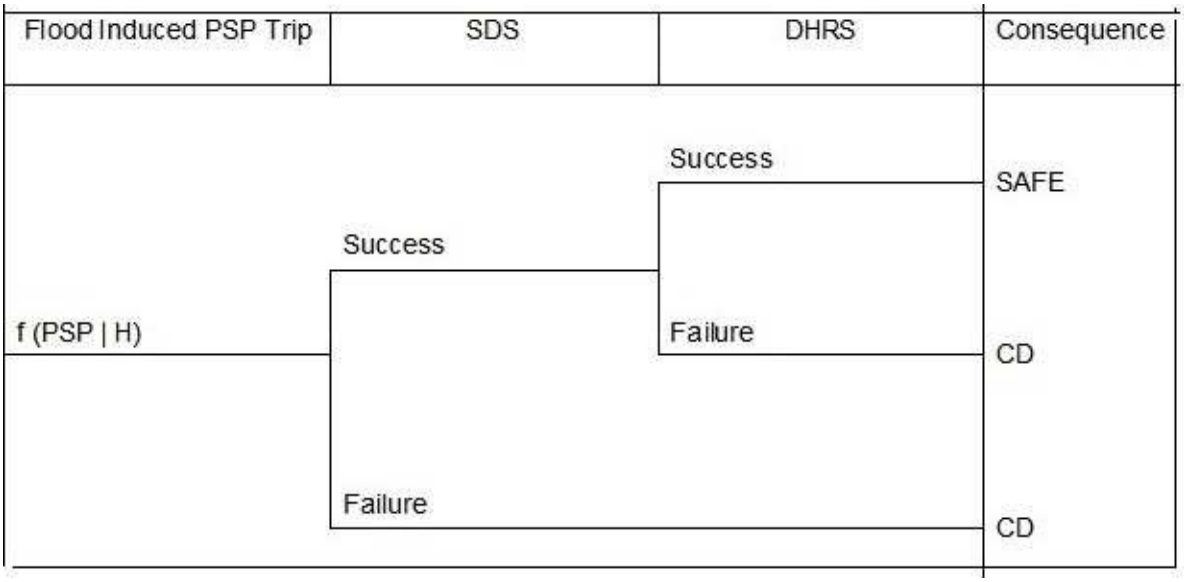

Fig.14: Event Tree with Flood Induced PSP Trip as Initiating Event

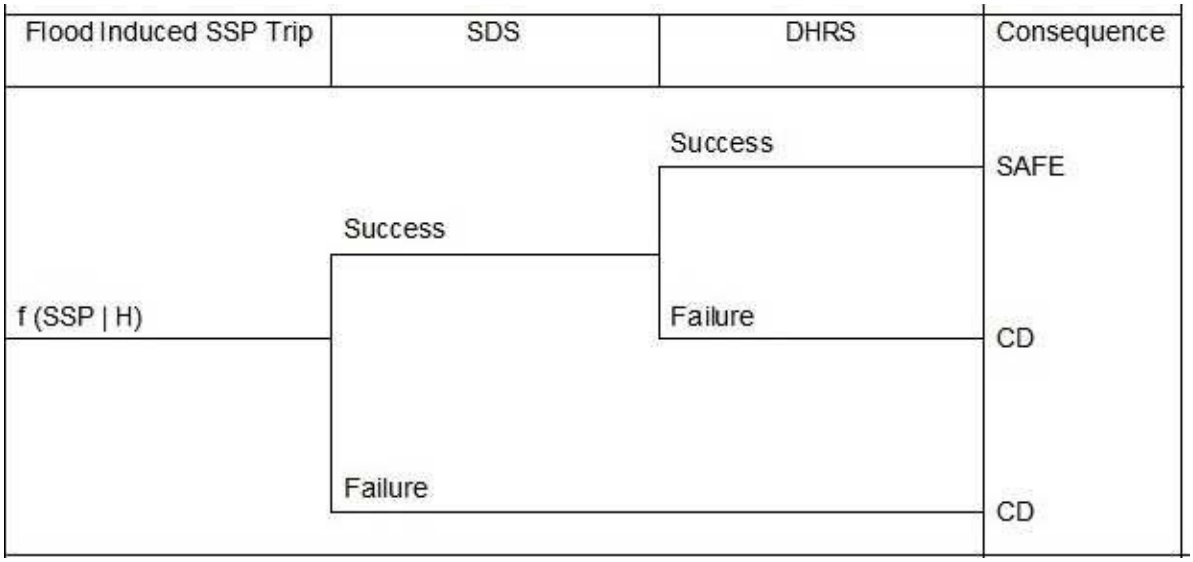

Fig.15: Event Tree with Flood Induced SSP Trip as Initiating Event

taken care of in the estimate of CDF by the event tree framework. This equivalence in both approaches is explained in Table 8. P (x) is the total failure probability of a basic event x for a given hazard level. This notation is followed in Table 8 to write minimal cut sets. Dependent failures are not considered in this example. The CDF expression from event tree with flooding event as initiator and total CDF from event trees with conditional internal events initiators are same.

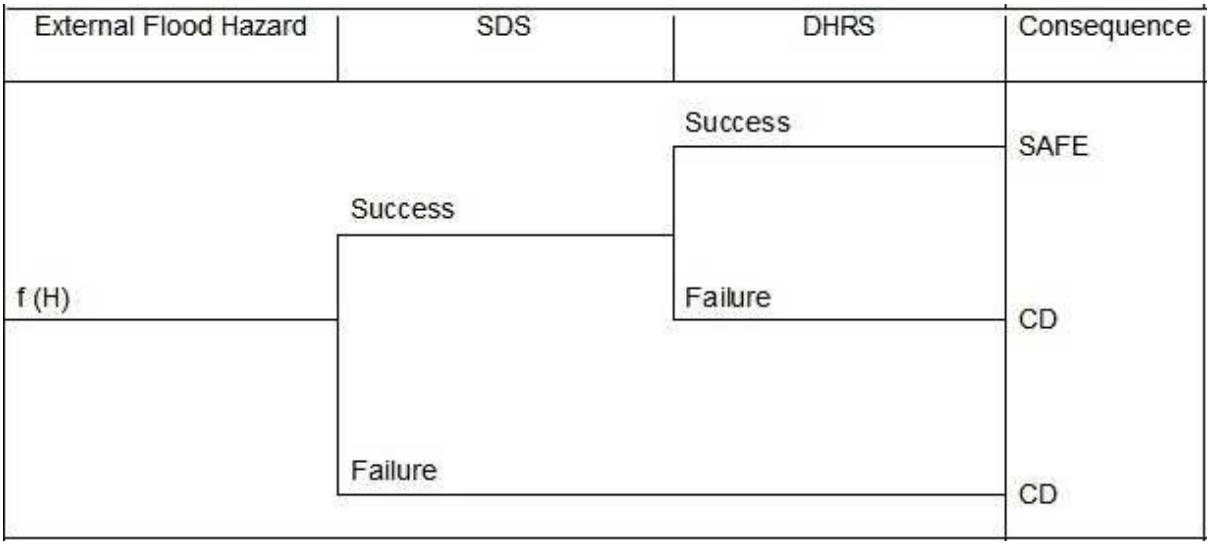

Fig.16: Event Tree with Flooding Event as Initiator

Table-8: Analytic expressions for CDF from Two Approaches

Initiating Event	Initiating Event Frequency (/y)	Expression for CDF (/y)
Event Tree with external event initiator		
External Flood	f (H)	f (H) { P (SDS1).P (SDS2) + P (PSP).P (ICKT) + P (PSP).P (ACKT) + P (SSP).P (ICKT) + P (SSP).P (ACKT) }
Event Tree with conditional internal event initiators		
PSP failure due to flood	f (PSP|H)	f (H) P (PSP) { P (SDS1).P (SDS2) + P (ICKT) + P (ACKT) }
SSP failure due to flood	f (SSP|H)	f (H) P (SSP) { P (SDS1).P (SDS2) + P (ICKT) + P (ACKT) }
Total CDF		f (H) { P (SDS1).P (SDS2) + P (PSP).P (ICKT) + P (PSP).P (ACKT) + P (SSP).P (ICKT) + P (SSP). P (ACKT) }

4.2.2.3 Summary

Two different accident sequence modelling approaches viz. event tree with external event initiator and event tree with conditional internal event initiator for External Flood Probabilistic Safety Analysis are compared with respect to quantitative predictions and resource requirement. It is found that both lead to similar results for core damage frequency expressions. This is explained with the help of a typical accident sequence example from

Prototype Fast Breeder Reactor. This study enables us to use the level-1 PSA internal events event tree with suitable modifications for EFPSA of PFBR. The level-1 internal events PSA study has been already completed and the accident sequence models are readily available. This will be useful in saving some time and effort in developing separate accident sequence models.

This Page is left blank

Chapter-5 Overview of Dynamic Reliability Analysis

5.0 Introduction

There are two elements in the analysis of a safety system. The first element is the underlying physical process and the second element is the hardware components. The deterministic safety analysis, models in more detail the underlying physical process assuming specific configuration of hardware of the safety system. The classical PSA approaches concentrates on modelling the hardware / software / human components for specific process conditions. The success / failure criteria and mission time for classical PSA approaches are derived for specific process conditions. The division of safety analysis into two parts can lead to incomplete picture of risk significant accident scenarios. The time dependent interaction between the physical process and different hardware / software / human components of a safety system is not considered in classical approaches to PSA. The dynamic approaches to PSA attempt to model integrated system evolution with a time dependent physical model and stochastic behaviour of hardware / software / human components [5-1].

The studies reported in chapters 3 and 4 are based on classical approaches to probabilistic safety analysis of reactors. Fault tree / Event Tree techniques are the widely used classical approaches in PSA of reactors. The popularity of fault tree / event tree techniques is due to the large experience gained with these methods, its simplicity and the adaptability to large safety systems of reactors. These methods have good clarity in communicating the results of the analysis which helps in easy review of these analyses.

5.1 Drawbacks of Classical Approaches

Following are the draw backs of classical approaches in addition to the advantages discussed briefly in the previous section.

a) The fault tree / event tree techniques are static in nature. Time Dependent evolution of system is not possible in fault tree / event tree approaches. The order of events is preset by

the analyst in classical approaches.

b) The system failure probability is evaluated by fault tree by assuming the components of the system to be independent. Recent fault tree software tools have limited capability to model the common cause failures. The other types of dependencies between components are increased stress on one component due to the degraded performance of the other component, dependence in testing, repair and maintenance. These types of dependencies cannot be modelled in classical approaches [5-2].

c) One of the challenges in fault tree / event tree methodology is the modelling of logical loops.

d) The classical PSA approaches require simplifications in modelling the safety system under consideration [5-3]. The burden of justification of the correctness of the methodology lies on the analyst. It is very difficult to systematically incorporate time and process variable dependence in fault tree / event tree approach.

e) The probability of system failures can be sensitive to the uncertainties in the physical process. It is difficult to account for such sensitivities in classical approaches in a systematic manner [5-1]. This drawback is relevant to passive systems which rely on natural phenomena.

5.2 Dynamic Approaches to PSA

Due to the above mentioned drawbacks of classical approaches, dynamic PSA approaches are gaining importance. Dynamic approaches to PSA present a unified framework to account for the joint effects of two types of uncertainties [5-1]. The first type of uncertainty[1] is the lack of knowledge about the physical processes associated with the safety system. The second type of uncertainty[2] is due to the stochastic nature of events. One of the challenges mentioned in Strategic Research Agenda (SRA) of the Sustainable Nuclear Energy Technology Platform (SNETP) of the European Union is to address these two

[1] Generally referred as epistemic uncertainty
[2] Referred as aleatory uncertainty

uncertainties in a consistent manner. Integrated Deterministic Probabilistic Safety Assessment (IDPSA) [5-4] is a set of methods identified to address the above challenge. IDPSA methods are in general referred to as dynamic PSA in a broader context. Dynamic PSA approaches in general are classified into two major categories. They are i) Continuous time methods and ii) Discrete-time methods [5-1]. These two methodologies are explained in the subsequent paragraphs.

The first continuous time method developed was the theory of Continuous Event Trees (CET) [5-5]. Assuming the systems are markovian in nature, this approach models the dependence between physical process and hardware / human components using the Chapman-Kolmogorov equation (5-1).

$$\frac{\partial}{\partial t}\,\varphi(x,y,t) + \nabla_x.\left[\varphi(x,y,t)f_y(x,t)\right] + \lambda_y(x)\varphi(x,y,t) - \sum_{z\neq y} p(z \to y|x)\varphi(x,z,t) = 0 \qquad (5\text{-}1)$$

x is a vector of process variables and y represents the states of components. The process dynamics is given by equation (5-2).

$$\frac{\partial x}{\partial t} = f_y(x,t) \qquad (5\text{-}2)$$

p (z⟶y | x) in (5-1) is the transition rate to system configuration y given that the system is in configuration z at time t with process variable x. $\lambda_y(x)$ is defined by equation (5-3).

$$\lambda_y(x) = \sum_{z\neq y} p(y \to z|x) \qquad (5\text{-}3)$$

The solution to equation (5-1) φ(x,y,t) is the probability density of the x space that the process variables are at x with the system in configuration y at time t. An integral formulation of equation (5-1) is also available which is more general. The changes in system hardware configurations due to the process variables crossing some threshold limits cannot be modelled by equation (5-1). Continuous cell-to-cell mapping technique (CCCMT) was developed to model such scenarios.

The continuous time methods such as continuous event tree attempts to solve equations such as (5-1) or its integral form to obtain the probability density φ (x,y,t). Once φ (x,y,t) is known all the statistical properties of the system regarding failure events can be determined. The application of continuous time methods to realistic systems has been limited due to the difficulty in solving the relevant equations.

The discrete time methods generate branches of system evolution due to component failure / malfunction at user specified time intervals and follow the branches using appropriate process models. Discrete Dynamic Event Trees (DDET) is the most popular discrete time method. There are different variants of DDET like Dynamical Logical Methodology (DYLAM) and Dynamic Event Tree Analysis Method (DETAM). A medium break Loss of Coolant Accident of a pressurized water reactor using discrete dynamic event tree is reported in [5-6]. The Monte Carlo Simulation simulates the actual process and stochastic transitions in system hardware configuration by sampling the transition times. The probabilities of failure events are estimated from these simulation runs. The branching times in Monte Carlo simulation are selected stochastically whereas branching times are selected using deterministic rules in other discrete time methods [5-7]. This is the difference between Monte Carlo simulation and other discrete time methods.

Dynamic reliability methods model the dependence between physical process and system hardware / human components of a safety system. The interaction between the physical process and hardware components can be of three types. The first type is the changes in physical process parameters due to stochastic changes in system hardware configuration. The second type is the changes in system hardware configuration induced by the process parameter conditions. Failure of components due to extreme conditions like high temperature and pressure are examples of this type. The third type of interaction is the changes in system hardware configuration due to the process parameters crossing some threshold limits. Both

second and third type of interactions depends on process conditions. There is a significant change in failure probabilities due to the extreme process conditions in the second type of interaction. Such changes in failure probabilities are not likely in the third type of interaction because the components are designed for those process conditions. Component transition rates do not vary as a function of process parameters in the third type of interaction. A particular type of dependence or all the types of dependences may be present in a safety system depending on the scenario being analysed. Discrete time method using Monte Carlo simulation of the actual process and stochastic changes in system hardware will be used for dynamic PSA of safety systems.

5.3 Monte Carlo Simulation of System Hardware

A Monte Carlo simulation tool is needed to model the stochastic changes in system hardware with time. In Monte Carlo simulation of a safety system the simulated system traverses from one state to another in state space. A hardware component in a system can be in any one of the possible states. Due to lack of availability of transition rates data for many states, only two component states namely operating and failed states are considered. The system state is a function of operating and failed components. The transition rate and possible transitions are functions of system state. It is possible to compute the necessary parameters for simulation as a function of present system state. Failure and repair rates of components and a small amount of CCF data are sufficient for simulation. An overview of different Monte Carlo simulation techniques for system hardware is presented in the following section.

5.3.1 Overview of Monte Carlo Simulation Techniques

Reactor safety system failures are rare events. Direct Monte Carlo simulation requires a large computational effort to get statistically significant results. Biased simulation techniques are necessary for rare event simulation. One of the desirable properties of biased simulation schemes is the Bounded Relative Error (BRE). Relative error is connected with

variance of the estimate. In direct Monte Carlo simulation, the relative error tends to infinity as the probability of the rare event tends to zero for a fixed computational effort (number of simulations). For a fixed computational effort, the relative error remains bounded as the probability of the rare event tends to zero in a biased simulation scheme having BRE property. Two popular biased simulation approaches are importance sampling and splitting [5-8]. Importance sampling is based on the idea of sampling from another probability density than the original one. The biased probability density is selected in such a way that the rare events are sampled more. Also it should give rise to a reduced variance than the original density function. The splitting technique does not change the underlying probability laws. An artificial drift towards the rare event is created by terminating some realisations that seems to go away from the rare event. Splitting involves generating identical copies of the random variable when the random variable reaches a certain level. The identical copies of the random variable evolve independently. Several methods are available in importance sampling and splitting. A brief overview of the different methods using importance sampling is presented in the following paragraphs. The detailed description of each method is given in [5-8, 5-9]. A general approach followed in importance sampling is to look for an ideal density function which will give rise to a zero-variance estimator. This is possible in theory but difficult to achieve in practice. This requires prior knowledge of the quantity which we need to compute. But the theoretical zero variance estimators are helpful in deriving the probability density which gives better variance reduction.

The basic principle of importance sampling is to increase the occurrence of rare events of interest. System failures are the events of interest in the present context. The Monte Carlo simulation scheme of a system can be broadly classified into two categories [5-10]. The two categories are indirect method and direct method. The next transition time of the system is sampled from the conditional probability density of the system in indirect method. The

transition times of individual components are sampled in the direct approach. The implementation of biasing in the indirect approach is straightforward whereas it is somewhat difficult in the direct approach. Indirect approaches are widely used for system simulation and it is discussed further. The different indirect methods based on importance sampling for Markov Chain Monte Carlo simulation can be divided into three categories. They are the basic schemes, schemes based on system structure information and schemes which try to approach zero variance importance measure. Failure biasing schemes are one of the basic schemes of importance sampling. Failure biasing schemes were first introduced in [5-2]. This method increases the failure probability by a fixed factor ρ. The transition probabilities among the possible failure transitions are modified in proportion to the original probabilities of failure. This method is suitable for systems in which the failure rates of components are of the same order of magnitude. For these classes of systems BRE property is satisfied by simple failure biasing. Subsequently Balanced Failure Biasing (BFB) scheme was developed [5-11]. It differs from simple failure biasing in the way transition probabilities are calculated for possible failure transitions. The transition probabilities among the possible failure transitions are uniform in BFB. This scheme is suitable for systems having different orders of failure rates of components. BRE property is satisfied by BFB irrespective of whether the failure rates are of the same order or different orders of magnitude. The drawback of BFB is that it gives more weight to some of the failure paths than necessary [5-12]. Inverse Failure Biasing (IFB) is developed [5-13] for queuing systems in which the total failure probability and total repair probability are interchanged. This method has BRE property for systems in which failure rates are of the same order. To improve the performance of simulation for systems with large redundancies, Balanced Likelihood Ratio methods [5-14] were introduced. The basic idea of this method is to define stacks for each order of failure rate magnitude. The likelihood ratios are put on top of corresponding stack and this value is removed from the

stack when there is a component repair which has a failure rate with the same order of magnitude.

