DEVELOPMENT AND APPLICATION OF PROBABILISTIC SAFETY ASSESSMENT METHODOLOGIES FOR ESTIMATING RISK FROM NUCLEAR POWER PLANTS

By

VARUN HASSIJA

(Enrollment No.: ENGG02201104032)

Indira Gandhi Centre for Atomic Research, Kalpakkam

A thesis submitted to the Board of Studies in Engineering Sciences

In partial fulfillment of requirements

For the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

September, 2016

Homi Bhabha National Institute

Recommendations of the Viva Voce Board

As members of the Viva Voce Board, we certify that we have read the dissertation prepared by **Mr. Varun Hassija** entitled **"Development and Application of Probabilistic Safety Assessment Methodologies for estimating Risk from Nuclear Power Plants"** and recommend that it may be accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy.

Chairman: **Dr. M. Sai Baba** Date: 23-9-16

Guide / Convener: **Dr. K. Velusamy** Date: 23/9/2016

Co-Guide / Member: **Dr. B. K. Panigrahi** Date: 23/9/16

Technology Advisor / Member: **Dr. C. Senthil Kumar** Date: 23/9/16

Member: **Dr. B. P. C. Rao** Date: 23/9/2016

External Examiner: Dr. T. Paul Robert Date: 23/9/16

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

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

Date: 23/9/2016

Place: Indira Gandhi Centre for Atomic Research (IGCAR)
Kalpakkam

Dr. K. Velusamy
(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.

Kalpakkam **(Varun Hassija)**

September, 2016

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.

Kalpakkam
September, 2016

(Varun Hassija)

PUBLICATIONS BASED ON THE THESIS

INTERNATIONAL JOURNAL PAPERS

1) "A pragmatic approach to estimate alpha factors for common cause failure analysis", **Varun Hassija**, C. Senthil Kumar, K. Velusamy, *Annals of Nuclear Energy*, **January 2014**, *Volume 63*, Pages 317-325.

2) "Markov analysis for time dependent success criteria of passive decay heat removal system", **Varun Hassija**, C. Senthil Kumar, K. Velusamy, *Annals of Nuclear Energy*, **October 2014**, *Volume 72*, Pages 298-310.

3) "Probabilistic safety assessment of multi-unit nuclear power plant sites – An integrated approach", **Varun Hassija**, C. Senthil Kumar, K. Velusamy, *Journal of Loss Prevention in the Process Industries*, **November 2014**, *Volume 32*, Pages 52-62.

4) "Integrated risk assessment for multi-unit NPP sites – A comparison", C. Senthil Kumar, **Varun Hassija**, K. Velusamy and V. Balasubramaniyan, *Nuclear Engineering and Design*, **November 2015**, *Volume 293*, Pages 53-62.

CONFERENCE PROCEEDINGS

1) "Development in PSA methodology based on the lessons learnt from the Fukushima nuclear disaster", **Varun Hassija**, C. Senthil Kumar, K. Velusamy, *Second International Conference on Advances in Industrial Engineering Applications (ICAIEA 2014)*, Anna University, Chennai, **2014**.

2) "Common cause failure analysis for engineered safety systems using alpha factors obtained by mapping technique", **Varun Hassija**, C. Senthil Kumar, K. Velusamy, *International Workshop on New Horizons in Nuclear Reactor Thermal Hydraulics and Safety (IW-NRTHS 2014)*, Mumbai, **2014**.

3) "Risk assessment of multi-unit nuclear power plant sites against external hazards", C. Senthil Kumar, **Varun Hassija**, K. Velusamy, *International Workshop on New Horizons in Nuclear Reactor Thermal Hydraulics and Safety (IW-NRTHS 2014)*, Mumbai, **2014**.

4) "Risk assessment of multi-unit nuclear power plant sites", C. Senthil Kumar, **Varun Hassija**, V. Balasubramaniyan, A. John Arul, M. Prasad, V. Gopika, R. Nama, Rajee Guptan and P. V. Varde, *International Workshop on Multi-Unit Probabilistic Safety Assessment (IW-MUPSA 2014)*, Ottawa, Canada, **2014**.

5) “A comparative risk assessment for sites with single and double units”, **Varun Hassija**, C. Senthil Kumar, K. Velusamy, *Advances in Reliability Maintenance and Safety - International Conference on Reliability Safety and Hazard Conference (ICRESH-ARMS 2015)*, Luleå University of Technology, Lulea, Sweden, **2015**.

This work is dedicated to

'My Brother and My Parents'

(For their love, care, and support)

ACKNOWLEDGEMENTS

I take this opportunity for expressing my gratitude to the people who have been very helpful to me in carrying out my research work and accomplishing the thesis.

First and foremost I acknowledge my Guide **Dr. K. Velusamy,** *Head, Mechanics and Hydraulics Division, Reactor Design Group (RDG), IGCAR* for his persistent encouragement and valuable technical inputs right from the very first day I joined the Ph.D. programme. He has always been a source of inspiration and motivation for me, especially during the troubled waters in the course of Ph.D.

I record my sincere gratitude to my Co-guide **Dr. B. K. Panigrahi,** *Head, Materials Physics Division, Materials Science Group, IGCAR* for being the source of guidance to my Ph.D.

I feel words are not enough to express my sincere gratitude to my Technology Adviser **Dr. C. Senthil Kumar,** *Head, Risk Assessment and GIS Application Section, AERB-Safety Research Institute* for his valuable guidance, persistent support, everlasting patience, crucial technical inputs and reviews right from the day I joined the organization.

I am highly grateful to my Doctoral Committee Chairman and our guardian **Dr. M. Sai Baba,** *Associate Director, Resources Management Group, IGCAR* for his care and support since the inception of my research career.

I express my heartiest gratitude to my Doctoral Committee member **Dr. B. P. C. Rao,** *Head, Non-Destructive Evaluation Division, Metallurgy & Materials Group, IGCAR* for mentoring and supporting me throughout my Ph.D. tenure.

I sincerely thank to **Shri V. Balasubramanian**, *Director, AERB-Safety Research Institute,* **Dr. P. Chellapandi**, *Chairman & Managing Director, BHAVINI* and **Shri. G. Srinivasan**, *Director, RDG, IGCAR* for their perpetual support and encouragement

throughout my research period. I thank to **Dr. S. A. V. Satya Murty**, *Director, IGCAR*, **Prof. G. Sasikala,** *Dean, Engineering Sciences, IGCAR* and **Prof. B. K. Dutta,** *Dean, HBNI, Mumbai* for allowing me to continue my research work.

I express my intense gratitude to **Dr. A. John Arul,** Head, Reactor Shielding and Data Division*, Reactor Design Group, IGCAR* for sharing his technical expertise and for the valuable discussions.

My sincere thanks to the Scientific Officers of *Reactor Design Group, IGCAR* **Shri. M. Ramakrishnan, Shri. Pramod Kumar Sharma, Shri. L. Satish Kumar , Shri. U. Partha Sarathy, Shri. K. Natesan, Shri. Ashish Shukla, Shri. Ram Kumar Maity** and **Ms. S. Usha** for sharing their scientific and technical knowledge.

I express my sincere acknowledgement to the Scientific Officers of *Madras Atomic Power Station, NPCIL* **Shri. J. M. Pillai** and **Smt. Nachammai** for sharing their rich knowledge and experience on Indian nuclear power plants and multi unit sites.

My special thanks to the Scientific Officers of *AERB-Safety Research Institute* **Dr. Seik Mansoor Ali, Dr. D. K. Mohapatra, Dr. Nilesh Aggarwal, Shri. Jagannath Mishra, Dr. C. Anandan, Shri. Arun Aravind, Shri. Sudhanshu Sekar** and **Dr. L. Thilagam** for their kind help and support during my research tenure in the institute.

Many thanks to the Scientific Officers of *Reactor Operations & Maintenance Group, IGCAR* **Shri. S. Varatharajan, Shri. G. Bhaskaran, Shri. M. Elango, Shri. M. Arulanadam** and **Shri. K. Kalyana Rao** for enriching my knowledge on fast reactors.

I thank to other members of staff at *AERB-Safety Research Institute* **Shri. P. Varadarajan, Smt. C. Jayalaxmi** and **Ms. T. H. Jayalaxmi** for their kind help during my work in the institute.

My heart is filled with diligent gratitude to all my faculty members of *School of Nuclear Energy (SNE), Pandit Deendayal Petroleum University (PDPU), Gandhinagar*

especially **Shri. S. B. Bhoje, Shri. D. K. Dave, Shri. Virendar Chaudhary, Shri. M. S. Gupta, Shri. Alok Shobhan Bhattacharya, Shri. B. L. Sharma** and **Dr. V. Venkat Raj** for nurturing the seeds of mine interest in "Design of Nuclear Power Plants".

It is my pleasure to thank all my friends, seniors and colleagues **Darshan, Ashish, Prashant, Shankar, Vaibhav, Chandan, Swapnil, Nakul, Raj, Karthik, Ilyas, Neeraj, Sampath, Tejaswi, Gopal, Adinarayana, Veer, Paawan, Govind, Arun, Ashutosh, Srihari, Anil, Ravi, Naveen, Subrata, Rakesh, Bonu, Aditya, Vikas, Jammu, Jagadeesh, Kalyan, Chiranjit, Kartik, Barath, Darpan, Suman, Rahul, Sahoo** and **Prasanna** for their support and care, and for making my stay joyous and peaceful at Kalpakkam.

I am also heartily thankful to my friends at *School of Nuclear Energy, Pandit Deendayal Petroleum University* **Ankush, Manish, Sunil, Surinder, Sahoo, Sridhar and Sagar** for their support, care and company, and for making my life enthusiastic, joyous and peaceful during my post graduation in nuclear engineering.

I express my sincere thanks to the **Department of Atomic Energy (DAE)** for providing me with generous research fellowship and excellent benefits under *DGFS-Ph.D. programme*.

I am very thankful to my dear brother **(Tarun)** and my parents for their love, patience and constant support.

At length, I thank to the **Lord Hari** for bestowing me with multiple gifts like intelligence, wisdom, proper guidance and the right environment for pursuing the research and accomplishing the thesis.

(Varun Hassija)

Kalpakkam
September, 2016

CONTENTS

SYNOPSIS

The India's indigenous three stage nuclear power programme aims to utilise country's nuclear resource profile of modest uranium and abundant thorium reserves optimally with the core objective of meeting the energy requirement of the nation. As of now, India has 21 nuclear power plants at seven sites with an installed capacity of 5780 MWe while six nuclear power plants are under construction with generation capacity of additional 4,300 MWe. Ensuring high levels of safety in nuclear installations is a national responsibility and is achieved by following international standards and guidelines. The objectives of nuclear safety are: (i) to ensure that the risk from the operation of nuclear power plant (or nuclear facilities) is acceptably low, (ii) to prevent the occurrence of incidents or accidents and (iii) to limit the consequences of any incidents or accidents that might occur.

For limiting the consequences of the accident, it is imperative to ensure safe shutdown, continued core cooling, adequate confinement integrity and off-site emergency preparedness. Therefore, "Safety Analysis" is performed for a nuclear power plant (NPP) in order to demonstrate that for all plant states, the engineered safety barriers will prevent an uncontrolled release of radioactive material to the environment. To ensure this, the concept of defence in depth is generally adopted. There are basically two types of safety analysis, viz., Deterministic Safety Analysis (DSA) and Probabilistic Safety Analysis (PSA). The deterministic approach studies the behaviour of the plant under various operational states and accident conditions identified on the basis of engineering evaluations whereas PSA is a systematic and comprehensive tool for deriving the numerical estimates of risk. PSA provides a methodological approach for identifying accident sequences issued from a broad range of initiating events, which includes the systematic and realistic determination of accident frequencies and consequences. The present thesis is focused towards, (i) common cause

failure analysis for engineered safety systems using alpha factors obtained by mapping technique, (ii) dynamic modelling of the scenarios with time dependent success criteria and (iii) development of an integrated approach to assess the risk from multi unit nuclear power plants sites with consideration of both external and internal hazards.

As the first part of the research work, common cause failure analysis for engineered safety systems using alpha factors obtained by mapping technique, is carried out. It is well known that redundancy is the fundamental technique adopted for fault tolerance in safety critical applications. However, in the redundant systems, common cause failures (CCFs) are the major contributor to risk and therefore quantifying CCF is essential to demonstrate the reliability of a system. Various models exist for estimation of risk from common cause failures. In the present work, the alpha factor model is applied for the assessment of CCFs of safety systems deployed at two nuclear power plants. An approach described in NUREG/CR-5500 is extended in this study to derive plant specific coefficients for CCF analysis especially for high redundant systems. A critical comparison of alpha factor method and beta factor method is also performed by taking insights from the case studies of engineered safety systems installed in existent nuclear power plants.

In the second part of the research work "Markov Analysis for Time Dependent Success Criteria of Passive Decay Heat Removal System" is carried out. In real world applications such as power generation from nuclear power plants, the engineered safety systems are required to accomplish the specified tasks with varying mission times depending on the requirement and are subjected to different operating and environmental conditions. However, availability of such systems with redundant configuration depends upon success criteria and is application-specific. The Safety Grade Decay Heat Removal (SGDHR) System of Indian Prototype Fast Breeder Reactor is such a system which is required to operate with different success criteria during the specified mission time on account of steady decline in

decay heat produced by the reactor core. In this work, Markov analysis is carried out to estimate the availability of the system under both continuous and periodic monitoring schemes. The study estimates the upper bound and lower bound for mean unavailability of SGDHR system for the specified mission time. The approach followed can be used to dynamically model the scenarios with time dependent success criteria in a comprehensive manner and to study various factors affecting the availability of such systems.

Finally, in the last part of the research work "Integrated risk assessment for multi-unit NPP sites" is performed. Traditionally, a PSA is carried out to evaluate the risk associated with single unit NPP taking into account the defence in depth features and postulating combination of potential accident initiators for different hazards. But, a majority of nuclear power generating sites in the world houses more than one nuclear power plant. These sites are vulnerable to various hazards generated from external origin like earthquake, tsunami, flood, etc. and which can jeopardise the safety of the plants. Further, the risk from a multiple unit site and its impact on the public and the environment was evident during the Fukushima nuclear disaster of March 2011. At present, there exists no established approach or methodology to estimate the risk from a multi-unit nuclear power plant site due to internal and external hazards. Hence, there is an urgent need to evolve a methodology which can systematically assess the safety of the multi-unit site. In the present work, an integrated approach is developed to assess the risk contribution of multiple nuclear plants at the site. The work highlights the importance of risks for multi-unit sites arising from shared system, common cause failures, failure correlations, cliff-edge effects, etc. from different hazards. Though the main emphasis on multi-unit safety is on external hazards, the proposed approach also includes risk from random internal events. The approach developed not only quantifies the frequency of multiple core damage for a multi unit site but also evaluates site core damage frequency which is the frequency of at least single core damage per site per year.

Subsequently, the developed integrated approach is used to estimate and compare the risk from multi unit sites housing single, double, triple and quadruple nuclear plants. The study when extended, through sensitivity analysis can form the basis to optimize the shared resources effectively at the multi-unit sites. The spin-off from such a study carried out during the design stage will provide an input to decide the optimum number of units at a site, the optimal distance between two units, layout diversity and configuration of shared systems, etc. Finally, the approach developed is expected to be useful in developing safety goals, procedures and guidelines for a multi-unit NPP site.

NOMENCLATURE

List of Abbreviations

AERB	Atomic Energy Regulatory Board
AHX	Air Heat Exchanger
ALARA	As Low as Reasonably Achievable
AOOs	Anticipated Operational Occurrences
BDBA	Beyond Design basis Accident
BFR	Binomial Failure Rate
BWR	Boiling Water Reactor
CCF	Common Cause Failures
CDF	Core Damage Frequency
CEH	Conditional external Hazard
CFR	Code of Federal Regulations, United States
CIIE	Conditional Internal Initiating Events
DBA	Design basis Accidents
DEH	Definite External Hazard
DIIE	Definite Internal Initiating Events
DBE	Design basis Events
DHR	Decay Heat Removal
DHX	Decay Heat Exchanger
DSA	Deterministic Safety Analysis
ECCS	Emergency Core Cooling System
ESSs	Engineered Safety Systems
FTA	Fault Tree Analysis
MGL	Multiple Greek Letter Model

MTTR	Mean Time To Repair
IAEA	International Atomic Energy Agency (IAEA)
ICRP	International Commission on Radiological Protection
IIE	Internal Independent Events
INSAG	International Nuclear Safety Group
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LOSP	Loss of offsite Power
LOUHS	Loss of ultimate Heat Sink
NEA	Nuclear Energy Agency
NPPs	Nuclear Power Plant
NRC	Nuclear Regulatory Commission*, United States*
NUREG	United States Nuclear Regulatory Commission technical report designation
OECD	Organisation for Economic Co-operation and Development
OGDHRS	Operating Grade Decay Heat Removal System
PFBR	Prototype Fast Breeder Reactor
PGA	Peak Ground Acceleration
PSA	Probabilistic Safety Analysis
PHWR	Pressurized Heavy Water Reactor
PWR	Pressurized Water Reactor
QRA	Quantitative Risk Assessment
RIDM	Risk Informed Decision Making
RPS	Reactor Protection System
RR	Repair Rate
SBO	Station Blackout

SCDF	Site Core Damage Frequency
SDCP	Shutdown Cooling Pump
SDHX	Shutdown Heat Exchanger
SNETP	Sustainable Nuclear Energy Technology Platform
SSCs	Systems, Structures & Components
SGDHRS	Safety Grade Decay Heat Removal System

List of Symbols

'a'	Peak ground acceleration (PGA) value
A_{ej}	Conditional probability of initiating event e for the specified/particular unit k due to a direct impact of conditional external hazard
A_m	Median ground acceleration capacity
$BExp_{ijk}$	Boolean expression for j^{th} initiating event due to definite external hazard i for unit k
c_{iG}	Probability of conditional external hazard i affecting shared systems group 'G'
C_{ij}	Probability of a conditional external hazard 'i' that directly affects unit j
C_{ijk}	Probability that the conditional external hazard 'i' that directly affects unit j affects unit k (k=1, 2, 3…n and k≠j) also
d_{iGjk}	Probability of initiating event j for unit k due to the impact of hazard i on the shared system group G
D_{ijk}	Probability of initiating event j due to definite external hazard i for unit k
DG_{u1}	DG unavailability for unit 1
DG_{u1}	DG unavailability for unit 1
H_i	Frequency of (definite) external hazard i
IE_i	i^{th} initiating event

IE_{iG}	Frequency of conditional internal initiating event i for the shared systems group 'G'
IE_{ij}	i^{th} initiating event for unit j
$MTTR_{loop}$	Mean time to repair for the SGDHR loop
p_{eGj}	Conditional probability of initiating event e for unit j due to the indirect impact of corresponding conditional external hazard on shared systems group 'G'
Pf_{u1}	Preference probability of shared diesel generator for unit 1
P_{DG}	Probability of DG failure
P_{iGk}	Represents the probability of conditional internal initiating event i affecting shared systems group 'G' affects unit k
$P_i(t)$	Probability of the system to be in state i at time t
$P_k(j)$	the k^{th} element of the impact vector for event j, and n is the number of CCF events
Q_{CCF}	Failure probability of k and greater than k components due to CCF
Q_i	Unavailability of the i^{th} event in the cut set
Q_{m1}	Mean value of unavailability for time 0 to t1 hr
Q_{m2}	Mean value of unavailability for time t=t1 to MT
$Q(t)$	Component unavailability at time t
Q_T	Total failure probability of each component (includes independent and common-cause events)
$\alpha^{(m)}_k$	Fraction of the total probability of failure events that occur in the system involving the failure of k components in a system of m components due to a common-cause.

$\alpha^{(m)}_i$	The ratio of i and only i CCF failures to total failures in a system of m components
α_t	Sum of Alpha Factors
β_r	Logarithmic standard deviations of aleatory uncertainty
β_u	Logarithmic standard deviations of epistemic uncertainty
λ	Failure rate of the component
λ_{loop}	Single loop failure rate of SGDHR system
$\lambda_{1/4}$	(a), failure rate of a specific single loop out of four loops
$\lambda_{2/4}$	(b), failure rate of a specific two loops out of four loops
$\lambda_{3/4}$	(c), failure rate of a specific three loops out of four loops
$\lambda_{4/4}$	(d), failure rate of all the four loops
ρ	Conditional probability of each component failure given a shock
$\omega(t)$	Failure frequency of the component
ω_{cut}	Cut set failure frequency
ω_j	Failure frequency of the j^{th} event in the cut set

LIST OF FIGURES

LIST OF TABLES

CHAPTER-1

INTRODUCTION

1.0 FOREWORD

The global demand for energy has surged inexorably in the past 100 years on account of rapid industrialization and steady population growth. The global quest for energy is predicted to rise continuously, as developing countries like China and India are endeavouring hard to fuel their rapidly growing economy.

Therefore, keeping the human development and the economic growth in mind, there is a need to make use of all the available energy sources. The energy resources of India are experiencing severe constraints to meet the current demand. At present, the generating capacities in the country are under-performing on account of constraint in fuel supply. The Energy Policy document of the country indicates exhaustion of conventional fuel resources by the middle of the century. Moreover, the concern has also grown in recent times about the environmental impact caused by burning fossil fuels on account of greenhouse gas emissions which causes dangerous climate changes. The pressure to replace fossil fuels for assuring energy independence and to curb the climate change has focused more attention on nuclear power and renewable sources - e.g. solar, wind and biomass. Therefore, to meet the growing demand, to restrain the greenhouse gas emissions and to ensure the energy security of the country in the long term, it is imperative to develop and employ nuclear energy and renewable natural resources like wind, bio-gas and solar energy (Bhardwaj, 2013). The modern technology has enabled us to tap energy from the renewable natural resources. However, these are still limited in their scope and potential. Therefore nuclear energy is a viable option, enabling us to address the twin challenges of energy security and environmental sustainability.

The India's indigenous three stage nuclear power programme aims to utilise country's nuclear resource profile of modest uranium and abundant thorium reserves optimally with the multiple objectives of improving the quality of life of the people, reducing carbon emissions, attaining self-reliance and in achieving technological independence to meet the energy requirements of the nation (Jain, 2010). It is apparent that any means of generating electricity produces some wastes and causes some environmental hazard. The nuclear industry is unique in itself since it is the only energy-producing industry that takes the full responsibility for disposal of all its wastes and meets the complete cost for the same (World Nuclear Association, Radioactive Waste Management). The electricity generated from nuclear power plants (NPPs) in many regions is competitive with electricity generated from coal power plants including the cost provisions made for management and disposal of radioactive wastes and decommissioning of the NPPs (World Nuclear Association, The Economics of Nuclear Power). Therefore, nuclear energy is a clean, environment friendly, affordable and a promising source of energy.

At present nuclear power is the fourth-largest source of electricity in India after thermal, hydroelectric and renewable sources of electricity. As of now, India has 21 nuclear power plants at seven sites with an installed capacity of 5780 MWe while six nuclear power plants are under construction with a generation capacity of additional 4,300 MWe.

1.1 NUCLEAR SAFETY

The objective of nuclear safety is to protect the plant, plant personnel and public at large. However nuclear safety requires continuous quest for excellence. All individuals concerned should consistently endeavour to reduce the risk to the lowest practical level. The understanding of various objectives and principles of nuclear safety and the way in which its various aspects are interrelated is imperative to make the endeavour fruitful. In nuclear

parlance, “the objectives state what is to be achieved and the principles state how to achieve it” (INSAG-12, 1999).

Three safety objectives for nuclear power plants as defined in INSAG-12, 1999 are:

1. General Objective: “To protect individuals, society and the environment by establishing and maintaining in nuclear power plants an effective defence against radiological hazard”.

It is observed that each viable method of generation of electricity has its own merits and demerits. Therefore, nuclear power plants are equipped with various engineered safety systems to protect the plant, plant personnel and prevent any uncontrolled release of radioactivity to the environment. As per the objective, the engineered safety system is effective if it prevents significant addition either in risk to the health or risk of other damage to the exposed individuals, society and the environment as a consequence of the already accepted industrial activity.

2. Radiation Protection Objective: “To ensure in normal operation that radiation exposure within the plant and due to any release of radioactive material from the plant is as low as reasonably achievable, economic and social factors being taken into account, and below prescribed limits, and to ensure mitigation of the extent of radiation exposure due to accidents.”

Radiation protection is ensured in nuclear power plants under normal conditions and separate provisions are provided for accident scenarios. Various planned plant operating conditions and anticipated operational occurrences are made in compliance with radiation protection standards based on the recommendations by International Commission on Radiological Protection (ICRP) to ensure adequate radiation protection. In the event of an accident in which the source of exposure is not entirely under control, various safety

provisions in the plant and countermeasures outside the plant are planned and prepared in such a way to reduce the harm to individuals, populations and the environment to as low as possible.

3. Technical Safety Objective: "To prevent accidents in nuclear plants with high confidence; to ensure that, for all accidents taken into account in the design of the plant, even those of very low probability, radiological consequences, if any, would be minor; and to ensure that the likelihood of severe accidents with serious radiological consequences is extremely small."

The prevention of the accident is the first priority, which is achieved by the use of reliable structures, components, systems and procedures. However, no human endeavour can ever guarantee that in future there will never be an accident. Nuclear power plant designers, therefore assume that failures in component, system and human actions are possible, which can cause repercussions in the form of abnormal occurrences, ranging from minor disturbances to highly unlikely accident sequences. The additional protection required to mitigate such occurrences is achieved by incorporating various Engineered Safety Systems (ESSs) into the plant. In case of quite unlikely beyond design basis accidents, certain accident management provisions are provided for controlling their course and mitigating the consequences.

Finally, the safety objectives can be concluded as:

1. To ensure that the risk from the operation of nuclear power plant (or nuclear facilities) is acceptably low.
2. To prevent the occurrence of incidents or accidents.
3. To limit the consequences of any incidents or accidents that may occur.

For limiting the consequences of the accident it is imperative to ensure safe shutdown, continued core cooling, adequate containment integrity and off-site emergency preparedness.

These are ensured by following the principle of "Defence in Depth" as discussed in the following section.

1.2 BASIC REQUIREMENTS FOR ENSURING NUCLEAR POWER PLANT SAFETY

Three basic requirements to ensure the safety of a NPP are (INSAG-12, 1999; INSAG-10, 1996) to:

1. Control the reactor power: At all times the power of the reactor should be under control.
2. Cool the fuel: The core of the reactor comprising of fuel needs regular cooling to prevent its melting and release of radioactive substances.
3. Contain the radioactive substances: In case of any incident causing release of radioactive substances from the coolant system of the NPP, it should be confined within the plant with the help of containment systems.

1.3 BASIC PRINCIPLES OF NUCLEAR SAFETY

Two main basic principles (Safety Series No. 75-INSAG-4; INSAG-12, 1999; INSAG-10, 1996) are followed to prevent releases of radioactivity into the environment during an incident.