The above simulation schemes attempt to reach the failure states simply by increasing the failure transitions over repair transitions. More generally, the system structural information can be used to reach the system failure states more efficiently. The basic principle in Selective failure biasing or bias2 failure biasing [5-15] is to increase the number of failures of component types which have already failed components. This will take the system closer to failure state. The other method which uses system structural information is the failure distance biasing [5-16]. In this scheme the system goes mainly along the most likely paths to failure. This method requires the computation of distance of the current state from failure state. A non linear Monte Carlo simulation scheme based on the introduction of distances between the present state and cut set configuration is presented in [5-17]. Even though the balanced versions of these simulation schemes [5-16, 5-18] have BRE property, these methods require more computational over head for each state transition.

The third type of schemes is those which try to approach the zero variance importance measure. The approaches under this scheme attempt to reduce the variance of the calculated quantity to a great extent. The theoretical zero variance schemes need the knowledge of the quantity which we need to compute. But in practice it can be approximated by different approaches. In adaptive importance sampling technique [5-19], the zero variance importance measure is learned in an iterative manner. This method requires generation of many independent identically distributed sample paths in an iteration using a fixed change of measure. Each path typically involves a large number of transitions of the Markov chain. The change of measure is then updated for the next iteration based on these observations. A variant of this adaptive importance sampling in which the change of measure is updated at every transition using constant or decreasing step-size stochastic approximation is presented

in [5-20]. The Cross-Entropy method [5-21] is an adaptive procedure for estimating the optimal values of the set of parameters for the biasing probability distributions. But this method requires the storage of entire transition matrix. Subset simulation [5-22] is an adaptive method for efficiently estimating small failure probabilities. This scheme was developed for the reliability analysis of structural systems. The basic principle is to express the failure probability as a product of larger conditional probabilities of some intermediate failure events. This method converts the rare event simulation into a sequence of simulation of more frequent events. The subset simulation is applied to the reliability analysis on a system of discrete multi-state components in a series parallel configuration [5-23]. All these methods need additional storage or additional computational efforts. A zero variance estimator without any extra storage and computation is desired. One such approach uses the shortest path from the present state to the set of failed states as an approximate zero variance estimator [5-24]. This approach needs the identification of shortest path from each state.

A host of methods are available based on importance sampling for rare event simulation. The different biasing schemes are presented in a tree structure in fig.17. The methods which use system structural information and methods which approach the zero variance importance measure have better variance reduction capabilities as compared to basic importance sampling schemes in general. But in dynamic reliability applications where physical process evolution is integrated with system hardware changes, implementing the above schemes needs additional computational burden for differing process conditions. So the basic importance sampling simulation schemes are used in this study. The objective of the present study [5-25] is to compare a few simple importance sampling based simulation methods on typical reactor safety systems and identify a better method. This is achieved by applying these methods on a typical reactor safety system. The reactor safety system is characterised by rarity of system failure and dependence between component failures through

common causes. The method which gives better performance in terms of variance reduction is identified.

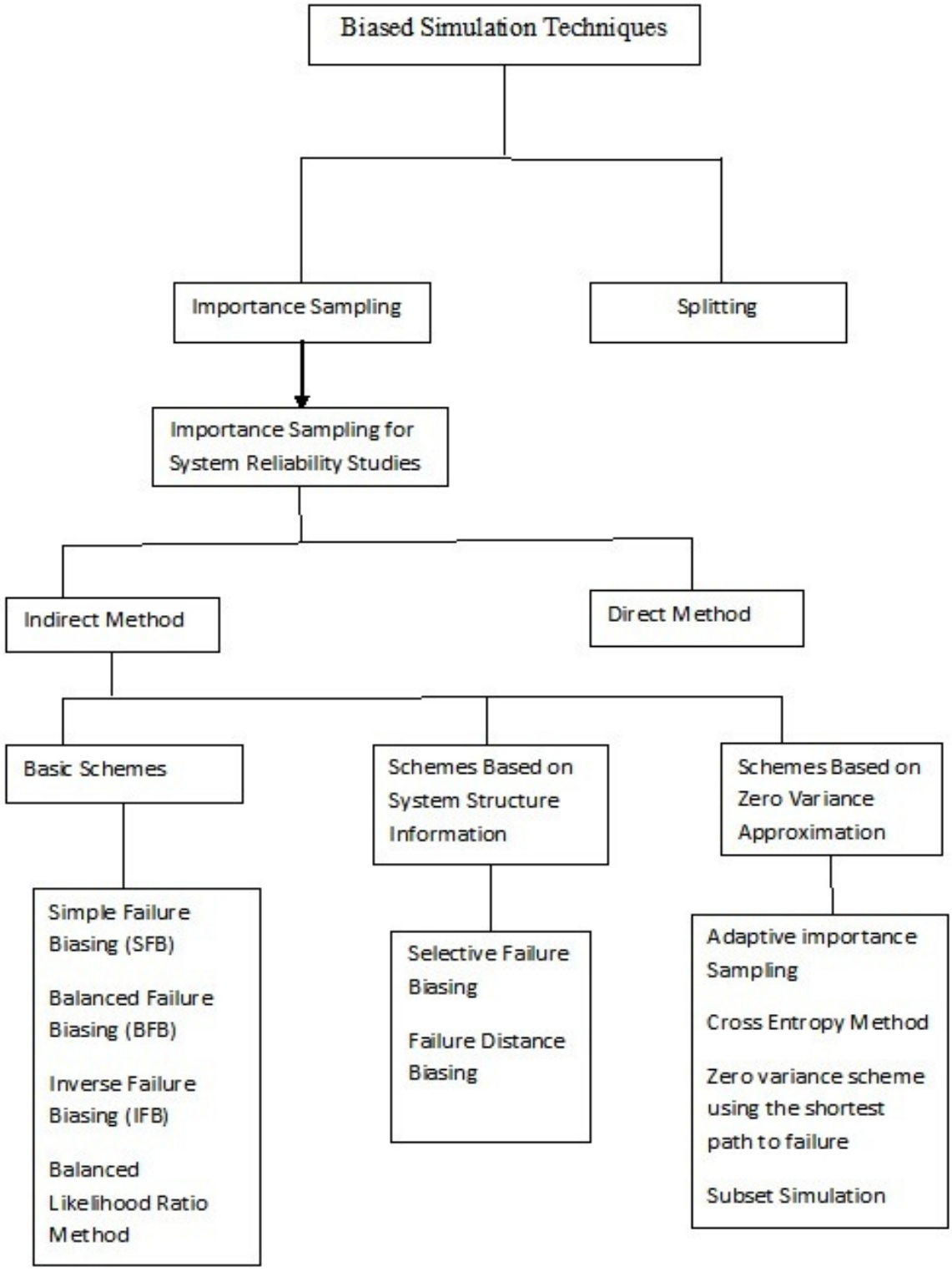

Fig.17: Different Biasing Schemes

5.3.2 Objective

The present study has two objectives. The first objective is to identify a simple importance sampling based simulation scheme which can be used to combine with physical process evolution. This is achieved by applying a few selected simulation schemes on a typical reactor safety system which is characterised by rarity of system failure and common cause failure between components. The performance of different simulation schemes are compared in terms of variance reduction and a better method is identified. The second objective is to combine the identified method with physical process evolution for dynamic PSA applications. The second objective is explained in chapter-6.

This study demonstrates the applicability of different methods on a typical reactor safety system and compares the performance of a few methods. Most literature studies are carried out on example systems with a few components.

5.3.3 Monte Carlo Simulation Scheme

A brief description of the Monte Carlo simulation scheme is presented here. For detailed description the readers can refer [5-15]. A system state represents a combination of operating and failed components in the system. Consider a system with N_c components of the same type. The possible system states are denoted by $X=\{X_0, X_1,..., X_{NC}\}$. Let X_n denotes the state of the system at time t_b, b=0,1,2... . The suffix n denotes the number of operating components in the system. $n = N_c-n_f$. n_f is the number of failed components of the system. Let the system makes a transition at time t_{b+1}. In the absence of dependent failures, the system can reach either X_{n+1} or X_{n-1} depending on the nature of transition. The transition can be either a failure transition or a repair transition. The sequence of states visited by the system can be represented by a Continuous Time Markov Chain (CTMC). Two random numbers are required in CTMC simulation. One random number is used for sampling next transition time. The other random number decides the system state. The system state space X contains two set

of states, namely operating and failed states. The all components operating state X_{Nc} is defined as the regenerative state of the system and this is the only regenerative state. A regenerative state of the system is defined as the state from which the evolutions of the system are independent and identically distributed. The system is assumed to be in the regenerative state at time t_0. Subsequently the system evolves through different states until it returns to the regenerative state. A particular random walk simulation is terminated once the system returns to the regenerative state and the next random walk simulation will be started. This is called one regenerative cycle. This is the basic idea of regenerative simulation.

The CTMC simulation is used for the computation of transient measures like failure probability within a mission time, interval availability etc. The system spends most of its time in the regenerative state. For transient measures, the system failures are to be observed within a short mission time. The biasing schemes for such simulations should satisfy the following requirements. The first requirement is that the system should be brought out of the regenerative state to a non-regenerative state in a short time. Once the system comes out of the regenerative state, it has to be driven towards the system failure state. This is the second requirement. Any biasing scheme for transient measures should satisfy the above two requirements. The steady state measures like steady state unavailability and Mean Time To Failure (MTTF) can be estimated with reduced variance by simulating the Discrete Time Markov Chain (DTMC) [5-15, 5-26] as compared to CTMC. The time interval for which the system stays in a particular state is called the holding time. The holding times in DTMC simulation are deterministic. The holding time is set equal to the mean of the holding times in CTMC. The DTMC method does not require one random number for sampling the next transition time. The Direct Monte Carlo simulation using DTMC is explained in the next section.

5.3.4 Direct Monte Carlo Simulation

The direct Monte Carlo simulation is carried out using the DTMC and natural probabilities of transition. The system is in regenerative state at the beginning of each random walk. The various steps in this simulation scheme are given below.

1. The first step is to calculate the transition rate of the system $\gamma_{k'}$ at state k'. The transition rate is given by equation (5-4a).

$$\gamma_{k\prime} = \lambda_{k\prime} + \mu_{k\prime} \qquad (5\text{-}4a)$$

$\lambda_{k'}$ and $\mu_{k'}$ are the failure transition rate and repair transition rate of the system from state k'. $\lambda_{k'}$ and $\mu_{k'}$ are given by the following expressions.

$$\lambda_{k\prime} = \sum_{i \epsilon U} \lambda_i \qquad \mu_{k\prime} = \sum_{i \epsilon F} \mu_i \qquad (5\text{-}4b)$$

U is a set of operating components at a specific system state k'. λ_i and μ_i are the failure rate and repair rate of the i^{th} component. F is a set of failed components at a particular system state k'.

2. The type of system transition is decided in this step. For a failure transition from state k' to state k, number of failed components in state k will be greater than the number of failed components in state k'. The criterion to determine the type of transition is as follows. A random number e is generated. If $e \leq \frac{\lambda_{k\prime}}{\gamma_{k\prime}}$ then the transition is a failure transition. Otherwise the system undergoes repair transition.

3. The component responsible for change in system state is identified in this step. The random number generated in step-2 is used for this purpose. It is compared with the individual component failure or repair probabilities in that particular system state. The system state is updated by appropriately changing the component state. The holding time in the new state k is calculated as $h_k=1/\gamma_k$. The respective time variables are updated.

4. The steps 1-3 are repeated until the regenerative state is reached. Results of each random walk simulation are stored depending on the measures of interest. The holding time in failed

state of the system and overall holding time for the random walk simulation need to be stored for unavailability estimation. The minimum of the time to reach failed state and time to return to regenerative state is stored for MTTF estimation. The time taken for one regenerative cycle is also stored.

Steps 1-4 describe one regenerative cycle. These steps are repeated for the required number of regenerative cycles. The results of the regenerative cycles form a sample. The mean and variance of the required reliability measures are estimated from the sample values.

5.3.5 Importance Sampling and Biasing Schemes

A reactor safety system consists of highly reliable components. The safety systems are also characterised by sufficient redundancy and diversity wherever required. The failure rates of components are also small. The system failure occurs due to the failure of multiple components. The probability of reaching the system failure state is very small and it is a rare event. Direct Monte Carlo simulation takes large computational effort to estimate reliability measures of interest. Variance reduction techniques like importance sampling are needed for the Monte Carlo simulation of a reactor safety system. The basic principle of importance sampling is explained in the following paragraph.

Let X is a random variable with probability density f (x). The expectation of a function of random variable g(X) is given by equation (5-5).

$$E\,[g(X)] = \int_{-\infty}^{\infty} g(x)f(x)dx \qquad (5\text{-}5)$$

This expectation is evaluated by taking N independent samples χ_i from the probability density f(x). The expectation value is computed by the estimate $\frac{1}{N}\sum_{i=1}^{N} g(\chi_i)$. The variance of this estimate is given by $\int_{-\infty}^{\infty}(g(x)-\Theta)^2 f(x)dx$ where Θ = E [g(X)]. Direct Monte Carlo simulation uses equation (5-5) to estimate the quantities of interest. Equation (5-5) can be rewritten without affecting the expectation as given in equation (5-6).

$$E\,[g(X)] = \int_{-\infty}^{\infty} g(x)\frac{f(x)}{h(x)}h(x)dx = \int_{-\infty}^{\infty} g(x)\Phi(x)h(x)dx \qquad (5\text{-}6)$$

In equation (5-6), h(x) is the modified probability density and $\Phi(x) = \frac{f(x)}{h(x)}$ is the likelihood ratio. The estimate of the above expectation value is computed by taking N independent samples χ_i from the probability density h(x). The estimate of this expectation is $\frac{1}{N}\sum_{i=1}^{N} g(\chi_i)\ \Phi(\chi_i)$. The variance of this estimator is given by equation (5-7).

$$Var(g(X)) = \int_{-\infty}^{\infty}(g(x)\Phi(x) - \Theta)^2 h(x)dx \qquad (5\text{-}7)$$

From equation (5-7) it is clear that, if h(x) is chosen such that $h(x) = g(x)f(x)\Theta^{-1}$, the variance of g(X) becomes zero. But this approach requires the knowledge of Θ = E [g(X)] which is an unknown quantity. Our objective is to calculate Θ.

The above discussion helps us to understand how the function h(x) is to be selected. The likelihood ratio Φ (x) can be computed only if h(x) > 0 for possible values of x with f(x) >0. The shape of h(x) function should closely follow the function g(x) f(x) [5-26]. The choice of h(x) depends on the problem on hand. An understanding of the stochastic structure of the problem will give better insights on the choice of h(x).

In the present context, the biased Monte Carlo simulation scheme should satisfy the two requirements mentioned in section-5.3.3 for transient measures and the second requirement should be satisfied for steady state measures. The importance sampling based biasing techniques to meet these requirements are forced transition and failure biasing. Forced transition technique is used to bring the system out of its regenerative state within a short time. Failure biasing technique is applied to drive the system towards failures. These two techniques are explained in the subsequent sections.

5.3.5.1 Principle of Forced Transitions

This technique was first introduced in [5-2]. Let γ_0 denotes the transition rate of the system in the regenerative state. γ_0 is simply the sum of failure rates of all components in the

regenerative state. The mean holding time in the regenerative state is $1/\gamma_0$. This holding time is much greater than the mission time. The time to failure and repair are assumed to be exponentially distributed in this study. Let T_m denotes the mission time. The next transition time is sampled from the exponential distribution in direct Monte Carlo simulation approach. When forced transition technique is applied, the next transition time t is sampled from the density function in equation (5-8).

$$\tilde{f}(t|t', k') = \frac{\gamma_0 e^{-\gamma_0(t-t')}}{1-e^{-\gamma_0(T_m-t')}} \quad t' \leq t \leq T_m \qquad (5\text{-}8)$$

The system is assumed to be in state k' at time t'. This technique is only applied when the system is in regenerative state. When at least one failed component is present, its repair rate will contribute to the system transition rate. This will reduce the holding time in that particular state to a great extent. Transition times are sampled from exponential density function for all other states.

5.3.5.2 Principle of Failure Biasing Schemes

The objective of failure biasing is to force the system towards states with more component failures. This will bring the system closer to failure. The set of all possible transitions from any system state X_{n1} to another system state X_{n2} is divided into two classes. Let Λ denotes a set of states in which n2 is less than n1. This denotes a failure transition. The set of system states in which n2 is greater than n1 is denoted by R. This corresponds to a repair transition. The following equation (5-9) is true for any non absorbing system state.

$$\sum_{X_{n2} \in \Lambda} P(X_{n2}|X_{n1}) + \sum_{X_{n2} \in R} P(X_{n2}|X_{n1}) = 1 \qquad (5\text{-}9)$$

$P(X_{n2} \mid X_{n1})$ is the transition probability of the system, from state X_{n1} to another state X_{n2}. Let λ_{Xn1} and μ_{Xn1} denotes the failure transition rate and repair transition rate from system state X_{n1}. γ_{Xn1} represents the transition rate of the system from state X_{n1}. λ_{Xn1}, μ_{Xn1} and γ_{Xn1} can be computed by using equations (5-4a) and (5-4b) in section-5.3.4. The probability in the first

term of equation (5-9) is given by $\frac{\lambda_{X_{n1}}}{\gamma_{X_{n1}}}$. The probability in the second term of equation (5-9) is given by $\frac{\mu_{X_{n1}}}{\gamma_{X_{n1}}}$. The second term of equation (5-9) dominates. This is because the repair rates are much larger than failure rates. Equation (5-9) is used in direct Monte Carlo simulation. In direct Monte Carlo simulation if a component failure occurs, immediately it will be followed by a repair transition. So system failures which are combination of multiple component failures are rare events. A parameter ρ is defined to bias transitions towards additional failures as given in equation (5-10).

$$\sum_{X_{n2}\in\Lambda} \widetilde{P}\,(X_{n2}|X_{n1}) = \rho \qquad \sum_{X_{n2}\in R} \widetilde{P}(X_{n2}|X_{n1}) = 1-\rho \tag{5-10}$$

The notation $\widetilde{P}$ in equation (5-10) represents the biased probabilities of transition which are different from original probabilities in equation (5-9). The likelihood ratio is multiplied by $\frac{P}{\widetilde{P}}$ for each transition. The initial likelihood ratio is 1. Two failure biasing schemes are used in this study. They are simple failure biasing and balanced failure biasing. Let F (X_{n1}) is the total probability of making a failure transition from system state X_{n1}. R (X_{n1}) is the total probability of making a repair transition from system state X_{n1}. The biased transition probabilities $\widetilde{P}$ are constructed from original transition probabilities P by using equation (5-11) [5-27] for simple failure biasing.

$$\widetilde{P}(X_{n2}|X_{n1}) = \begin{cases} \rho\frac{P(X_{n2}|X_{n1})}{F(X_{n1})} & \text{if } X_{n1} \to X_{n2} \text{ is a failure transition} \\ (1-\rho)\frac{P(X_{n2}|X_{n1})}{R(X_{n1})} & \text{if } X_{n1} \to X_{n2} \text{ is a repair transition} \\ 0 & \text{Otherwise} \end{cases} \tag{5-11}$$

The simulation is carried out with natural probabilities P (X_{n2} | X_{n1}), if the system is in regenerative state or in one of the failed states. The biased transition probabilities $\widetilde{P}$ for balanced failure biasing are calculated using equation (5-12). Let n_F (X_{n1}) represents the number of possible failure transitions from state X_{n1}.

a) When the system is in regenerative state the biased transition probability is given by equation (5-12a).

$$\widetilde{P}(X_{n2}|X_{n1}) = \frac{1}{n_F(X_{n1})} \qquad (5\text{-}12a)$$

b) The biased transition probability for other states is given by equation (5-12b).

$$\widetilde{P}(X_{n2}|X_{n1}) = \begin{cases} \frac{\rho}{n_F(X_{n1})} & \text{if } X_{n1} \to X_{n2} \text{ is a failure transition} \\ (1-\rho)\frac{P(X_{n2}|X_{n1})}{R(X_{n1})} & \text{if } X_{n1} \to X_{n2} \text{ is a repair transition} \\ 0 & \text{Otherwise} \end{cases} \qquad (5\text{-}12b)$$

The simulation is carried out with natural probabilities if the system has reached one of the failed states. The failure biasing is done in proportion to the original probabilities $P(X_{n2} \mid X_{n1})$ in simple failure biasing technique. All failure transitions are equally probable in balanced failure biasing. This is one of the difference between the two failure biasing schemes.

5.3.5.3 Biased Simulation Procedure for Estimating Steady State Measures

The regenerative state of the system is assumed to be the initial condition. All the components are in the operating state. The transition rate of the system is computed as mentioned in equation (5-4a) and equation (5-4b). This step is similar to direct Monte Carlo simulation scheme explained in section 5.3.4. The second step is to identify the type of system transition. A random number e is generated for this purpose. If $e \leq \rho$, the type of transition is a failure transition else it is a repair transition. The parameter ρ is used to decide the type of transition whereas in direct simulation it is compared with the ratio $\frac{\lambda_{k\prime}}{\gamma_{k\prime}}$ in section 5.3.4. The component responsible for change in system state is identified in the third step. The random number generated in step-2 is used for this purpose. It is compared with the biased failure or repair probabilities computed from equations (5-11) or (5-12) depending on the simulation scheme employed. The system state is appropriately modified.

Steps 1-3 are carried out iteratively until the system returns to the regenerative state. This is one regenerative cycle. The likelihood ratio is updated for each transition in a regenerative cycle. The likelihood ratio is stored for each regenerative cycle in a variable $w_{J_k}(s_k)$. J_k is the number of jumps in the k^{th} regenerative cycle and s_k is the sequence of states visited in the k^{th} regenerative cycle. Let the sequence of states visited during a regenerative cycle is $s_k = (x_0, x_1, x_2 \ldots x_{Jk-1}, x_0)$. The suffix in x represents the number of jumps or transitions. The system will be in the regenerative state when the number of jumps is zero. The system will reach the regenerative state in the J_k^{th} jump of the system. The likelihood ratio for this particular regenerative cycle is given by equation (5-13).

$$w_{J_k}(s_k) = \frac{P(x_1|x_0)\ldots..P(x_0|x_{J_k-1})}{\widetilde{P}(x_1|x_0)\ldots..\widetilde{P}(x_0|x_{J_k-1})} \qquad (5\text{-}13)$$

In equation (5-13), $\widetilde{P}$ represents the biased probabilities. The likelihood ratio $W_{Jk} = 1$ for direct Monte Carlo simulation because $P = \widetilde{P}$. Let h_{xJ} represents the mean holding time in state x_J. Consider a function θ_{xJ} which is defined as in equation (5-14).

$$\theta_{x_J} = \begin{cases} 1 & \text{if state } x_J \text{ is a failed state} \\ 0 & \text{if state } x_J \text{ is an operating state} \end{cases} \qquad (5\text{-}14)$$

The steady state unavailability is calculated by using equation (5-15).

$$Q = \frac{\frac{1}{N}\sum_{k=1}^{N}\left(\sum_{J=0}^{J_k-1}\theta_{x_J}(k)h_{x_J}(k)\right)w_{J_k}(s_k)}{\frac{1}{N}\sum_{k=1}^{N}\left(\sum_{J=0}^{J_k-1}h_{x_J}(k)\right)w_{J_k}(s_k)} \qquad (5\text{-}15)$$

The contribution from the numerator will be zero, if the system returns back to the regenerative state without visiting the failed state. The holding times of all the states are accumulated in the denominator. The holding times in the failed states are accumulated in the numerator. Once the system reaches the failed state, the failure biasing scheme is turned off. The subsequent simulation is carried out with natural probabilities (direct Monte Carlo simulation). This enables the system to return to the regenerative state quickly. Random walk simulation is terminated once the system reaches the regenerative cycle. The biased

simulation is used until the system reaches the failure state. This method of enabling the biased simulation as and when required is referred to as Dynamic Importance Sampling (DIS) in literature [5-15, 5-26]. The notations used in equations (5-13) to (5-15) are given in table-9.

Table-9: List of Notations used

Notation	Description
K	Index for regenerative cycle
J	Index for number of jumps / transitions
x_J	System state after J^{th} jump / transition
S	Sequence of states visited
h_{xJ}	Holding time in state x_J
θ_{xJ}	Indicator function for state x_J
w_J	Likelihood ratio after J^{th} jump / transition

The Mean Time To Failure (MTTF) is expressed as a ratio of two quantities. The expression for MTTF is given in equation (5-16) [5-15].

$$E(\tau_F) = \frac{E\,[\min(\tau_F,\tau_0)]}{P\,(\tau_F < \tau_0)} \qquad (5\text{-}16)$$

In equation (5-16), τ_F denotes the time of first entry of the Markov chain to the failed state. τ_0 is the time of returning to the regenerative state. Let H_k denotes the sum of holding times in each state for k^{th} regenerative cycle until the system reaches the failed state or regenerative state whichever is earlier. The numerator in equation (5-16) is computed by using equation (5-17).

$$\mathrm{E}(\min(\tau_F, \tau_0)) = \frac{1}{N}\sum_{k=1}^{N} H_k \qquad (5\text{-}17)$$

N is the number of regenerative cycles in equation (5-17). Let W_{Fk} is the likelihood ratio for the k^{th} regenerative cycle in which system enters the failed state before returning to the

regenerative state. W_{Fk} is zero, when the system returns to the regenerative state without entering the failed state. Let W_k is the likelihood ratio in the k^{th} regenerative cycle when the system returns to the regenerative state. W_k is stored for each regenerative cycle irrespective of whether the system has reached the failed state or not in that particular regenerative cycle. The denominator in equation (5-16) is computed by using equation (5-18).

$$P(\tau_F < \tau_0) = \frac{\sum_{k=1}^{N} W_{Fk}}{\sum_{k=1}^{N} W_k} \qquad (5\text{-}18)$$

Equations (5-15) and (5-16) are used to compute the steady state unavailability and Mean Time To Failure.

5.3.5.3.1 Variance Estimation for Steady State Measures

N independent identically distributed (iid) random walks (regenerative cycles) are simulated to estimate steady state unavailability and MTTF. It is possible to estimate the confidence bounds from the samples directly by using central limit theorem [5-12]. The relative error of an estimator is defined [5-13] to be the expected relative width of its confidence interval for a fixed number of samples N and a given confidence level (1-δ)×100%. Let Z_δ denotes the (1-δ/2) confidence level of the normal distribution. The relative error for the desired estimate $\hat{\theta}$ is given in equation (5-19).

$$\text{RE of } \hat{\theta} = \frac{Z_\delta}{\hat{\theta}} \sqrt{\frac{\sigma^2(\theta)}{N}} \qquad (5\text{-}19)$$

The symbol $\hat{\theta}$ represents the steady state unavailability or MTTF value calculated from equation (5-15) or (5-16). Let us consider the equations (5-15) and (5-16). Let A_i and B_i denote the values of the numerator and denominator for the i^{th} random walk simulation. The variance $\sigma^2(\theta)$ in equation (5-19) is estimated by using equation (5-20) [5-15].

$$\sigma^2(\theta) = \frac{\text{Var}\,(A_i - \hat{\theta}\, B_i)}{E(B_i)^2} \qquad (5\text{-}20)$$

The numerator of equation (5-20) is the variance of the quantity A_i-$\hat{\theta}$ B_i. The denominator of equation (5-20) is the squared mean value of B_i.

5.3.5.4 Biased Simulation Procedure for Estimating Transient Measures

CTMC simulation is used for estimating transient measures like failure probability as explained in section-5.3.3. The system is assumed to be in the regenerative state at the initial time. In the previous section, the objective is to estimate the steady state measures. The probability of failure transitions are increased to make the system reach the failed state quickly. There is no constraint on the simulation with respect to time. The mean holding time in each state is used to estimate the steady state measures. For the estimation of transient measures, the system should reach the failed state within a specific mission time. This introduces an additional constraint with respect to time. Forced transition is the technique to meet this constraint. Let T_R denote the time spent by the system in the initial regenerative state. Let T_m be the mission time. Usually T_R is greater than T_m. So it is difficult to observe system failures in direct Monte Carlo simulation within the mission time. Forced transition technique is applied when the system is in regenerative state at the initial time. In other states forced transition need not be applied. This is due to the presence of at least one failed component whose repair rate will contribute to system transition rate. This results in a significant reduction in mean holding time of that state. Once the system comes out of its initial regenerative state, failure biasing is applied to make the system reach the failed states quickly. The simulation scheme explained in section 5.3.5.3 is applicable here also except for one difference. The difference is the application of forced transition at the initial regenerative state of the system. For failure probability estimation, the system failed state is considered as the absorbing state. The random walk simulation is terminated once the system reaches the failed state or the system reaches the regenerative state whichever is earlier.

Let W_i denotes the value of the likelihood ratio when the system has entered the failure state in the i^{th} regenerative cycle. This likelihood ratio value W_i consists of two parts. The first part is due to the application of forcing technique. In direct Monte Carlo simulation,

the time to failure is sampled from the exponential density function denoted by f. In biased simulation using forcing technique, the time is sampled from the density function in equation (5-8). The likelihood ratio contribution due to the application of forcing technique is given by $\frac{f}{\tilde{f}}$. The second part of W_i is due to the application of failure biasing schemes which is explained in section-5.3.5.3. The likelihood ratio from the second part is given by $\frac{P}{\tilde{P}}$. W_i is given by equation (5-21).

$$W_i = \left(\frac{f}{\tilde{f}}\right)\left(\frac{P}{\tilde{P}}\right) \qquad (5\text{-}21)$$

The value of W_i is zero if the system returns to the regenerative state without reaching the failed state. The system failure probability (P_F) is calculated by using equation (5-22).

$$P_F = \frac{1}{N}\sum_{I=1}^{N} W_i \qquad (5\text{-}22)$$

The relative error on P_F is computed by using equation (5-19). $\sigma^2(\theta)$ in equation (5-19) for this case is simply the variance in W_i.

5.4 Modelling of ShutDown System

The description of ShutDown System and the success criteria are explained in section 2.1.1. In this study events which have an impact on whole core alone are considered. The events which affect a particular subassembly or few sub assemblies are not considered. The system model in this study consists of 78 components and 15 common cause component groups. There are two possible states for each component. One is the operating state and the other is the failed state. The state space of the system is huge with 2^{78} states. The input data required for this analysis are the failure and repair rates of components and common cause failure data. The failure and repair rates of components along with common cause factors are given in table- 10. The level of redundancy varies from 3 to 14.

Table-10: Component Data used for Shut Down System

Component Category	Failure Rate (/h)	MTTR (h)	Test Interval (h)	CCF Factors	Remarks
Control Safety Rods (CSR)	1.25E-06	24	-	β_1= 5% β = 2%	β_1 models the CCF among CSR and β models the CCF between CSR and DSR.
Diverse Safety Rods (DSR)	1.25E-06	24	-	β_1= 5% β = 2%	β_1 models the CCF among DSR and β models the CCF between CSR and DSR.
Scram Circuit	2.0E-07	4	24	β_1= 5%	β_1 models the CCF among scram circuits. Two groups are considered for two sets of scram circuits.
Scram Switches	4.2E-09	24	-	β_1= 10%	CCF of scram switches. Two groups are considered.
Signal Processing Cards (temperature)	3.0E-06	4	-	β_1= 5%	CCF of signal processing cards (temperature)
Signal Processing Cards (Flow)	3.0E-06	4	-	β_1= 5%	CCF of signal processing cards (Flow)
Signal Processing Cards (Neutronic)	3.0E-06	4	-	β_1= 5%	CCF of signal processing cards (Neutronic)
Thermocouple	1.0E-06	100	-	β_1= 5%	CCF of thermocouples
EM Flow meter	4.2E-06	4	-	β_1= 5%	CCF of EM Flow meters
P/Q Computing Element	1.0E-05	4	-	β_1= 5%	CCF of P/Q computing element
Neutron Sensor	7.0E-06	4	-	β_1= 5%	CCF of P/Q sensors
Safety Logic with Fine Impulse Test (SLFIT)	1.0E-07	48	-	-	-
Optical Link	2.1E-08	48	-	-	-
Pulse Coded Safety Logic (PCSL)	3.33E-08	48	-	-	-

The β factor model is used to model common cause failures. The steady state unavailability and MTTF were calculated by four different methods. A fault tree was developed for the shutdown system using ISOGRAPH software and the steady state unavailability and MTTF were calculated. Programs were developed to implement direct

Monte Carlo simulation, biased Monte Carlo simulation with simple failure biasing and balanced failure biasing. For the Monte Carlo simulation the number of simulations is kept fixed at N = 3×10^5 simulations for direct and biased simulations. This will help us to understand the amount of variance reduction achieved for the given computational effort by different simulation schemes. The inputs required for the program are 1) failure and repair rates of components 2) The combination of component failures which define the failed state of the system and 3) the common cause component groups which define the failure rate of that group and list of components affected by the common cause event. 30 high risk significant combinations of component failures which define the failed state of the system are considered for this study. There is only one repair facility available which selects the failed components at random. The time to failure and time to repair are assumed to be exponentially distributed. Separate variables keep track of the measures for unavailability estimation and MTTF estimation.

The regenerative method of simulation as explained in section 5.3.5.3 is used here. Some of the random walks (regenerative cycle) may take a large time to reach the regenerative state due to the huge state space. This difficulty is overcome by setting a cut-off value on the likelihood ratio. The likelihood ratio is continuously monitored and if it reaches a value less than or equal to the cut-off value [5-26], the biasing is turned off. Subsequent simulation is continued with natural probabilities which will move the system towards regenerative state quickly. The cut-off value for likelihood ratio used in this study is 1e-40 for both simple failure biasing and balanced failure biasing schemes. The value of the biasing parameter ρ used in this study is 0.5 as suggested in [5-26].

5.5 Results

The unavailability and MTTF of shutdown system obtained from the four different methods indicated in section 5.4 are presented in table-11. The component data in table-10 is

used for carrying out the simulation. The 3σ confidence bounds are given in brackets.

Table-11: Comparison of Unavailability and MTTF by Different Methods

Method	No. of Simulations	Unavailability	MTTF (hrs)
Fault Tree Analysis	-	3.17E-08	7.38E+08
Direct Monte Carlo Simulation	3.0E+05	3.47E-08 (± 6.33E-08)	6.87E+08 (± 1.25E+09)
Biased Simulation With Simple Failure Biasing	3.0E+05	3.49E-08 (± 6.33E-08)	6.80E+08 (± 1.22E+09)
Biased Simulation with Balanced Failure Biasing	3.0E+05	3.19 E-08 (± 1.42 E-09)	7.67 E+08 (± 3.24 E+07)

Following observations are made from the results reported in table-11.

1. The relative error percentage corresponding to 3σ confidence bounds as computed by equation (5-19) for the three simulation schemes can be compared. The relative error is ~182% for unavailability and MTTF using direct Monte Carlo simulation. The relative error is ~181% for unavailability and ~179% for MTTF by simple failure biasing. The relative error for unavailability and MTTF from balanced failure biasing scheme is ~4.5% and ~4.2%. The computational effort in terms of number of simulations is the same in all the three cases (N=3.0E+05). The balanced failure biasing outperforms the other two methods in terms of variance reduction for the given computational effort.

2. The computational effort needed to reduce the relative error corresponding to 3σ confidence bounds around 5% in simple failure biasing and direct Monte Carlo simulation is approximately 6.0E+07 simulations (regenerative cycles). The steady state unavailability and MTTF results obtained from direct Monte Carlo simulation and simple failure biasing method are comparable with fault tree results in this case. The reduction in computational

effort due to the balanced failure biasing is approximately 200 times for achieving the same relative error.

3. It is also found that the results obtained by balanced failure biasing Monte Carlo simulation closely matches with fault tree results. This gives confidence to use this method for future system analysis and to combine physical process with system hardware evolution.

Different biased Monte Carlo simulation schemes are applied on a typical reactor safety system and its performance are compared. In most literature studies, different Monte Carlo simulation schemes are applied on example systems with few components. A suitable Monte Carlo simulation scheme is identified, which will be combined with physical process evolution. Use of Monte Carlo simulation for system hardware changes helps to model both failure and repair transitions. Repair transitions are not addressed in other widely used dynamic PSA tools such as dynamic flow graph methodology and Markov CCMT. Another advantage of combining Monte Carlo simulation of system hardware with physical process is that the branching times are stochastic where as it has to be specified by analyst in the above dynamic PSA methods. The Monte Carlo simulation of system hardware is combined with a simple physical process in the next chapter. Subsequently it is applied to a passive decay heat removal system of a FBR.

This page is left blank

Chapter-6 Dynamic Reliability Analysis of a Passive Safety System

6.0 Introduction

The Monte Carlo simulation of system hardware identified in the previous chapter is combined with a physical process in a simple example system. The example is chosen such that, it is possible to evaluate the failure probabilities through analytical integration. This example demonstrates that in the absence of significant interactions between physical process and system hardware, the effect of timing of failures can be addressed by using appropriate classical models. When there is significant interaction between physical process and system hardware, dynamic PSA tools are needed. The interaction between the physical process and hardware components can be of three types. The first type is the changes in physical process parameters due to stochastic changes in system hardware configuration. The second type is the changes in system hardware configuration induced by the process parameter conditions. Failure / degradation of components due to extreme conditions like high temperature and pressure are examples of this type. The third type of interaction is the changes in system hardware configuration due to the process parameters crossing some threshold limits. A particular type of interaction or all types of interactions may be present in a safety system depending on the scenario being analysed. A passive decay heat removal system of a FBR is chosen as the second example. The general perception is that passive systems are more reliable and offer enhanced safety than active systems. This is due to the dependence of active systems on external power sources in contrast to the passive systems which rely on natural forces like gravity. Due to the weak driving forces in a passive system, the process uncertainties are significantly large. The dynamic PSA of a passive decay heat removal system is carried out with the following objectives.

i) Development and demonstration of a method to carry out the dynamic PSA of a passive decay heat removal system in the absence of full featured dynamic PSA tools. This is

achieved by combining the process uncertainty quantification in functional reliability analysis and system hardware evolution through Monte Carlo simulation. This method is applicable when only the first type of interaction is present between the process and system hardware.

ii) One of the open issues in dynamic PSA is under what conditions dynamic PSA results are significantly different from classical approaches. An attempt to address this issue with an example passive decay heat removal system which has the first type of process and system hardware interaction is made. It is shown that when the contribution of process uncertainty to total failure probability dominates, the results from classical and dynamic approaches converge. The results are significantly different from the two approaches when the contribution of process uncertainty to total failure probability is not dominant.

6.1 Dynamic Reliability Analysis of a simple example system

Consider a tank of liquid sodium with a constant heat source. The sodium in the tank is assumed to be at a uniform temperature. The initial temperature of the fluid is 590^{o}C. At t=0, heat addition to the fluid starts and is given by equation (6-1).

$$q(t) = q_0 \qquad (6\text{-}1)$$

This heat addition leads to increase in temperature of the fluid. The temperature of sodium at any time t is given by equation (6-2).

$$T(t) = T_{init} + \frac{1}{MC_p}\int_0^t q(t)dt \qquad (6\text{-}2)$$

T_{init} is the initial temperature and T (t) is the temperature at time t. M is the mass of the fluid in the tank (1000 Kg). C_p is the specific heat capacity of liquid sodium (1240 J/Kg/K). q_0 value is assumed to be 0.52 kW. Two temperature limits are defined for this system. The first temperature limit is called the Threshold limit (T_L), and the other temperature limit is called Design Safety Limit (DSL) such that DSL > T_L. The initial temperature (T_{init}) of the fluid is less than the threshold temperature limit (T_L). A demand is placed on the safety system at the

temperature T_L. If the temperature crosses the DSL it is failure of the system. The objective is to find the probability P (T (t) ≥ DSL).