1.3.1 Safety Culture

The IAEA Safety Series No. 75-INSAG-4 states that "Safety Culture is that assembly of characteristics and attitudes in organizations and individuals, which establishes that as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance." It also mentions that the safety culture is composed of two general components. The first one is the essential frame work within the organization and it is to be taken care by the management. The second component of the safety culture is the attitude and

commitment of the staff of the organization in responding to and benefiting from the framework.

The major components of Safety Culture are shown in Figure 1.1 (IAEA Safety Series No. 75-INSAG-4). These components involve many elements which are crucial for instituting safety in the individual and organization.

- Individual awareness about the need and importance of safety.
- Knowledge and competence as conferred by the mentoring of personnel and coupled with their self-education.
- Commitment, which should be demonstrated by senior management by commending high priority to safety and should be adopted by the individuals for achieving the utmost important common goal of safety.
- Motivation, by management through leadership by setting the objectives and system of rewards and sanctions, and by individuals self-generated attitudes.
- Supervision which includes audit and review practices, with readiness to duly acknowledge the individuals questioning attitudes.
- Responsibility, by formally assigning and describing the duties to the individuals.

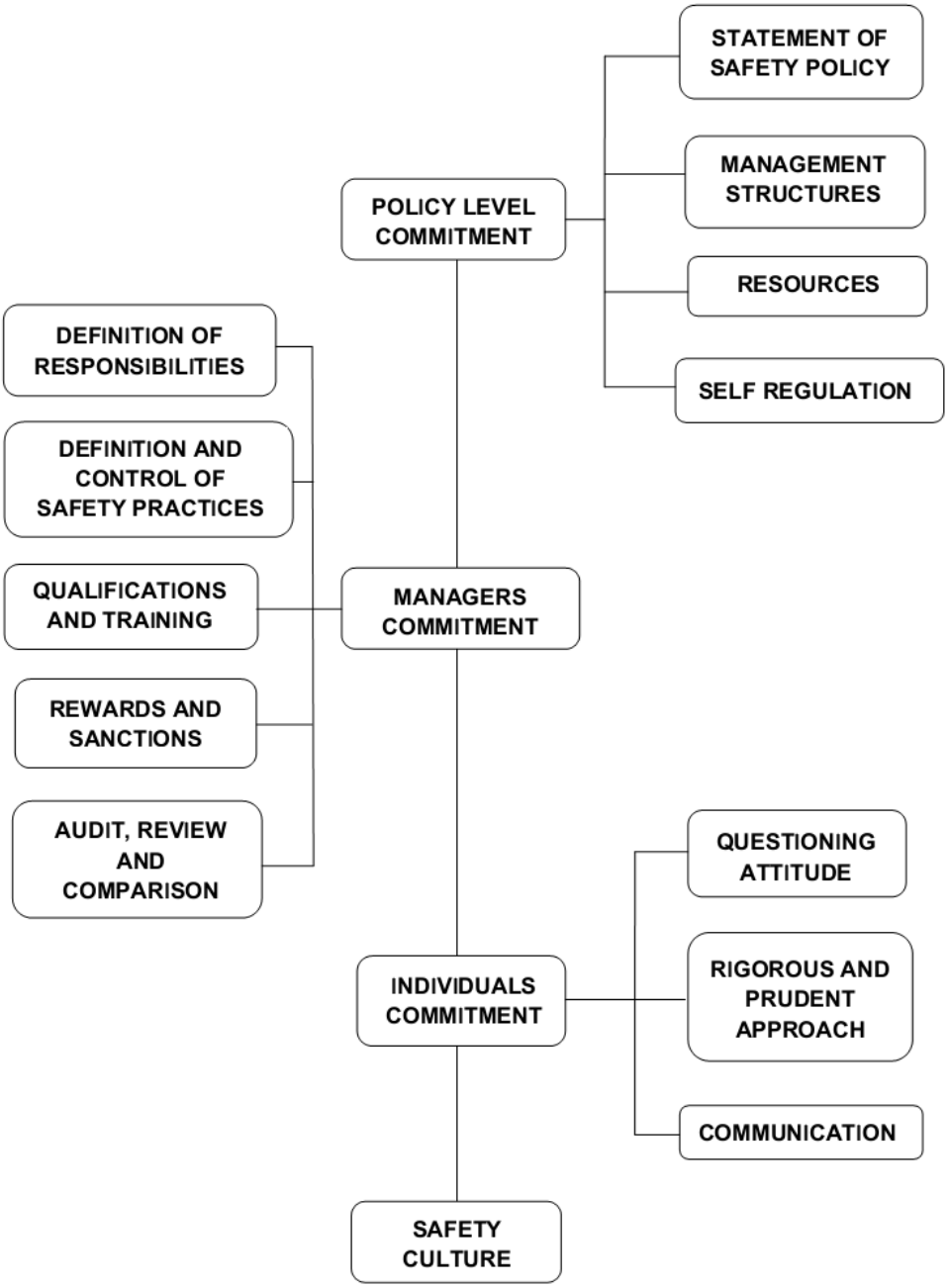

Figure 1.1: Main Components of Safety Culture

1.3.2 Defence in depth

The IAEA technical document, INSAG-12 states that "To compensate for potential human and mechanical failures, the concept of defence in depth is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting

damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective".

The concept of defence in depth provides an overall strategy to implement various safety measures and engineered features/provisions for the nuclear power plants. Diligent application of the concept ensures that no single human or equipment failure will lead to harm to the public, and even extremely unlikely scenarios of combinations of failures will cause little or no harm. The philosophy of defence in depth helps to ensure that the three basic safety functions, i.e., controlling the reactor power, cooling of the nuclear fuel and confinement of the radioactive material are preserved, and the radioactivity is not released into the environment or public domain.

A two-fold strategy is adopted for the principle of defence in depth. The first is to prevent accidents and the second is, in case the prevention fails, limit the potential consequences of accidents and to avert them from developing into more serious conditions. The philosophy of defence in depth is structured in five levels. Each level of protection has a specific objective and the essential means of achieving the same as shown in Table 1.1, which is taken from INSAG-10 and INSAG-12. While implementing the strategy of defence in depth, if one level fails, the subsequent level comes to action into the scenario, and so on. The hazards that have the potential to impair several levels of defence, such as fire, flooding or earthquakes are paid special attention. Wherever possible, appropriate precautions are taken to the best possible extent in order to prevent such hazards, and the plant and its engineered safety systems are designed to withstand them.

Table 1.1: Levels of Defence in Depth for Nuclear Power Plants

Levels	Objective	Essential means
Level - 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation

Level - 2	Control of abnormal operation and detection of failures	Control, limiting and protective systems and other surveillance features
Level - 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level - 4	Control of severe plant conditions including prevention of accident progression and mitigation of consequences of severe accidents	Complementary measures and accident management
Level - 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

The importance of prevention and mitigation of accidents in defence in depth as stated in the IAEA TECDOC INSAG-12 is expressed in the following two corollaries.

Corollary on accident prevention: "Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents, particularly any which has a potential to cause severe core damage".

The first approach to prevent accidents is to make sure that the deviations from normal operational states are infrequent which can be made possible by instituting such high quality in design, construction and operation of the plant. Various safety systems are engineered into the plant to prevent such deviations turning into accidents. The concepts of redundancy and diversity are used in the design of the safety systems to increase their robustness. Moreover, wherever required, to reduce the possibility of the loss of a vital safety function, a physical separation between the parallel components is also provided. Apart from that, the systems and components deployed in the plant are inspected and tested periodically to reveal any degradation which may have a potential to cause abnormal operating conditions or inadequate performance of the safety systems. The monitoring systems promptly detect abnormal conditions which are threat to the nuclear safety thereby giving alarms and in many cases initiating the corrective actions automatically. The second means of preventing

accidents is to develop a questioning attitude in the staff and to encourage discussions on what can go wrong prior and later to initiating events and motivate them to always strive for the ways to improve nuclear safety. The operators should be well trained in appropriate operating procedures and they must be able to timely recognize the onset of an accident and should be able to respond properly and in an appropriate and systematic manner to such abnormal conditions.

According to the tecdoc, the prevention of accidents depends on various factors viz.

- Conservatively designed equipment.
- Quality assurance checks to verify the achievement of the design intent.
- Periodic surveillance activities/checks to detect degradation or an incipient failure during operation and good operational practices to prevent failure.
- The steps to be followed to ensure that a minor perturbation or incipient failure will not develop into a more serious situation.

Corollary on accident mitigation: "In-plant and off-site mitigation measures are available and are prepared for that would substantially reduce the effects of an accidental release of radioactive material".

The provisions provided for accident mitigation takes the concept of defence in depth beyond accident prevention. The three kinds of accident mitigation provisions are accident management, engineered safety features and off-site counter-measures. In those circumstances when the design specifications of the plant are exceeded, accident management which includes pre-planned and ad hoc operational measures is carried out to restore the control by making optimum use of the existing plant equipment in normal and unusual ways. The three main objectives of the phase of accident management are i) shutting down the reactor and restoring it into the safe state, ii) ensuring continued cooling of the nuclear fuel iii) confinement of the radioactive material and protection of the confinement function. In

such circumstances, the engineered safety systems will operate to confine the released radioactive material from the core, thereby ensuring that the release of the radioactivity to the environment is kept at the minimum. Apart from various engineered safety systems, provision exists for off-site countermeasures also, which goes beyond the level of protection provided by the most diligent human effort, to account for the remote possibility of failure of the plant's safety provisions. In such remote cases, the effects on the environment and the neighbouring population can be mitigated by taking protective measures like sheltering or evacuation of the population, and by preventing the ingress of radioactivity material into the humans via food-chains and other pathways.

The concept of defence in depth is implemented by the following means (Dave, Nuclear Power Plant Safety-Nuclear Engineering-301):

- Providing multiple means for the basic safety functions
- Incorporating inherent safety features and reliable protections
- Plant control by automatic engineered safety systems and operator actions
- Adequate provisions for accident prevention and mitigation
- Providing multiple physical barriers for the release of radioactivity

The provision of leak tight barriers between the radioactive source and the public is shown in Figure 1.2 (World Nuclear Association, Nuclear Fuel Fabrication). These barriers consist of:

1. Fuel pellet
2. Fuel cladding
3. Primary coolant system
4. Containment building
    a. Primary
    b. Secondary (optional)

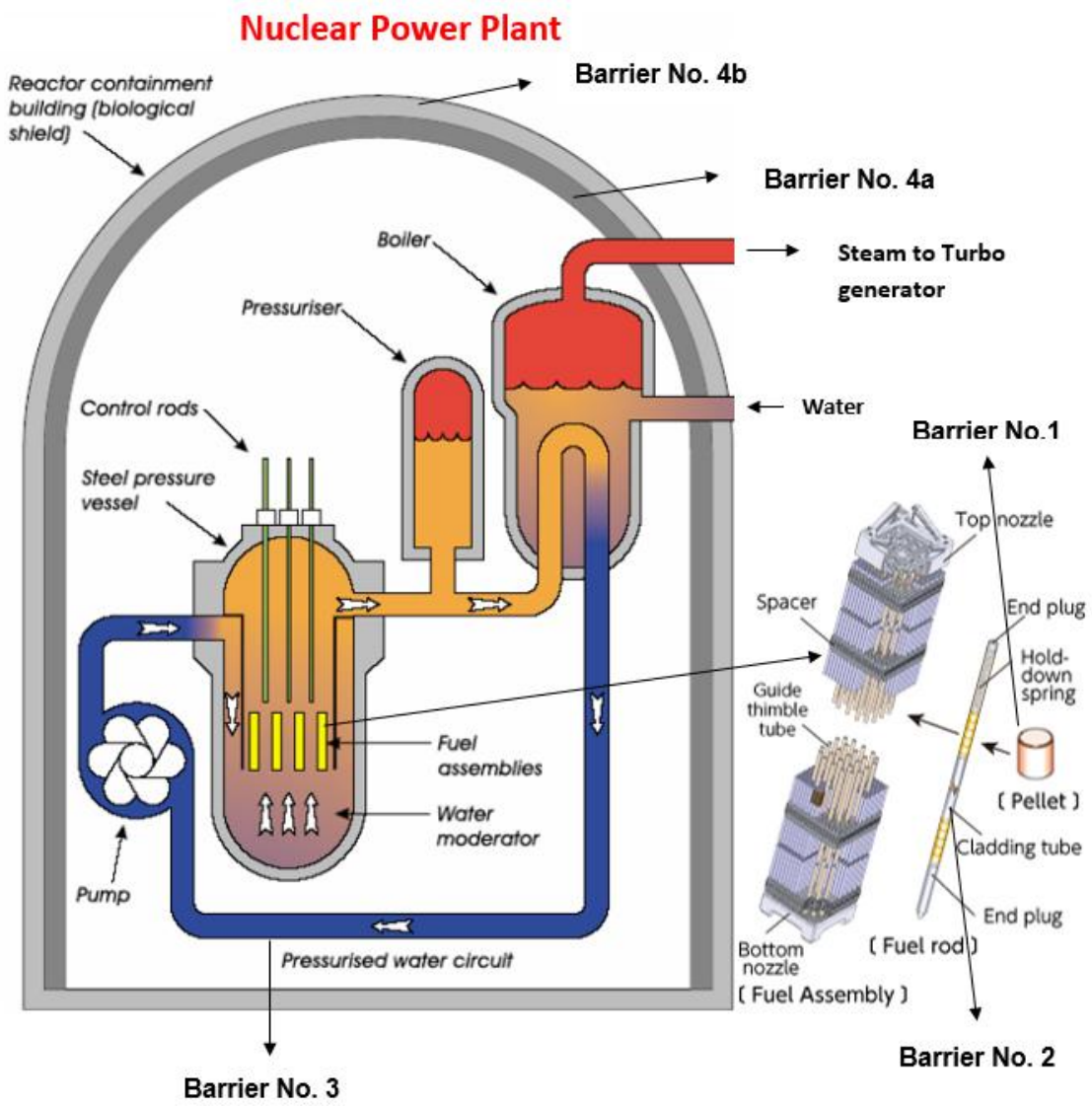

Figure 1.2: Multiple physical barriers to prevent the release of radioactivity

The Figure 1.3 shows the relation between physical barriers and levels of protection in defence in depth (BARC, Safety of nuclear reactors).

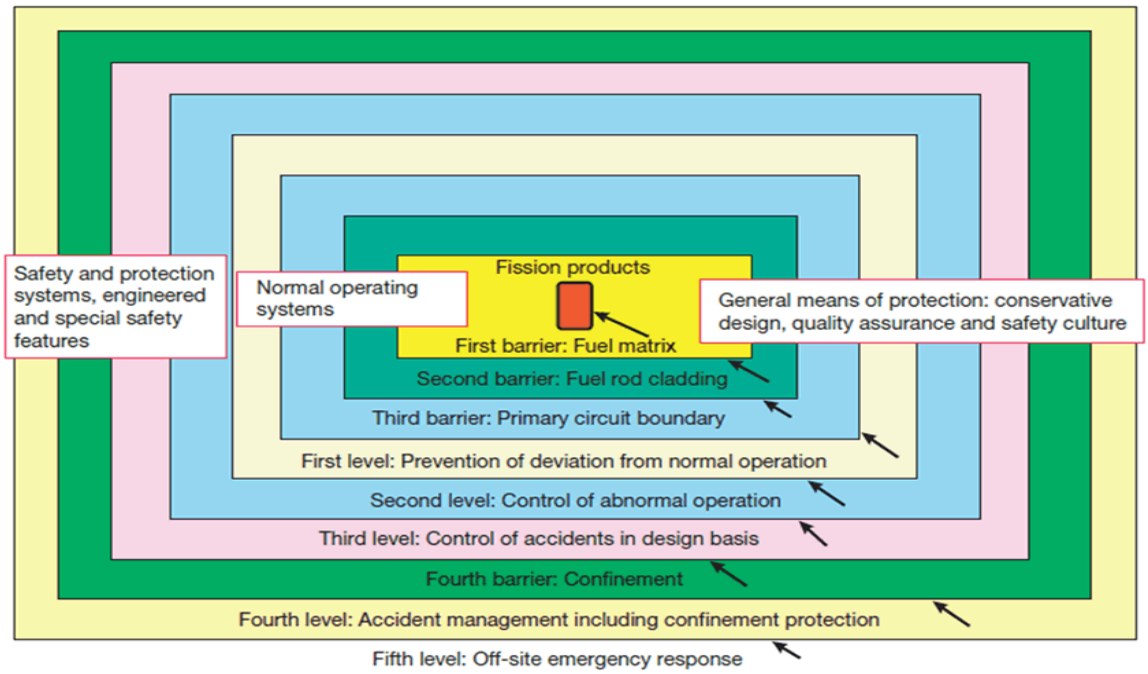

Figure 1.3: The relation between physical barriers and levels of protection in defence in depth

1.4 METHODS FOR SAFETY ANALYSIS

The IAEA safety guide (IAEA Specific Safety Guide No. SSG-2, 2009) states that "Safety analysis are analytical evaluations of physical phenomena occurring at nuclear power plants, made for the purpose of demonstrating that safety requirements, such as the requirement for ensuring the integrity of barriers against the release of radioactive material and various other acceptance criteria, are met for all postulated initiating events that could occur over a broad range of operational states, including different levels of availability of the safety systems".

Safety analysis should consider all plant states ranging from normal operation, operational occurrences and accident conditions.

- Operational states
    - Normal operation
    - Anticipated operational occurrences
- Accident conditions

- Within design basis accidents
- Beyond design basis accidents, i.e., severe accidents.

1.4.1 Requirement of Safety Analysis

Safety analysis is required to be performed for an NPP (IAEA Specific Safety Guide No. SSG-2, 2009; Dave, Nuclear Power Plant Safety-Nuclear Engineering-301) to demonstrate that:

- For all plant states, the engineered safety barriers will prevent an uncontrolled release of radioactive material to the environment.
- The concept of defence in depth has been properly implemented.
- The process of fission can be controlled within the design limit and to ensure that the reactor core can be cooled in case of an occurrence of any event by effectively removing the generated heat.

1.4.2 Types of Safety Analysis

There are two basic types of safety analysis:

- Deterministic Safety Analysis (DSA), and
- Probabilistic Safety Analysis (PSA)

1.4.3 Deterministic Safety Analysis (DSA)

The DSA studies the behaviour of the plant under various operational states and accident conditions identified through comprehensive engineering evaluations. It also intends to establish the behaviour of the plant in compliance with the chosen criteria (Gianni Petrangeli, 2006).

The deterministic safety analysis for a nuclear power plant predicts the response of the plant for various postulated initiating events. While carrying out the analysis, specific set of rules and acceptance criteria are applied. The analysis focuses on neutronic, thermo hydraulic, radiological, thermo-mechanical and structural aspects, which are analysed using

various computational tools. The computations are performed for all pre-determined operating modes and operational states of the plant for various events like anticipated transients, postulated accidents, selected beyond DBA and severe accidents with core degradation (IAEA Specific Safety Guide No. SSG-2, 2009; Dave, Nuclear Power Plant Safety-Nuclear Engineering-301; Gianni Petrangeli, 2006).

The spatial and time dependences of various physical variables, viz., neutron flux, thermal power of the reactor, pressure, temperature, flow rate and velocity of the primary coolant, stresses in structural materials, physical and chemical compositions, concentrations of radio nuclides are obtained as the results of computations carried out for DSA. Radiation doses to workers or the public are obtained from the computations carried out for the assessment of radiological consequences.

On the basis of this analysis, the design basis for items important to safety is established and confirmed. For example, we can consider partial blockage in a fuel subassembly of a nuclear reactor as a 'cause,' and by carrying out suitable analytical modelling and computations one can determine the maximum clad temperature as a function of time or as a function of blockage . The clad temperature would be the 'effect' and when related to prescribed limits, provides us with a 'safety margin'. These safety margins are required in licensing applications. Such a DSA is usually carried out by a designer, as part of the design and construction process or by the utility firm to confirm the design and by the regulatory organisation to regulate and ensure nuclear safety.

As specified by IAEA Specific Safety Guide, No. SSG-2, 2009, there are three ways for carrying out deterministic safety analysis for various anticipated operational occurrences and design basis accidents. The first one is via conservative analysis. Here, conservative computer codes with conservative initial and boundary conditions are used. Another way is by carrying out combined analysis. Here, best estimate computer codes are used in

combination with conservative initial and boundary conditions. And finally, the third approach is use of best estimate analysis. In this approach the best estimate computer codes with conservative and/or realistic input data are used, wherein the evaluation of the uncertainties in the calculation results is also carried out by accounting for both the uncertainties, i.e., uncertainties in the input data and uncertainties associated with the models of the best estimate computer code.

Amongst the three approaches, the best estimate analysis together with an evaluation of the uncertainties is most popularly used nowadays because of many reasons. The first reason is, the use of conservative assumptions can lead to an incorrect prediction of progression of events or an inaccurate estimation of the timescales or it can also lead to exclusion of some critical physical phenomenon. Also, the use of a conservative approach often facilitates reduced operational flexibility. On the contrary, the use of best estimate approach provides more profound information about the plant's behaviour, aids in identification of the most significant safety parameters and provides greater insight on the existing margins between the calculated results and the acceptance criteria thereby facilitating better operational flexibility.

The following points describe the importance of DSA (IAEA Specific Safety Guide No. SSG-2, 2009; Dave, Nuclear Power Plant Safety-Nuclear Engineering-301; Gianni Petrangeli, 2006):

- It is used for developing plant protection and control systems, set points and control parameters.
- It is also used for developing technical specifications of the plant.
- It is used to demonstrate that various anticipated operational occurrences and design basis accidents can be safely managed by automatic response of safety systems in combination with appropriate operator actions.

- It aids in establishing a set of Design Basis Events (DBEs) and it further facilitates analyses of their consequences through various subsequent computations.
- It demonstrates the effectiveness and robustness of various equipment and the engineered safety systems deployed to prevent escalation of AOOs and DBAs to severe accidents. It is also used to design mitigation strategies for the resulting severe accidents.
- It demonstrates that the safety systems can:
    i. Cause shutdown of the reactor and maintain it in safe shutdown state during and post DBA.
    ii. Efficiently remove the decay heat from the core of the reactor post shutdown for all operational states and DBA conditions.
    iii. Ensure that the release of radioactivity following a DBA is below acceptable limit.

- DSA for normal operation of the plant (IAEA Training Course on Safety Assessment of NPPs, Safety Analysis: Event Classification):
    i. It ensures that normal operation is safe and plant parameters do not exceed operating limits with radiological doses and release of radioactivity within the acceptable limits.
    ii. It also helps in ensuring that the doses from the operation of the plant follow the principle of ALARA. "ALARA is an acronym for 'As Low As (is) Reasonably Achievable,' which means making every reasonable endeavour to minimize the exposure of ionizing radiation below the dose limits as low as possible".
- Establishes the conditions and limitations for safe operation of the reactor which includes safety limits for reactor protection and control and other engineered safety systems, reference settings and operational limits for the control system, procedural constraints for operation of various processes.

- Finally, the DSA determines whether a reactor design is adequate and licensable.

1.4.4 Probabilistic Safety Analysis (PSA)

Probabilistic Safety Assessment/Analysis or Probabilistic Risk Assessment is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity like NPP, Oil and Gas facilities, Chemical & Process Industries, etc. In general, it can be said that it is a conceptual tool for deriving the numerical estimates of risk for nuclear plants and industrial installations, and also for evaluating the uncertainties in these estimates. It differs from deterministic safety analysis, as it facilitates systematic identification of the accident sequences that can arise from a wide range of events including design basis and beyond design basis. It includes logical determination of accident frequencies and consequences, component and human data for arriving at a realistic estimate of risk (IAEA-TECDOC-1200, 2001; Solanki & Prasad, 2007).

In the last couple of decades, the PSA has emerged as an increasingly popular analytical tool. It addresses three basic questions: "(i) What can go wrong with the entity under study? (ii) What and how severe are the potential detriments or consequences that the entity under study may be subjected to? and (iii) How likely these undesirable consequences may occur ?" (Solanki & Prasad, 2007). Thus, PSA in nuclear domain provides insight into the strength and weakness of the design of the nuclear power plant and helps to achieve a balanced design of the plant.

The objective of PSA is to identify issues that are important to safety, and to demonstrate that the plant is capable of meeting authorized limits on the release of radioactive material and on the potential exposure to radiation for each plant state. Since, deterministic safety analysis does not alone demonstrate the overall safety of the plant, and it should be complemented by probabilistic safety analysis. While deterministic analysis is typically used to verify that acceptance criteria are met, PSA is generally used to estimate the

probability of damage for each barrier (Dave, Nuclear Power Plant Safety-Nuclear Engineering-301).

1.4.5 Various Levels of PSA

The development of PSA over the years has led to three internationally accepted levels of analysis (i.e., Level 1 PSA, Level 2 PSA and Level 3 PSA).

1.4.5.1 Level 1 PSA

This is the foremost and founding level of the PSA. This level of PSA assesses the plant design and operation with focus on various initiating events and corresponding accident sequences which can potentially/possibly lead to core damage. This part of the PSA helps to figure out various strengths and weaknesses in the plant design. It also helps to identify possible ways to prevent core damage, which in most cases will be a precursor to accidents leading to major release of radioactivity with potential health and environmental consequences (IAEA Safety Series No. 50-P-4, 1992; Solanki & Prasad, 2007).

1.4.5.2 Level 2 PSA

A Level 2 PSA examines severe reactor accident through a combination of probabilistic and deterministic approaches in order to quantify the magnitude and frequency of radioactive release to the environment following the core damage and containment failure. This level of PSA builds on the analysis already undertaken in the Level 1 PSA study. A Level 2 PSA evaluates accident phenomena, predicts various containment failure modes that can lead to radioactive releases (source term) and estimates large early release frequency (LERF). Finally it provides insight into the weaknesses and strengths of onsite accident mitigation and management measures to reduce the impact of the accident (IAEA Safety Series No. 50-P-8, 1995; Solanki & Prasad, 2007).

1.4.5.3 Level 3 PSA

A Level 3 PSA analysis the transport of radio nuclides into the environment and assesses the public health risk and economic consequences due to the accident. It evaluates frequency and magnitude of radiological consequences to the public, environment and the society with consideration of meteorological conditions, topography, demographic data, radiological release and dispersion models (IAEA Safety Series No. 50-P-12, 1996; Solanki & Prasad, 2007).

Atmospheric dispersion and deposition of radioactive releases are also analysed by a Level 3 PSA study. It identifies various exposure pathways, estimates health effects on plant workers and the public and also arrives at the estimates of other societal risks. Moreover it is used to gain insights into the strengths and weaknesses of various possible countermeasures or protective actions.

The Figure 1.4 presents an overview of PSA (Paul Scherrer Institute, 2013; IAEA-Technical Report, 1991). The Level 1 PSA yields an estimate of 'core damage frequency', Level 2 PSA provides an estimate of the frequency of radioactive release to the environment and finally Level 3 PSA estimates the impact of the released radioactivity to the health of humans. Hence, it is worthwhile to note that for a comprehensive risk assessment all the levels of PSA are required.

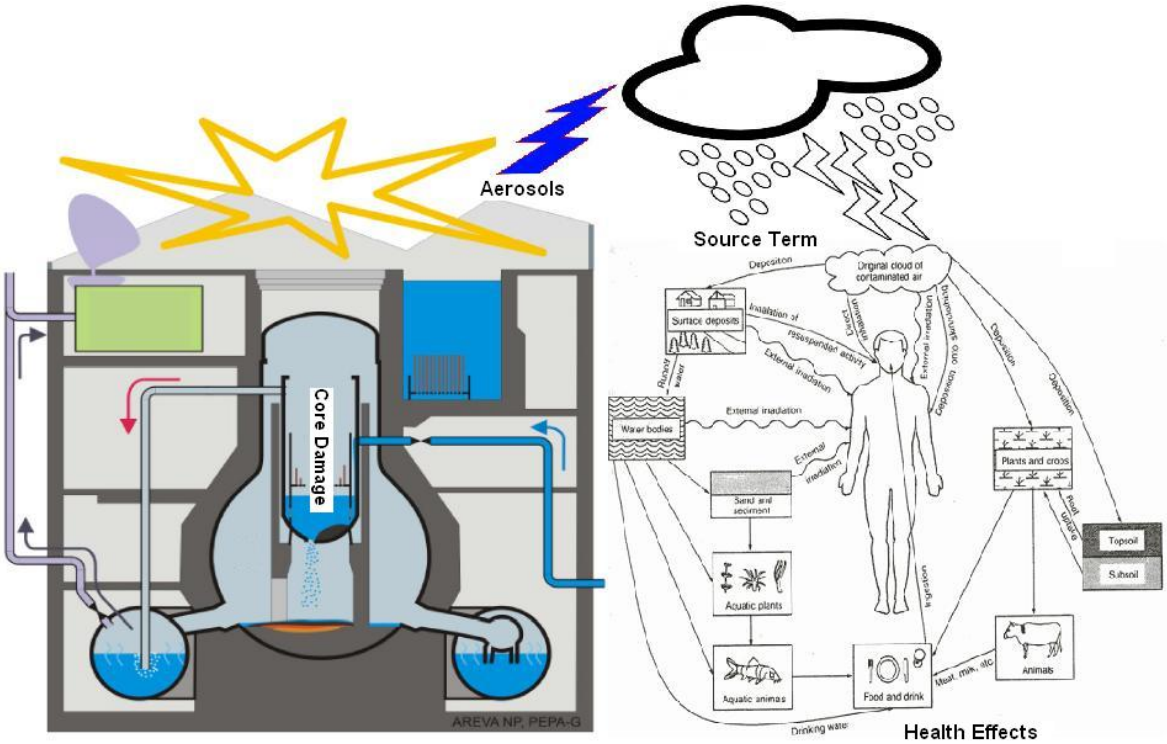

Figure 1.4: Core Damage, Source Term and Health Effects

1.4.6 Applications of PSA

The use of PSA covers three main applications (IAEA-TECDOC-1200, 2001; Solanki & Prasad, 2007):

1.4.6.1 During the Design of the NPP

The PSA provides insight into the strength and weakness of the design of the plant and helps to achieve a balanced design. It is used to examine the risk from various external hazards and internal events. It also allows designer to analyse the risk from various single and multiple failures in the plant. It also facilitates study of various inter-system and inter-unit dependencies to enhance the safety of plant and site. Finally, it is used to verify the target values as set by the regulatory organization. The internationally recommended targets for the frequency of core melt for new nuclear reactors including external events is less than or equal to 10^{-5} per year and the frequency of high release of fission product should be less than or equal to 10^{-6} per year (INSAG-12, 1999).

1.4.6.2 In Regulatory Activities

The PSA is being used by the regulators in order to ensure the safety of the plant. This is done through regulatory reviews in order to ensure that the utility is meeting the safety targets for the plant. Apart from this, the insights obtained from PSA are also used for carrying out risk-informed decision making (RIDM).

1.4.6.3 Safety in Operation

PSA is used in a variety of ways in the operation of NPPs. It is used as a tool to monitor the real time risk status of the NPP. This helps to keep the risk from the plant attributable to its actual configuration and various plant activities at an acceptable level. It is also used to evaluate optimized limits of allowed outage times, surveillance test intervals and testing strategies for various components and systems of the plant. Furthermore it is also used in periodic safety reviews. This is done in order to ensure that the plants built by the old standards are sufficiently safe and also, to support upgrades and back fitting activities to further enhance their safety. Finally, it is also used for evaluation of operating experience, training programme for operators and strategies for accident management and emergency planning.

1.5 PROBABILISTIC SAFETY ANALYSIS VS DETERMINISTIC SAFETY ANALYSIS

The Table 1.2 shows a comparison of PSA and DSA under various aspects (RISKworld, 2002; Solanki & Prasad, 2007).

Table 1.2: A comparison of PSA and DSA

Element of Approach	Deterministic Safety Analysis	Probabilistic Safety Analysis
Hazards/Initiating Events	• All frequently occurring events, commonly known as "Design Basis accidents" are covered in the analysis. • Beyond Design Basis Events are covered to less extent.	• All design basis events are considered in the analysis. • Most of the beyond design basis events are also considered in the analysis.

Analysis Method	• Conservative rules, standards and guidelines are followed. • A variety of techniques, including engineering judgment, factors of safety, etc are used in the analysis.	• A well established methodology is followed. • Best estimate assumptions are made for the analysis.
Failure Analysis	• Single failure criterion is generally adopted for the analysis.	• Multiple failures and common cause failures are also accounted in the analysis.
Design	• Supports the design process to a significant extent. • It is used to design the facility for the so called Design Basis Events. • It demonstrates the effectiveness of safety systems to cope with the accidents.	• Risk and Reliability insights are used to design the Systems, Structures and Components of the facility and make it more robust to withstand the accidents. • Through optimization studies it also helps in making cost effective safety improvements for the existing facilities.
Operator Behaviour	• Operator actions are not credited in first 15/30 minutes following an accident. • Operator errors are not postulated after 15/30 minutes.	• Throughout the accident sequence, errors in human actions are considered.
Results	• It is used to design the plant for the Design Basis Events. • It is used to provide provision of mitigation for the Beyond Design Basis Events. • It can't estimate the residual risk.	• It estimates the risk from the facility. • Helps to achieve balanced design of the plant. • Provides insight to design strength and weakness. • It also helps in planning maintenance activities.

1.6 OBJECTIVES AND SCOPE OF THE THESIS WORK

1.6.1 Alpha Factor Model for Common Cause Failure Analysis of Engineered Safety Systems using Mapping Technique

Most of the modern technological systems are deployed with high redundancy but still they fail mainly on account of common cause failures (CCF). Various models such as Beta Factor, Multiple Greek Letter, Binomial failure Rate and Alpha Factor exist for estimation of risk from common cause failures. Amongst all, alpha factor model is considered the most suitable

for high redundant systems as it arrives at common cause failure probabilities from a set of ratios of failures and the total component failure probability Q_T. In this work, alpha factor model is applied for the assessment of CCF of safety systems deployed at two nuclear power plants. A method to overcome the difficulties in estimation of the coefficients, viz., alpha factors in the model, importance of deriving plant specific alpha factors and sensitivity of common cause contribution to the total system failure probability with respect to hazard imposed by various CCF events is highlighted. An approach described in NUREG/CR-5500 is extended in this study to provide more explicit guidance for a statistical approach to derive plant specific coefficients for CCF analysis especially for high redundant systems. A comparison of Alpha factor method and Beta factor method is also presented by taking insights from the case studies of engineered safety systems installed in Indian Nuclear Power Plants. The procedure is expected to aid regulators for independent safety assessment.

1.6.2 Markov Analysis for Time Dependent Success Criteria of Passive Decay Heat Removal System

Safety systems deployed in nuclear industry are generally required to operate for a particular mission time. Most of such systems employ redundancy to ensure their high availability over the stipulated mission time. However, availability of a system with redundant configuration depends upon success criteria and is application-specific. The Safety Grade Decay Heat Removal (SGDHR) system of Indian Prototype Fast Breeder Reactor is required to operate with different success criteria during the specified mission time on account of steady decline in decay heat produced by the reactor core.

In this work, Markov analysis is carried out to evaluate the availability of the system under both continuous and periodic monitoring schemes. The study estimates the upper bound and lower bound for mean unavailability of SGDHR system for the specified mission time. Sensitivity analysis of the system attributable to important parameters is also carried out. The analysis has been carried with and without the consideration of common cause

failures. The study provides a comprehensive approach to model scenarios with time dependent success criteria and provides an insight on to the factors affecting the availability of such systems.

1.6.3 Integrated Risk Assessment for Multi-Unit NPP Sites

Multi-unit safety assessment has gained global importance after the Fukushima disaster in March 2011. Most of the nuclear sites in the world have more than one reactor and hence it is imperative to evolve a methodology to systematically assess the safety of the multi-unit site. In this work, unique features to be addressed in multi-unit safety assessment are discussed and an integrated approach is developed to assess the risk contribution of multiple nuclear plants at the site. The work highlights the importance of risks for multi-unit sites arising from shared system, common cause failures, failure correlations, cliff-edge effects, etc. for various hazards. Though the main emphasis on multi-unit safety is on external hazards, the proposed approach also includes risk from random internal events. The approach developed not only quantifies the frequency of multiple core damage for a multi unit site but also estimates site core damage frequency which is the frequency of at least single core damage per site per year with consideration of various inter-unit dependencies. The outcome of such integrated PSA helps in identification of those structures, system and components (SSCs) that are inter unit dependent and play a vital role in multi-unit safety.

Subsequently, the developed integrated approach is used to estimate and compare the risk for sites housing single, double, triple and quadruple nuclear plants. The outcome of such integrated PSA will also help in identification of those structures, systems and components that play important role in safety at multiple units and in regulatory decisions such as optimum number of units at a site, distance between two units, layout diversity and configuration of shared systems, etc. to minimize risk to the public and environment.

1.7 ORGANISATION OF THE THESIS

The thesis is divided into five major parts. The first part comprises of Chapter-1 which discusses nuclear safety, safety analysis methodologies and finally specifies the objectives of the thesis. The second part comprises of Chapter-2 in which common cause failure analysis for engineered safety systems using alpha factors obtained by mapping technique is carried out. The third part consists of Chapter-3 in which Markov analysis is carried out for passive decay heat removal system which has time dependent success criteria. The fourth part comprises of the two chapters (Chapter-4 & Chapter-5) dealing with the most critical issue of the hour, i.e., multi unit risk assessment. The chapter-4 presents the integrated approach which has been developed to estimate the risk from a multi unit NPP site whereas in chapter-5 the developed methodology is used to estimate and compare the risk for the sites housing single, double, triple and quadruple nuclear plants. The final part of the thesis (Chapter-6) reports the major findings of the thesis and also outlines the scope of future research work based on the thesis .

CHAPTER-2

Alpha Factor Model for Common Cause Failure Analysis of Engineered Safety Systems using Mapping Technique

2.0 INTRODUCTION

Probabilistic Safety Assessment (PSA) is a systematic and comprehensive methodology to evaluate risks associated with every life-cycle aspect of a complex engineered technological entity such as a facility, a spacecraft, or a nuclear power plant. The PSA has emerged as an increasingly popular analytical tool among various industries in the last couple of decades as it provides quantitative results and qualitative insights that help to make decisions regarding design and operational issues from safety view point (IAEA-TECDOC-1511, 2006). In nuclear industry, it is prominently used as a tool in design optimization studies and as a regulatory tool to assess, evaluate and enhance the safety of the plant (IAEA-TECDOC-1200, 2001).

In nuclear safety systems, redundancy is the fundamental technique adopted for fault tolerance. However, in redundant systems, common cause failures (CCF) are considered to be the major contributor to risk and therefore quantifying CCF is absolutely imperative to demonstrate the reliability of a system. In this context, various methods such as Beta factor, Multiple Greek Letter, Binomial Failure Rate, Alpha factor are developed (Mosleh et al., 1989). The Beta factor model is a single parameter model and it assumes that whenever a CCF event occurs, all components within the CCF group fail. This model assumes that a constant fraction beta of the component failure can be associated with the common cause events shared by other components in that group. In Multiple Greek Letter model other parameters in addition to the beta factor are introduced to account more explicitly for higher order redundancies and to allow for different probabilities of failures of subgroups of the common cause component group (Sanyasi, 2010). Binomial Failure Rate model estimates

multiple failure probabilities by postulating a shock that impacts the system at certain frequency to cause multiple failures. The alpha factor model defines common cause failure probabilities from a set of failure frequency ratios and the total component failure probability Q_T (IAEA-TECDOC-648, 1992). Among all the CCF models, alpha factor is considered to be more realistic as it can model the real scenario to a greater extent. Alpha factor method does not assume that in each CCF event all components share the common cause but assigns probabilities to the different degrees of the cause and is based on clearly formulated probabilistic assumptions. Thus, this approach poses a more complex structure to determine the alpha factors when the level of redundancy increases. One main advantage of this method is the ability to analyze various CCF events of different intensity as applicable to plant/system specific requirements. CCF quantification based on CCF impact rate, number of components of the common cause component group affected has shown realistic behaviour of the model and is found suitable for high redundant systems (Berg et al., 2008). Mapping up technique enables the estimation of CCF basic event probability in a highly redundant system based on the plant specific data available for lower redundant system (Wierman et al., 2001). In the current study, an attempt is made to exhibit the technique of mapping up of event impact vectors to determine alpha factor for high redundant systems. An impact vector is a numerical representation of a CCF event. Alpha factors are then used to estimate the CCF contribution to the system. A comparison of Alpha factor method and Beta factor method is also presented taking insights from the case studies of safety systems of the Indian Nuclear Power Plants.

2.1 BACKGROUND AND MOTIVATION

Redundancy not only ensures enhanced safety but also improves the availability thereby improving the economics in almost all applications. In a Nuclear Power Plant (NPP) two

most important safety systems are Reactor Protection System (RPS or Shutdown Systems) and Decay Heat Removal Systems. Of these, the shutdown system possesses a more redundant configuration; Table 2.1 below indicates redundant configuration in shutdown systems of Indian Nuclear Power plants. Apart from shutdown systems, there are many other systems where redundancy is adopted such as Class III systems, heat removal systems, etc.

Table 2.1: Configuration of shutdown systems in Indian reactors

Reactor Type	Configuration of Shutoff rods
220 MWe Standardized Pressurized Heavy Water Reactor	Primary Shut down system comprises of fourteen mechanical Cadmium sandwiched stainless steel rods (Bajaj and Gore, 2005)
540 MWe Pressurized Heavy Water Reactor	Twenty eight mechanical Cadmium sandwiched stainless steel rods are used as Primary Shutdown System (Seth, 1988).
500 MWe Prototype Fast Breeder Reactor	Primary shutdown systems consisting of nine control rods for power regulation and shutdown function and one secondary shutdown system with three absorber rods for shutdown (Kumar, 2005).
160 MWe Boiling Water Reactor	Sixty nine cruciform type control rods made of stainless steel (Katiyar and Bajaj, 2005)

In order to better estimate the reliability of such redundant safety systems, regulatory authorities recommend the use of Alpha factor model over Beta factor model in the reliability studies .The present study is carried out from these considerations to estimate the alpha factors for common cause failures associated with systems with high degree redundancy to finally arrive at CCF basic event probability. Such realistic probability estimates will help in arriving at more meaningful risk assessments.

2.2 MATERIALS AND METHODS

2.2.1 CCF Event

A CCF event is a result of simultaneous failure of two or more individual components failure due to a single shared cause, thus defeating redundancy or diversity which is intentionally employed to improve reliability of system (Wierman et al., 2007). Such an event can significantly affect the availability of safety systems.

2.2.2 Estimation of CCF Probability

Computation of a CCF probability is a multi-step process. Firstly, system fault trees are developed to identify the CCF events that contribute to the possible failure of the system. Then a selection of model to analyse the CCF event is made. Basic Parameter model, Beta model, Multiple Greek Letter (MGL) model, and Alpha Factor model are some of the CCF models to estimate the probability of a common-cause event involving k specific components in a common-cause component group (CCCG) of size m (Wierman et al., 2001).

In the present study, the parametric Alpha Factor model is chosen because the alpha factor model can handle common cause component group sizes of different levels; can be adopted even when no statistical data on common cause failure rates are available; and is more accurate compared to other parametric models (Wierman et al., 2001).

The alpha factor model estimates the CCF frequencies from a set of ratios of failures and the total component failure rate. The parameters of the model are

Q_T ≡ total failure probability of each component (includes independent and common-cause events)

$\alpha^{(m)}_k$ ≡ fraction of the total probability of failure events that occur in the system involving the failure of k components in a system of m components due to a common-cause.

The CCF basic event equation for any *k* out of *m* components failing in case of staggered testing is given by (Wierman et al., 2001) equation 2.1:

$$Q_{CCF} = Q_T \sum_{i=k}^{m} \begin{pmatrix} m \\ i \\ m-1 \\ i-1 \end{pmatrix} \alpha_i^{(m)} \quad = \quad Q_T \sum_{i=k}^{m} \binom{m}{i} \alpha_i^{(m)} \tag{2.1}$$

where:

$\alpha^{(m)}_i$= the ratio of i and only i CCF failures to total failures in a system of m components

m = the number of total components in the component group

k = the failure criteria for a number of component failures in the component group

Q_T = the random failure probability (total)

Q_{CCF} = the failure probability of k and greater than k components due to CCF

2.3 ESTIMATION OF ALPHA FACTOR

NUREG/CR-5485 proposed a technique for CCF analysis using 'event impact vector'. An impact vector is a numerical representation of a CCF event and is classified according to the level of impact of common cause events. In this technique, the impact vectors are modified to reflect the likelihood of the occurrence of the event in the specific system of interest. This method is also known as mapping. The mapped impact vectors are finally used to arrive at alpha factors.

For a CCCG of size m, an impact vector will have m elements and the k^{th} element is denoted by P_k. Here P_k denotes the probability of k component failing due to a common cause. For e.g., the impact vector a CCCG of size 5, is $\left[P_1^{(5)} \;\; P_2^{(5)} \;\; P_3^{(5)} \;\; P_4^{(5)} \;\; P_5^{(5)} \right]$. Appropriate mapping technique is adopted to determine the value of P_k.

2.3.1 Mapping Techniques

Mapping process is performed from three different routines depending on the relationship between the original system and the size of target system of interest.

- Mapping down is for computing impact vectors when exposed population size is larger than that of the target group size, e.g., from four component system to two component system.
- Mapping up is when the impact vector exposed population size is smaller than that of the target group size e.g., from two component systems to four component systems.
- The special case where the impact vector has been identified as a "lethal shock," the impact vector for the new system of m components comprises a 1.0 in the F_m position and rest all values are zero, for example, $\left[P_1^{(5)} \;\; P_2^{(5)} \;\; P_3^{(5)} \;\; P_4^{(5)} \;\; P_5^{(5)}\right] = \left[0 \;\; 0 \;\; 0 \;\; 0 \;\; 1\right]$. A lethal shock is one which wipes out all redundant components present within a common cause group (Mosleh et al., 1998).

This work focuses on estimation of Alpha factors for large redundant configurations with the help of mapping up technique. Hence the technique of mapping up is described in a comprehensive manner. To reasonably map up the effect of non-lethal shocks, it is required to relate the probability of failure of k or more components in terms of parameters that can be determined from measurements of number of failure events involving i=0,1,2 ….k-1 components. For each shock, there is a constant probability ρ, which is the conditional probability of each component failure given a shock. It is also known as mapping up parameter and is expressed as the probability that the non-lethal shock or cause would have failed a single component added to the system. The mapping up is performed for all the CCF events affecting the system and it is based on the subjective assessment of ρ. The assessment

of ρ is performed for each CCF event and may be different for different events depending on the application.

The frequency of events that occur within an n train system resulting in r failures due to non-lethal shocks is expressed using Binomial Failure Rate (BFR) model as $P_r^{(n)} = \mu . C_r^n \rho^r (1-\rho)^{n-r}$ where ρ is the occurrence rate of shock.

For a system of size 5, the observed values of $P_i^{(5)}$ i=1 .. 5 are generated in a BFR process with parameters μ and ρ.

$$P_1^{(5)} = 5\mu\rho\ (1-\rho)^4, \quad P_2^{(5)} = 10\mu\rho^2(1-\rho)^3, \quad P_3^{(5)} = 10\mu\rho^3(1-\rho)^2$$
$$P_4^{(5)} = 5\mu\rho^4(1-\rho), \quad P_5^{(5)} = \mu\rho^5$$

Table 2.2 shows the impact of CCF events on the redundant configuration of five train system to lower redundant configurations of up to one train system. Ideally, it is sufficient to model the impact of CCF events till the level from where the system is mapped up.

Table 2.2: Impact of CCF events

Event Type	Basic Events in Five Train System (A,B,C,D,E)	Impact on four Train System (A,B,C,D)*	Impact on three Train System (A,B,C)*	Impact on two Train System (A,B)*	Impact on one Train System (A)*
Independent	A, B, C, D, E	A, B, C, D, Nn	A, B, C, Nn, Nn	A, B, Nn, Nn, Nn	A, Nn, Nn, Nn, Nn
Common Cause Impacting Two Components	AB, AC, AD, AE, BC, BD, BE, CD, CE, DE	AB, AC, AD, A, BC, BD, B, CD, C, D	AB, AC, A, A, BC, B, B, C, C, Nn	AB, A, A, A, B, B, B, Nn, Nn, Nn	A, A, A, A, Nn, Nn, Nn, Nn, Nn, Nn
Common Cause Impacting Three Components	ABC, ABD, ABE, ACD, ACE, ADE, BCD, BCE, BDE, CDE	ABC, ABD, AB, ACD, AC, AD, BCD, BC, BD, CD	ABC, AB, AB, AC, AC, A, BC,BC, B, C	AB, AB, AB, A, A, A, B, B, B, Nn	A, A, A, A, A, A, Nn, Nn, Nn, Nn

Common Cause Impacting Four Components	ABCD, ABCE, ABDE, ACDE, BCDE	ABCD, ABC, ABD, ACD, BCD	ABC, ABC, AB, AC, BC	AB, AB, AB, A, B	A, A, A, A, Nn
Common Cause Impacting Five Components	ABCDE	ABCD	ABC	AB	A

* indicates one component is removed; Nn refers to none

To map up from a system of size 2 to system of size 5, the observed value of $P_2^{(5)}$ is modified as

$$P_2^{(5)} = \ 10\mu\rho^2(1-\rho)^3 \tag{2.2}$$

which is further simplified as follows:

$$P_2^{(5)} = \mu\rho^2(1-\rho)^3 + \ 9\mu\rho^2(1-\rho)^3 \tag{2.3}$$

$$P_2^{(5)} = (1-\rho)^3\left[\mu\rho^2\right] + \ \rho\,(1-\rho)^2\frac{9}{2}\left[2\mu\rho(1-\rho)\right] \tag{2.4}$$

$$P_2^{(5)} = (1-\rho)^3 P_2^{(2)} + \ \frac{9}{2}\rho\,(1-\rho)^2 P_1^{(2)} \tag{2.5}$$

$$P_2^{(5)} = (1-\rho)^3 P_2^{(2)} + \ 9\left[\frac{\rho}{2}\,(1-\rho)^2 P_1^{(2)}\right] \tag{2.6}$$

In order to estimate the contribution of $P_1^{(2)}$ and $P_2^{(2)}$ to $P_2^{(5)}$, the number of doubles, singles and zeros needs to be determined from Table 2.2. This contribution is derived in Table 2.3 and it can be inferred that one tenth of $P_2^{(5)}$ is observed as $P_2^{(2)}$ in a two train system. The other part is observed as $P_1^{(2)}$.

Table 2.3: CCF Contribution of components after mapping up

Number of components affected by CCF	Number of zeros when mapped to two components	Number of singles when mapped to two components	Number of doubles when mapped to two components
1	3	2	0
2	**3**	**6**	**1**
3	1	6	3
4	0	2	3
5	0	0	1

Repeating the mapping up procedure, expressions for events classified as non-lethal shocks are obtained as shown in Table 2.3.

2.3.2 Estimation of Impact Vectors

On scrutinizing the columns of Table 2.4 generated by applying the BFR model, it is obvious that the uncertainty inherent in mapping up impact vectors is reduced to the uncertainty in estimating the conditional probability, ρ of non-lethal shock to fail a single component. A higher value of ρ indicates the probability of more components failing due to the shock.

Table 2.4: Mapping up procedure

		SIZE OF THE SYSTEM MAPPED TO			
		2	3	4	5
SIZE OF SYSTEM MAPPING FROM	1	$P_1^{(2)} = 2(1-\rho)P_1^{(1)}$ $P_2^{(2)} = \rho P_1^{(1)}$	$P_1^{(3)} = 3(1-\rho)^2 P_1^{(1)}$ $P_2^{(3)} = 3\rho(1-\rho)P_1^{(1)}$ $P_3^{(3)} = \rho^2 P_1^{(1)}$	$P_1^{(4)} = 4(1-\rho)^3 P_1^{(1)}$ $P_2^{(4)} = 6\rho(1-\rho)^2 P_1^{(1)}$ $P_3^{(4)} = 4\rho^2(1-\rho)P_1^{(1)}$ $P_4^{(4)} = \rho^3 P_1^{(1)}$	$P_1^{(5)} = 5(1-\rho)^4 P_1^{(1)}$ $P_2^{(5)} = 10\rho(1-\rho)^3 P_1^{(1)}$ $P_3^{(5)} = 10\rho^2(1-\rho)^2 P_1^{(1)}$ $P_4^{(5)} = 5\rho^3(1-\rho) P_1^{(1)}$ $P_5^{(5)} = \rho^4 P_1^{(1)}$
	2		$P_1^{(3)} = \frac{3}{2}(1-\rho) P_1^{(2)}$ $P_2^{(3)} = \rho P_1^{(2)} + (1-\rho) P_2^{(2)}$ $P_3^{(3)} = \rho P_2^{(2)}$	$P_1^{(4)} = 2(1-\rho)^2 P_1^{(2)}$ $P_2^{(4)} = \frac{5}{2}\rho(1-\rho) P_1^{(2)} + (1-\rho)^2 P_2^{(2)}$ $P_3^{(4)} = \rho^2 P_1^{(2)} + 2\rho(1-\rho) P_2^{(2)}$ $P_4^{(4)} = \rho^2 P_2^{(2)}$	$P_1^{(5)} = \frac{5}{2}(1-\rho)^3 P_1^{(2)}$ $P_2^{(5)} = \frac{9}{2}\rho(1-\rho)^2 P_1^{(2)} + (1-\rho)^3 P_2^{(2)}$ $P_3^{(5)} = \frac{7}{2}\rho^2(1-\rho) P_1^{(2)} + 3\rho(1-\rho)^2 P_2^{(2)}$ $P_4^{(5)} = \rho^3 P_1^{(2)} + 3\rho^2(1-\rho) P_2^{(2)}$ $P_5^{(5)} = \rho^3 P_2^{(2)}$
	3			$P_1^{(4)} = \frac{4}{3}(1-\rho) P_1^{(3)}$ $P_2^{(4)} = \rho P_1^{(3)} + (1-\rho) P_2^{(3)}$ $P_3^{(4)} = \rho P_2^{(3)} + (1-\rho) P_3^{(3)}$ $P_4^{(4)} = \rho P_3^{(3)}$	$P_1^{(5)} = \frac{5}{3}(1-\rho)^2 P_1^{(3)} + 9\mu\rho^2(1-\rho)^3$ $P_2^{(5)} = \frac{7}{3}\rho(1-\rho) P_1^{(3)} + (1-\rho)^2 P_2^{(3)}$ $P_3^{(5)} = \rho^2 P_1^3 + 2\rho(1-\rho) P_2^{(3)} + (1-\rho)^2 P_3^{(3)}$ $P_4^{(5)} = \rho^2 P_2^3 + 2\rho(1-\rho) P_3^{(3)}$ $P_5^{(5)} = \rho^2 P_3^3$
	4				$P_1^{(5)} = \frac{5}{4}(1-\rho) P_1^{(4)}$ $P_2^{(5)} = \rho P_1^{(4)} + (1-\rho) P_2^{(4)}$

					$P_3^{(5)} = \rho\ P_2^4 + (1-\rho) P_3^{(4)}$ $P_4^{(5)} = \rho\ P_3^4 + (1-\rho) P_4^{(4)}$ $P_5^{(5)} = \rho\ P_4^4$

Four CCF events with ρ values of 0.1, 0.2, 0.3 and 0.8 and a beta value of 5% are taken for $P_1^{(2)}$ and $P_2^{(2)}$. Based upon the subjective assessment on the value of ρ and with the help of mapping techniques established earlier, impact vectors to map up a system of size 2 to system of size 5 have been calculated as shown in Table 2.5.