A schematic diagram of the above system is shown in fig.18. The system consists of two temperature sensors (S1 and S2), a controller (CONT) and a heat removal circuit (HRC). All components in this system are assumed to be repairable. The temperature of the fluid in the tank is continuously monitored by two sensors S1 and S2. The controller will actuate the heat removal circuit when the temperature of the fluid reaches the threshold temperature limit (T_L). Each component in the safety system is assumed to have binary states. One state is the operating state and the other is the failed state. The failure and repair rates of components are given in table-12. The safety system may be unavailable due to any of the component failures as given by the cut sets in table-13. Let t_L denotes the time at which the temperature of the fluid reaches T_L. The time taken by the fluid to reach the temperature limit DSL is denoted by t_{DSL}. This can be computed from equation (6-2). The mission is assumed to be a success if the system is available at any instant between t_L and t_{DSL}. The time interval between t_L and t_{DSL} is called the critical time interval. The temperature of the fluid evolves as per equation (6-2) if the safety system is unavailable. Let Ψ(t) denotes an indicator function of system state at time t. Ψ (t) can be either 1 or zero representing operating and failed states of the system respectively. The failure criterion of the system can be given in terms of the indicator function as in equation (6-3).

$$\text{Failure: if } \psi(t) = 0;\ \forall t,\ t_L \le t < t_{DSL} \qquad (6\text{-}3)$$

else it is success

Equation (6-3) implies that if the system has failed before t_L and it is not able recover within the critical time interval then the mission is a failure.

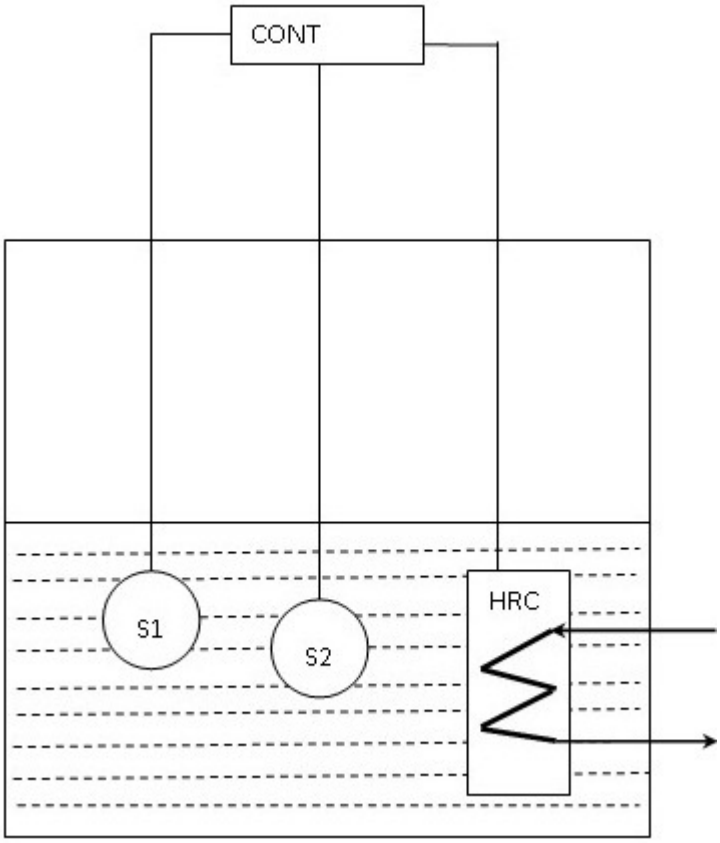

Fig.18: Schematic Diagram of Example System

Table-12: Failure and Repair Rates of Components of Example System

Component Number	Component	Failure Rate (/h)	Repair Rate(/h)
1.	Sensor-S1	1E-03	0.125
2.	Sensor-S2	1E-04	0.125
3.	Controller-CONT	1E-03	0.0833
4.	Heat Removal Circuit-HRC	1E-04	0.0625

Table-13: Minimal Cut sets for the Example System

Cut set Number	Minimal Cut sets
1.	HRC
2.	CONT
3.	S1.S2

The following scenario is modelled with the example system. The T_L value is assumed to be 600^{o}C and the DSL is varied from 600^{o}C+ ϵ to 650^{o}C. Here $\epsilon < 0.5^o$C. The objective is to find the failure probabilities as a function of critical time interval. The system hardware is dependent on the process through the parameter critical time interval. The critical

time interval depends on the process evolution with time. If the failed system can recover to its operating state within the critical time interval then it is a successful mission. A simple constant heat addition process model is used in this example. Also there is no change in process evolution due to the failure of any of the components. The results obtained from simulation can be compared with analytical integration with appropriate time limits because of the above assumptions. The approach adopted here for analytical integration is Time Dependent Cut set Evaluation (TDCE) [6-1, 6-2]. There are three minimal cut sets in this example. The probability of the fluid temperature crossing the DSL is calculated by analytical integration using equation (6-4).

$$P\ (T(t) \geq DSL) = \sum_{j=1}^{N_{cs}} \int_{t=0}^{t_L} \prod_i \lambda_{ij}\ e^{-\lambda_{ij}t}.e^{-\mu_{ij}(t_{DSL}-t)}\ dt \qquad (6\text{-}4)$$

λ_{ij} is the failure rate of i^{th} component appearing in j^{th} cut set. μ_{ij} is the repair rate of the i^{th} component in j^{th} cut set. N_{cs} is the number of cut sets. Π_i is the product over the components i appearing in j^{th} cut set.

A program is developed to implement the Monte Carlo simulation scheme explained in section 5.3.5.4. In this simulation scheme both process and system hardware state evolves with time. The fluid is assumed to be at the initial temperature of T_{init} and the system is assumed to be in the operating state. Also it is assumed that all hardware components in the system are in the operating state at t=0. The next transition time of the hardware state is sampled assuming exponential times to failure and repair for hardware components. Normally this time will be much greater than the mission time (~40 hours in this example). It is difficult to observe system failures within the stipulated mission time. So CTMC simulation is used in this study. The biased simulation schemes for CTMC simulation need to satisfy the two requirements mentioned in section 5.3.3. So forced transition technique is combined with balanced failure biasing in this study. Forced transition technique is explained

in section 5.3.5.1. The number of regenerative simulation cycles is 3×10^5. The relative error is less than 6% corresponding to 95% confidence bounds for all the cases.

The fault tree approach can be used in this simple example to estimate the failure probabilities. The steady state unavailability calculated from fault tree is ~1.34E-02. The fault tree used for this calculation is shown in figure.19. This is a straight forward analysis in

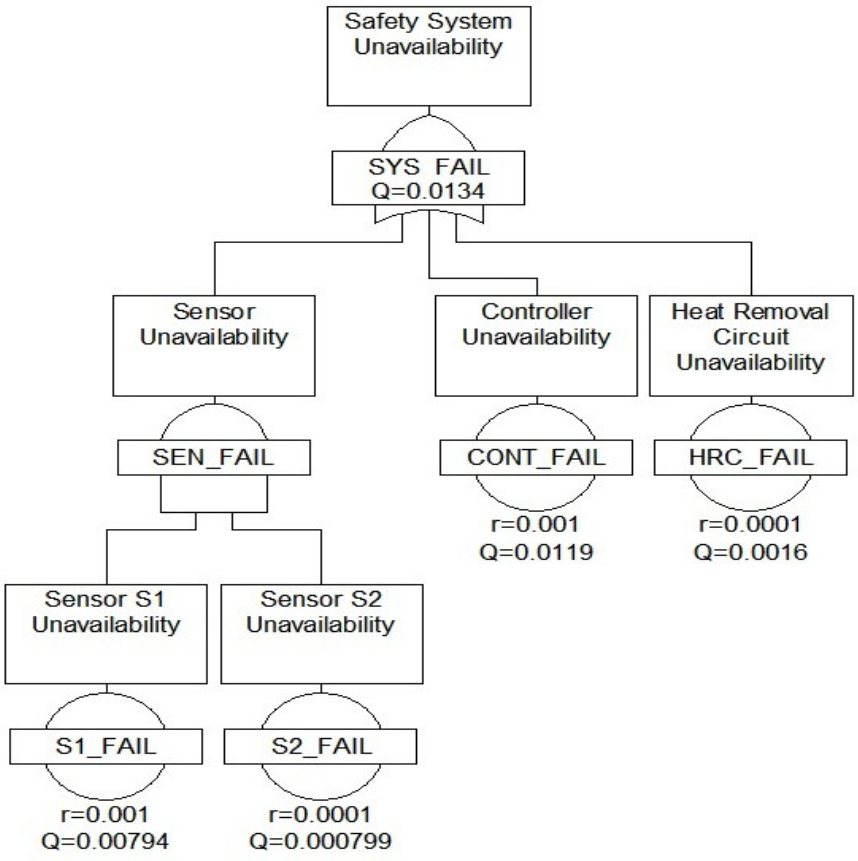

Fig.19: Simple Fault Tree for the example system

which steady state component unavailability of different components are combined using fault tree. The above simple fault tree approach can be improved by taking into consideration the time intervals available for the recovery (repair) of different components. In this approach the failure and non-recovery of components are separated into two parts. The improved fault tree is shown in figure.20.

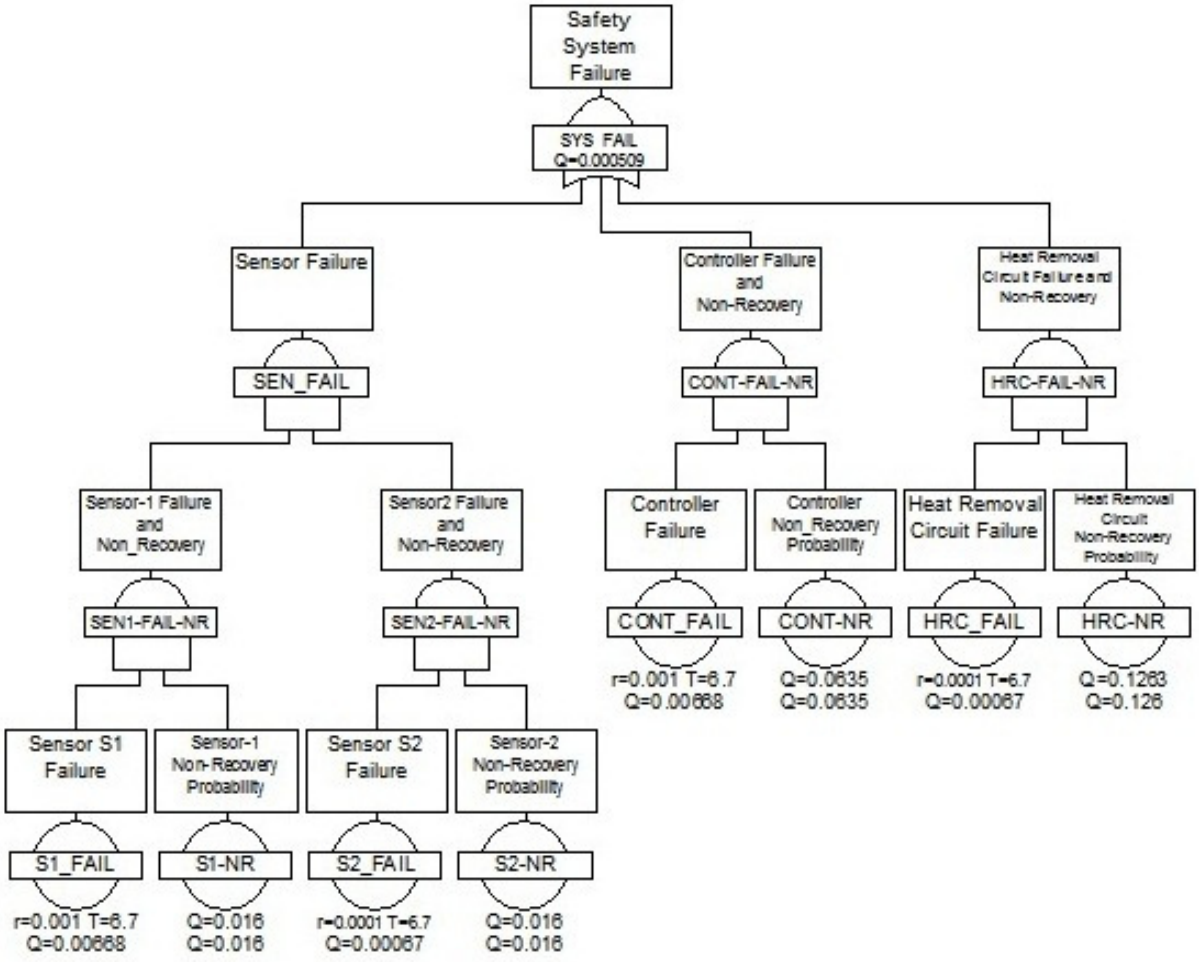

Fig.20: Improved Fault Tree for the example system

The failure probability of the components is calculated for the duration t_L. The non-recovery probability of components is estimated for the duration $(t_{DSL}-t_L)$. The non-recovery probabilities are computed by assuming exponential times to repair for components. The results obtained from all the four methods are compared in figure.21.

The results obtained from Monte Carlo simulation and Time Dependent Cut set Evaluation method matches closely. The steady state unavailability calculated from simple fault tree approach is conservative. The improved fault tree approach gives better results as compared with simple fault tree approach. The application of TDCE method and construction of improved fault tree is difficult in general for reactor safety systems due to the following reason.

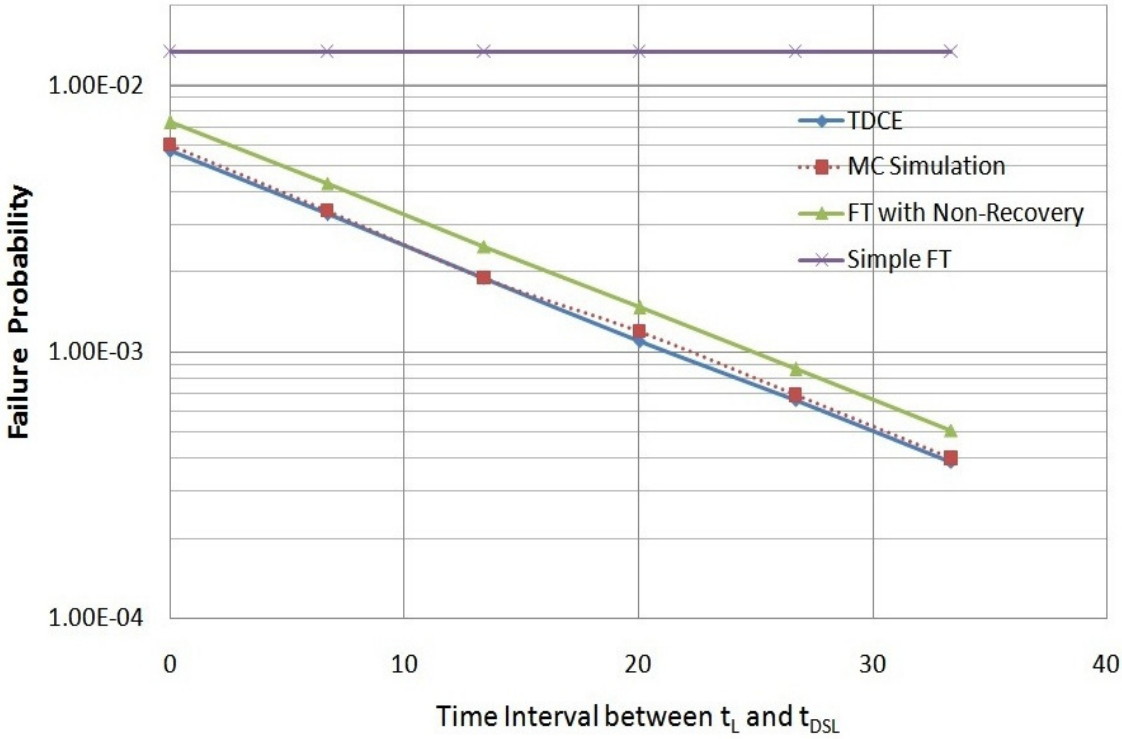

Fig.21: Results from the four Methods for the example system

In the present example, restrictive assumptions are made to compare the results from different methods. The uncertainties in physical process evolution are not considered. Also a simple process evolution is assumed which does not change with hardware component failure / recovery. The physical process evolution can change as a function of system hardware configuration. The calculation of non recovery probability for each component as a function of process evolution is difficult due to the process uncertainties. Use of TDCE method and improved fault tree under such conditions will be very difficult.

This study demonstrates that in the absence of significant process and system hardware interaction, TDCE method and fault tree with non recovery can predict close results with dynamic PSA method. The TDCE method and fault tree with non-recovery are difficult to model when there is significant interaction between process and system hardware. The dynamic reliability analysis of a passive decay heat removal system of a FBR is explained in the next section.

6.2 Description of Passive Decay Heat Removal System

The system considered for this study is similar to the Safety Grade Decay Heat Removal System (SGDHRS) explained in section 2.1.3. Detailed fault tree model of this system is used to carry out the level-1 internal events PSA explained in chapter-3. However for the present study only 65 risk significant components identified from fault tree analysis are used. The system function is explained in the following section.

6.2.1 System Function

During normal reactor operation all the four loops are in poised state [6-3]. In this state the four dampers in each loop are in cracked open position allowing about 35% nominal flow in the intermediate loop. This helps to quickly establish natural convection flows when dampers are opened. Following a demand on this decay heat removal system, all the dampers are opened from crack open to full open on auto or manual allowing natural convection in the loops to increase. Forced convection in the loop can be maintained by primary sodium pumps operating on class-III power or battery backed class-II power. The reactor is not permitted to be on power without the availability of all the four loops of this decay heat removal system. When leak detectors provided for pipes and components detect a sodium leak, the sodium from the loops is drained to the storage tank by opening the dump valves on manual command. The sodium leak in AHX is detected by leak detectors. The leak detectors are arranged in two out of three logic. On detecting a sodium leak, the air dampers close automatically and nitrogen is supplied to AHX cabin. The sodium is drained to the storage tank on manual command.

6.2.2 Safety Limits on Temperature

The hot pool is one of the important locations for which the temperatures are to be kept below certain safety limits. The design safety limits for Hot Pool Temperature (HPT) are given in table-14. There are three categories of safety limits on HPT. Cumulative Damage

Fraction (CDF) approach is followed for defining temperature limits. If hot pool temperature crosses category-3 DSL one time, the apportioned damage fraction will be exhausted and the plant integrity may be impaired to the extent that reactor restart may not be possible. But public health and safety are assured. The probability of exceeding the category-3 DSL is significant in the context of plant availability and economics. If the hot pool temperature is crossing the category-4 DSL, critical structural damage can occur which can lead to radioactivity release. The probability of exceeding the category-4 DSL is significant from the context of public safety. Plant restart is possible if category-2 DSL is crossed. Frequent crossing of category-2 DSL may exhaust the apportioned cumulative damage fraction.

Table-14: Design Safety Limits on Hot Pool Temperature

Parameter	Category-2	Category-3	Category-4
Hot Pool Temperature	600^{o}C	625^{o}C	650^{o}C

The objective of the present study is to evaluate the probability of crossing the different category of design safety limits on hot pool temperature.