Table 2.5: Mapping up of impact vectors

EVENT NO	SYSTEM SIZE	IMPACT VECTOR				
		P1	**P2**	**P3**	**P4**	**P5**
	NON LETHAL SHOCK (ρ = .1)					
1.	Original Two Train System	0.95	0.05	-	-	-
	Identical Three Train System	1.28	0.14	0.01	-	-
	Identical Four Train System	1.54	0.25	0.02	0.00	-
	Identical Five Train System	1.73	0.38	0.04	0.00	0.00
	NON LETHAL SHOCK (ρ = .2)					
2.	Original Two Train System	0.95	0.05	-	-	-
	Identical Three Train System	1.14	0.23	0.01	-	-
	Identical Four Train System	1.22	0.41	0.05	0.00	-
	Identical Five Train System	1.22	0.57	0.13	0.01	0.00
	NON LETHAL SHOCK (ρ = .3)					
3.	Original Two Train System	0.95	0.05	-	-	-
	Identical Three Train System	1.00	0.32	0.02	-	-
	Identical Four Train System	0.93	0.52	0.11	0.01	-
	Identical Five Train System	0.81	0.65	0.23	0.04	0.00
	NON LETHAL SHOCK (ρ = .8)					
4.	Original Two Train System	0.95	0.05	-	-	-
	Identical Three Train System	0.29	0.77	0.04	-	-
	Identical Four Train System	0.68	0.38	0.62	0.03	-
	Identical Five Train System	0.02	0.14	0.43	0.51	0.03

2.3.3 Estimation of Alpha factors from impact vectors

The number of events in each impact category (n_k) is calculated by adding the corresponding elements of the impact vectors.

$$n_k = \sum_{j=1}^{n} P_k(j) \tag{2.7}$$

where: $P_k(j)$ = the k^{th} element of the impact vector for event j, and n is the number of CCF events.

Finally, the alpha factors are estimated using the following expression (Wierman et al., 2001):

$$\alpha_k^{(m)} = \frac{n_k}{\sum_{k=1}^{m} n_k} \tag{2.8}$$

A plot of Alpha factor for the example is shown in Figure 2.1.

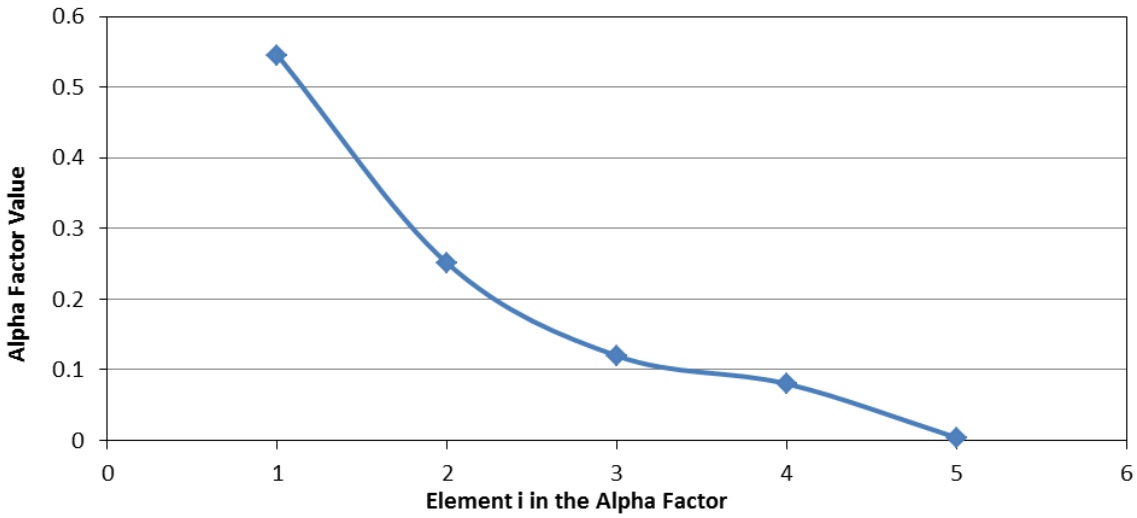

Figure 2.1: Alpha Factors for 5 component system

The estimation of alpha factors in CCF analysis is further demonstrated with three varied real applications for Indian nuclear power plants in the following section. A MATLAB code is developed to estimate the alpha factors and then compute CCF contribution to total

failure probability. Following case studies are carried out with the help of same code as it is capable of handling various redundant configurations.

2.4 APPLICATIONS TO NUCLEAR POWER PLANT

2.4.1 Safety Grade Decay Heat Removal System of Prototype Fast Breeder Reactor

The 500 MW Indian pool type Prototype Fast Breeder Reactor (PFBR), is provided with two independent and diverse Decay Heat Removal (DHR) systems viz., Operating Grade Decay Heat Removal System (OGDHRS) and Safety Grade Decay Heat Removal System (SGDHRS). OGDHRS utilizes the secondary sodium loops and Steam–Water System with special decay heat removal condensers for DHR function (Arul et al., 2006). A passive SGDHR system using four completely independent thermo-siphon loops in natural convection mode is provided to ensure adequate core cooling for all Design Basis Events. Since SGDHR is a passive system, the functional failure probability depends on the time up to which two loops are available (Mathews. et al., 2009). The event simulated in this study demand operation of two SGDHR loops for initial 24 hr and subsequent availability of one loop till 720 hr after the shutdown for successful decay heat removal of the reactor.

In the present study the effect of three non-lethal CCF events affecting the SGDHR system have been studied for various values of ρ. The objective of the case study is to first estimate the alpha factors and then arrive at the contribution of the CCF events to total failure probability of the system. The case when an additional CCF event is a lethal shock has also been analysed to study the effect of lethal shock. Finally, a broad comparison between the alpha factor method and Beta factor method for their assessment of CCF contribution to total failure probability of the system due to various CCF events is made. Since the mapping up is performed from two component data, a term ‘mapping up beta’ (denoted as MBeta) is used

which is expressed as the fraction of total failure probability of the two component system attributable to dependent failures (Mosleh, 1991).

Mapping up $Beta=Q_m/Q_t$ (2.9)

where Q_m = Dependent failure probability and Q_t = Total failure probability for each component

The value of MBeta has been taken to represent all extreme values of common cause failures for a two component system. A set of conservative values for ρ has also been assumed for the study. The study has also been carried out with consideration of a lethal shock. Another term 'Common Beta' is also used to denote CCF for the complete system. Beta expressed in percentage is the CCF contribution to total failure probability in these cases.

The case is studied under two parts. Part one for the first 24 hour of mission time when the success criterion is two out of four and part two for rest of the mission time when success criterion is one out of four. The inputs for the alpha factor model are success criteria, Mbeta value and set of values of ρ.

Part 1: When two out of four loops are required

After the shutdown of the reactor for first 24hr two loops of SGDHR are required. The contribution of CCF events to total failure probability for various set of values of ρ is presented in Table 2.6.The results of the case with extra CCF event as lethal shock is presented in Table 2.7 and the graphs plotted for the results are shown in Figure 2.2 and Figure 2.3.

Table 2.6: CCF Contribution to total system failure probability for different CCF events

Values of ρ	CCF Contribution to total system failure probability (%)			
	MBeta=10%	MBeta=5%	MBeta=1%	MBeta=.1%
ρ =.1,.2,.3	6.151154	4.85	3.854994	3.634923
ρ =.2,.3,.4	11.69249	9.84	8.414538	8.098896
ρ =.3,.4,.5	19.43477	17.17	15.41352	15.02437

ρ =.4,.5,.6	29.73186	27.25	25.30687	24.8764

Table 2.7: CCF Contribution to total system failure probability for different CCF events along with lethal shock

Values of ρ	CCF Contribution to total system failure probability (%)			
	MBeta=10%	MBeta=5%	MBeta=1%	MBeta=.1%
ρ =.1,.2,.3,1	21.92	20.55	19.49	19.26
ρ =.2,.3,.4,1	27.42	25.65	24.27	23.96
ρ =.3,.4,.5,1	34.62	32.57	30.98	30.62
ρ =.4,.5,.6,1	43.73	41.57	39.88	39.51

Alpha factors and estimated contribution of CCF events to total failure probability for ρ value of 0.4, 0.5, 0.6 and by various values of mapping up beta are presented in Table 2.8. The results for the case when lethal shock is also considered are presented in Table 2.9. Figure 2.4 shows the alpha factors for different MBeta values for lethal and non-lethal cases.

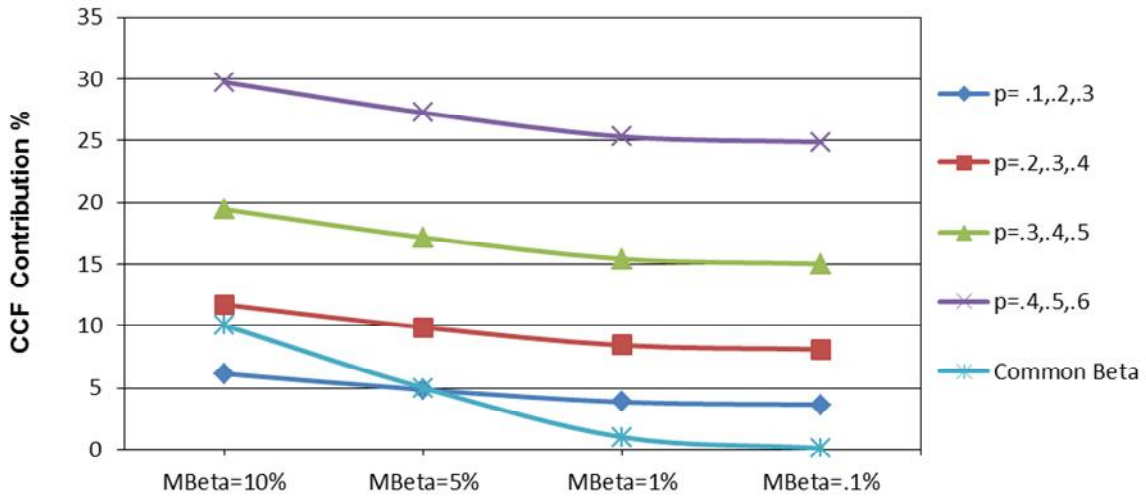

Figure 2.2: CCF contribution in 2 out of 4 system without lethal shock

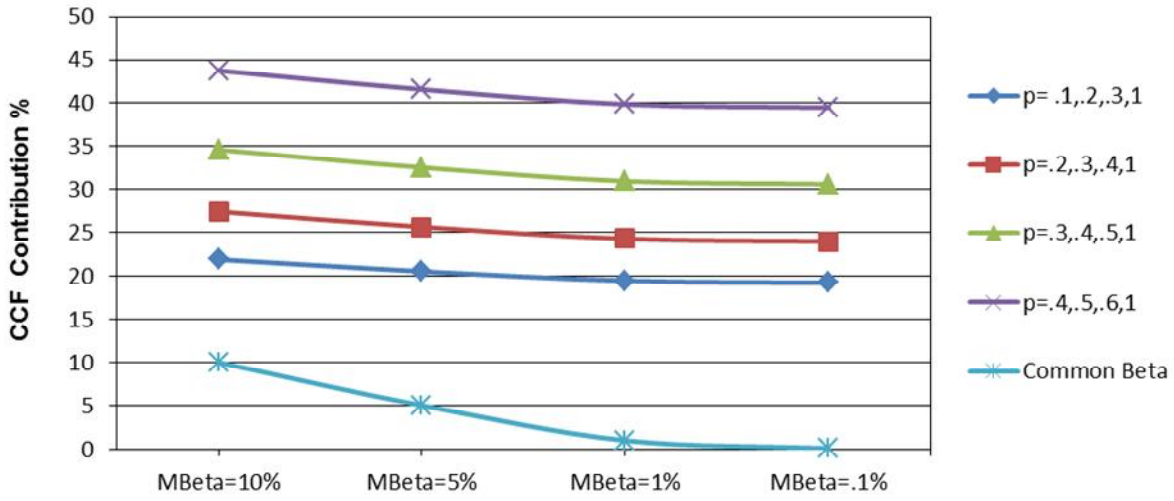

Figure 2.3: CCF contribution in 2 out of 4 system with lethal shock

Table 2.8: Estimation of Alpha factors for ρ = 0.4, 0.5, 0.6

Alpha Factors	MBeta=10%	MBeta=5%	MBeta=1%	MBeta=.1%
α1	0.344648	0.358732	0.369721	0.37216
α2	0.427577	0.434561	0.440011	0.44122
α3	0.208629	0.197266	0.188401	0.186433
α4	0.019147	0.00944	0.001867	0.000186
Q(CCF)/Q(TOTAL)	0.297319	0.272462	0.253069	0.248764
Q(CCF)/Q(TOTAL) %	29.73186	27.24616	25.30687	24.8764

Table 2.9: Estimation of Alpha factors for ρ = 0.4, 0.5, 0.6 and 1

Alpha Factors	MBeta=10%	MBeta=5%	MBeta=1%	MBeta=.1%
α1	0.2760131	0.28809137	0.29756	0.299669
α2	0.3424276	0.34898833	0.35413	0.355277
α3	0.1670815	0.15842072	0.15163	0.150119
α4	0.2144777	0.20449958	0.19668	0.194935
Q(CCF)/Q(TOTAL)	0.4372531	0.4157272	0.39885	0.395093
Q(CCF)/Q(TOTAL) %	43.725314	41.5727203	39.885	39.50935

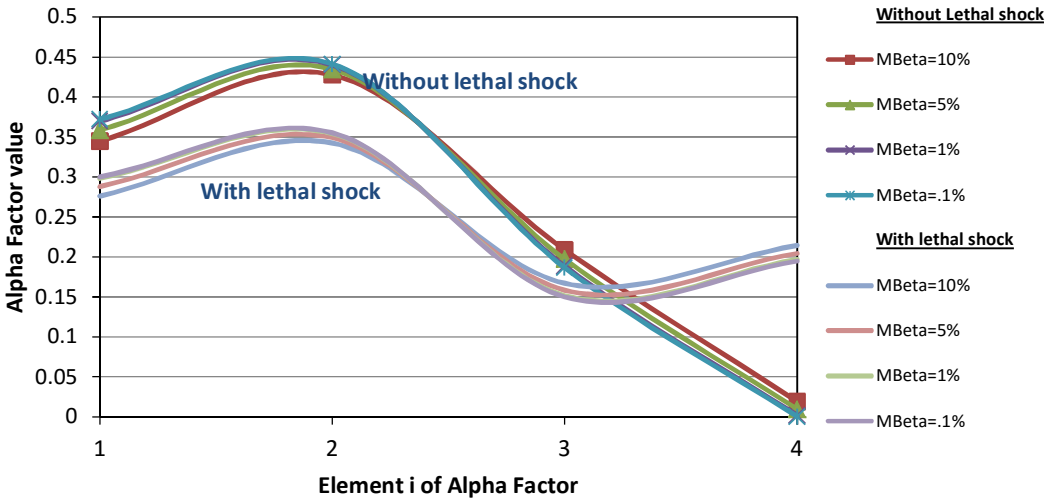

Figure 2.4: Comparison of Alpha Factors for lethal and non-lethal shock

Part 2: When one loop is required out of four

This case is applicable after the first 24hr of shutdown of the reactor till the end of mission time (720 hr). The contribution of CCF events to total failure probability for various set of values of ρ is shown in Figure 2.5. The case with extra CCF event as lethal shock is given in Figure 2.6.

Following inferences are made from the results obtained:

1. Contribution of CCF events to total failure probability is found to be very less sensitive to the value of mapping up beta. (Figures 2.2, 2.3, 2.5 & 2.6)
2. As the success criterion becomes more stringent, the CCF contribution increases appreciably for the same values of ρ.(Figure 2.5 vs Figure 2.2 & Figure 2.6 vs Figure 2.3)
3. Sensitivity of CCF contribution to change in value of ρ increases significantly as the success criteria requirement gets more stringent.(Figure 2.5 vs Figure 2.2 & Figure 2.6 vs Figure 2.3)

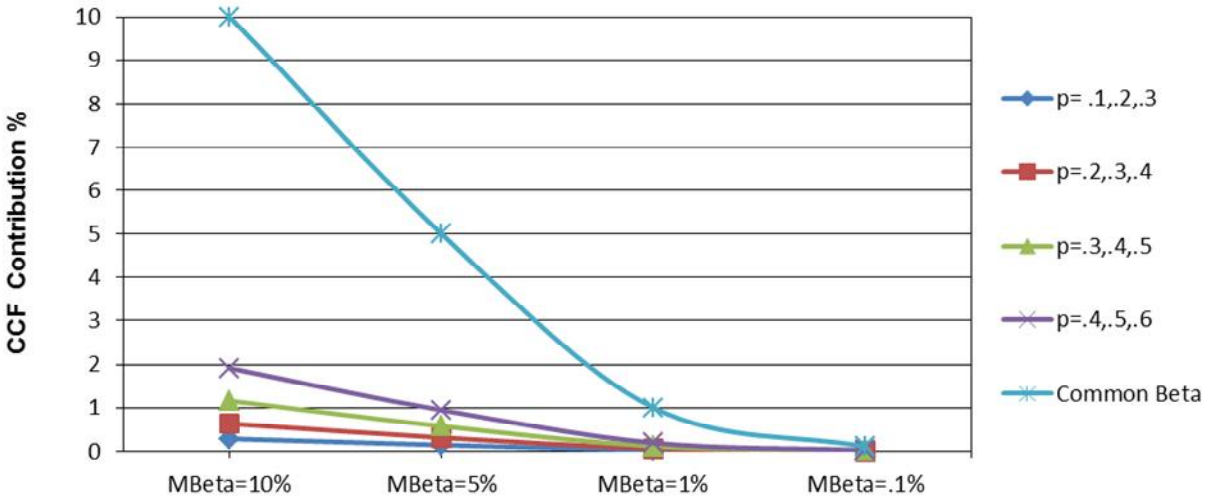

Figure 2.5: CCF contribution in 1 out of 4 system without lethal shock

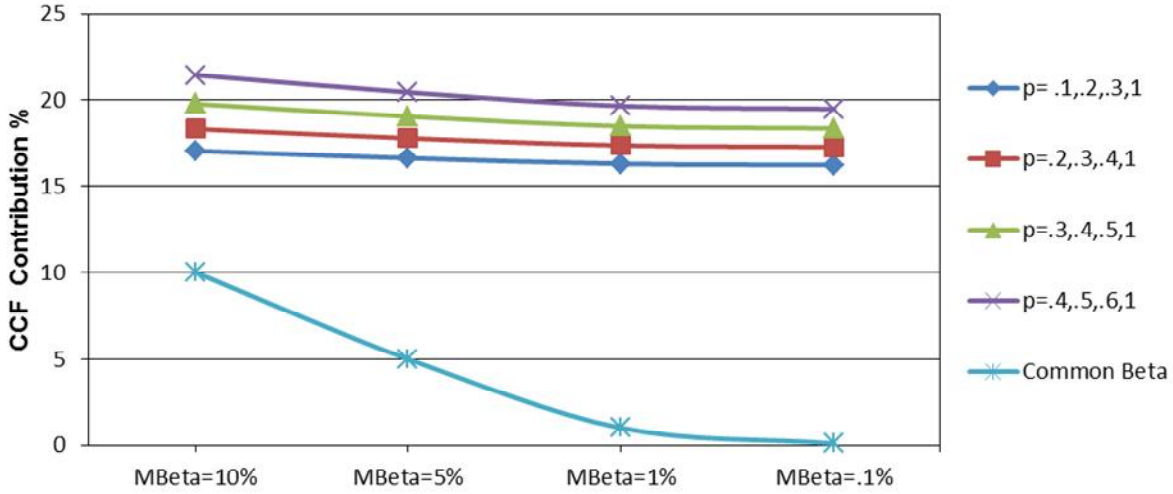

Figure 2.6: CCF contribution in 1 out of 4 system with lethal shock

4. As the hazard from shocks increase (Figures 2.2, 2.3, 2.5, 2.6), Beta factor method provides unrealistic assessment of CCF contribution to the failure of system.
5. In presence of lethal shock, CCF contribution to total failure probability increases appreciably and beta factor model fails to address this case subjectively yielding highly repressed estimates. (Figure 2.3 & Figure 2.6)
6. The values of Alpha factors are found to be less sensitive to change in the value of mapping up beta in both lethal and non-lethal cases. (Figure 2.4)

2.4.2 Shutdown System (SDS) of PFBR

PFBR has two shutdown systems; SDS1 and SDS2. Each shutdown system consists of Reactor Protection system, Actuation System and safety support systems. RPS consists of instrumentation, i.e., sensors to monitor plant parameters, analog signal processing circuits, SCRAM logic, SCRAM switches (power gates) and power supply. Actuation System consists of Absorber Rods (AR), electromagnets and drive mechanisms to drop or drive the absorber rods into the core. Absorber rods (AR) of system 1 are called Control and Safety Rods (CSR) and the absorber rods of system 2 are called diverse safety rods (DSR). There are 9 CSR and 3 DSR (Kumar et al., 2005). Here, successful insertion of nine out of twelve rods is considered sufficient for the safe shutdown of the reactor.

Three CCF events affecting the shutdown system are considered to estimate the alpha factors and finally arrive at the CCF contribution to the total failure probability of the system. Results obtained for various set of values of ρ of the CCF events and by varying MBeta are presented in Figure 2.7. Alpha factors obtained for ρ value of 0.2, 0.25, 0.3 with mapping up beta as 10% is shown in Figure 2.8.

The key findings from the results of the case study are:

1. Here the system is in high redundant configuration with a requirement to meet a stringent success criterion of 9 out of 12. Therefore the estimated CCF contribution to the failure of the system is high even for the CCF events having low value of conditional probability of failure. It is confirmed that CCF contribution estimated from beta factor model is extremely repressed making it highly unsuitable to be used for such configurations (Figure 2.7).
2. Sensitivity of the CCF contribution to change in values of conditional probability of failure for various CCF events (set of ρ) is observed to be high (Figure 2.7).

3. The sensitivity of the CCF contribution to change in value of mapping up beta is low which is clearly observed in Figure 2.7.
4. It is observed that for system in high redundant configuration, the values of Alpha factors become even less sensitive to change in the value of mapping up beta as compared to low redundant configuration (Figure 2.8 vs. Figure 2.4).

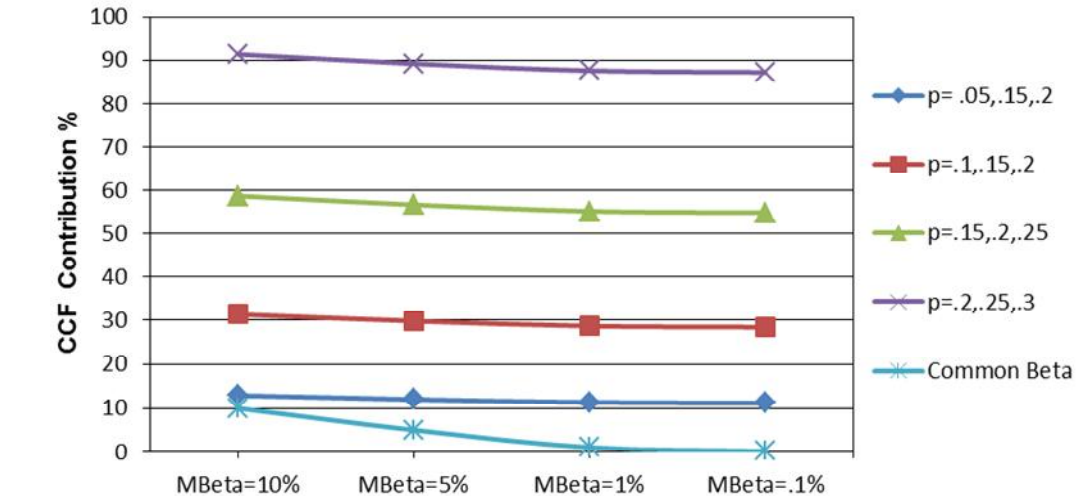

Figure 2.7: CCF contribution in PFBR Shutdown System

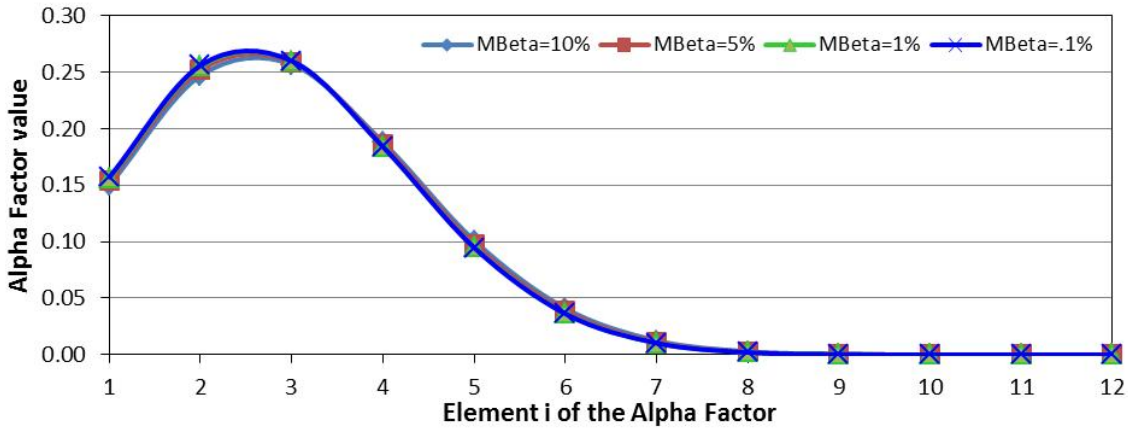

Figure 2.8: Alpha Factors for ρ = 0.2, 0.25, 0.3 and by using different mapping up beta

2.4.3 Primary Shutdown System of Tarapur Atomic Power Station (TAPS) units 3 & 4

Twin units at TAPS (Units 3 and 4) are of 540 MWe Pressurised Heavy Water Reactor (Bajaj and Gore, 2005). The Primary Shutdown System (PSS) for each of the unit has twenty eight

shut off rods. Successful insertion of twenty six of its twenty eight rods will guarantee a safe shutdown of the reactor with sufficient shutdown margins (Lasitha et al., 2006).