6.3 Comparison of Failure Probability Estimation by Different Methods

Due to the weak driving forces in passive systems, the uncertainties associated with process parameters are significantly large in passive systems as compared to active systems. Dynamic reliability approaches model the uncertainties in process parameters together with stochastic changes in system hardware configuration. These approaches require the integration of detailed process models (process computer codes) with system hardware evolution models. The development of such a tool requires a lot of resources and time. The following approach is adopted in this study in the absence of above mentioned tools.

A part of the dynamic reliability problem is solved in functional reliability analysis [6-4]. The functional reliability analysis of passive systems quantifies the uncertainties in process parameters for a fixed system hardware configuration. If the results of functional

reliability analysis are available, then the following approach can be adopted to estimate the probability of crossing the safety limits on temperature. The first step is to carry out the functional reliability analysis by appropriate method and quantify the response parameter distribution for nominal system hardware configuration. The response parameter distribution obtained from functional reliability analysis is split into different bins. An approximate process model is identified which can model the process dynamics in different bins by varying certain parameters of the model. The approximate process model is then combined with changes in system hardware configuration through Monte Carlo simulation.

Let φ (x,y,t) be the solution to the Chapman-Kolmogorov equation (5-1). x is a vector of process variables and y represents the system hardware state. Both x and y evolves as a function of time. The process evolves with time as given by equation (5-2). The methods of dynamic reliability analysis, functional reliability analysis and the present approach can be compared with the help of the following integrals. In dynamic reliability analysis, the probability of crossing the safety limits on process response parameter (hot pool temperature in this case) is estimated by using the integral in equation (6-5).

$$P\,(x(t) \geq T_{DSL}) = \int\int \sum_y \varphi(x, y, t)\, dx\, dt \qquad (6\text{-}5)$$

The system hardware states are assumed to be discrete. Both process and system hardware evolves with time. The probability of crossing the safety limits in the case of functional reliability analysis is estimated by using equation (6-6).

$$P\,(x(t) \geq T_{DSL}) = \int\int \varphi\,(x, y_{0,}\, t) dx dt \qquad (6\text{-}6)$$

y_0 is the fixed hardware configuration of the system and it does not evolve with time. The time integral in equation (6-6) is applied for x alone.

If the functional reliability analysis is carried out for all possible system hardware configurations, then the failure probability is estimated by using equation (6-7).

$$P(x(t) \geq T_{DSL}) = \int\int \sum_{y_i} \varphi\,(x, y_i\,, t) dx\, dt \qquad (6\text{-}7)$$

The summation is over y_i , a set of all possible discrete hardware states. The time integral is applied to x. y_i does not evolve with time. The functional reliability analysis is simply carried out for different possible hardware states. This is an extension of equation (6-6) in which only a specific hardware state is considered.

6.3.1 Failure Probability Estimation in the Present Method

The process evolution with time in dynamic PSA is given by equation (5-2). The evolution of x depends on both y (system hardware state) and time t. When the system hardware state is independent of t (fixed for the entire mission time), the process evolution depends only on t. This assumption requires that the second and third types of interaction between system hardware and process (section-5.2) are not present. Then equation (5-2) can be written as in equation (6-8).

$$\frac{dx}{dt} = f(x,t) \qquad (6\text{-}8)$$

The solution of the above equation is $x(t) = \int f(x,t)dt$. x is a vector of process variables. The result from functional reliability analysis is the response process parameter distribution which is a function of the initial condition on response process parameter and other process parameters. The selection of a particular response process parameter from the distribution is equivalent to sampling the vector x indirectly. The response process parameter is a deterministic function of given sample vector x. The functional reliability analysis results are used to sample the process parameters indirectly.

Having sampled the process parameters indirectly, the next step is to identify an approximate model for process evolution with time. Equation (5-2) is a deterministic code model. It is approximated by another model given by equation (6-9).

$$\frac{\partial\theta}{\partial t} = g_y(\theta,t) \qquad (6\text{-}9)$$

This approximate model is chosen such that it closely matches the deterministic code model in equation (5-2) for the initial system hardware configuration. The number of process

parameters in this model is less than the number of parameters in (5-2). The parameters in this model are adjusted such that max (θ(t)) calculated from equation (6-9) matches with max (x(t)) obtained from equation (5-2). Also the approximate model should closely match with the code model in equation (5-2) for other regions of the curve. This approximate model is then integrated with system hardware Monte Carlo simulation. The initial system hardware configuration in dynamic reliability analysis is assumed to be the same as the hardware configuration used for functional reliability analysis.

The response parameter distribution can be used to sample different response parameters. The other way is to divide the response parameter distribution into different bins and use one representative response parameter from each bin. Let x_1 and x_2 be two adjacent response parameters such that $x_1 - x_2 = \Delta$. Δ is of the order of few degree Celsius. P_1 and P_2 are the respective failure probabilities estimated by combining x_1 and x_2 with stochastic changes in system hardware. The difference P_1-P_2 is very small. The sampling from the response parameter distribution is not required because of the above reasons. The second approach is adopted in this study. Let the representative response parameter is denoted by x_i. The failure probability integral in the present method is given by equation (6-10).

$$P\,(x(t) \geq T_{DSL}) = \int \sum_{x_i} \sum_{y} \varphi\,(x_i, y, t)dt \qquad (6\text{-}10)$$

In the above integral, both x_i and y evolves with time.

The differences in evaluating equation (6-5) and equation (6-10) are the following.

a) The input process parameters are sampled from respective probability distributions and it is integrated with system hardware evolution with time. This is a straight forward approach and this is followed in evaluating the integral in equation (6-5). The present approach samples the process parameters in an indirect manner by selecting a representative response parameter from each bin. Also an approximate mathematical model for response parameter evolution with time is required. This approximate model is

integrated with system hardware evolution through Monte Carlo simulation. This approach is followed in evaluating the integral in equation (6-10).

b) The evaluation of the integral using equation (6-5) can be used for all types of process and hardware interactions described in section 5.2. It needs the process code to be coupled with Monte Carlo simulation of system hardware. The evaluation of the integral in equation (6-10) is possible if the second and third type of interactions between process and system hardware are not present. This assumption is used in deriving equation (6-8).

The present method is necessitated due to the non availability of dynamic PSA tools where deterministic process codes are integrated with system hardware evolution. If such tools are available it is preferable to use those tools instead of making several assumptions.

6.4 Functional Reliability Analysis of Passive Decay Heat Removal System

The two widely used methodologies for functional reliability analysis are REPAS [6-5] and RMPS [6-6]. The functional reliability analysis of the passive decay heat removal system under consideration is carried out using RMPS method [6-7, 6-8, 6-9]. The RMPS method involves the following steps. The first step is to identify the important process parameters and quantifying the uncertainties in those parameters. The second step is to propagate the uncertainties in process parameters through a best estimate code and deriving the uncertainty of response parameter. The failure probability contribution from process uncertainty is then estimated from the distribution of response parameter. The existing deterministic codes for process models are used to derive the response parameter distribution. While [6-7] estimates the functional failure probability without considering inter wrapper flow, [6-9] includes the modelling of inter wrapper flow. The modelling includes primary, intermediate and air circuits. There are 21 process parameters identified in [6-9] and their uncertainties are quantified. These uncertainties are propagated through a best estimate code DHDYN and the response parameters were evaluated. Response surface models were

constructed to relate the response parameter and 21 process input parameters. These response surface models are used to construct the distribution of response parameters through Monte Carlo simulation. The distributions of three response parameters namely Peak Hot Pool Temperature (HPT), Central Sub assembly Clad Hot Spot Temperature and Storage Sub assembly Clad Hot Spot Temperature are derived. The functional failure probabilities are estimated with and without forced circulation in primary. Different hardware configurations are considered in this study.

The response parameter of interest in this study is hot pool temperature. The peak hot pool temperature probability density without forced circulation for all the four loops available configuration is one of the results from functional reliability analysis [6-9]. The following results reported in [6-9] are used to derive the peak hot pool temperature distribution.

- The estimated functional failure probability for category-4 limits without primary forced circulation for all loops available configuration is less than 1E-8.
- The mean value of the peak hot pool temperature distribution is 580^{o}C.

It should be noted that the above mean value is reported for a particular hardware configuration. The hardware configuration considered is two loops are available for initial two hours and subsequently one loop is available. The following conservative assumptions are made on the above results to derive the response parameter distribution.

- The functional failure probability is assumed to be 1E-08 even though it is less than this value when all the four loops are available.
- The mean value of peak hot pool temperature distribution is assumed to be 580^{o}C. But when all the four loops are available it will be less than this value.

The peak hot pool temperature is normally distributed [6-7]. Based on the above conservative assumptions a normal distribution with mean 580^{o}C and standard deviation of 12.5^{o}C is derived for peak hot pool temperature and it is shown in figure-22. The selection of a

representative response parameter (x_i) from the distribution in fig.22 is equivalent to choosing a representative temperature profile from a bin, x(t) in equation (6-11).

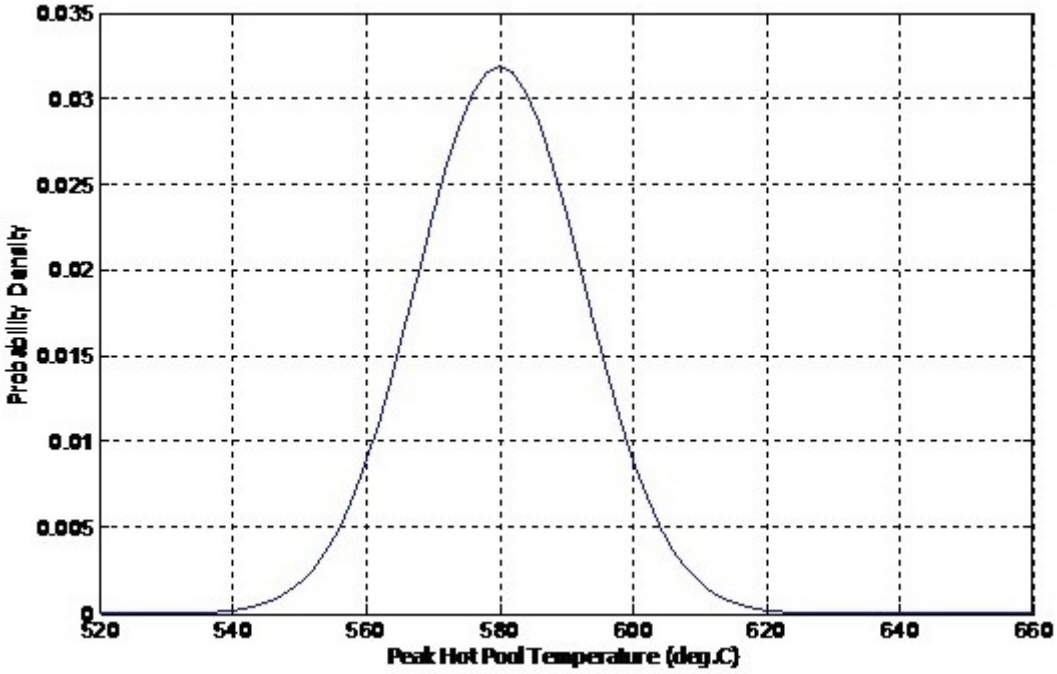

Fig.22: Probability Density of Peak Hot Pool Temperature

6.5 Approximate Process Model for Hot Pool Temperature Evolution

The next step is to identify an approximate model which can model the hot pool temperature evolution with time. This approximate model is integrated with system hardware evolution. The entire hot pool is assumed to be at a uniform temperature. The time dependence of sodium hot pool temperature is modelled by a first order differential equation given by equation (6-11) [6-10].

$$MC_p \frac{dx(t)}{dt} = P(t) - UA_j(x(t) - T) \qquad (6\text{-}11)$$

M denotes the mass of liquid in the pool. C_p is the specific heat capacity and x (t) is the hot pool temperature as a function of time. The effective heat transfer area is denoted by A_j. A_j is a function of system hardware state. T is the atmospheric temperature. The heat transfer coefficient is denoted by U. The heat deposited in the hot pool is removed by the sodium to air heat exchanger (AHX). The effective heat transfer area is the heat transfer area of AHX.

The initial hot pool temperature is 550^{o}C. P (t) is decay power which is given by equation (6-12) [6-11].

$$P(t) = P_0\, t^{-0.28} \quad \text{for } t \geq 1 \text{ sec} \qquad (6\text{-}12)$$

$$P(t) = P_0 \text{ for } t < 1 \text{ sec}$$

Short time steps are used for the initial three hours of process evolution (0.5 seconds) and subsequently large time steps are used (10 seconds). A typical set of temperature profiles are given in fig.23. The temperature profile with its peak hot pool temperature given by the mean of the distribution (in fig.22) is indicated by a solid line. The other temperature profiles occur due to the uncertainties in various parameters. The probability density of peak temperatures of all possible temperature profiles is shown in fig.22. The distribution in fig.22 gives a set of possible temperature profiles due to the uncertainty in process parameters.

A specific peak hot pool temperature (x_i) in fig.22 occurs due to the specific combination of the 21 process parameters considered in functional reliability analysis. Of the 21 process parameters, the response parameter (peak hot pool temperature) is highly sensitive to decay power [6-9]. The parameter P_0 in equation (6-12), is adjusted satisfying the conditions mentioned in section 6.3.1. All other parameters in the approximate model in equation (6-11) are kept at their nominal values. It is to be noted that the temperature profiles shown in fig.23 are for all loops available system hardware configuration obtained from the adjusted model of equation (6-11). Let the temperature profiles shown in figure.23 be identified by TP_i satisfying the condition max (TP_i) = x_i. The temperature profiles are arranged in such a way that max (TP_{i-1}) < max (TP_i) with i = 2,3,...n_b. n_b represents the number of bins.

6.6 System Hardware Model

The system hardware boundary includes DHX, components in the intermediate and air circuit. Totally 64 hardware components were identified based on an initial screening

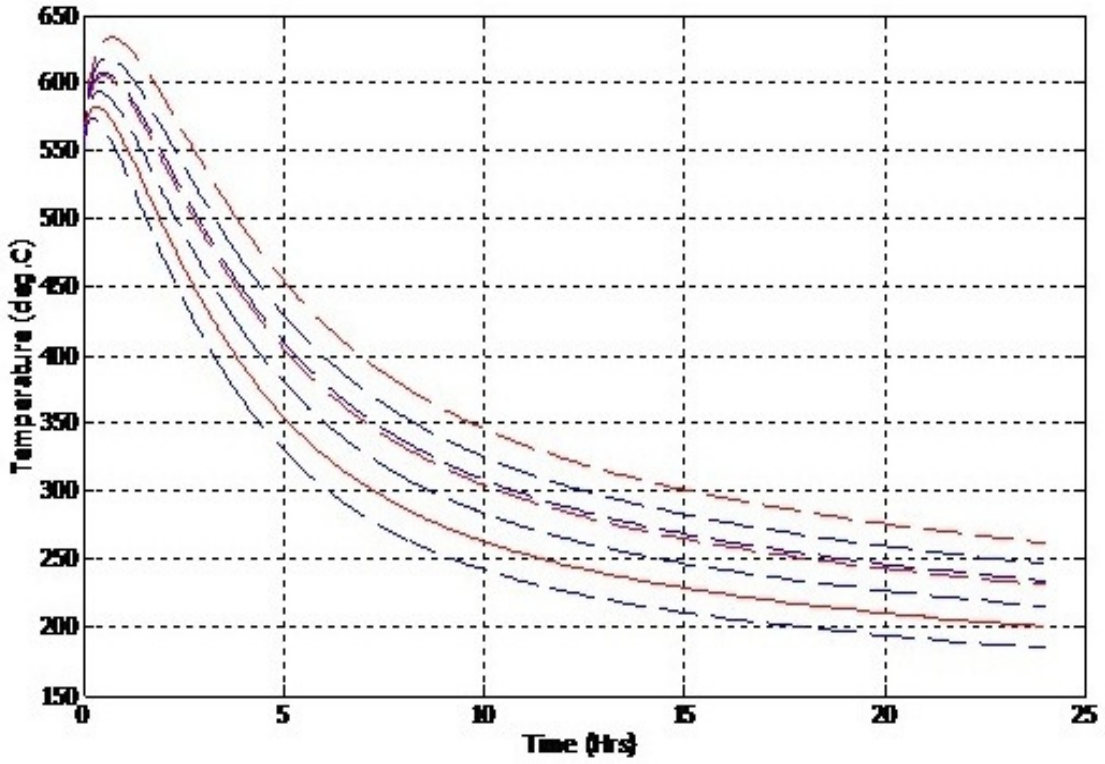

Fig.23: Typical Temperature Profiles

analysis. The parameter A_j in equation (6-11) relates the system hardware state and process evolution. A_j is given by equation (6-13).

$$A_j = n.A_l \quad n = 0,1,2,3,4 \qquad (6\text{-}13)$$

A_l denotes the effective heat transfer area of a single loop. Each loop is modelled with 16 hardware components and a particular loop may be unavailable due to the failure of a single or multiple components in that loop. More than one loop may be unavailable due to common cause failures. The number of available loops determines the process evolution. These 64 components can be grouped into 9 categories. The failure rates, Mean Time To Repair (MTTR) and common cause groupings used for this analysis are given in table-15. The details of common cause component groups and the combination of component failures which can lead to a loop / loops failure is another required input for this analysis. In this analysis it is assumed that there in only one repair facility where failed components are

repaired at random. The failure modes considered for different categories of components are given in brackets along with component category.

Table-15: Component Data used for Passive Decay Heat Removal System

Component Category	Failure Rate (/h)	MTTR (h)	Common Cause Factors	Remarks
Sodium to Sodium heat exchanger (DHX) (Tube leak)	2.5E-07	720	β_1 = 4 % β_2 = 4 %	Two DHX are of one design and another two different design-Two CCF groups
Sodium to Air Heat Exchanger (AHX) (Leak in tubes)	3.0E-06	360	β_1 = 4 % β_2 = 4 %	Two AHX are of one design and another two different design-Two CCF groups
Dump Valves (Leak)	1.0E-06	72	β_1 = 1 % β_2 = 1 %	Two CCF groups based on location
Check Valves (Leak)	1.0E-06	72	β_1 = 1 % β_2 = 1 %	Two CCF groups based on location
Instrumentation (Fail to function)	1.0E-07	4	β_1 = 1 %	One CCF group
Stack (blockage or collapse)	1.0E-08	108	β_1 = 1 %	One CCF group
Intermediate circuit pipeline (leak)	1.0E-08	360	β_1 = 1 %	One CCF group
Air dampers (stuck in crack open / closed condition)	4.2E-05	24	β_1 = 1 %	One CCF group
Inadvertent loss of sodium in loops	1.0E-05	4	β_1 = 0.01%	One CCF group

Human plays a role in the opening of air dampers. Following reactor SCRAM, there will be an alarm in control room and the air dampers will open automatically. If the dampers fail to open on auto, the operator can open the dampers manually. If the dampers are not opening on auto and manual then it is assumed to be a failure. A screening value of 1.0E-03 for human error probability [6-12] to manually open the damper is used in this analysis.

A short term demand on the passive decay heat removal system is the scenario analysed here. Short term demand can arise on the system during short duration Loss of

Offsite Power, spurious SCRAM of reactor etc. A mission time (T_m) of 24 hours is used in this analysis. It is assumed that steam water system is unavailable and sodium in secondary circuit is available. The primary and secondary sodium pumps are assumed to be unavailable. There is no forced circulation in primary [6-9]. This is a conservative initiating event. The initial condition on the process variable is initial hot pool temperature (x (0)). The initial condition on the system hardware state is the availability of all the four loops of the decay heat removal system. Let y (t) be the variable representing the system hardware state at t. y (0) is the initial hardware state at t=0.

6.7 Integration of Process and System Hardware Evolution

As explained in section 6.3.1 the response parameter distribution is divided into different bins. The approximate model in equation (6-11) is tuned to satisfy the conditions mentioned in section 6.3.1. This approximate model is then combined with system hardware evolution using Monte Carlo simulation. The method explained in section 5.3.5.4 in chapter-5 for estimating transient measures is used in this simulation. The regenerative cycle is terminated if the system returns to the regenerative state at a time $t>0$. This is applicable when Monte Carlo simulation is used to model system hardware alone. When process evolution is combined with system hardware evolution, the termination conditions are based on hot pool temperature and mission time. During the combined simulation, the system hardware may reach the regenerative state at a time $t>0$ and $t<T_m$. The simulation will not be terminated under this condition since the mission time has not been completed. The biasing will be turned off and the simulation will be carried out with natural probabilities. This makes the simulation cycle to terminate most probably in the regenerative state.

The various steps involved in integrated simulation of process and system hardware are given as a flow chart in fig.24. The flow chart gives the steps for one regenerative cycle using direct Monte Carlo approach. These steps have to be repeated for each regenerative

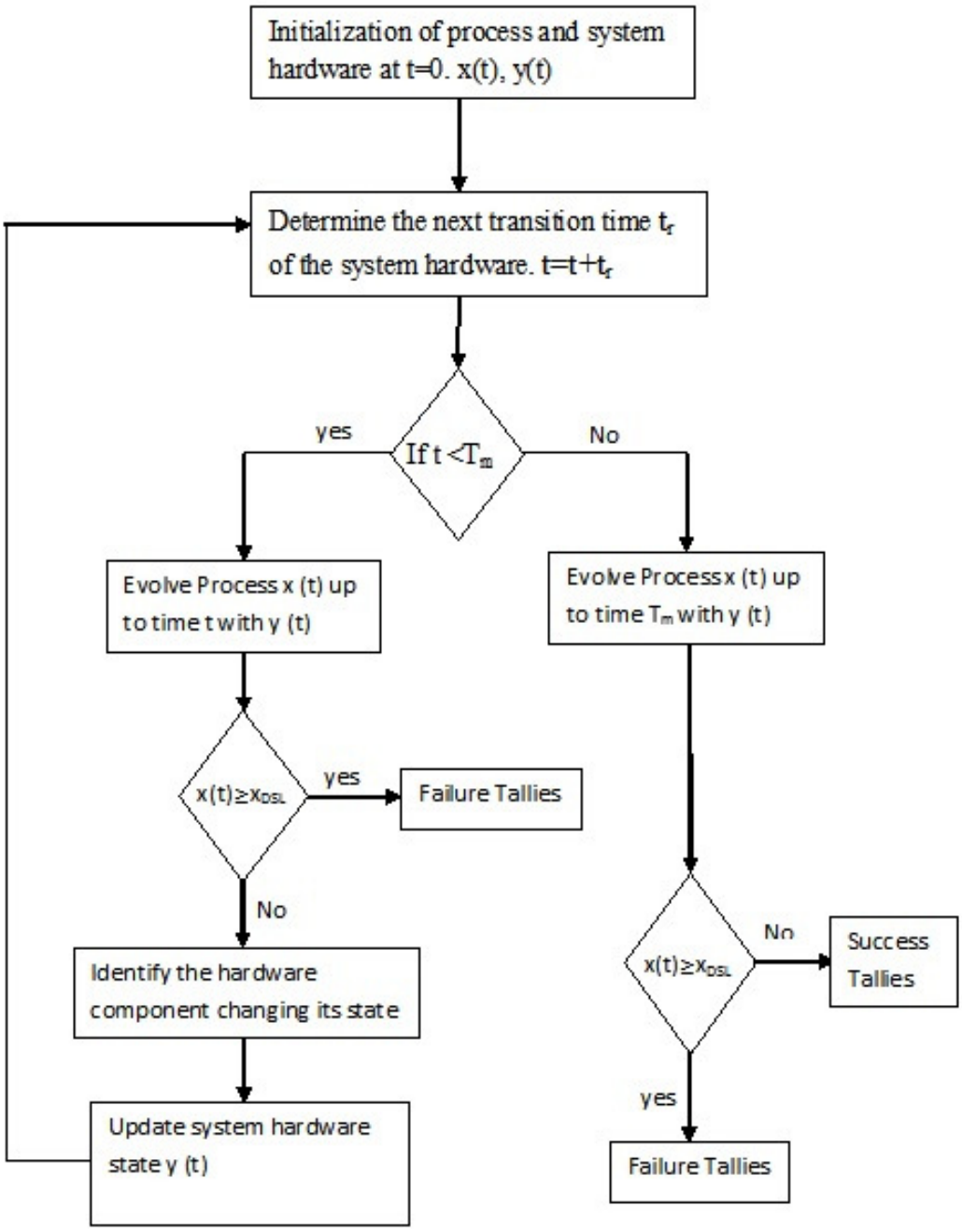

Fig.24. Integrated Simulation Scheme with Direct Monte Carlo Approach

cycle. The same simulation scheme is applicable for biased simulations also except that the biased probability densities are used for sampling. The likelihood ratios are to be computed for each transition and stored for each regenerative cycle. The hot pool temperature at time t is denoted by x (t) and system hardware state at time t is denoted by y (t). t_r is the system hardware transition time. X_{DSL} is the design safety limit for hot pool temperature as given in table-14. The mean value of failure probability and relative error on failure probability are

estimated as explained in section 5.3.5.4. The peak hot pool temperature distribution is divided into twelve bins for category-4 and nine bins for category-3 limits. Seven bins are considered for category-2 limits. The number of regenerative cycles (N) used for each bin is 3×10^5. This number is chosen because it gives a relative error of <10% for the calculated failure probabilities.

6.8 Results and Discussion

The probabilities of crossing the DSL (failure probability) on hot pool temperature for category-4, category-3 and category-2 temperature limits are calculated. The results are shown in figures 25 to 27. The failure probabilities are calculated for different evolutions of hot pool temperature. The ordering of temperature profiles is as explained in section-6.5. The cumulative failure probability is plotted on the Y-axis. The different possible hot pool temperature evolutions are given in the X-axis. The maximum cumulative failure probability is the probability of crossing the respective DSL on hot pool temperature due to the combined effect of process uncertainty and stochastic changes in system hardware.

The estimated total failure probability for category-4 temperature limits is ~ 4.0E-07. For category-3 and category-2 limits the total failure probability is ~2.0E-04 and 5.5E-02 respectively. There is a sharp increase in total failure probability in the case of category-3 and category-2 temperature limits after reaching a steady value. This increase is due to the failure probability contribution from the uncertainty in process parameters. The variation of total failure probability as a function of standard deviation of the peak hot pool temperature probability density is studied. The results are given in Fig.28.

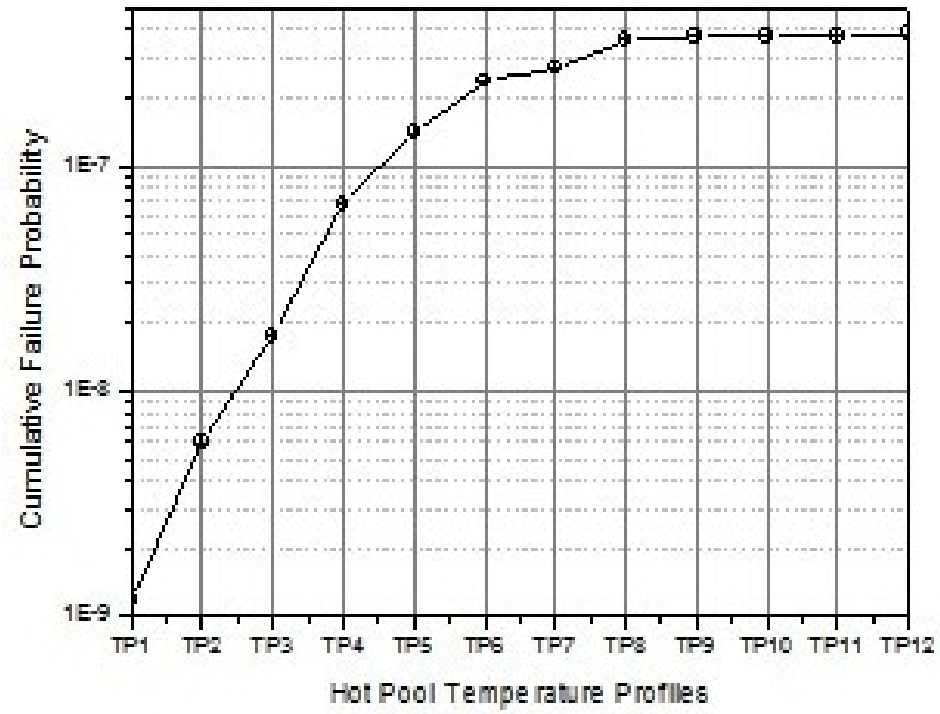

Fig.25: Cumulative Failure Probability of Different Hot Pool Temperature Profiles for Category-4 limits

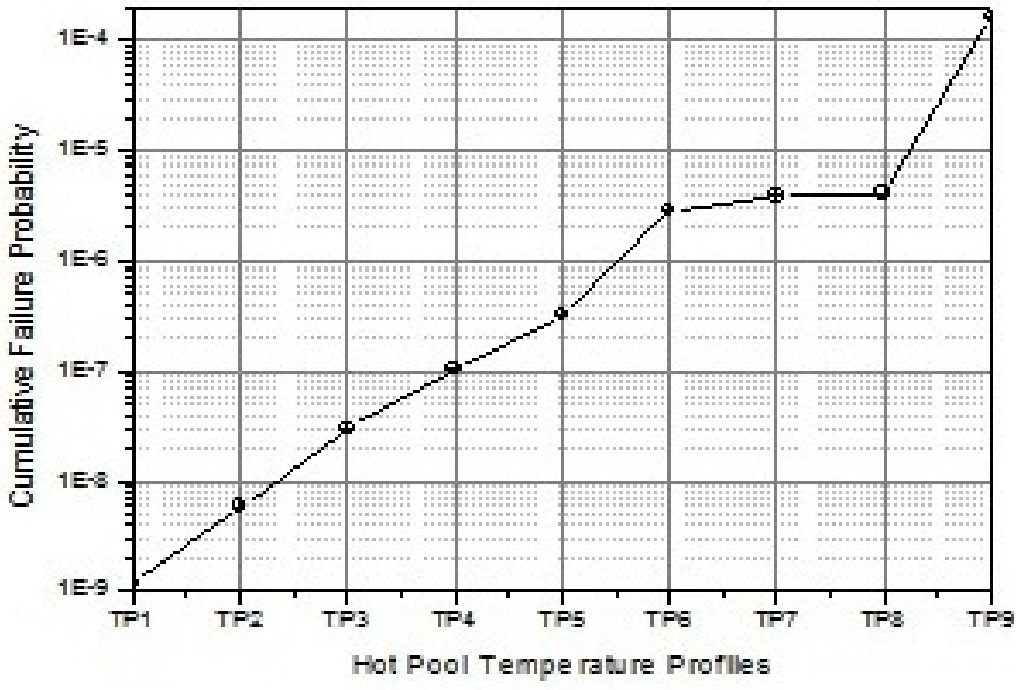

Fig.26: Cumulative Failure Probability of Different Hot Pool Temperature Profiles for Category-3 limits

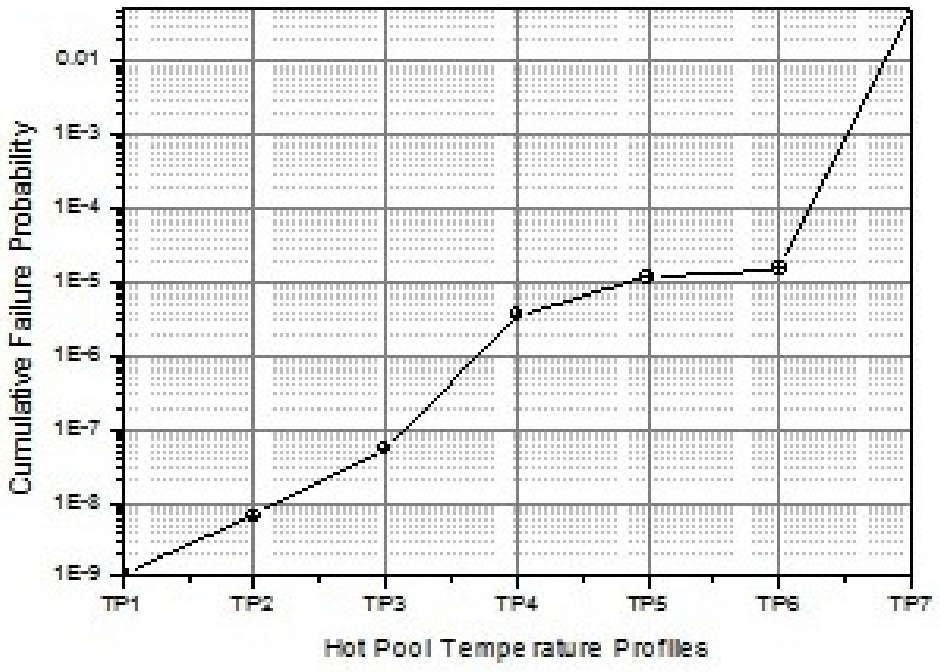

Fig.27: Cumulative Failure Probability of Different Hot Pool Temperature Profiles for Category-2 limits

From fig.28 it can be observed that there are two regions in these curves. They are a low standard deviation region (7.5^{o}C to 10^{o}C) and a high standard deviation region (12.5^{o}C to 20^{o}C). The slopes for the low standard deviation region for category-4, category-3 and category-2 temperature limits are 0.08, 0.304 and 0.309 respectively. The slopes calculated for the high standard deviation region are 0.379, 0.248 and 0.061 for category-4, category-3 and category-2 limits respectively. The slopes of category-4 and category-2 limits are significantly different in low and high standard deviation regions. These slopes give the change in failure probability for unit temperature change in standard deviation. Let P_0 be the failure probability corresponding to the standard deviation σ_0 of peak hot pool temperature probability density. If $\Delta\sigma$ is the change in the standard deviation of peak hot pool temperature probability density, then the failure probability due to this change in standard deviation is given by equation (6-14).

$$\frac{P_1}{P_0} = 10^{(m.\Delta\sigma)} \qquad (6\text{-}14)$$

In equation (6-14) m is the slope of the curve in the respective regions as discussed above. Appropriate signs of m needs to be used in the above relation. Equation (6-14) is helpful to compute the failure probability if P_0 is known.

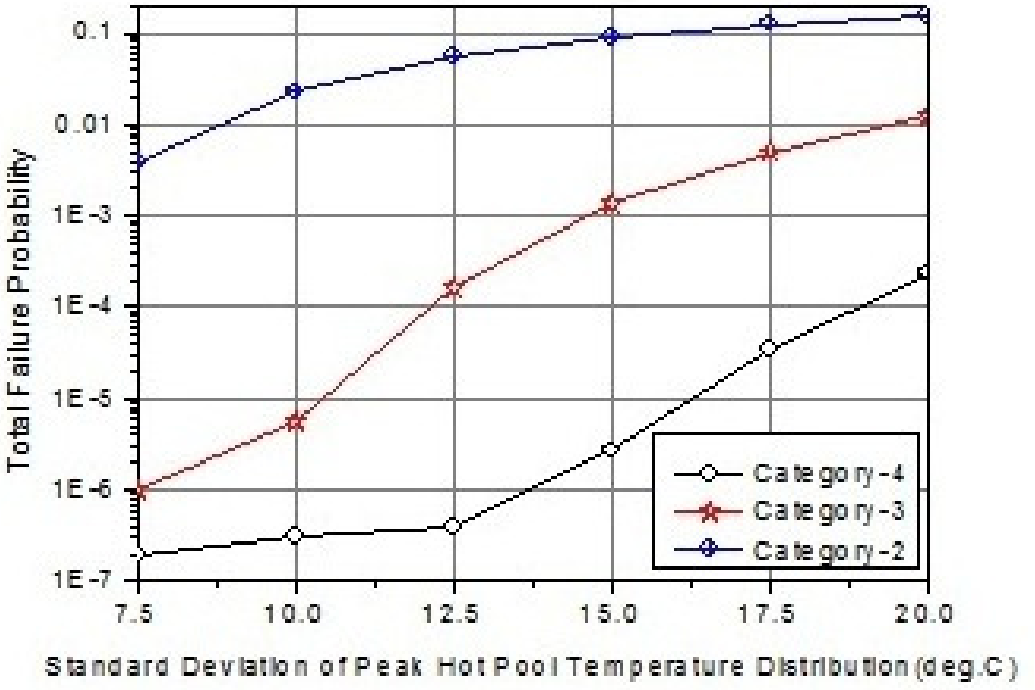

Fig.28: Total Failure Probability as a Function of Standard Deviation of Peak Hot Pool Temperature Distribution for Different DSL

Another outcome of this study is how the results from this study compares with other methods like functional reliability analysis alone and functional reliability analysis combined with fault tree. The failure probability from functional reliability analysis alone is calculated from the peak hot pool temperature probability density assuming all the four loops available as the hardware state. The functional reliability analysis alone gives the contribution of process uncertainties to total failure probability. The inclusion of this method in the comparison of results helps us to understand the process uncertainty values at which the results from different methods converge or diverge. The functional reliability analysis was combined with fault tree as follows. The failure criteria in terms of number of loops for each bin in the peak hot pool temperature probability density were determined from equation (6-

11). The failure probabilities for these different loop configurations are estimated from fault tree. The estimated failure probabilities from fault tree are given in Table-16. The estimated failure probabilities for different loop configurations are multiplied with the respective bin areas from response parameter distribution. This is carried out for different values of standard deviation. The results from these methods are compared in fig.29-31 for category-4, category-3 and category-2 DSL respectively.

Table-16: Failure Probabilities Estimated From Fault Tree for Different Loop Configurations

Sl. No	Failure Criteria	Failure Probability
1.	4/4 : Failure	7.3 E-08
2.	3/4 : Failure	4.7E-07
3.	2/4: Failure	1.25E-04
4.	1/4: Failure	7.17E-03
5.	0/4: Failure	1

For category-4 limits, the results are significantly different for small values of standard deviation in peak hot pool temperature distribution. As the standard deviation increases, the results from different methods converge. For low values of standard deviation, the functional reliability analysis alone under predicts the failure probability due to the non-inclusion of hardware failure probability contribution to the total failure probability. The functional reliability analysis combined with fault tree results is on the higher side. For category-3 and category-2 limits, the results are matching closely except at one or two points. Functional reliability analysis and fault tree combined with functional reliability analysis predicts close results with present study when the uncertainties in the response parameters are large. The results can be explained in the following way.