The present study estimates the CCF risk imposed by three CCF events for shutdown of the reactor for various values of conditional probability of failure. The contribution of CCF events to total failure probability for various set of values of ρ is presented in Figure 2.9 and a plot of alpha factors for CCF events having ρ value of .02,.03,.04 by using 10% mapping up beta is used is shown in Figure 2.10.

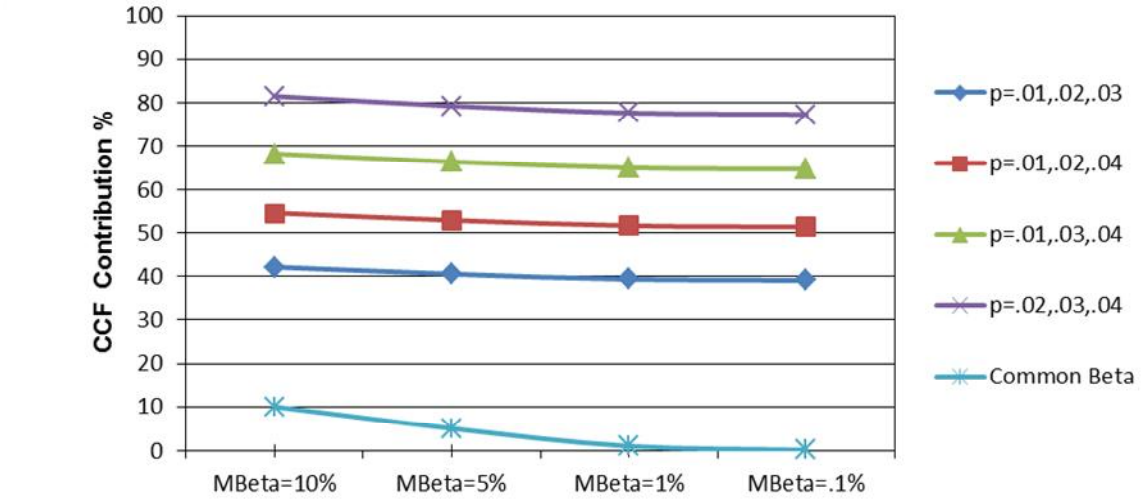

Figure 2.9: CCF contribution in Primary Shutdown System

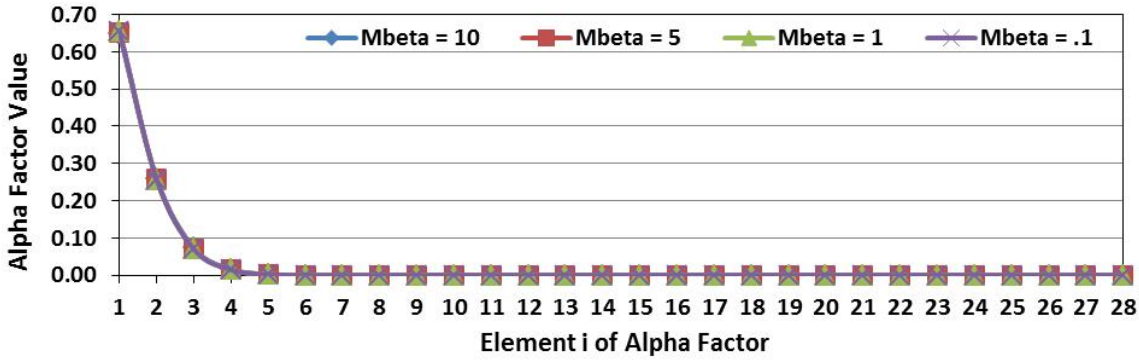

Figure 2.10: Alpha Factors for ρ value of 0.02, 0.03, 0.04 and by using different mapping up beta

The insights brought out from the results of the case study are:

1. In this case study the success criterion is even more stringent with 26 out of 28 shutoff rods to function for success, hence the observed CCF contribution to total failure

probability is very high even for CCF events having very low conditional probability of failure (Figure 2.9).

2. For the same reason, the observed sensitivity of the CCF contribution to change in values of conditional probability of failure for various CCF events is very high (Figure 2.9).
3. In this case study also it is apparent from Figure 2.9 that sensitivity of the CCF contribution to change in value of mapping up beta is low.
4. Here the system comprises of twenty eight components, hence the values of Alpha factors are almost coinciding for various values of mapping up beta (Figure 2.10).

2.5 CONCLUSIONS

The study carried out clearly indicates that alpha factor model can be used to realistically estimate the contribution of CCF events to the total system failure probability. The model assesses the contribution of each of the CCF event based upon subjective assessment of a constant ρ which is conditional probability of each component failure given a shock. The values of Alpha factors are found to be less sensitive to change in the value of mapping up beta and this sensitivity further reduces with more number of components added to the system. Contribution of CCF events to total failure probability is also found to be less sensitive to the value of mapping up beta but it is highly sensitive to the change in success criterion for the system.

The use of alpha factors is found to be highly suitable, especially for the cases exhibiting large redundant configuration and with a requirement to meet a stringent success criteria. It is also demonstrated that the use of beta factor model in these cases yields highly repressed estimates of CCF contribution especially when the lethal behaviour of common shocks is high, thereby underestimating the risks imposed by common cause events.

CHAPTER-3

MARKOV ANALYSIS FOR TIME DEPENDENT SUCCESS CRITERIA OF PASSIVE DECAY HEAT REMOVAL SYSTEM

3.0 INTRODUCTION

In real world applications such as nuclear power plants, safety systems are required to accomplish the specified tasks with varying mission times depending on the requirement and may be subject to different operating and environmental conditions. Hence, the system configuration and the success criteria may change with time. Generally, such systems are generally termed as phased mission systems (Alam and Ubaid, 1986; Xing et al., 2000). A realistic reliability analysis of such systems must take into account the above described dynamics in system configuration and success criteria. The two commonly used methods in risk analysis for computing unavailability of a system are fault tree method and Markov model method (Andrews and Clifton, 2000; Xing et al., 1996). The classical fault tree method is a static tool and is not suitable to model the time requirements in safety systems whereas Markov modelling is a traditional modelling technique used to assess the time-dependent behaviour of dynamic systems. Hence Markov modelling technique is adopted in the current work. Moreover, a review of different techniques suggests, Markov analysis covers most aspects of quantitative safety evaluation of systems (Zhang et al, 2003; Rouvroye and Brombacher, 1999). In the present study, Markov model technique has been applied on SGDHR system of PFBR to model time dependent success criteria and estimate the unavailability of the system under two monitoring schemes: continuous and periodic monitoring. Generally, in redundant safety systems, common cause failure (CCF) of components significantly contributes to the unavailability of the system and hence contribution from CCF is evaluated (Zhihua and Bechta, 2004). Sensitivity analysis of important parameters like time across which success criteria changes, test interval and repair

time is also carried out. The analysis carried out estimates the upper bound and lower bound for the mean unavailability of SGDHR system over the mission time (720 hrs). In the Markov model of the SGDHRS system, the lower bound for the mean unavailability of the system is evaluated when repair process is considered from the failed state and the upper bound for the mean unavailability of the system is computed when the repair process is not considered from the failed state. The value of upper bound can be considered for conservative assessment. The remainder of the chapter is organized as follows. Section 1 describes the system under study. Section 2 presents the Markov model of SGDHR, the success criteria, different scenarios under continuously and periodic monitoring schemes. Section 3 discusses the results and finally section 4 concludes the chapter.

3.1 SYSTEM DESCRIPTION

Prototype Fast Breeder Reactor is a 500 MWe, sodium cooled, mixed oxide fuelled, pool type fast reactor being constructed at Kalpakkam, India. PFBR has two independent & diverse Decay Heat Removal (DHR) systems viz., Operating Grade Decay Heat Removal System (OGDHRS) and Safety Grade Decay Heat Removal System (SGDHRS). OGDHRS utilizes the secondary sodium loops and Steam–Water System with special decay heat removal condensers for DHR function and SGDHRS is a passive decay heat removal system with four independent loops. The SGDHR system consists of 4 identical loops of each 8 MW_{th} heat removal capacity (Arul et al, 2006). The subsystems required for SGDHR are: primary sodium circuit system, intermediate sodium circuit and air circuit. A schematic of SGDHR is shown in Figure 3.1.

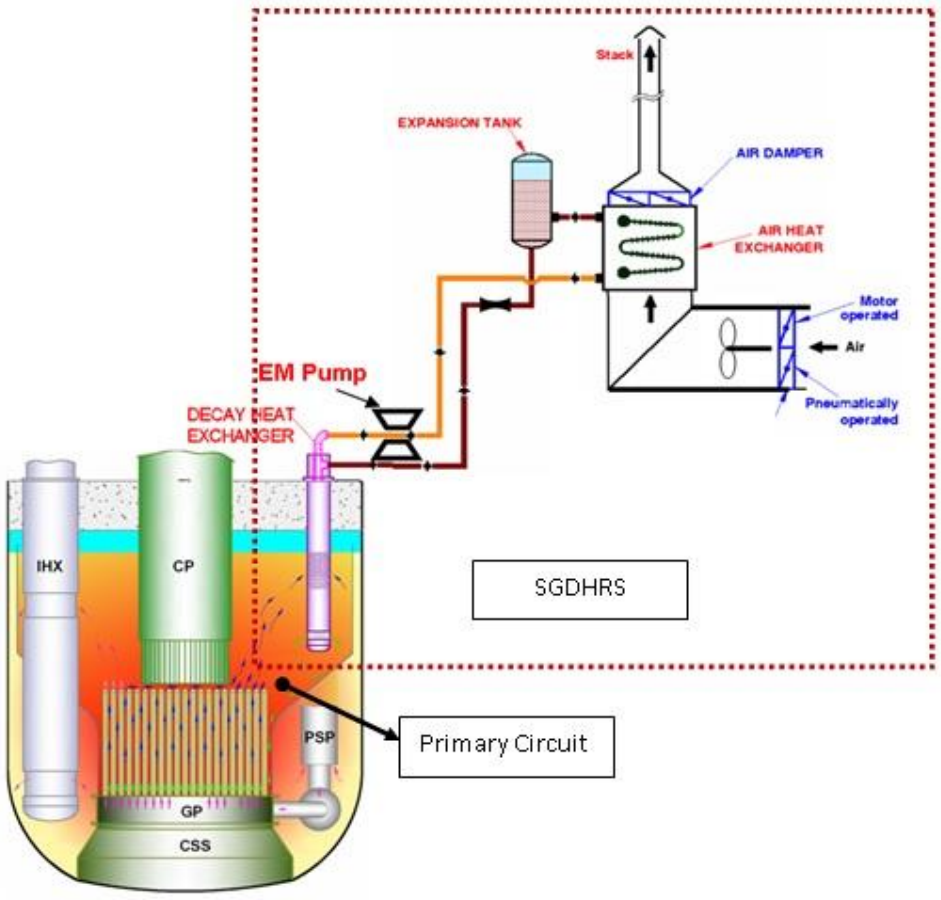

Figure 3.1: Schematic of Safety Grade Decay Heat Removal System

The sodium to sodium heat exchanger (DHX) transfers heat from radioactive primary sodium to non-radioactive intermediate sodium. The sodium to air heat exchanger (AHX) dissipates heat from intermediate sodium to atmospheric air. The intermediate sodium flow by natural convection is obtained by placing the thermal centre of AHX ~ 41 m above the thermal centre of DHX. The driving force for the flow of air over the finned tubes of AHX is obtained by providing a stack of height 30 m (Athmalingam and Vijayakumaran, 2000).

AHX casing is provided with 2 dampers in the inlet and 2 in the outlet to enhance the reliability of circuit activation. The dampers located downstream (outlet) are used as open/close device and has no control function. The dampers located upstream (inlet) are used for control of air flow. At both the inlet and outlet of AHX, one damper is motor operated

with dedicated class 2 power supply and the other damper is pneumatically operated with air bottles (Sakthival et al., 2012).

3.2 MARKOV MODELLING OF SGDHR

3.2.1 Success Criteria

For PBFR, it has been estimated through deterministic analysis that for all postulated initiating events, the DHR requirements can be met adequately by successful operation of 2 SGDHR loops for a duration of 24 hr and one loop thereafter for the rest of the mission time (i.e., up to 720 hr) for maintaining the cold shutdown state of the reactor (Parthasarathy et al., 2003; Kumar et al., 2011). To account for the uncertainties, further analysis has been carried out, by considering the requirement of two loops for initial period of 12 hr and 36 hr.

3.2.2 Different cases analysed on SGDHR system

Four different scenarios are studied in detail:

- Continuously monitored: With & without CCF
- Periodically monitored: With & without CCF

3.2.2.1 Estimation of failure rates without CCF

Fault tree analysis of SGDHR loop (Arul et al., 2006) is used to obtain the value of loop failure rate, λ_{loop}. The governing equations for the computation of λ_{loop} are (Isograph Software manual version 11.2; RiskSpectrum Theory Manual, Version 3.0.0):

$$\omega(t) = \lambda(1 - Q(t)) \quad \text{(For constant failure and repair model)} \tag{3.1}$$

$$\omega(t) = 0 \quad \text{(For constant failure frequency model)} \tag{3.2}$$

where $Q(t)$ denotes the component unavailability at time t, $\omega(t)$ is the failure frequency and λ is the failure rate of the component.

Cut set failure frequency ω_{cut} is evaluated using the following equation.

$$\omega_{cut} = \sum_{j=1}^{n} \omega_j \prod_{i=1,i\neq j}^{n} Q_i \tag{3.3}$$

where Q_i is the unavailability of the i^{th} event in the cut set and ω_j is the failure frequency of the j^{th} event in the cut set

Loop failure frequency ω_{loop} is determined by the following expression

$$\omega_{loop} = \sum_{i=1}^{n} \omega_{cuti} \prod_{j=1,i\neq j}^{n} \left(1 - Q_{cutj}\right) \tag{3.4}$$

where ω_{cuti} is the failure frequency of cutset i and Q_{cutj} is the unavailability of cutset j

Single loop conditional failure intensity λ_{loop} is obtained by following expression

$$\lambda_{loop} = \frac{\omega_{loop}}{1 - Q_{loop}} \tag{3.5}$$

where Q_{loop} is the loop unavailability and is estimated from the fault tree of SGDHR loop.

And Mean time to repair ($MTTR_{loop}$) of the loop is obtained by

$$MTTR_{loop} = \frac{Q_{loop}(\infty)}{\omega_{loop}(\infty)} \tag{3.6}$$

3.2.2.2 Estimation of failure rates with CCF

The ratio of the probability of failures involving any k components over the total probability of all failure events in a group of m components is given by [IAEA-TECDOC-648, 1992]:

$$\alpha_k^{(m)} = \frac{\binom{m}{k} Q_k^{(m)}}{\sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)}} \tag{3.7}$$

Basic event probabilities are obtained as a function of Q_t and the alpha factors as:

$$Q_k^{(m)} = \frac{m\alpha_k^{(m)}}{\binom{m}{k}\alpha_t} Q_t \tag{3.8}$$

Thus, failure rate of specific number of loops is derived from the Alpha factor and time to failure for specific number of loops in a system is assumed to follow exponential distribution.

Therefore,

$$Q_1^{(4)} = \frac{\alpha_1^{(4)}}{\alpha_t} Q_t \tag{3.9}$$

Since the value of specific loop failure rate is expected to be small, probability of failure of specific k out of m loop, $Q_k^{(m)} = (1\text{-}e^{-xt}) \cong xt$, where x is the failure rate of k specific loops.

If failure rate of 1, 2, 3 and 4 specific components in a system of 4 redundant trains is represented as a, b, c and d respectively, then

$$Q_1^{(4)}(t) \cong at \tag{3.10}$$

$$\begin{aligned} a &= \left(\frac{1}{t}\right)\left(\frac{\alpha_1^{(4)}}{\alpha_t}\right) Q_t \\ b &= \frac{2}{3}\left(\frac{1}{t}\right)\left(\frac{\alpha_2^{(4)}}{\alpha_t}\right) Q_t \\ c &= \left(\frac{1}{t}\right)\left(\frac{\alpha_3^{(4)}}{\alpha_t}\right) Q_t \\ d &= \left(\frac{4}{t}\right)\left(\frac{\alpha_4^{(4)}}{\alpha_t}\right) Q_t \end{aligned} \tag{3.11}$$

where:

t = Mission time of the system.

Q_t= Loop unavailability at the end of the mission time.

Q_t at 720 hr is 0.0016 as computed by FT analysis for SGDHR loop.

α_t denotes sum of Alpha Factors

$$\alpha_t = \alpha_1^{(4)} + 2\alpha_2^{(4)} + 3\alpha_3^{(4)} + 4\alpha_4^{(4)} \quad (3.12)$$

Using the impact vector method (Wierman et al., 2001; Wierman et al., 2007; Mosleh et al., 1998) as demonstrated in chapter 2, alpha factors are obtained as:

$$\alpha_1^{(4)} = 0.8059; \quad \alpha_2^{(4)} = 0.1791; \quad \alpha_3^{(4)} = 0.0149; \quad \alpha_4^{(4)} = 0.0001$$

Hence, derived specific failure rates are:

a =1.48E-06; b =2.19E-07; c =2.73E-08 and d =9.98E-10

3.2.3 Introduction to Markov model

A Markov model depicts the lifetime behaviour of the system in a state-time space. The Markov modelling technique starts by representing the system in number of distinct system states which corresponds to certain combination of component states. Transitions between these system states are governed/attributed by the events like: component failure or repair, common cause failures of components (for example due to loss of offsite power), environmental factors, etc. These transitions bring the time factor into the model. At any instant of time, the system is allowed to change its state in accordance with the competing processes which are appropriate for that plant state. This way, the Markov model is able to model the system dynamically (Ebeling, 2011; Fleming, 2004; Fullwood, 2000). The state probabilities of the system P(t) in Markov analysis are obtained by the solution of a coupled set of first order, constant coefficient differential equations (Pages and Gondran,1986) :

$$dP/dt = M.P(t) \quad (3.13)$$

where M is the matrix of coefficients whose off-diagonal elements are the transition rate and whose diagonal elements are such that each of the matrix columns sum to zero.

It is to be noted that the following assumptions are made in the markov modelling of the SGDHR system:

- Only one repair crew is assumed while modelling.
- The failure and repair rates are constant.
- The repair restores the system as new one.
- In continuously monitored, all the failures are detected immediately and repair starts without any delay.
- In periodic monitoring all the failures are detected during inspection and repair starts without any delay.

3.2.4 Markov model for continuously monitored cases

3.2.4.1 Without CCF

State transition diagram from time t=0 to t1 (t1 is the time across which success criteria changes) is shown in Figure 3.2 and from time t = t1 to 720 hr (Mission time) is shown in Figure 3.3. The equations as obtained from the state transition diagram are presented in Table 3.1. Fail states are indicated by a circle (^{o}) above the state in the diagram. Since states have been combined the failure rate when four loops are working is 4λ, when three loops are working is 3λ and when two loops are working is 2λ. It may be seen from Figure 3.2 and Figure 3.3 that with change in success criteria repair from state 4 to state 3 is modelled for time t=t1 to 720 hrs and number of failed states reduces from two to one. $P_i(t)$ = Probability of the system to be in state i at time t.

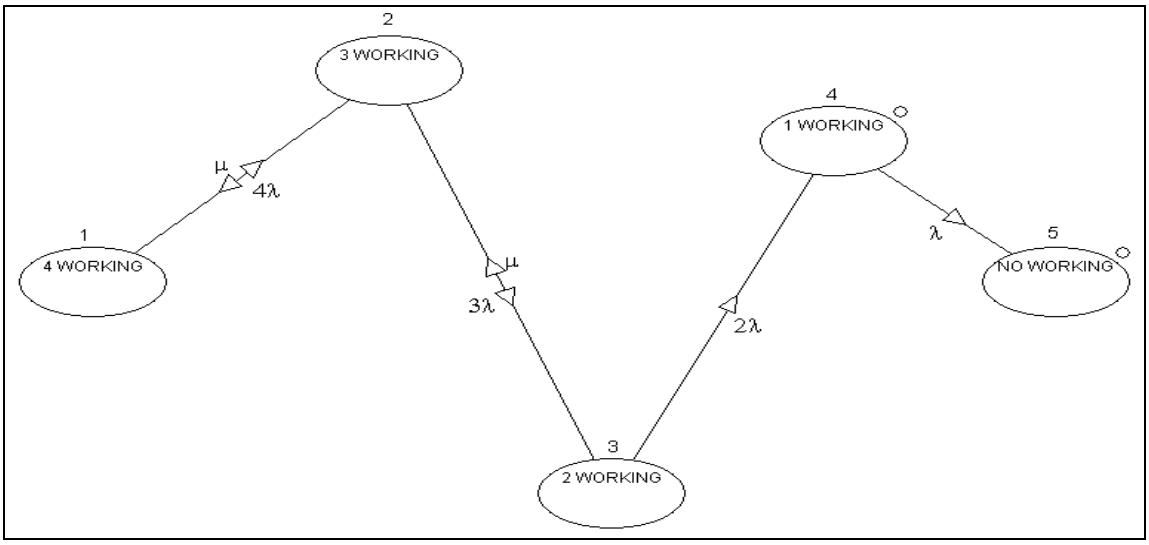

Figure 3.2: State transition diagram from time t=0 to t=t1 (Continuously Monitored & Without CCF)

The state 1 in the Figures 3.2-3.5 represents the operation of four SGDHR loops whereas state 2 and state 3 indicates the operation of three and two SGDHR loops respectively. The state 4 represents the operation of a single loop of SGDHR system and finally state 5 represents the failure of all the four loops. It is to be noted that in the first interval from t=0 to t=t1 the repair process has been modelled from state 2 and state 3 only, and in the second interval the credit of repair has been taken from state 2, state 3 and state 4. Hence in both the intervals for all mentioned figures, the repair from the failed state is not considered.

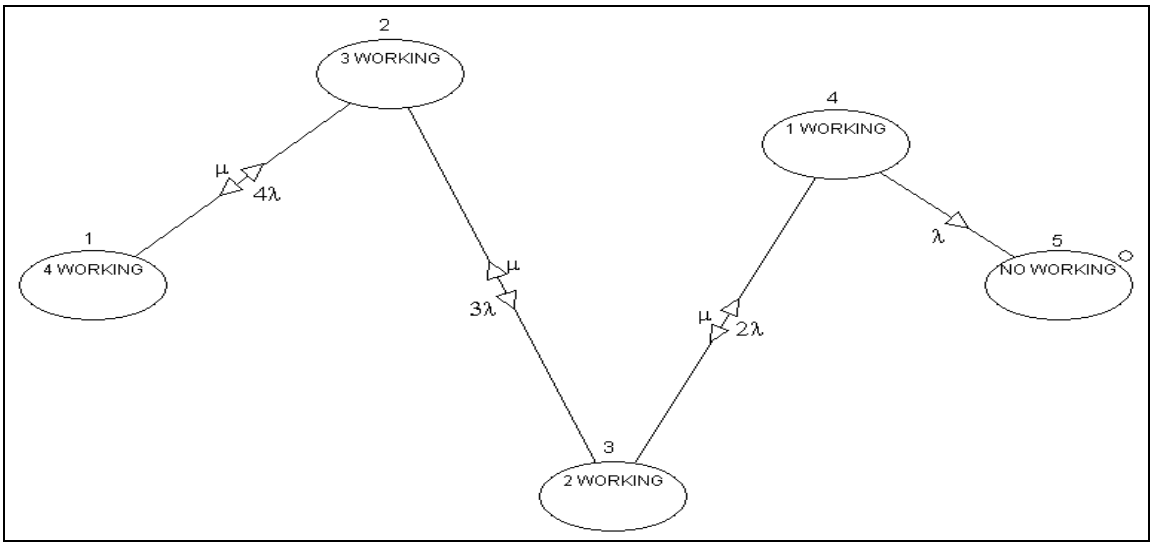

Figure 3.3: State transition diagram from time t=t1 to t=M.T (Continuously Monitored & Without CCF)

Table 3.1: Equations of State transition diagram (Continuously Monitored & Without CCF)

Equations of State transition diagram	
For time t=0 to t1 hr	**For time t=t1 to 720 hr**
$\frac{dP_1(t)}{dt} = -4\lambda P_1(t) + \mu P_2(t)$	$\frac{dP_1(t)}{dt} = -4\lambda P_1(t) + \mu P_2(t)$
$\frac{dP_2(t)}{dt} = 4\lambda P_1(t) + \mu P_3(t) - (\mu+3\lambda)P_2(t)$	$\frac{dP_2(t)}{dt} = 4\lambda P_1(t) + \mu P_3(t) - (\mu+3\lambda)P_2(t)$
$\frac{dP_3(t)}{dt} = 3\lambda P_2(t) - (\mu+2\lambda)P_3(t)$	$\frac{dP_3(t)}{dt} = 3\lambda P_2(t) + \mu P_4(t) - (\mu+2\lambda)P_3(t)$
$\frac{dP_4(t)}{dt} = 2\lambda P_3(t) - \lambda P_4(t)$	$\frac{dP_4(t)}{dt} = 2\lambda P_3(t) - (\mu+\lambda)P_4(t)$
$\frac{dP_5(t)}{dt} = \lambda P_4(t)$	$\frac{dP_5(t)}{dt} = \lambda P_4(t)$

3.2.4.2 With CCF

Specific failure rate of the loops of SGDHR, i.e., a, b, c, d are denoted by $\lambda_{1/4}$, $\lambda_{2/4}$, $\lambda_{3/4}$, $\lambda_{4/4}$ in the Figure 3.4, 3.5 and Table 3.2 representing 'with CCF' cases.