The probability of crossing the different categories of DSL (failure probability) can be written as in equation (6-15).

$$P\,(x \geq DSL) = \sum_{TP_i} P(TP_i).\,P(x \geq DSL|TP_i) \qquad i = 1,2,\ldots n_b \qquad (6\text{-}15)$$

TP_i is the temperature profile from i^{th} bin. The different temperature profiles TP_i can be divided into two possible sets. Let θ_1 represents a set of temperature profiles for which

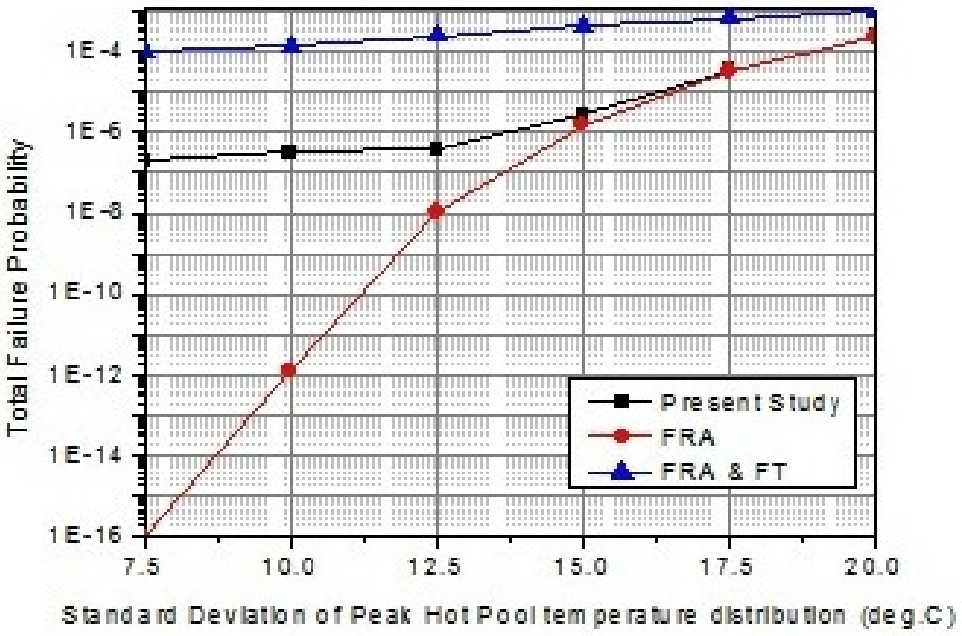

Fig.29: Comparison of Results from Different Approaches for Category-4 limits

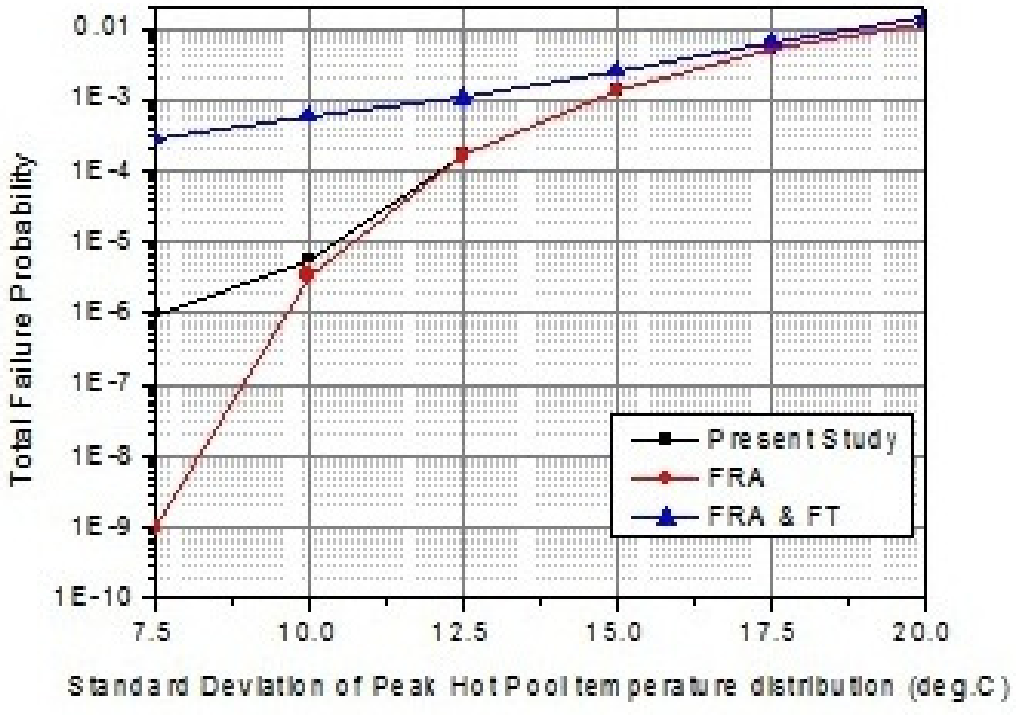

Fig.30: Comparison of Results from Different Approaches for Category-3 limits

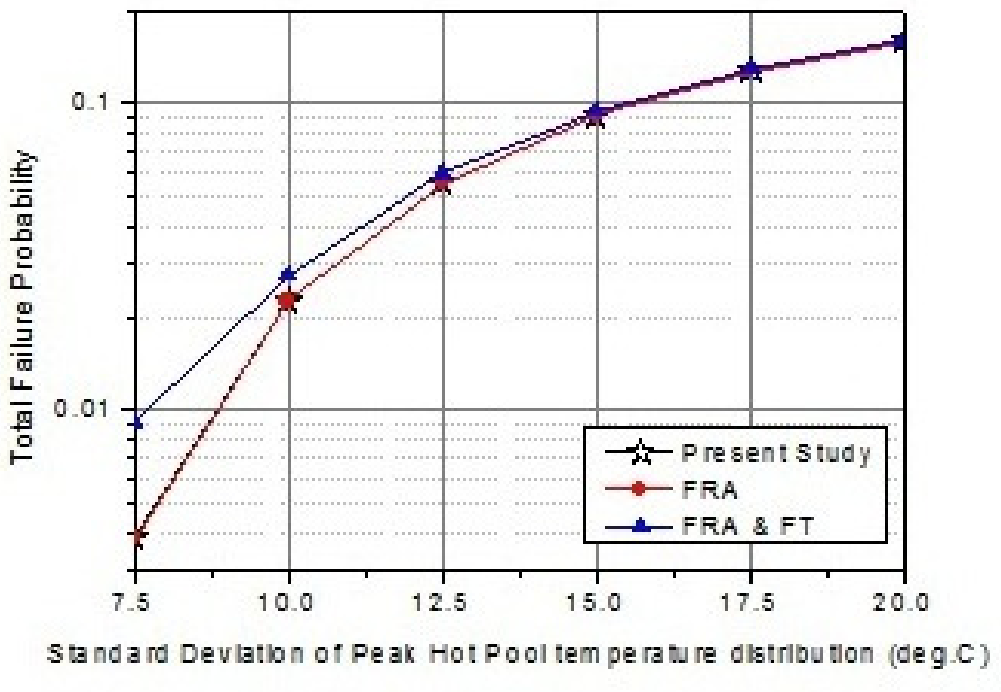

Fig.31: Comparison of Results from Different Approaches for Category-2 limits

max (TP_i) < DSL. θ_2 be the set of temperature profiles for which max (TP_i) ≥ DSL. Equation (6-15) can be written as in equation (6-16).

$$P(x \geq DSL) = \sum_{TP_i \epsilon \theta_1} P(TP_i).P(x \geq DSL|TP_i) + \sum_{TP_i \epsilon \theta_2} P(TP_i).P(x \geq DSL|TP_i) \quad (6\text{-}16)$$

In the second summation, the hot pool temperature is equal to or crosses the DSL irrespective of the system hardware state. The probability $P(x \geq DSL|TP_i) = 1$ for $TP_i \epsilon \theta_2$. Equation (6-16) reduces to the equation (6-17).

$$P(x \geq DSL) = \sum_{TP_i \epsilon \theta_1} P(TP_i).P(x \geq DSL|TP_i) + \sum_{TP_i \epsilon \theta_2} P(TP_i) \quad (6\text{-}17)$$

$$P\ (x \geq DSL) = C_1 + C_2 \quad (6\text{-}18)$$

where $C_1 = \sum_{TP_i \epsilon \theta_1} P(TP_i).P(x \geq DSL|TP_i)$ and

$$C_2 = \sum_{TP_i \epsilon \theta_2} P(TP_i)$$

C_1 is the failure probability contribution from the combined effect of process uncertainty and stochastic changes in system hardware. C_2 is the failure probability contribution due to process uncertainty. Three different cases are possible based on the values of C_1 and C_2.

Case-1: $C_2 >> C_1$ $P\ (x \geq DSL) = C_2$

In this case the failure probability is dominated by the second term. The results from classical approach (functional reliability combined with fault tree) and dynamic PSA agree well under this condition. Examples of such cases in the present analysis are i) σ = 20.0 for category-4 temperature limits ii) $\sigma \geq$ 15.0 for category-3 limits and iii) $\sigma \geq$ 10.0 for category-2 limits. The results from both approaches are different for the cases σ =17.5 for category-4 limits, σ =12.5 for category-3 limits and σ =7.5 for category-2 limits even though they also fall under this category. But the general trend indicates broadly under the above condition, the results started converging from classical and dynamic approaches.

Case-2: $C_2 \sim C_1$ $P\ (x \geq DSL) = C_1 + C_2$

C_1 and C_2 are of comparable magnitude in this case. Both terms contribute significantly to failure probability. The results obtained from classical approach are different from the results obtained from dynamic PSA. Examples of such cases in the present analysis are i) σ < 17.5 for category-4 limits ii) σ < 12.5 for category-3 limits. The failure probability is under predicted if functional reliability alone is used in this case.

Case-3: $C_2 << C_1$ $P\ (x \geq DSL) = C_1$

The contribution to failure probability in this case is due to the combined effect of process and system hardware. Depending on the nature of the process two approaches can be used. If the process evolution is sensitive to the timing of hardware transitions, the present approach is suitable. If the process evolution is not sensitive to the timing of hardware transitions, then the hardware reliability can be quantified by any of the classical approaches.

The functional reliability analysis combined with classical fault tree approach is the upper bound value in all the cases. It is suitable for conservative quantification of failure probability. The inclusion of the hardware failure probability contribution to the total failure

probability through fault tree approach makes the results highly conservative. The present method reduces the conservatism in the total failure probability estimate significantly.

6.9 Conclusion

The Monte Carlo simulation scheme identified in the last chapter is used for carrying out dynamic PSA of an example system. It is found that in the absence of significant process and system hardware interaction, classical approaches with appropriate time models are sufficient to estimate the required probabilities. The results from dynamic PSA match with the results from classical approaches with appropriate time models. Dynamic reliability analysis of a passive decay heat removal system is carried out in the second example. A method to integrate the process uncertainty quantification in functional reliability analysis with system hardware Monte Carlo simulation is presented. This method assumes specific type of process and hardware interaction. This method is helpful when full featured dynamic PSA tools are not available. The condition for which the classical and dynamic approaches lead to different results is one of the open issues of dynamic PSA. An attempt is made to address the above issue with the above example. It is found that the contribution of process uncertainty to total failure probability plays a significant role in this aspect. The results from dynamic PSA approach are significantly different from classical approaches when the contribution of process uncertainty to total failure probability is not dominant. Classical approaches here represent the process uncertainty quantified by functional reliability analysis combined with fault tree for system hardware. The results from different methods started converging as the contribution of process uncertainty to total failure probability dominates. This can be inferred from equation (6-18). Dynamic PSA approach reduces the conservatism introduced by classical approaches when the contribution of process uncertainty to total failure probability is not dominant. The results are qualitatively explained with a model for total failure probability.

Chapter-7 Summary and Future Directions

7.0 Summary

The safety analysis of reactors is essential for understanding the dynamic behaviour and quantifying the safety characteristics. Enhanced safety leads to wide public acceptance. In general the safety analysis is divided into two major categories namely deterministic and probabilistic safety analysis. The classical methods developed for probabilistic safety analysis is applied for the first time to a pool type FBR namely Prototype Fast Breeder Reactor. This reactor is under construction at Kalpakkam. PFBR marks the entry of India into its second stage of three stage nuclear power programme. A brief description of the reactor and its various safety systems are explained. The level-1 probabilistic safety analysis of the reactor was carried out. The scope is limited to full power internal events. The initiating events were grouped into 16 groups. Fault tree and event tree techniques are used for this analysis. The safety systems analyses were carried out with fault trees and accident sequences were modelled with event trees. The unavailability of various safety systems were dominated by the Common Cause Failure events. This implies that in safety systems employing high level of redundancy as in nuclear power plants, the modelling of CCF plays a crucial role in safety system unavailability calculations. A careful choice of CCF model parameters based on plant specific design, operation and environment inputs are the best way out to prevent over/under prediction of Core Damage Frequency. The estimated CDF value is ~0.9E-06 / ry. The dominant initiating events which contribute to this result are Loss of Off Site Power and Loss of Steam Water System. The maximum relative contribution to the total CDF from an individual initiating event group is less than 25% implying that the major design features are balanced. Important contributions from this study are the introduction of diversity in the two shut down systems and different loops of SGDHRS. A core damage frequency of ~1.0E-06 /y is achieved mainly by these diverse features in design. This study is also helpful in improving

the future FBR designs in the country. The CDF can be still reduced if the contribution from initiating event groups loss of offsite power and loss of steam water system are reduced further. Insights for further reduction in CDF have been obtained from the analysis as the need for further diversification of shutdown devices and enhancing the reliability of Safety Grade Decay Heat Removal System. The inclusion of functional reliability of SGDHRS in the accident sequence progression helps in identifying additional accident sequences which might have been missed out if conventional event tree is used.

The importance of external events PSA is highlighted by the Fukushima accidents in Japan. External events can affect several important safety systems simultaneously. The benefits of redundant safety systems and components may not be applicable for an external event scenario. Seismic events are one of the important external events which need to be considered for external events PSA. Level-1 seismic PSA of PFBR is carried out. The site specific seismic hazard analysis for Kalpakkam is carried out based on detailed characterisation of seismic sources and earthquake data reported in literature. The attenuation relation developed for peninsular India is used for estimating Peak ground Acceleration (PGA). The fragility assessment of different components was carried out by Zion method. Plant specific data for main vessel and roof slab are used. The results from the qualification experiments of instrumentation panels were used to estimate the median acceleration capacities. High Confidence Low Probability of Failure method was used for this purpose. Components for which plant specific data is not available, the data for fragility assessment were collected from literature. The system fragilities for different PGA values were estimated by using fault trees. The median Core Damage Frequency estimated from this study is 1.5E-06 / ry. The contribution from this study is the validation of seismic ground motion parameters of the plant arrived from deterministic seismic hazard analysis. The ground motion parameters obtained from deterministic seismic hazard analysis for OBE and SSE

level earthquakes matches with the values obtained from probabilistic seismic hazard analysis in this study at 50% exceedence probability level.

The other important external event is flood. PFBR is located on the east coast of India. Being a coastal plant, flood is one of the external events which need to be considered. As part of External Flood Probabilistic Safety Analysis of PFBR two studies were carried out. The first study is the tsunami hazard analysis for PFBR. The existing model for tsunami wave run up height prediction is improved by including local bathymetry into the model. For PFBR, tsunami wave run up height governs the flood CDF contribution. In the absence of bathymetry, the tsunami wave run up heights were under predicted as compared to the observed run up height at the plant site during the 2004 tsunami event. The inclusion of bathymetry significantly increases the tsunami wave run up height predictions. The local bathymetry was included in the run up height model by using work-energy theorem method. The important safety systems of PFBR are located at an elevation of 9.6m above MSL. The frequency of occurrence of tsunami wave run up height equal to or above this level is small based on tsunami hazard analysis. Even if a tsunami occurs with this run up height, the power supplies required for decay heat removal function are located at 17.6m above MSL. The core damage frequency is expected to be very small due to the above mentioned reason and fail safe design of shutdown system. This inference is possible based on the tsunami hazard analysis. The second study is the comparison of two different accident sequence modelling approaches. The first approach uses the accident sequences developed for level-1 internal events PSA for EFPSA also. The second approach involves the development of a separate event tree with flood event as initiator. Both these approaches lead to identical expressions for CDF implying that these approaches are equivalent. This is demonstrated by considering simplified models from PFBR as example. This study enables the use of existing level-1 internal events PSA accident sequence models for external events also with suitable

modifications. This study is useful in reducing considerable time and effort in developing separate accident sequence models for external events.

Classical tools were used for the level-1 PSA of PFBR. Fault tree and Event tree were used for the level-1 internal events PSA and seismic PSA of PFBR. Fault tree / Event tree techniques are relatively simple to develop and easy for review. These tools are helpful in the safety analysis of nuclear power plants. However modern safety systems analysis has become increasingly complex with the use of passive features, instrumentation and control logics, software and human intervention. The uncertainties in process and stochastic changes in system hardware are not addressed in a systematic manner in classical PSA approaches. The other drawback of these methods is in the modelling of time dependent interactions between the process and system hardware. It is necessary to look for methods beyond the classical approaches to PSA to meet the above challenges. Dynamic approaches to PSA have the capability to address these challenges. Dynamic approaches to PSA present a unified framework to account for the joint effects of process uncertainty and stochastic changes in system hardware. These approaches model the time dependent interaction between physical process and system hardware. Dynamic reliability analysis through Monte Carlo simulation is discussed in this thesis. The development of a dynamic PSA tool can be realised by the following steps.

a) Identification of a suitable Monte Carlo simulation scheme for system hardware.

b) Application of this simulation scheme on a typical reactor safety system and comparing the results from simulation with other approaches.

c) Integration of Monte Carlo simulation of system hardware with simple physical process. A simple model is chosen in such a way that the results obtained from such a simulation tool can be compared with analytical integral expressions.

d) Combining the results from uncertainty quantification of process parameters with system hardware Monte Carlo simulation. This step combines the results from functional reliability analysis with system hardware evolution. This is applied to a passive decay heat removal system of a FBR.

Steps a and b are achieved in this study by selecting a few basic Monte Carlo simulation methods for system hardware and applying it on the shutdown system of a fast breeder reactor. One particular method gives better variance reduction and leads to significant saving in computational efforts as compared to other methods. The results obtained from this simulation scheme matches with the results from fault tree analysis. The contribution from this study is the application of Monte Carlo simulation scheme for system hardware on a typical reactor safety system characterised by rarity of system failure and dependent failures through common cause failures. These simulation schemes were tested on example systems in most of the literature. Step c is carried out by integrating a simple process model with stochastic system hardware evolution. The probability of crossing the safety limits on temperature is estimated. The results obtained from such a simulation are compared with the results from analytical integral expression and fault tree. The analytical integration was carried out using Time Dependent Cut set Evaluation method (TDCE). This study demonstrates that in the absence of significant interaction between physical process and system hardware, classical approaches with appropriate time models are sufficient to quantify probabilities of interest. The results from dynamic PSA closely match with the results from TDCE and fault tree with non-recovery.

A method to combine the results obtained from functional reliability analysis of a passive decay heat removal system and Monte Carlo simulation of system hardware is developed in step-d. This is possible only when specific type of interactions between physical process and system hardware are present. This method is needed in the absence of full

featured dynamic PSA tools. The system considered is similar to the Safety Grade Decay Heat Removal System of PFBR. An approximate model for hot pool temperature evolution is combined with system hardware Monte Carlo simulation. The probability of crossing the various safety limits on hot pool temperature is estimated. One of the issues in dynamic PSA is the lack of understanding in the conditions for which dynamic PSA results are significantly different from classical approaches. An attempt is made to address this issue with an example system and under specified conditions of process and system hardware interaction. It is found that the extent of process uncertainty contribution to total failure probability can be used to decide the application of different methods at least in the example system. When the contribution of process uncertainty to total failure probability is not dominant, the results from dynamic PSA and functional reliability approach combined with fault tree (classical approach) are significantly different. The results from both approaches converge as the contribution of process uncertainty to total failure probability is dominant. The failure probability estimated by combining functional reliability analysis and fault tree is highly conservative. The dynamic reliability reduces the conservatism in the failure probability. These results are explained by expressing the failure probability as the contribution from two parts. The applicability of different methods is also explained.

7.1 Future Directions

The level-1 internal events PSA of PFBR is carried out based on the design inputs. The data used for different components are collected from international literature like thermal and fast reactor operating experience, testing of components and different standards. The data collected from the operational experience of the plant and its impact on the CDF will be one of the interesting future studies. The experience from level-1 internal events PSA shows that the common cause failures dominate the results. Data collection on this account is also needed to reduce the conservatism introduced by the common cause factors.