a = $\lambda_{1/4}$ = failure rate of a specific single loop out of four loops

b = $\lambda_{2/4}$ = failure rate of a specific two loops out of four loops

c = $\lambda_{3/4}$ = failure rate of a specific three loops out of four loops

d = $\lambda_{4/4}$ = failure rate of all the four loops

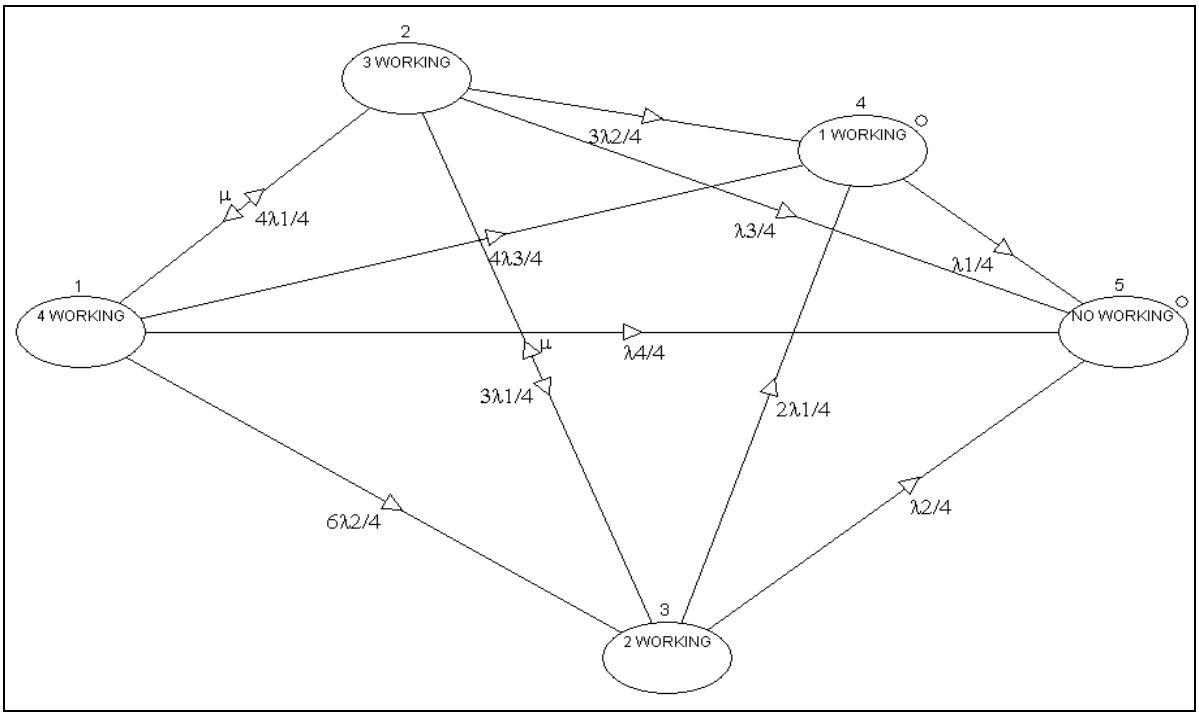

Figure 3.4: State transition diagram from time t=0 to t=t1
(Continuously Monitored & With CCF)

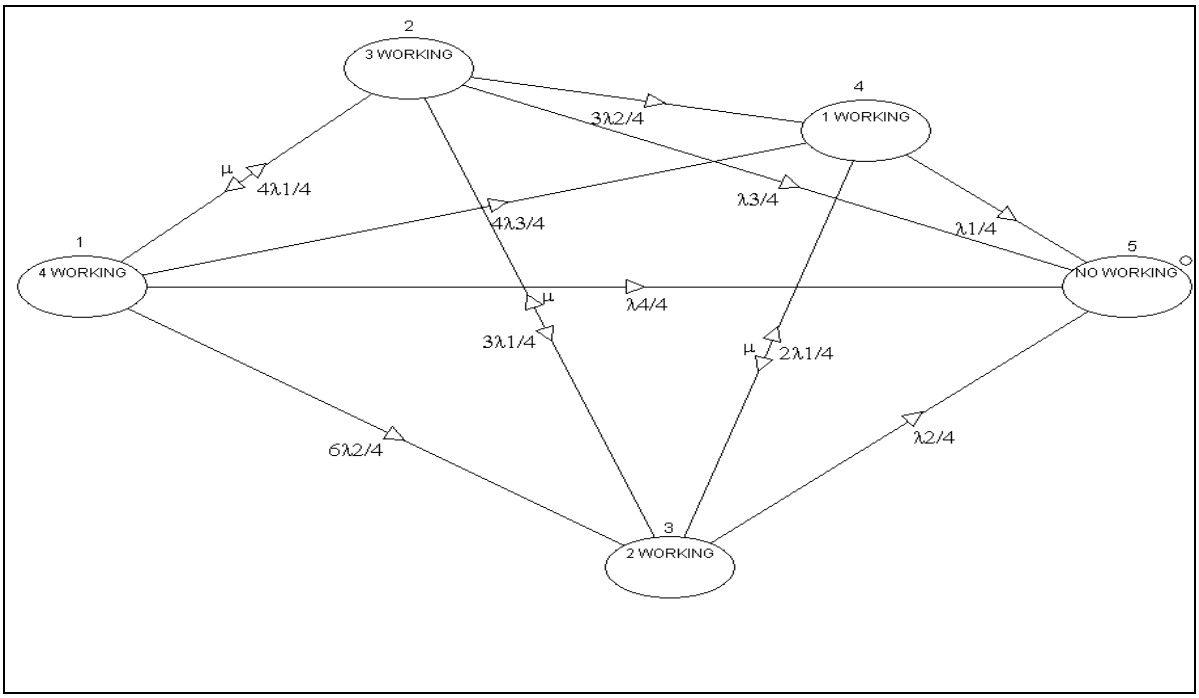

Figure 3.5: State transition diagram from time t=t1 to t=M.T
(Continuously Monitored & With CCF)

Table 3.2: Equations of State transition diagram (Continuously Monitored & With CCF)

Equations of State transition diagram	
For time t=0 to t1 hr	**For time t=t1 to 720 hr**
$\frac{dP_1(t)}{dt} = \mu P_2(t) - (4a+6b+4c+d)P_1(t)$	$\frac{dP_1(t)}{dt} = \mu P_2(t) - (4a+6b+4c+d)P_1(t)$
$\frac{dP_2(t)}{dt} = 4aP_1(t) + \mu P_3(t) - (\mu+3a+3b+c)P_2(t)$	$\frac{dP_2(t)}{dt} = 4aP_1(t) + \mu P_3(t) - (\mu+3a+3b+c)P_2(t)$
$\frac{dP_3(t)}{dt} = 3aP_2(t) + 6bP_1(t) - (\mu+2a+b)P_3(t)$	$\frac{dP_3(t)}{dt} = 3aP_2(t) + 6bP_1(t) + \mu P_4(t) - (\mu+2a+b)P_3(t)$
$\frac{dP_4(t)}{dt} = 2aP_3(t) + 3bP_2(t) + 4cP_1(t) - aP_4(t)$	$\frac{dP_4(t)}{dt} = 2aP_3(t) + 3bP_2(t) + 4cP_1(t) - (\mu+a)P_4(t)$
$\frac{dP_5(t)}{dt} = aP_4(t) + bP_3(t) + cP_2(t) + dP_1(t)$	$\frac{dP_5(t)}{dt} = aP_4(t) + bP_3(t) + cP_2(t) + dP_1(t)$

3.2.5 Markov model for periodically monitored cases

3.2.5.1 Without CCF

State transition diagram from t=0 to t=t1 and t=t1 to 720 hr are shown in Figure 3.6 and Figure 3.7 respectively. W stands for Working, FND for Failed and Not Detected and UR for Under Repair. Figure 3.8 shows the state transition diagram during inspection phase. The Table 3.3 presents the equations as obtained from the state transition diagrams for the specified case.

The state 1 in the Figures 3.6-3.10 represents the operation of four SGDHR loops whereas state 2 indicates the operation of three SGDHR loops and one undetected failure of a SGDHR loop. The state 3 represents the operation of a two loops of SGDHR system and state 4 represents the operation of a single loop with undetected failures of a two and three SGDHR loops respectively. The state 5 indicates that three loops are working and one loop is under repair. Similarly in state 7 two loops are working and two are under repair and in state 10 one loop is working and one is undergoing repair process. The state 6 represents operation of two SGDHR loops, one loop undergoing repair process and the undetected failure of the leftover

loop. Similarly, state 8 represents operation of one SGDHR loops, one loop undergoing repair process and the undetected failure of the two leftover loops. The state 9 similarly represents operation of one SGDHR loops, two loops undergoing repair process and the undetected failure of the one leftover loop. Finally, the state 11 indicates the failure of all the four SGDHR loops. It is to be noted that in the first interval from t=0 to t=t1 the repair process has been modelled from state 5, 6 and 7 only, and in the second interval the credit of repair has been taken from state 5, 6, 7, 8, 9 and 10. Hence in both the intervals for all mentioned figures, the repair from the failed state is not considered.

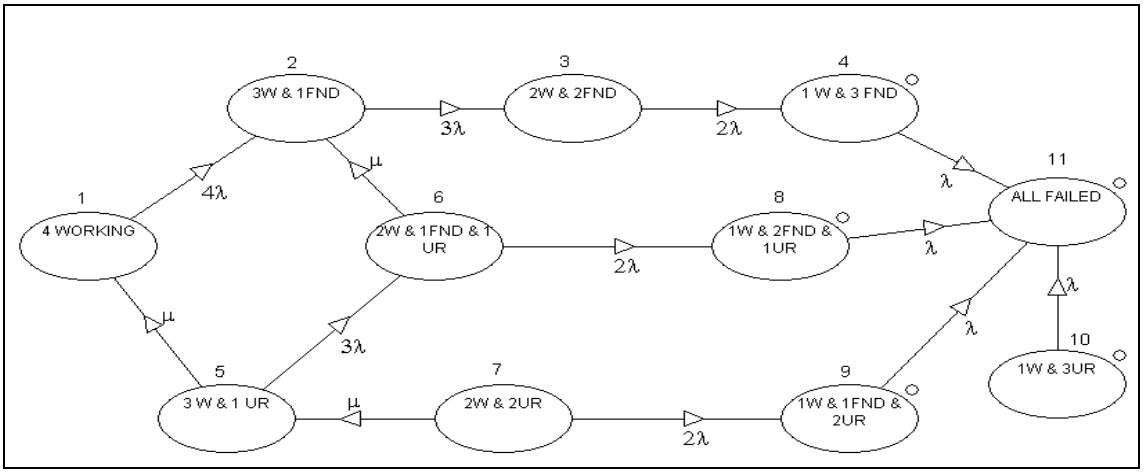

Figure 3.6: State transition diagram from time t=0 to t=t1
(Periodically Monitored & Without CCF)

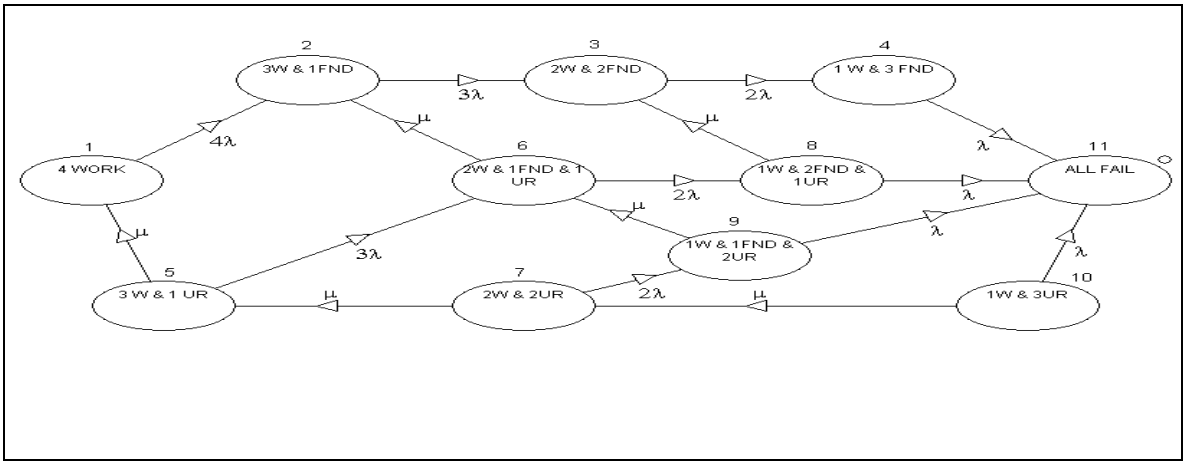

Figure 3.7: State transition diagram from time t=t1 to t=MT
(Periodically Monitored & Without CCF)

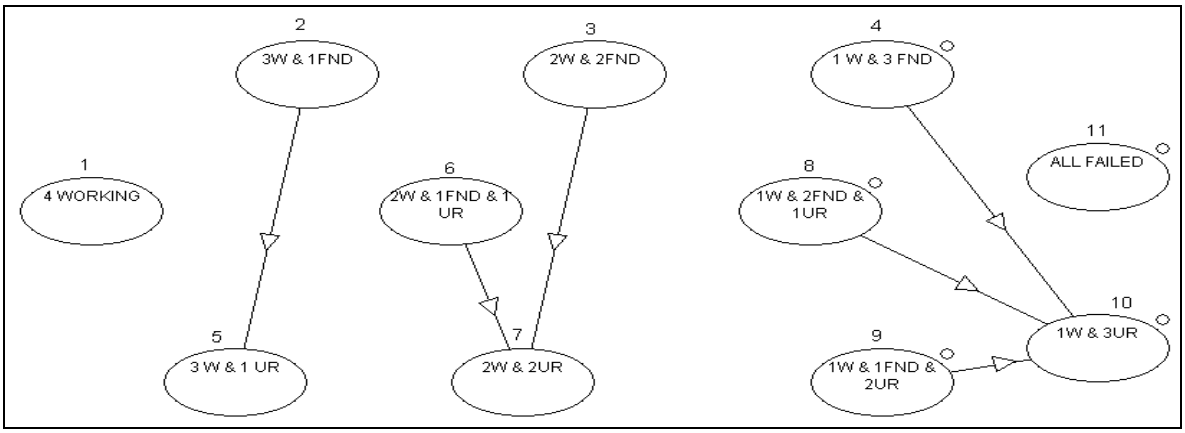

Figure 3.8: State transition diagram during inspection phase (Periodically Monitored & Without CCF)

Table 3.3: Equations of State transition diagram (Periodically Monitored & Without CCF)

Equations of State transition diagram	
For time t=0 to t1 hr	**For time t=t1 to 720 hr**
$\frac{dP_1(t)}{dt} = \mu P_5(t) - 4\lambda P_1(t)$	$\frac{dP_1(t)}{dt} = -4\lambda P_1(t) + \mu P_5(t)$
$\frac{dP_2(t)}{dt} = 4\lambda P_1(t) + \mu P_6(t) - 3\lambda P_2(t)$	$\frac{dP_2(t)}{dt} = 4\lambda P_1(t) + \mu P_6(t) - 3\lambda P_2(t)$
$\frac{dP_3(t)}{dt} = 3\lambda P_2(t) - 2\lambda P_3(t)$	$\frac{dP_3(t)}{dt} = 3\lambda P_2(t) - 2\lambda P_3(t) + \mu P_8(t)$
$\frac{dP_4(t)}{dt} = 2\lambda P_3(t) - \lambda P_4(t)$	$\frac{dP_4(t)}{dt} = 2\lambda P_3(t) - \lambda P_4(t)$
$\frac{dP_5(t)}{dt} = \mu P_7(t) - (\mu+3\lambda)P_5(t)$	$\frac{dP_5(t)}{dt} = \mu P_7(t) - (\mu+3\lambda)P_5(t)$
$\frac{dP_6(t)}{dt} = 3\lambda P_5(t) - (\mu+2\lambda)P_6(t)$	$\frac{dP_6(t)}{dt} = 3\lambda P_5(t) + \mu P_9(t) - (\mu+2\lambda)P_6(t)$
$\frac{dP_7(t)}{dt} = -(\mu+2\lambda)P_7(t)$	$\frac{dP_7(t)}{dt} = \mu P_{10}(t) - (\mu+2\lambda)P_7(t)$
$\frac{dP_8(t)}{dt} = 2\lambda P_6(t) - \lambda P_8(t)$	$\frac{dP_8(t)}{dt} = 2\lambda P_6(t) - (\mu+\lambda)P_8(t)$
$\frac{dP_9(t)}{dt} = 2\lambda P_7(t) - \lambda P_9(t)$	$\frac{dP_9(t)}{dt} = 2\lambda P_7(t) - (\mu+\lambda)P_9(t)$
$\frac{dP_{10}(t)}{dt} = -\lambda P_{10}(t)$	$\frac{dP_{10}(t)}{dt} = -(\mu+\lambda)P_{10}(t)$
$\frac{dP_{11}(t)}{dt} = \lambda(P_4(t) + P_8(t) + P_9(t) + P_{10}(t))$	$\frac{dP_{11}(t)}{dt} = \lambda(P_4(t) + P_8(t) + P_9(t) + P_{10}(t))$

3.2.5.2 With CCF

State transition diagram from t=0 to t=t1 and t=t1 to 720 hr are shown in Figure 3.9 and Figure 3.10 respectively. W stands for Working, FND for Failed and Not Detected and UR

for Under Repair. The Table 3.4 presents the equations as obtained from the state transition diagrams for the with CCF case in case of periodic monitoring.

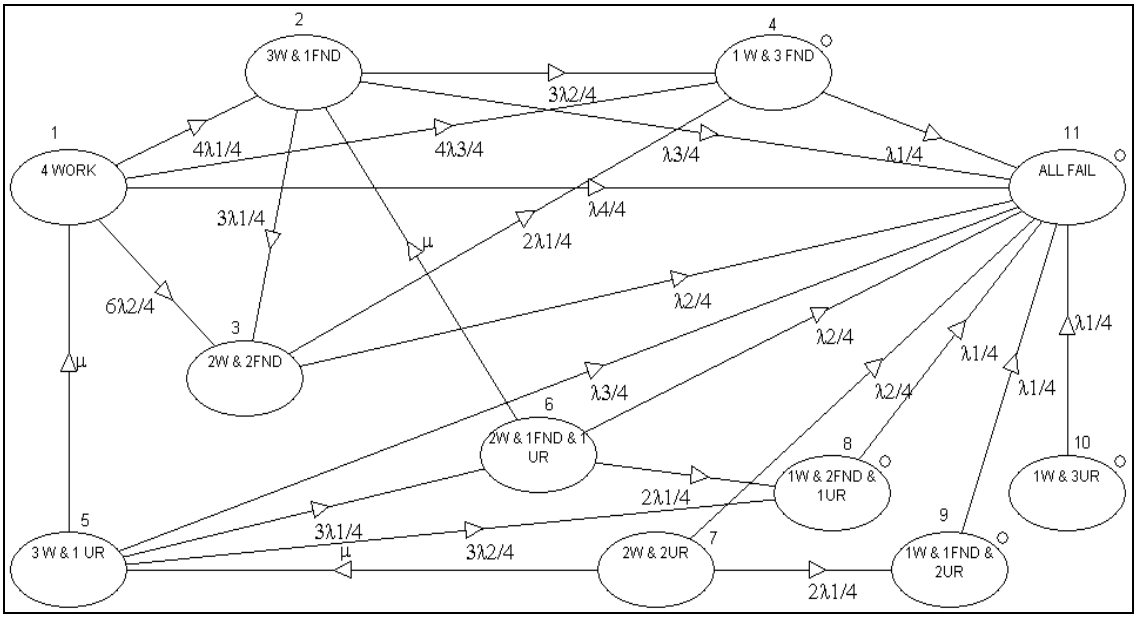

Figure 3.9: State transition diagram from time t=0 to t=t1 (Periodically Monitored & With CCF)

Table 3.4: Equations of State transition diagram (Periodically Monitored & With CCF)

Equations of State transition diagram	
For time t=0 to t1 hr	**For time t=t1 to 720 hr**
$\frac{dP_1(t)}{dt} = \mu P_5(t) - (4a+6b+4c+d)P_1(t)$	$\frac{dP_1(t)}{dt} = \mu P_5(t) - (4a+6b+4c+d)P_1(t)$
$\frac{dP_2(t)}{dt} = 4aP_1(t) + \mu P_6(t) - (3a+3b+c)P_2(t)$	$\frac{dP_2(t)}{dt} = 4aP_1(t) + \mu P_6(t) - (3a+3b+c)P_2(t)$
$\frac{dP_3(t)}{dt} = 3aP_2(t) + 6bP_1(t) - (2a+b)P_3(t)$	$\frac{dP_3(t)}{dt} = 3aP_2(t) + 6bP_1(t) - (2a+b)P_3(t) + \mu P_8(t)$
$\frac{dP_4(t)}{dt} = 2aP_3(t) + 3bP_2(t) + 4cP_1(t) - aP_4(t)$	$\frac{dP_4(t)}{dt} = 2aP_3(t) + 3bP_2(t) + 4cP_1(t) - aP_4(t)$
$\frac{dP_5(t)}{dt} = \mu P_7(t) - (\mu+3a+3b+c)P_5(t)$	$\frac{dP_5(t)}{dt} = \mu P_7(t) - (\mu+3a+3b+c)P_5(t)$
$\frac{dP_6(t)}{dt} = 3aP_5(t) - (\mu+2a+b)P_6(t)$	$\frac{dP_6(t)}{dt} = \mu P_9(t) + 3aP_5(t) - (\mu+2a+b)P_6(t)$
$\frac{dP_7(t)}{dt} = -(\mu+2a+b)P_7(t)$	$\frac{dP_7(t)}{dt} = \mu P_{10}(t) - (\mu+2a+b)P_7(t)$
$\frac{dP_8(t)}{dt} = 2aP_6(t) - aP_8(t) + 3bP_5(t)$	$\frac{dP_8(t)}{dt} = 2aP_6(t) + 3bP_5(t) - (\mu+a)P_8(t)$

$\frac{dP_9(t)}{dt} = 2aP_7(t) - aP_9(t)$	$\frac{dP_9(t)}{dt} = 2aP_7(t) - (\mu+a)P_9(t)$
$\frac{dP_{10}(t)}{dt} = -aP_{10}(t)$	$\frac{dP_{10}(t)}{dt} = -(\mu+a)P_{10}(t)$
$\frac{dP_{11}(t)}{dt} = a(P_4(t)+P_8(t)+P_9(t)+P_{10}(t)) + b(P_3(t)+P_6(t)+P_7(t)) + c(P_2(t)+P_5(t)) + dP_1(t)$	$\frac{dP_{11}(t)}{dt} = a(P_4(t)+P_8(t)+P_9(t)+P_{10}(t)) + b(P_3(t)+P_6(t)+P_7(t)) + c(P_2(t)+P_5(t)) + dP_1(t)$

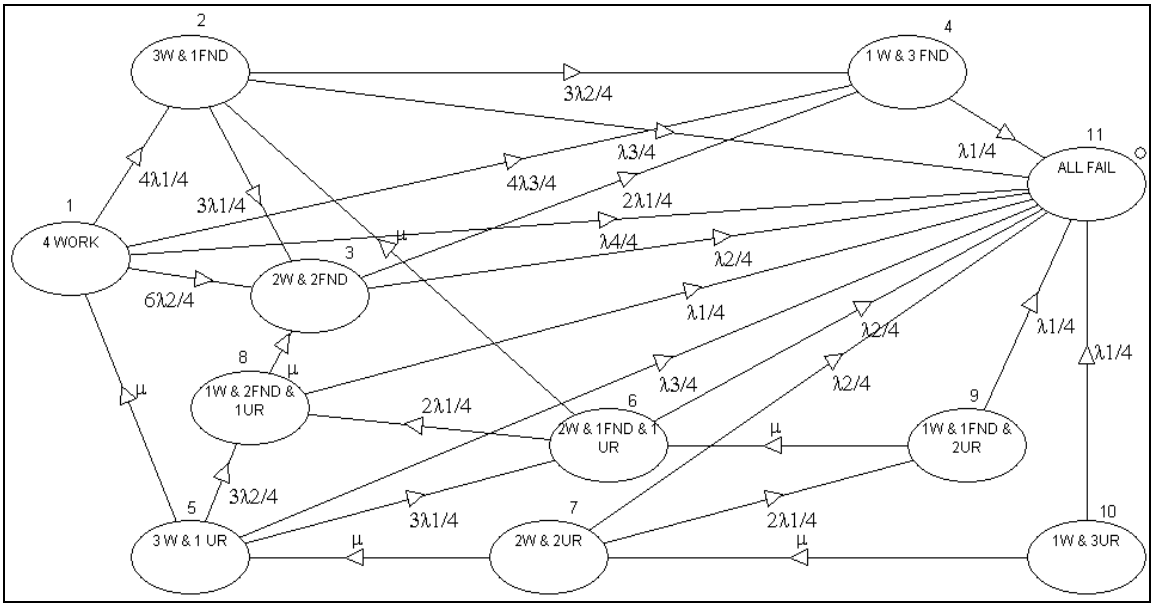

Figure 3.10: State transition diagram from time t=t1 to t=M.T (Periodically Monitored & With CCF)

3.3 RESULTS AND DISCUSSION

Using numerical techniques, MATLAB codes are developed to solve the equations for all the cases. Mean unavailability is calculated over the interval using numerical integration and results obtained for all cases of continuous monitoring are presented in Table 3.5. Results of all cases of periodic monitoring are presented in Table 3.6. Test interval is takes as 24 hr for illustration purpose.

In case of continuously monitored system, the unavailability expression for the first interval (t = 0 to t1) of mission time is given by

$$Q_1(t) = P_4(t) + P_5(t) \quad (3.14)$$

and the unavailability expression for the second interval (t = t1 to mission time) is given by

$$Q_2(t) = P_5(t) \tag{3.15}$$

For periodically monitored system, the unavailability expression for the first interval (t=0 to t1) of mission time is given by

$$Q_1(t) = P_4(t) + P_8(t) + P_9(t) + P_{10}(t) + P_{11}(t) \tag{3.16}$$

and the unavailability expression for the second interval (t=t1 to mission time) is given by

$$Q_2(t) = P_{11}(t) \tag{3.17}$$

Now, we define

Q_{m1} = Mean value of unavailability for time 0 to t1 hr

$$Q_{m1} = \frac{1}{t1}\int_0^{t1} Q_1(t)dt \tag{3.18}$$

Q_{m2} = Mean value of unavailability for time t=t1 to MT

$$Q_{m2} = \frac{1}{MT-t1}\int_{t1}^{MT} Q_2(t)dt \tag{3.19}$$

At t1 (end time of first mission), the end states of first mission is taken as initial states for second mission.

The probability that the system fails for the mission time (Q_m) is

Pr(Mission 1 Fails U Mission 2 Fails) = Pr(Mission 1 Fails) + Pr(Mission 2 Fails)

$$Q_m = Q_{m1} + Q_{m2} \tag{3.20}$$

In the Markov model of the SGDHRS system when repair process is considered from the failed state, the lower bound for the mean unavailability of the system is evaluated and when the repair process is not considered from the failed state, the upper bound for the mean unavailability of the system is computed.

The Markov model and equations in section 3.2 correspond to the evaluation of the upper bound for the mean unavailability of the SGDHR system. For estimating lower bound,

a repair transition from the failed states which are considered unavailable should be drawn to the previous suitable state and corresponding change in equations is required. For example:

1. In Figure 3.2, repair transitions should be made from state 5 to state 4 and from state 4 to state 3.
2. In Figure 3.7, repair transition should be made from state 11 to state 10.

The state transition diagram will remain same over the entire mission time except change in number of failed states.

In section 3.3.1 and 3.3.3 graphs and results of Markov model meant for estimation of the upper bound for mean unavailability of the SGDHR system is presented and in section 3.4 a table comparing upper bound and lower bound for mean unavailability of the SGDHR system is presented for different schemes.

3.3.1 Graphs for continuous monitoring scheme

The results obtained in the case of continuously monitoring of SGDHR system for various repair times (MTTR) are shown in Figures 3.11-3.13 and presented in Table 3.5.

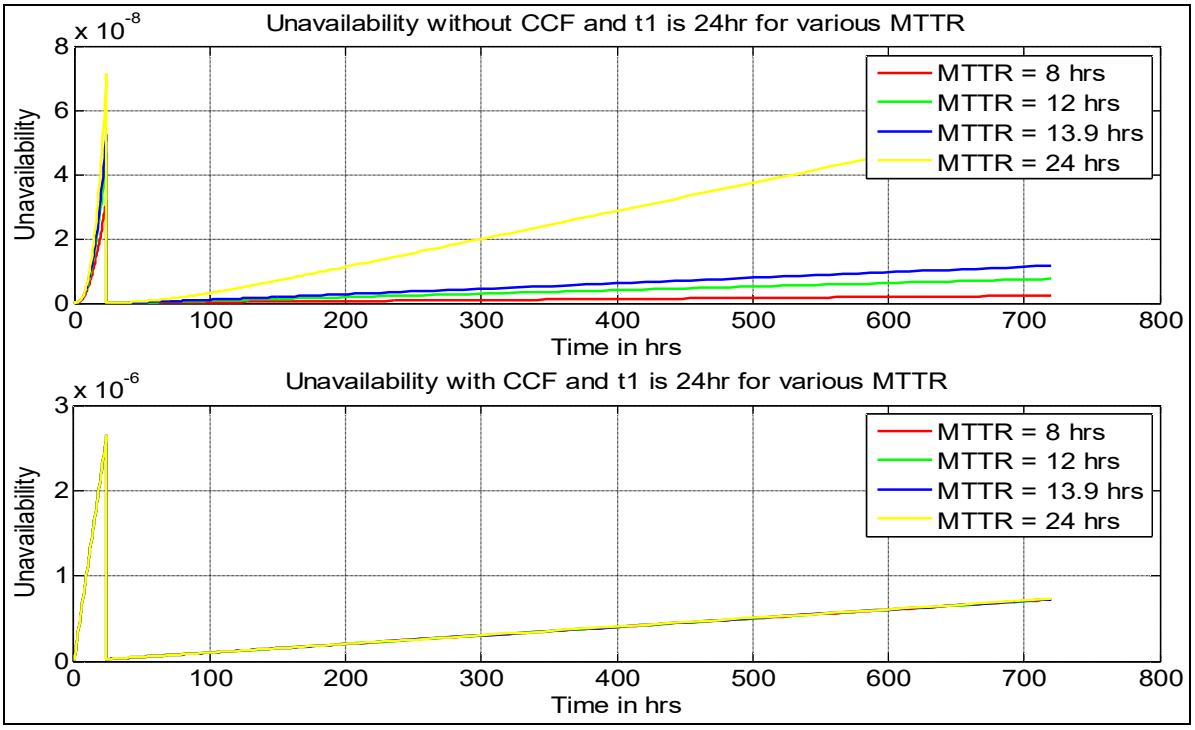

Figure 3.11: Unavailability for continuous monitoring scheme with t1 as 24 hr

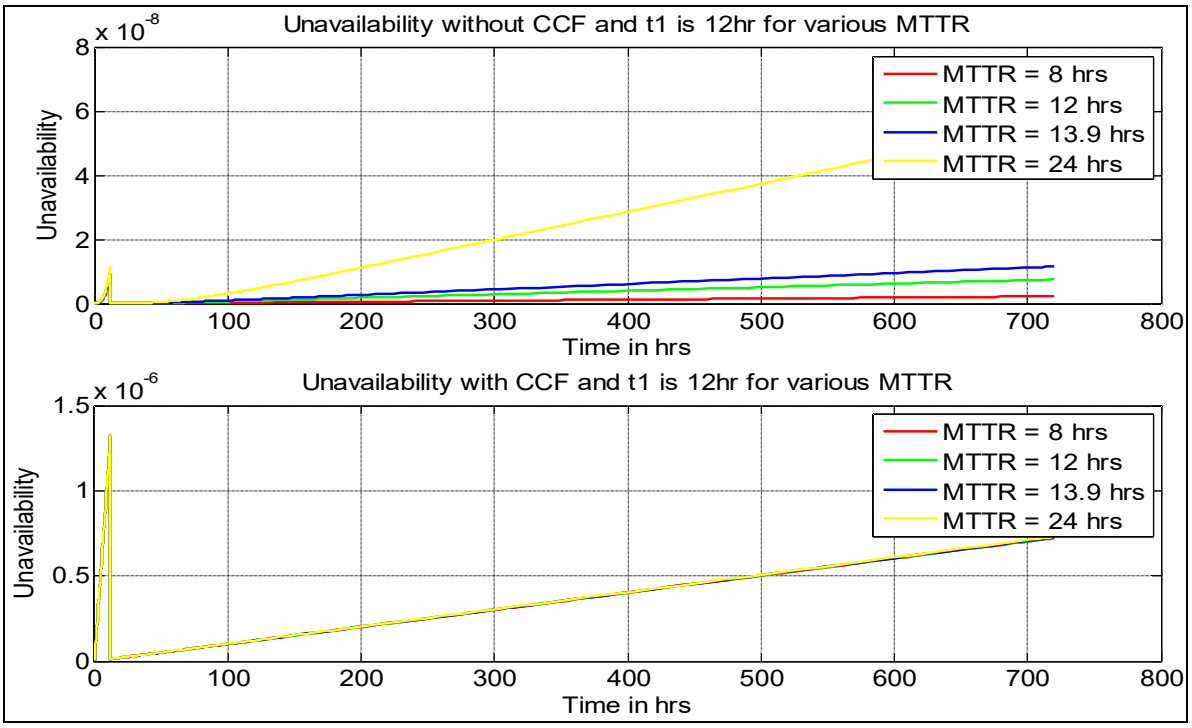

Figure 3.12: Unavailability for continuous monitoring scheme with t1 as 12 hr

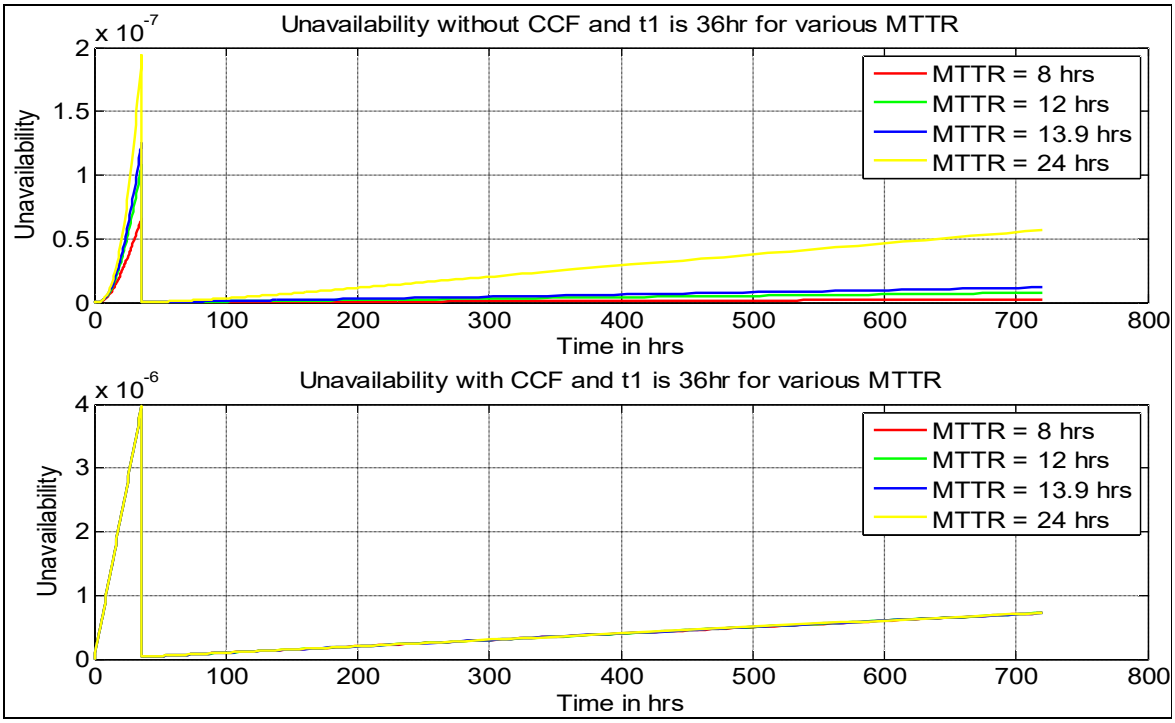

Figure 3.13: Unavailability for continuous monitoring scheme with t1 as 36 hr

Table 3.5: Results for unavailability of the SGDHR system for continuous monitoring scheme

Sl. No	Case	MTTR = 8 hrs RR = 0.125/h			MTTR = 12 hrs RR = 0.083/h		
		Q_{m1}	Q_{m2}	Q_m	Q_{m1}	Q_{m2}	Q_m
		t1 = 12 hr					
1	Without CCF	2.07E-09	1.13E-09	3.20E-09	2.47E-09	3.66E-09	6.13E-09
2	With CCF	6.62E-07	3.67E-07	1.03E-06	6.62E-07	3.68E-07	1.03E-06
		t1 = 24 hr					
3	Without CCF	1.03E-08	1.17E-09	1.15E-08	1.40E-08	3.76E-09	1.78E-08
4	With CCF	1.32E-06	3.73E-07	1.70E-06	1.32E-06	3.74E-07	1.70E-06
		t1 = 36 hr					
5	Without CCF	2.30E-08	1.27E-09	2.43E-08	3.46E-08	3.94E-09	3.86E-08
6	With CCF	1.99E-06	3.79E-07	2.36E-06	1.99E-06	3.80E-07	2.37E-06
Sl. No	**Case**	**MTTR =13.9 hrs RR = 0.072/h**			**MTTR = 24 hrs RR= 0.042/h**		
		Q_{m1}	Q_{m2}	Q_m	Q_{m1}	Q_{m2}	Q_m
		t1 = 12 hr					
7	Without CCF	2.60E-09	5.58E-09	8.18E-09	2.98E-09	2.61E-08	2.91E-08
8	With CCF	6.62E-07	3.69E-07	1.03E-06	6.62E-07	3.71E-07	1.03E-06
		t1 = 24 hr					
9	Without CCF	1.53E-08	5.72E-09	2.11E-08	1.97E-08	2.66E-08	4.64E-08
10	With CCF	1.32E-06	3.75E-07	1.70E-06	1.32E-06	3.77E-07	1.70E-06
		t1 = 36 hr					
11	Without CCF	3.92E-08	5.95E-09	4.51E-08	5.57E-08	2.73E-08	8.30E-08
12	With CCF	1.99E-06	3.81E-07	2.37E-06	1.99E-06	3.83E-07	2.37E-06

3.3.2 Discussions for continuous monitoring scheme

1. Significant difference in system unavailability is observed between the two cases, viz., 'with CCF' and 'without CCF' as can be seen from Figures 3.11, 3.12 and 3.13.
2. Change in MTTR has very minor effect on mean system unavailability for both the cases ('with CCF' and 'without CCF'). This may be specific to system being analysed, as in SGHDR, we have less number of failed states (Table 3.5, Figures 3.2, 3.3, 3.4 and 3.5)
3. It is also observed from Table 3.5 that as MTTR increases, relative contribution of mean system unavailability in first interval decreases and that of second interval increases. This is much more dominating in 'without CCF' case.
4. When the time across which success criteria (t1) changes, the relative contribution of mean unavailability in first interval to the total mean unavailability increases appreciably for both 'with CCF' and 'without CCF' cases as unavailability with two loops required out of four is more dominating.
5. It is also observed from Table 3.5 that as the time across which success criteria changes is increased relative contribution of mean unavailability in first interval to the total mean unavailability decreases at a lower rate as MTTR increases especially for 'without CCF' case.

3.3.3 Graphs for periodic monitoring scheme

The results obtained in the case of periodic monitoring of SGDHR system for various test interval and repair times (MTTR) are shown in Figures 3.14-3.17 and presented in Table 3.5.

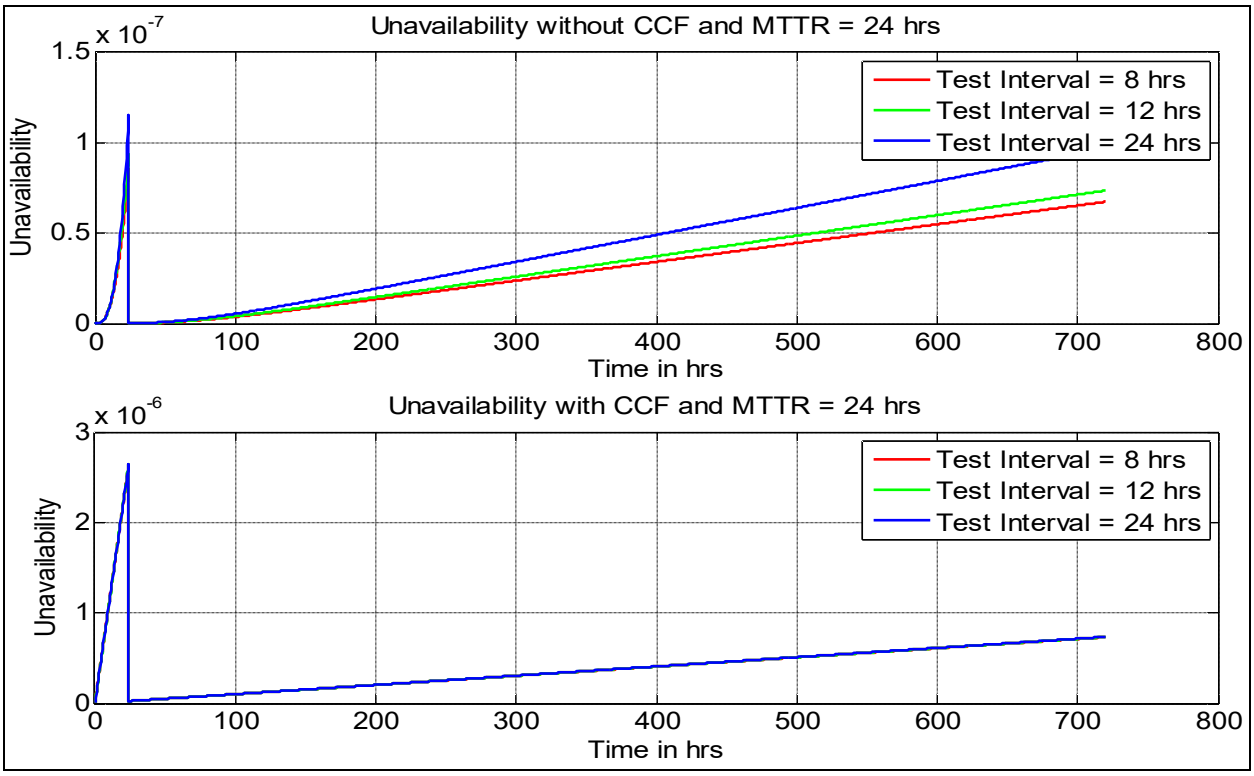

Figure 3.14: Unavailability for periodic monitoring scheme for various test intervals

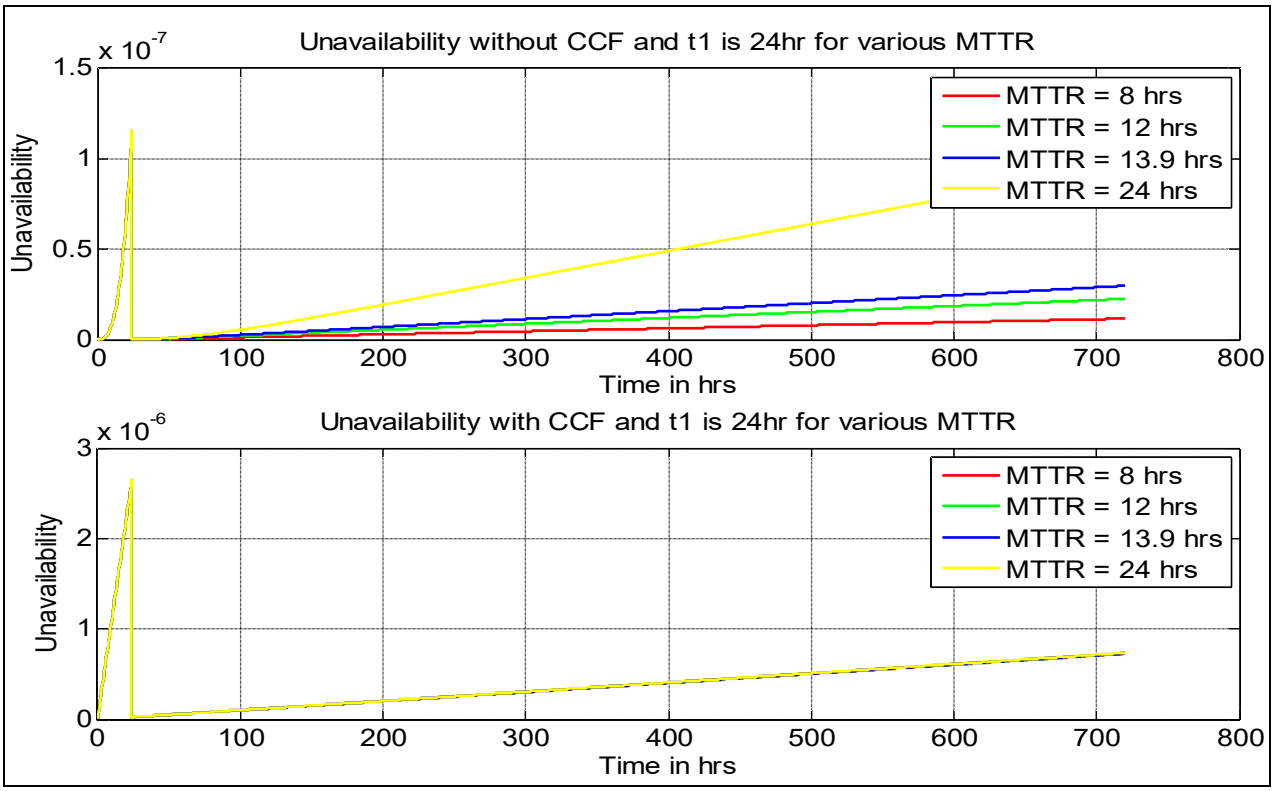

Figure 3.15: Unavailability for periodic monitoring scheme with t1 as 24 hr

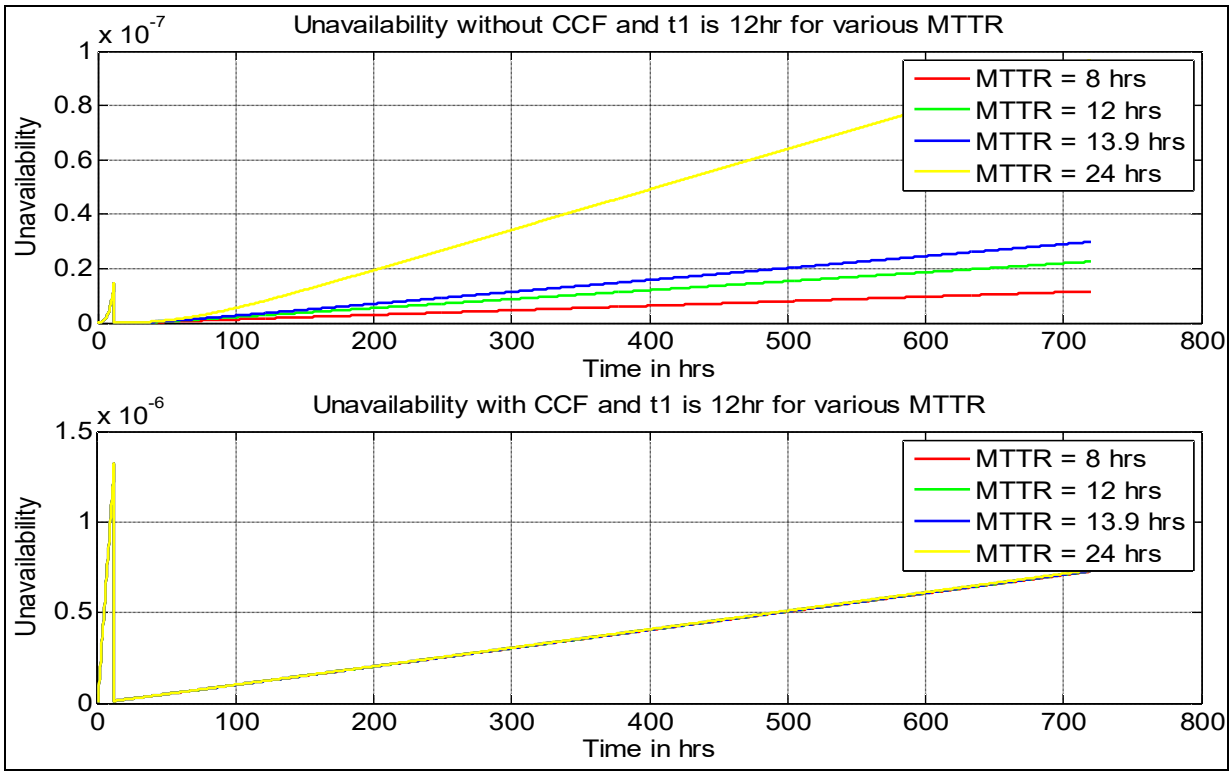

Figure 3.16: Unavailability for periodic monitoring scheme with t1 as 12 hr

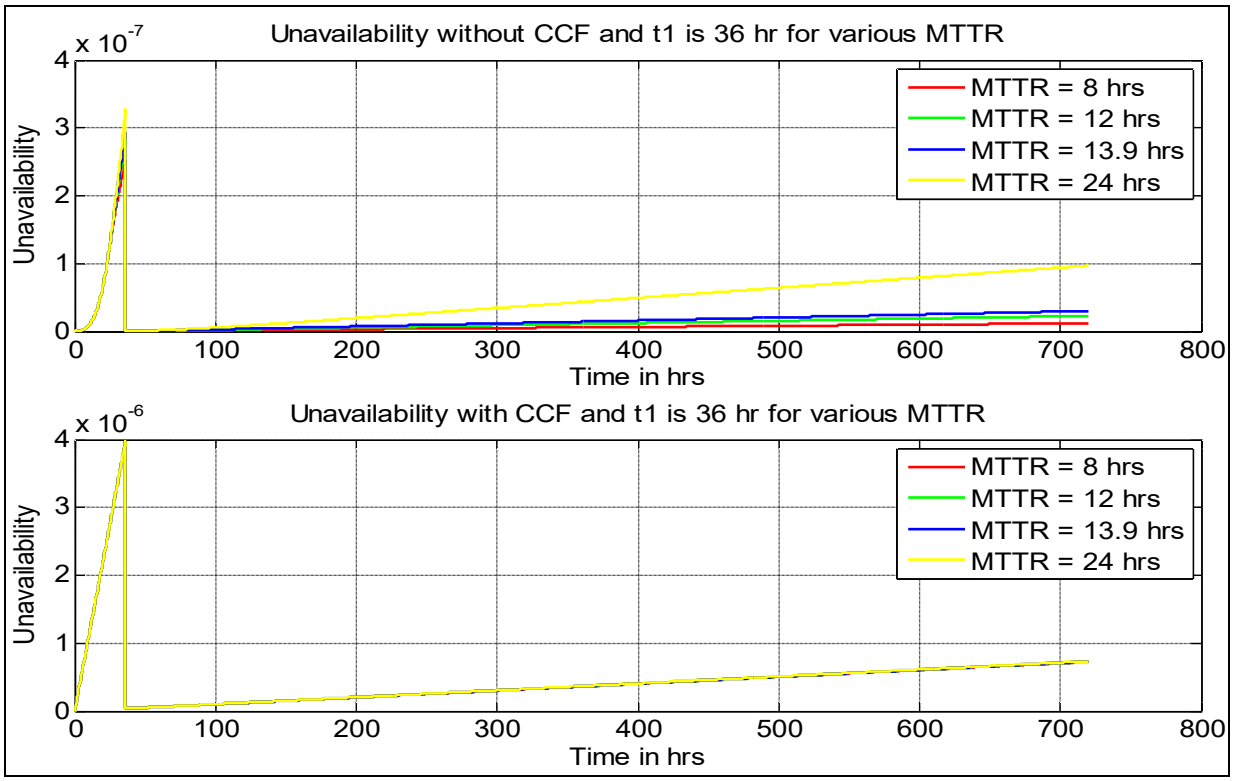

Figure 3.17: Unavailability for periodic monitoring scheme with t1 as 36 hr

3.3.4 Discussions for periodic monitoring scheme

Following inferences are obtained from Table 3.6 and Figures 3.14-3.17:

1. Significant difference in system unavailability is observed between the two cases, viz., 'with CCF' and 'without CCF'.
2. It is observed from Figure 3.14 that change in test interval (from 8 hr to 24 hr) has very minor increase in the system unavailability for both with CCF and without CCF cases.
3. Change in MTTR has very minor effect on mean system unavailability for both the cases ('with CCF' and 'without CCF'). This may be specific to system being analysed. In SGHDR, we have less number of failed states (Table 3.6, Figures 3.6, 3.7, 3.8, 3.9 and 3.10)
4. It is also observed that as MTTR increases, relative contribution of mean system unavailability in first interval is more as compared to that from the second interval. This effect is much more prominent when CCF is not modelled ('without CCF' case).
5. When the time across which success criteria (t1) changes, relative contribution of mean unavailability in first interval to the total mean unavailability increases appreciably for both 'with CCF' and 'without CCF' cases as unavailability with two loops required out of four is more dominating.