The detailed seismic hazard analysis for Kalpakkam site is carried out. The seismic sources are assumed to be point sources. There is scope for improving the seismic hazard assessment by improving the characterisation of seismic sources. The uncertainties in attenuation relationship, parameters of the Gutenberg-Richter relationship are to be considered. The local site effects are to be included in the analysis. The fragility analyses of main vessel and roof slab are based on plant specific data. The results from qualification experiments of instrumentation panels are used for fragility assessment. Data from literature is used for other components. The acceleration capacity can be assessed by structural analysis and it needs to be explored. A testing scheme for assessing the fragility of different components needs to be developed. For External Flood PSA (EFPSA) of PFBR, the reported tsunami hazard analysis predicts the run up height on plain beaches. The effect of bunds and tsunami protection walls on the wave height and wave velocity cannot be predicted by this simple model. A more detailed tsunami hazard analysis is to be carried out.

Dynamic reliability analysis of a passive decay heat removal system of PFBR is carried out by combining process uncertainty quantification from functional reliability analysis and system hardware reliability through Monte Carlo simulation. A simple process model is used for the physical process. Also restrictive assumptions on the type of interaction between system hardware and physical process are assumed. A more elegant way of carrying out the dynamic reliability analysis is to integrate the process codes with system hardware evolution. The computational efforts required for such an analysis is one of the important challenges. More efficient Monte Carlo simulation schemes for system hardware are required to significantly reduce the computational efforts. Development of a full featured dynamic PSA tool by integrating the process codes with Monte Carlo simulation of system hardware for fast reactor applications need to be explored.

The classical fault tree approach is highly insensitive to the varying physical process conditions and usually the modelling is such that it results in conservative results. This conservatism can be reduced with dynamic reliability analysis. Dynamic reliability analysis can be used as a tool for reliability based design optimisation studies of safety systems where physical process can evolve in different possible ways.

The scenario considered for dynamic reliability analysis is a simple one in the present study. In some of the complex reactor safety systems, there will be multiple top events competing with each other. The biasing of the simulation scheme towards one particular top event may affect the statistical properties of the other top event. The balanced failure biasing which assigns uniform probability to all failure events appears to be effective under such conditions. This has to be confirmed by applying this simulation scheme to a scenario where multiple top events are present. The sensitivity analysis using likelihood ratio gradient estimation is to be explored in the dynamic PSA context. The development of a dynamic reliability analysis tool will go a long way in the safety analysis of reactors.

REFERENCES

[1-1] IAEA-TECDOC-1436, Risk Informed Regulation of Nuclear Facilities: Overview of Current Status, IAEA, February, 2005.

[1-2] William Keller and Mohammad Modarres, A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late professor Norman Carl Rasmussen, Reliability Engineering and System Safety, 89, 2005, 271-285.

[1-3] Farmer.F, Reactor safety and siting: a proposed risk criterion, Nuclear Safety, 1967, 539-548.

[1-4] Starr.C, Social benefit versus technological risk, Science, 19, 1969, 1232-1238.

[1-5] USNRC, WASH-1400: Reactor Safety Study (NUREG-75/014), 1975.

[1-6] USNRC, PRA Procedures Guide, NUREG / CR-2300, Volume-I, 1983.

[1-7] Modarres Mohammad, Mark Kaminskiy, Vasiliy Krivtsov, "Reliability Engineering and Risk Analysis : A practical guide", Marcel Decker, Inc, 1999.

[1-8] Vesely W.E, Goldberg F.F, Roberts N.H, Haasl D.F, Fault Tree Handbook, NUREG-0492, USNRC, 1981.

[1-9] Barlett L.M, Progression of the binary decision diagram conversion methods, 21st international system safety conference, Aug 4-8, 2003, Ottawa, West in Hotel, pp 116-125, 2003.

[1-10] REMENYTE.R and Andrews J.D, Qualitative Analysis of Complex Modularised Fault Trees using Binary Decision diagrams IN: Proceedings of the 16th ARTS (Advances in Reliability Technology Symposium), Loughborough University, UK, April,2005, pp 379-394.

[1-11] M. Ajmone Marsan, "Stochastic Petri nets: An elementary introduction", chapter in advances in petri nets, Vol-424, Springer, 1989, pp 1-29.

[2-1] Chetal, S.C., Balasubramaniyan, V., Chellapandi, P., Mohanakrishnan, P., Puthiyavinayagam, P., Pillai, C.P., Raghupathy, S., Shanmugham, T.K., and Sivathanu Pillai, C., The design of prototype fast breeder reactor, Nuclear Engineering and Design 236 (7–8), 2006, 852–860.

[2-2] Prototype Fast Breeder Reactor- Final Safety Analysis Report, Revision-0, March-2010.

[2-3] Safety Criteria for Design of PFBR, AERB, April 1990.

[2-4] L. Satish Kumar, K. Natesan, A. John Arul, V. Balasubramaniyan and S.C. Chetal, Design and Evaluation of Operation Grade Decay Heat Removal System of PFBR, Nuclear Engineering and Design, 241, 2011, 4953-4959.

[3-1] M. Ramakrishnan, Pramod Kumar Sharma, V. Bhuvana, A. John Arul, P. Mohanakrishnan and S.C.Chetal, Insights from Level-1 Probabilistic Safety Analysis of Prototype Fast Breeder Reactor, Nuclear Engineering and Design, 250, 2012, 664-670.

[3-2] IAEA, Procedures for conducting level-1 PSA of Nuclear Power Plants (level-1), IAEA – Safety Series No. 50-P-4, Vienna, 1992.

[3-3] ASME, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications ASME-RA-S-2002, 2002.

[3-4] IAEA, Unusual Occurrences during LMFR Operation, IAEA-TECDOC-1180, Vienna, 2000.

[3-5] IAEA , Liquid Metal Cooled Reactors: Experience in Design and Operation, IAEA-TECDOC-1569, Vienna, 2007.

[3-6] Vaidyanathan, G., Design Basis Events, PFBR/RG/66040/DN/1013, 1995.

[3-7] T. Sajith Mathews, U.Parthasarathy, A.John Arul, C. Senthil Kumar, M. Ramakrishnan and K.V.Subbiah,, Integration of functional reliability analysis with hardware reliability:

an application to safety grade decay heat removal system of Indian 500 MWe PFBR, Ann. Nucl. Energy 36, 2009, 481–492.

[3-8] A. John Arul, M. Ramakrishnan, V.Rajan Babu and R.Vijayashree, Estimate of LMFBR Control / Safety Rod Failure Rate, REG/RPD/SAS/189, July 2009.

[3-9] A. John Arul, V. Bhuvana and C. Senthil Kumar, Relational Database for Fast Reactor Reliability Analysis, REG / RPD / SAS / 152-Rev.A, January 2007.

[3-10] V.Bhuvana and A.John Arul, 2011. A Program for Pre-Incident and Post-Incident Human Interaction Analysis, REG / RPhG / SAS / 190-Rev A.

[3-11] IAEA, Case Study on the use of PSA methods : Human Reliability Analysis, IAEA-TECDOC-592, Vienna, April 1991.

[3-12] USNRC, Procedures for treating Common Cause Failures in Safety and Reliability Studies, NUREG / CR-4780, 1989.

[3-13] D.J.Hill et al., The EBR-II probabilistic risk assessment: results and insights, Proceedings of the International Meeting on Probabilistic Safety Assessment, 1993.

[3-14] W.M.Akhtar et al., Core damage frequency results for the Clinch River breeder reactor. In: International ANS/ENS Topical Meeting, 1985.

[3-15] A.Birkhofer, et al., Risk oriented analysis on the SNR-300. In: International Topical Meeting on Liquid Metal Fast Breeder Reactor Safety and Related Design and Operational Aspects, Lyon, July 19–23, 1982.

[4-1] IAEA, Probabilistic Safety Assessment for Seismic Events, IAEA-TECDOC-724, 1993.

[4-2] ASME, Standard for Level 1/ Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME / ANS RA-S-2008, 2008.

[4-3] M. Ramakrishnan, A. John Arul, V. Bhuvana and S.D.Sajish, Level-1 Seismic Probabilistic Safety Analysis of PFBR - Preliminary Analysis, February 2012.

[4-4] A.K. Ghosh, "Probabilistic Seismic Hazard Analysis for a site", Nuclear Engineering and Design 236 (2006), 1192-1200.

[4-5] Chandra. U, Earthquakes of Peninsular India, Seismotectonic Study, Bulletin of the Seismological Society of America, 67(5), 1977, pp 1387-1413.

[4-6] Ghosh A.K, and Rao K.S, Development of Uniform Hazard Response Spectra for Kalpakkam, Kaiga and Kudankulam, BARC / 2009 / E / 025, 2009.

[4-7] Geological Survey of India Web Portal http://www.portal.gsi.gov.in/public_html/gis/seismotectonic/viewer.htm

[4-8] Vipin K.S, Anbazhagan P and Sitharam T.G, Estimation of Peak Ground Acceleration and Spectral Acceleration for South India with Local Site Effects: Probabilistic approach, Natural Hazards and Earth System Sciences, 9, pp 865-878, June 2009.

[4-9] USNRC, PRA Procedures Guide, NUREG / CR-2300, 1983.

[4-10] Iyengar R.N and RaghuKanth S.T.G., Attenuation of Strong Ground Motion in Peninsular India, Seismological Research Letters, 75,4, pp 530-540 July/August 2004.

[4-11] Kennedy R.P and Ravindra M.K., Seismic Fragilities for Nuclear Power Plant Risk Studies, Nuclear Engineering and Design 79, 1984, pp 47-68.

[4-12] S.D.Sajish, "Assessment of Seismic Margin of PFBR Components Beyond Safe Shutdown Earthquake", PFBR/30000/DN/1111/Rev-A, 2012.

[4-13] Park Y.J, Hofmayer C.H and Chokshi N.C, Survey of Seismic Fragilities used in PSA studies of Nuclear Power Plants, Reliability Engineering and System safety 62, 1998, pp 185-195.

[4-14] Sajish S.D, Raghavendran C. and Babu Rao, Seismic Qualification Experiments on RTC Panel by Shake Table Testing, PFBR / 66120 / DN / 1035, March 2010.

[4-15] Berg Heinz-Peter and Fröhmel Thomas, "Analysis of the impact of external flooding to nuclear installations", R&RATA # 2 (Vol.1), June 2008.

[4-16] IAEA, Flood Hazard for Nuclear Power Plants on Coastal and River Sites, Safety Guide, No. NS-G-3.5, Vienna, 2003.

[4-17] Ghosh A.K., "Assessment of earthquake-induced tsunami hazard at a power plant site", Nuclear Engineering and Design 238 (2008) 1743-1749.

[4-18] M. Ramakrishnan and A. John Arul, "Preliminary Tsunami Hazard Analysis for a Power plant Site on East Coast of India", presented in the 2nd SRESA National Conference on Reliability and Safety Engineering (NCRS-15) held at Anna University, Chennai, Oct 8-10, 2015.

[4-19] Muraleedharan. G, Mourani Sinha, Rao A.D and Murty T.S., "Statistical Simulation of Boxing Day Tsunami of the Indian Ocean and a Predictive Equation for Beach Run up Heights Based on Work-Energy Theorem", Marine Geodesy,29: 2006, pp: 223-231.

[4-20] Anandan. C and Sasidhar. P, "Assessment of the impact of the Tsunami of December 26,2004, on the near-shore bathymetry of the Kalpakkam Coast, East Coast of India", Science of Tsunami Hazards, Vol 27, no 4, 2008, pp: 26-35 .

[4-21] M.Ramakrishnan, A. John Arul, V.Bhuvana, P.PuthiyaVinayagam and P. Chellapandi, "Accident Sequence Modeling Methodology for External Flood Probabilistic Safety Analysis of Prototype Fast Breeder Reactor", Applied Mechanics and Materials, Vols. 592-594 (2014), pp 2460-2464.

[5-1] Tunc Aldemir, "A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants", Annals of Nuclear Energy, 52, 2013, pp: 113-124.

[5-2] E.E.Lewis and Franz Bohm, "Monte Carlo Simulation of Markov Unreliability Models", Nuclear Engineering and Design, 77, 1984, pp: 49-62.

[5-3] P.E.Labeau, C.Smidts and S.Swaminathan, "Dynamic Reliability : Towards an integrated platform for probabilistic risk assessment", Reliability Engineering and System Safety, 68 , 2000, pp:219-254.

[5-4] Enrico Zio, "Integrated deterministic and probabilistic safety assessment: Concepts, challenges, research directions", Nuclear Engineering and Design, 280, 2014, pp: 413-419.

[5-5] Devooght.J, and Smidts.C, "Probabilistic Reactor Dynamics-I: The Theory of Continuous Event Trees", Nuclear Science and Engineering, 111, 1992, pp: 229-240.

[5-6] Durga Rao Karanki, Tae-Wan Kim and Vinh N.Dang, "A dynamic event tree informed approach to probabilistic accident sequence modeling: Dynamics and variabilities in medium LOCA", Reliability Engineering and System Safety, 142, 2015, pp: 78-91.

[5-7] Tunc Aldemir et.al, "Current State of Reliability Modelling Methodologies for Digital Systems and their Acceptance Criteria for Nuclear Power Plant Assessments", NUREG / CR -6901, February 2006.

[5-8] Gerardo Rubino and Bruno Tuffin, "Rare Event Simulation Using Monte Carlo Methods", John Wiley & Sons, 2009.

[5-9] Enrico Zio, "The Monte Carlo Simulation Method for System Reliability and Risk Analysis",Springer Series, 2013.

[5-10] Labeau, P. E., & Zio, E. "Procedures Of Monte Carlo transport simulation for applications in system engineering" Reliability Engineering and System Safety, 77, 2002, pp: 217–228.

[5-11] P.Shahabuddin, "Importance Sampling for The Simulation of Highly Reliable Markovian Systems", Management Science, 40, 1994, pp: 333-352.

[5-12] Victor F.Nicola, Perwez Shahabuddin and Marvin K.Nakayama, "Techniques for Fast Simulation of Models of Highly Dependable Systems", IEEE Transactions on Reliability,Vol.50, No.3, September 2001, pp: 246-264.

[5-13] C. Papadopoulos, "A New Technique for MTTF estimation in Highly Reliable Markovian Systems", Monte Carlo Methods and Applications, Vol 4 (2), 1998, pp: 95-111.

[5-14] C. Alexopoulos and B.C. Shultes. Estimating reliability measures for highly-dependable Markov systems, using balanced likelihood ratios. *IEEE Transactions on Reliability*, **50**(3): 265–280, 2001.

[5-15] Ambuj Goyal, Perwez Shahabuddin, Philip Heidelberger, Victor F. Nicola and Peter W.Glynn, "A Unified Framework for Simulating Markovian Models of Highly Dependable Systems", IEEE Transactions on Computers, Vol 41 (1), January 1992.

[5-16] H. Cancela, G. Rubino, and B. Tuffin. "MTTF estimation by Monte Carlo methods using Markov models", Monte Carlo Methods and Applications, **8**(4): 312–341, 2002.

[5-17] M.Marseguerra and E.Zio, "Nonlinear Monte Carlo reliability analysis with biasing towards top event", Reliability Engineering and System Safety 40, 1993, pp: 31-42.

[5-18] B. Tuffin, "Bounded normal approximation in simulations of highly reliable Markovian systems", Journal of Applied Probability, **36**(4): 974–986, 1999.

[5-19] Desai, P. Y. and P. W. Glynn, "A Markov chain perspective on adaptive Monte Carlo algorithms", Proceedings of 2000 Winter Simulation Conference, 2001, 379-384.

[5-20] Ahamed, I., Borkar, V.S., Juneja, S., "Adaptive importance sampling for Markov chains using stochastic approximation", Operations Research 54(3), 2006, 489–504.

[5-21] A. Ridder, "Importance sampling simulations of Markovian reliability systems using cross-entropy", Annals of Operations Research, **143**: 119–136, 2005.

[5-22] Au, S. K., & Beck, J. L., "Estimation of small failure probabilities in high dimensions by subset simulation", Probabilistic Engineering Mechanics, 16(4), 2001, 263–277.

[5-23] Zio, E. & Pedroni, N., "Reliability analysis of a discrete multi state system by means of subset simulation", Proceedings of European Safety and Reliability Conference, ESREL, 22–25 Sept 2008. Valencia, Spain, pp. 709–716.

[5-24] Pierre L'Ecuyer and Bruno Tuffin, "Approximating zero variance importance sampling in a reliability setting", Annals of Operations Research, 189 (1), 2011, pp: 277-297.

[5-25] M. Ramakrishnan, "Unavailability Estimation of Shutdown System of a Fast Reactor by Monte Carlo Simulation", Annals of Nuclear Energy 90, 2016, pp 264-274.

[5-26] A.E.Conway and A.Goyal, "Monte Carlo Simulation of computer system availability / reliability models", Proc. Seventeenth Symposium Fault Tolerant Computing., Pittsburgh, 1987, pp: 230-235.

[5-27]M. K.Nakayama, "A characterization of the simple failure biasing method for simulations of highly reliable Markovian systems", ACM Transactions on Modelling and Computer Simulation 4, 1994, pp: 52–88.

[6-1] USNRC, Evaluation of Station Blackout Accidents at Nuclear Power Plants, NUREG-1032, 1988.

[6-2] IAEA, Case study on the use of PSA methods: Station Blackout Risk at Millstone Unit 3, IAEA-TECDOC-593, Vienna, 1991.

[6-3] Sajith Mathews.T et.al, Integrated Reliability Analysis of safety grade decay heat removal system, PFBR / 34000 / DN / 1023 / Rev-A, April 2010, internal report.

[6-4] Burgazzi, L., "Reliability evaluation of passive systems through functional reliability assessment", Nucl. Technol. 144, 2002, pp 145–150.

[6-5] D'Auria, F., Bianchi, F., Burgazzi, L., Ricotti, M.E., The REPAS study: reliability evaluation of passive safety systems. In: Proceedings of the 10th International Conference on Nuclear Engineering ICONE 10-22414, Arlington, VA, USA, April 14–18, 2002.

[6-6] Marque` s, M., Pignatel, J.F., Saignes, P., D'Auria, F., Burgazzi, L., Muller, C., Bolado-Lavin, R., Kirchsteiger, C., La Lumia, V., Ivanov, I., Methodology for the reliability evaluation of a passive system and its integration into a probabilistic safety assessment. Nucl. Eng. Des. 235 (December (24)), 2005, 2612–2631.

[6-7] Sajith Mathews.T, Ramakrishnan.M, Parthasarathy.U, John Arul.A and Senthil Kumar.C, Functional Reliability Analysis Safety Grade Decay Heat Removal System of Indian 500MWe PFBR, Nucl. Eng. Des. 238, 2008, pp 2369-2376.

[6-8] Sajith Mathews.T et.al, Integrated Reliability Analysis of safety grade decay heat removal system, PFBR / 34000 / DN / 1023 / Rev-A, April 2010, internal report.

[6-9] Sajith Mathews.T, John Arul.A, Parthasarathy.U, Senthil Kumar.C, Subbiah.K.V, Mohanakrishnan.P, Passive System Reliability Analysis using Response Conditioning Method with an application to failure frequency estimation of Decay heat Removal of PFBR , Nuclear Engineering and Design, 241, 2011, pp 2257-2270.

[6-10] IAEA-TECDOC-1474, Natural Circulation in water cooled Nuclear Power Plants-Phenomena, Models and Methodology for system reliability assessments, IAEA, November 2005.

[6-11] A. John Arul, N. Kannan Iyer and K. Velusamy, "Efficient reliability estimate of passive thermal hydraulic safety system with automatic differentiation", Nuclear Engineering and Design, 240 (10), 2010, 2768-2778.

[6-12] IAEA-TECDOC-592, Case Study on the use of PSA Methods: Human Reliability Analysis, IAEA, April 1991.