Table 3.6: Results for unavailability of the SGDHR system for periodic monitoring scheme

Sl. No	Case	MTTR= 8 hrs RR =0.125/h			MTTR=12 hrs RR =0.083/h		
		Q_{m1}	Q_{m2}	Q_m	Q_{m1}	Q_{m2}	Q_m
		t1 = 12 hr					
1	Without CCF	3.62E-09	5.74E-09	9.36E-09	3.62E-09	1.10E-08	1.46E-08
2	With CCF	6.62E-07	3.70E-07	1.03E-06	6.62E-07	3.71E-07	1.03E-06
		t1 = 24 hr					
3	Without CCF	2.88E-08	5.84E-09	3.47E-08	2.88E-08	1.11E-08	4.00E-08
4	With CCF	1.32E-06	3.76E-07	1.70E-06	1.32E-06	3.77E-07	1.70E-06
		t1 = 36 hr					
5	Without CCF	8.20E-08	6.22E-09	8.83E-08	8.59E-08	1.16E-08	9.75E-08
6	With CCF	1.99E-06	3.82E-07	2.37E-06	1.99E-06	3.83E-07	2.37E-06
Sl. No	**Case**	**MTTR=13.9 hrs RR=.072/hr**			**MTTR=24 hrs RT =.042/hr**		
		Q_{m1}	Q_{m2}	Q_m	Q_{m1}	Q_{m2}	Q_m
		t1 = 12 hr					
7	Without CCF	3.62E-09	1.44E-08	1.80E-08	3.62E-09	4.46E-08	4.82E-08
8	With CCF	6.62E-07	3.71E-07	1.03E-06	6.62E-07	3.73E-07	1.03E-06
		t1 = 24 hr					
9	Without CCF	2.88E-08	1.46E-08	4.35E-08	2.88E-08	4.53E-08	7.42E-08
10	With CCF	1.32E-06	3.77E-07	1.70E-06	1.32E-06	3.79E-07	1.70E-06
		t1 = 36 hr					
11	Without CCF	8.71E-08	1.52E-08	1.02E-07	9.08E-08	4.64E-08	1.37E-07
12	With CCF	1.99E-06	3.83E-07	2.37E-06	1.99E-06	3.86E-07	2.37E-06

3.4 COMPARISON OF UPPER BOUND AND LOWER BOUND FOR THE MEAN UNAVAILABILITY OF SGDHR SYSTEM

For completeness, upper bound and lower bound for the mean unavailability of SGDHR system for various values of MTTR under both the monitoring schemes with and without consideration of CCF are evaluated and provided in Table 3.7. It is observed that the range is around one order magnitude and for safety application like SGDHR conservative value of upper bound can be used.

Table 3.7: Results for upper bound and lower bound for the mean unavailability of SGDHR system

	Continuously Monitored		**Periodic Monitoring with Test Interval 24hr**	
t1= 12 hr				
Without CCF				
MTTR	**Qm (Upper Bound)**	**Qm (Lower Bound)**	**Qm (Upper Bound)**	**Qm (Lower Bound)**
8	3.20E-09	1.57E-09	9.36E-09	3.75E-09
12	6.13E-09	2.15E-09	1.46E-08	3.99E-09
13.9	8.18E-09	2.41E-09	1.80E-08	4.19E-09
24	2.91E-08	4.52E-09	4.82E-08	6.78E-09
With CCF				
MTTR	**Qm (Upper Bound)**	**Qm (Lower Bound)**	**Qm (Upper Bound)**	**Qm (Lower Bound)**
8	1.03E-06	4.35E-07	1.03E-06	6.69E-07
12	1.03E-06	5.00E-07	1.03E-06	6.73E-07
13.9	1.03E-06	5.21E-07	1.03E-06	6.75E-07
24	1.03E-06	5.88E-07	1.03E-06	6.86E-07
t1= 24 hr				
Without CCF				
MTTR	**Qm (Upper Bound)**	**Qm (Lower Bound)**	**Qm (Upper Bound)**	**Qm (Lower Bound)**
8	1.15E-08	5.78E-09	3.47E-08	2.90E-08
12	1.78E-08	9.57E-09	4.00E-08	2.92E-08
13.9	2.11E-08	1.11E-08	4.35E-08	2.94E-08
24	4.64E-08	1.80E-08	7.42E-08	3.21E-08
With CCF				
MTTR	**Qm (Upper Bound)**	**Qm (Lower Bound)**	**Qm (Upper Bound)**	**Qm (Lower Bound)**
8	1.70E-06	6.14E-07	1.70E-06	1.33E-06
12	1.70E-06	7.66E-07	1.70E-06	1.33E-06

13.9	1.70E-06	8.20E-07	1.70E-06	1.34E-06
24	1.70E-06	1.00E-06	1.70E-06	1.35E-06
t1= 36 hr				
Without CCF				
MTTR	**Qm (Upper Bound)**	**Qm (Lower Bound)**	**Qm (Upper Bound)**	**Qm (Lower Bound)**
8	2.30E-08	9.99E-09	8.83E-08	5.50E-08
12	3.46E-08	1.95E-08	9.75E-08	6.49E-08
13.9	3.92E-08	2.39E-08	1.02E-07	6.83E-08
24	5.57E-08	4.32E-08	1.37E-07	8.12E-08
With CCF				
MTTR	**Qm (Upper Bound)**	**Qm (Lower Bound)**	**Qm (Upper Bound)**	**Qm (Lower Bound)**
8	1.99E-06	7.01E-07	2.37E-06	1.57E-06
12	1.99E-06	9.21E-07	2.37E-06	1.67E-06
13.9	1.99E-06	1.00E-06	2.37E-06	1.71E-06
24	1.99E-06	1.30E-06	2.37E-06	1.82E-06

3.5 CONCLUSIONS

The objective of the current study is to apply Markov model technique on SGDHR system of PFBR to efficiently model time dependent success criteria and estimate the unavailability of the system. The estimates of the upper bound and lower bound for the mean unavailability of SGDHR system over the mission time (720 hrs) are reported. The system has been modelled exhaustively under continuous and periodic monitoring schemes. It is noted from the analyses that change in the value of time (t1) across which success criteria is changed and its effect on the system unavailability is more comprehensively analysed with Markov analysis. This effect cannot be observed in other methods such as Fault tree analysis. Sensitivity analysis of other important parameters like mean time to repair, test interval, etc with time dependent success criteria is also carried out. The analysis has been carried with and without the consideration of CCF. Significant difference in system unavailability is observed between the two cases, viz., with CCF and without CCF under both continuous and periodic monitoring schemes. The results presented in the chapter are with consideration of one repair crew. On

detailed analysis with two repair crews, not much significant improvement in the system availability is observed since the failure rates are very low and number of states is large. The approach described in the chapter can be used to dynamically model the scenarios with time dependent success criteria in a comprehensive manner and to study various factors affecting the availability of such system.

CHAPTER-4

PROBABILISTIC SAFETY ASSESSMENT OF MULTI-UNIT NUCLEAR POWER PLANT SITES – AN INTEGRATED APPROACH

4.0 INTRODUCTION

The nuclear power generation involves several processes like extraction of nuclear fuel, refinement, conversion, enrichment and finally reprocess and waste treatment. Numerous hazards and risks are inherently involved in all these process and it is imperative to ensure nuclear and radiological safety to the public and environment.

In many industries, quantitative risk analysis (QRA) is performed to estimate risk and improve the safety therein. When performed systematically, it can provide a rational basis for evaluating process safety and comparing various improvement alternatives (Arendt and Lorenzo, 2000). Probabilistic Safety Assessment (PSA) which is similar to QRA is adopted in nuclear industry to estimate risk. The term ‘PSA’ and 'QRA' effectively mean the same (Hayns, 1999).

PSA is a systematic methodology and is a well-established tool for safety analysis and risk assessment in nuclear industry. It is complementary to deterministic analysis and provides both qualitative and quantitative assessment of the risks to enhance safety. PSA is now mature enough to provide insights into the single unit NPP to enhance its safety and thereby reducing the risk from the plant. However, the focus of this work is risk from multiple units of NPP located at a site. Simultaneous failures of systems and components in multiple nuclear plants at a site were earlier considered as rare event in PSA but have now proved to be a potential threat and have gained regulatory attention in risk assessment of nuclear power plants (NPPs). Fukushima accidents have revealed the necessity of multi-unit safety assessment and the need to develop safety goals, procedures and guidelines to achieve and maintain the basic safety goal to protect public and environment. Moreover most of the

countries in the world houses more than one NPP at a site. Specifically, there are 76 sites with 2 operating reactors, 15 sites with 3 reactors, 30 sites with 4 reactors and so on. More than 68% of the sites have more than one reactor (Figure 4.1).

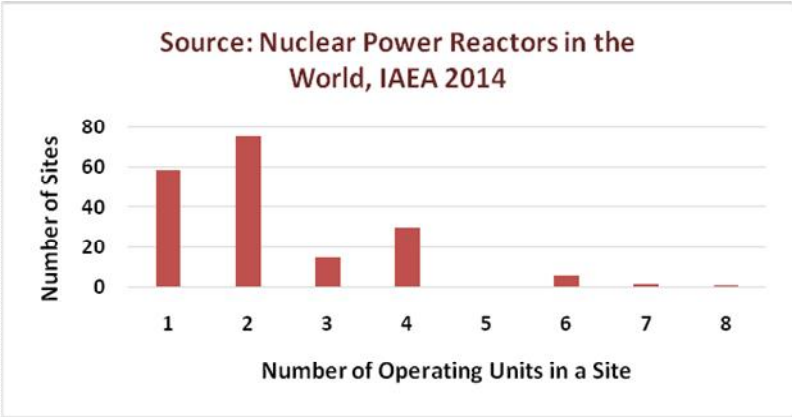

Figure 4.1: Distribution of number of operating units in a site around the world

In India, more than 90% of the reactors operate at a multi-unit site (Figure 4.2) and if new reactors under construction are included, 100% of the sites will have more than one reactor.

Figure 4.2: Distribution of Indian Nuclear Reactors

Individual plant specific PSAs yield major insights to operators, designers and regulators to improve safety of the plant in achieving holistic risk-informed, performance based regulatory approach (Apostolakis, 2012). However, regulations recognize the potential for multi-unit accidents. For example, NRC regulations (CFR-10, 2009) specifies the requirement for sharing of systems, structures and components important to safety among

nuclear power units and in addition NRC regulation (CFR-100, 2012) provides requirements for determining exclusion area, low population zone and population center distance for multi-unit sites.

To estimate risk for a multiunit site, accident likelihood is to be measured in 'events per site per year' instead of 'events per reactor year'. To do this, it is imperative to include various inter-unit dependencies and develop an approach to combine and obtain the overall site risk assessment. In this work, such an integrated approach is developed to address the unique features for risk assessment of a multi-unit NPP site. The approach is realistic as it addresses all possible accident scenarios that can result from different hazards and is demonstrated with typical initiating events. Finally, the approach developed quantifies the risk for a multi-unit NPP site and evaluates the risk metric, site core damage frequency (SCDF). SCDF is overall risk associated with the site obtained by means of integrating the risk of core damage in more than one unit at the site. In other words, it is the frequency of at least single core damage per site per year.

Though the approach developed in the work is demonstrated for nuclear power plants, the ideology of the approach can be extended to estimate risk for a site having multiple process or chemical industries. Suitable metric of interest like fatalities incurred, monetary loss, etc. can be adopted in such cases.

4.1 IMPORTANCE OF THE PROBLEM

The Fukushima accident has highlighted that the magnitude of natural events can be higher than what is considered in design. During such events, the impact of simultaneous failures of safety systems in multiple units at a site is catastrophic. It is therefore prudent to make additional design provisions in order to ensure that the basic safety functions for the NPPs are not impaired even under beyond design basis natural events (or extreme events). To achieve this, a systematic methodology is needed to address the issue of multi-unit safety and

determine safety margin / risk due to cliff-edge effects for extreme events. It should include the identification of rare extreme events that could lead to common cause failures in multiple units at a site, analyze the consequences and evaluate the effects of interrelation between systems and human actions (SNETP Fukushima Task Group, 2013). Recent studies (Schroer and Modarres, 2013; IAEA Report GC (56)/INF/2, 2012; Ebisawa et al., 2012; Muhlheim and Wood, 2007; Fleming, 2005; Yang, et al., 2009; Yang, 2012; Samaddar et al., 2014) have recommended ideas to deal with different aspects of a multi-unit risk assessment through probabilistic approach. Probabilistic safety assessment (PSA) is a preferred approach as it provides a systematic framework and has the potential to provide a deeper understanding of the potential risk resulting from an NPP over wide range of conditions. USNRC endorsed an integrated risk analysis using PSA approach in 2005 to quantify the risk from all units on a reactor site (SECY-05-0130, 2005). The outcome of such integrated PSA helps in identification of those structures, system and components (SSCs) that are inter unit dependent and play a vital role in multi-unit safety.

4.2 UNIQUE FEATURES IN MULTI-UNIT SAFETY ASSESSMENT

Events affecting more than one unit at a time pose an uphill task to the plant personnel during accidents. The event progression at one unit may affect the neighbouring unit and the availability of common shared resources which may include personnel, equipment, etc. Following are some of the unique challenges encountered in multi-unit safety assessment and each of the topics needs to be addressed in detail during safety assessment and the subsequent quantification process.

4.2.1 Mobility of crew during emergency

It is a general practice to have sharing of manpower at a multi-unit site to render mutual support in the event that a unit develops a problem. However, during an external event, due to

situations such as high background radiation levels, inaccessibility, etc., it may not be always possible to assume availability of crew. Hence, during multi-unit safety assessment availability of manpower needs to be addressed appropriately.

4.2.2 External resources not available during emergency

As part of accident management plan, during emergency situations, external resources can be brought to supplement or replace the onsite resources such as electricity, water or equipment such as pumps or generators to mitigate severity of accidents. In case of an external hazard affecting the whole site and prolonging for longer durations, it may not be possible to facilitate the access to additional external resources.

4.2.3 Cliff edge effect

A cliff edge effect in a nuclear power plant is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter (IAEA Specific safety Guide no. SSG-2, 2009). While it is true for an individual unit and for internal events, it is more important for some extreme events in which risk may grow significantly with slight variations in the external event and hence it is imperative to evaluate the cliff edge margin for multi-unit safety assessment. Therefore, identifying hazard related cliff edge factors in a multi-unit site is equivalent to avoiding a major accident. Sensitivity studies are required to be performed to identify cliff edge factors.

4.2.4 Mission time

Another important factor is the use of appropriate mission time. Several external hazards may require a longer mission time for various engineered safety systems to prevent the core damage. Hence mission time for the accident sequences should be decided based on the nature and severity of the hazard.

4.3 CONCEPT OF SITE CDF

Before introducing the concept of site core damage frequency, the term core damage needs to be defined. The use of the term "core damage" is subjective and several definitions that differ considerably with the reactor technology are available (SECY-05-0130, 2005). The IAEA defines core damage for a light water reactor as exceeding the design basis limit of any of the fuel parameters (IAEA Specific Safety Guide no. SSG-3, 2010). The NRC's SPAR models define core damage as the uncovery and heat up of the reactor core to the point where "severe" fuel damage is anticipated (IAEA Report, 2011). The Indian Atomic Energy Regulatory Board defines core damage as the state of the reactor brought about by the accident conditions with loss of core geometry or resulting in crossing of design basis limits or acceptance criteria limits for one or more parameters: fuel clad strain, fuel clad temperature, primary and secondary systems pressures, clad oxidation, amount of fuel failure, radiation dose, etc. (Atomic Energy Regulatory Board, Technical report, 2005). For PHWR type reactor, core damage is defined as loss of structural integrity of multiple fuel channels (OECD Technical Report NEA/CSNI/R(2009)16, 2009). Very precise definition of core damage such as local fuel temperature exceeding 1204 deg. C, the limit for ECCS for light-water reactors are defined in 10 CFR 50.46(1b) (Holmberg and Knochenhauer, 2010). Therefore, for nuclear power plants at a multi unit site, the definition of core damage will be as per the design and type (PWR/BWR/PHWR/etc) of the unit at the site.

At a multi-unit nuclear power plant site, there is a possibility of simultaneous occurrence of core damage for multiple units within a short interval of time due to external hazards or internal events. Hence, the metric developed or used for multi-unit nuclear power plant safety assessment should also account for all possible combinations of multiple core damages, apart from considering single core damage. The concept of site core damage frequency (SCDF) is considered which accounts for both single core damage and multiple

combinations of core damages occurring at the site (Schroer and Modarres, 2013). It is defined as the sum of all possible single and multiple combinations of core damage per site per year, with consideration of various inter-unit dependencies.

4.4 DEVELOPMENT OF AN INTEGRATED APPROACH

An integrated approach is developed to address both external and internal events that can affect a single / multiple units at a site. Each event is further classified into bins as the severities from various events may differ significantly. For e.g. earthquakes for a site can be categorized into bins such as 0 - 0.1g, 0.1g - 0.2g, etc. for evaluation. For internal events, identification of various initiating events takes into account the severity. For e.g. LOCA is categorized as small LOCA, medium LOCA and large LOCA. Techniques such as failure modes effects analysis can be adopted to identify the potential failure modes for all the components under each category of hazards / events. This section describes the methodology or approach followed to evaluate SCDF.

4.4.1 Identification of external hazards for the site

External hazards are both natural and man-made which originate outside the plant and create extreme environment conditions at the site. They are always site-specific and design dependent. As a first step for the multi-unit risk assessment, all possible site specific external hazards that can affect the multiple units of nuclear plant site needs to be identified (Khan and Abbasi, 1998; Papazoglou et al., 1992). These hazards could also be a result of correlated failures. However, during this process, those initiators that simply do not occur at a site or have a very low probability may be eliminated. The final list of external hazards is categorized as either definite or conditional (Schroer and Modarres, 2013; IAEA-TECDOC-1341, 2003; Zerger et al., 2013; Lowe and Garrick, 1983). The hazards that will always affect multiple units are called definite hazards and those which only under certain circumstances

affect multiple units are called conditional hazards. An illustrative list of both hazards is given in Table 4.1.

Table 4.1: List of external hazards

Definite External Hazards	Conditional External Hazards
Earthquakes	Aircraft Crash
Tsunamis	Explosions
External floods	Lightning
External fires	Fouling or clogging in Intake tunnel
High wind hazards like Cyclones	

4.4.2 Identification of internal initiating events for the site

Internal events are abnormal conditions generated within the plant as a result of failure or faulty operation of plant component through random failures, human errors, etc. The internal initiating events that have the potential to affect multiple units are called definite internal initiating events. And those which only under certain circumstances will affect multiple units are called conditional internal initiating events. An illustrative list of various internal definite and conditional initiating events (Schroer and Modarres, 2013) that could affect multiple units is given in Table 4.2.

Table 4.2: List of internal initiating events

Definite Internal Initiating Events	Conditional Internal Initiating Events
Loss of offsite power	Loss of emergency service water
Loss of ultimate heat sink	Loss of feed water
	Loss of DC bus
	Station Blackout (SBO)
	Turbine missile
	Loss of instrument air

4.4.3 Identification of internal independent initiating events

Internal independent events are those events whose occurrence and effect are limited to a single unit and will not extend to other units of the site e.g. Loss of coolant accidents, transients, etc.

4.4.4 Event Tree / Fault Tree models

After the initiating events for external hazards and internal events are identified and categorized, event tree / fault tree models are developed for each hazard category for further analysis (Saleh et al., 2014; Tixier et al., 2002). The total core damage frequency of multi-unit site is obtained by summing the frequencies of all possible single and multiple core damage. The detailed evaluation method for each category is given in section 5.6.

4.4.5 Parameters / Key issues

Schroer and Modarres (Schroer and Modarres, 2013) have identified the key issues which need to be addressed while modelling event trees and fault trees for a multi unit site safety assessment. The issues are classified as shared systems or connections, identical components, human dependencies and proximity dependencies. The issues account for dependencies between the units arising from shared physical links, similarity in the design, installation and operational approach for a component / system, same or related environment of positioning the systems and associated dependencies for various human interactions. The approaches to account for such dependencies are described in the following section. Further, unique features as described in section 3 of the work, should also be considered for evaluation of multi unit safety.

4.5 SAFETY ASSESSMENT METHODOLOGY

4.5.1 Quantification of Core Damage Frequency from the hazard

The quantification approach to account for the above mentioned four key parameters is explained below:

4.5.2 Modelling of key parameters

Shared Connections *or Systems:* Modelling and evaluation for shared systems is as follows:

- Single SSC shared between multiple units will be assigned the same name in fault trees / event trees and will be treated as a common component in all the respective units where it is shared. Thus, the shared component failure for one plant will automatically be reflected in the evaluation of all the fault trees or event trees of the other unit having the component.
- Time sequential sharing and Standby system sharing: Such types of sharing between the units can be modelled by assigning preference of the system for a particular unit (Schroer and Modarres, 2013). The same SSC is modelled suitably in the ETs and FTs of other units.

Identical components: From the Boolean expression of all event trees of a particular hazard, identical components can be grouped for common cause failures and Beta factor model can be used.

Human dependencies: DEPEND-HRA method developed by Marko Cepin (Čepin, 2008) for evaluation of human error probabilities can be extended to model the dependencies associated with human actions between multiple units. The method is fully capable to account and evaluate the dependency for both type of human actions pre-initiators and post initiators. It uses different parameters for dependency determination for pre-initiators and post-initiators as the two are quite different scenarios.

Proximity dependencies: Similar treatment as that of identical components can be made here. SCDF of each hazard is evaluated from the Boolean expression of all event trees of a particular hazard and components that share the same proximities can be grouped together for common cause failures with C factor model or Beta factor model.

4.5.3 Estimation of site CDF

As discussed earlier, SCDF accounts for both single and multiple core damages occurring at the site. Hence for a multi-unit site it can be expressed as

$$SCDF = \sum_{i=1}^{n} \text{Frequency of i number of core damage per site per year} \quad (4.1)$$

where n is the number of units at the site. The frequency of each number of core damage will be evaluated considering all internal and external hazards with consideration of various inter-unit dependencies.

The proposed method for quantification is explained in the subsequent sections, with a representative multi-unit site with four nuclear plants. Units 1 & 2 are identical and share some systems / resources (e.g. switchyard, sea water pump house, instrument air, feed water) and units 3 & 4 are identical and share some systems (e.g. switchyard, sea water pump house, DC bus). The shared systems between units 1 & 2 are denoted by 'Group A' and the shared systems between units 3 & 4 are denoted by 'Group B'.

Frequency of conditional initiating events is obtained based on likelihood of the initiating event that can affect various units. For example, based on operating experience / engineering judgment, if loss of instrument air for unit 1 has 40% chance of affecting unit 2 for the same event, then conditional initiating event frequency for unit 2 is 0.4*(IE frequency). Similarly all conditional initiating events in case of external or internal hazards for the site can be accounted.

4.5.4 Methodology for definite external hazards

In case of a definite external hazard, firstly the hazard induced initiating events are identified. Core damage expression for an initiating event induced directly by definite external hazard is denoted as $H_i(D_{ijk}.BExp_{ijk})$, where H_i denote frequency of (definite) external hazard i, D_{ijk} denote the probability of initiating event j due to definite external hazard i for unit k, $BExp_{ijk}$ denote the Boolean expression for j^{th} initiating event due to definite external hazard i for unit

k. For e.g., if we postulate three initiating events that affect units 1 & 2 and two initiating events that affect units 3 & 4, the Boolean expressions are as given in Table 4.3. In case of a definite external hazard, initiating events for the units can also arise indirectly, i.e., due to failure of shared SSCs between the units. The core damage expression for a definite external hazard induced indirect initiating event (due to failure of shared SSCs between the units) is denoted as $H_i(d_{iGjk}.BExp_{iGjk})$ where d_{iGjk} denotes the probability of initiating event j for unit k due to the impact of hazard i on the shared system group G. The Boolean expressions obtained due to indirect initiating events are presented in Table 4.4 with consideration of two such events for units 1 & 2 and one for units 3 & 4 (Figure 4.3).

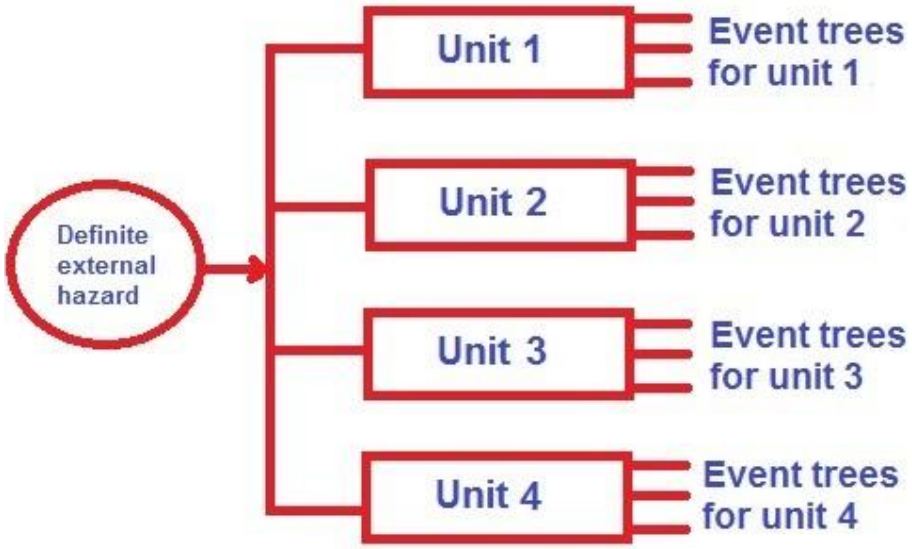

Figure 4.3: Schematic of definite external hazard for multi-unit site

Table 4.3: Boolean expressions for CDF due to direct initiating events induced by definite external hazard

Unit 1	Unit 2	Unit 3	Unit 4
H_1 ($D_{111}.BExp_{111}$)	H_1 ($D_{112}.BExp_{112}$)	H_1 ($D_{113}.BExp_{113}$)	H_1 ($D_{114}.BExp_{114}$)
H_1 ($D_{121}.BExp_{121}$)	H_1 ($D_{122}.BExp_{122}$)	H_1 ($D_{123}.BExp_{123}$)	H_1 ($D_{124}.BExp_{124}$)
H_1 ($D_{131}.BExp_{131}$)	H_1 ($D_{132}.BExp_{132}$)		

Table 4.4: Boolean expressions for CDF due to indirect initiating events induced by definite external hazard

Unit 1	Unit 2	Unit 3	Unit 4
H_1 ($d_{1A11}.BExp_{1A11}$)	H_1 ($d_{1A12}.BExp_{1A12}$)	H_1 ($d_{1B11}.BExp_{1B13}$)	H_1 ($d_{1B12}.BExp_{1B14}$)
H_1 ($d_{1A21}.BExp_{1A21}$)	H_1 ($d_{1A22}.BExp_{1A22}$)		

1. Four simultaneous core damage for the site can be obtained as the sum of { Boolean expression (core damage of unit 1 by any of its direct or indirect initiating events)* Boolean expression (core damage of unit 2 by any of its direct or indirect initiating events)* Boolean expression (core damage of unit 3 by any of its direct or indirect initiating events)* Boolean expression (core damage of unit 4 by any of its direct or indirect initiating events)}

   Total number of ways, four simultaneous core damages for the site can occur =

$$C_1^5 \times C_1^5 \times C_1^3 \times C_1^3 = 225$$

2. Three simultaneous core damage for the site is the sum of the following four expressions:

   A. Sum of {Boolean expression(core damage of unit 1)* Boolean expression (core damage of unit 2)* Boolean expression (core damage of unit 3)}

      Total number of such cases = $C_1^5 \times C_1^5 \times C_1^3 = 75$

   B. Sum of {Boolean expression(core damage of unit 1)* Boolean expression (core damage of unit 2)* Boolean expression (core damage of unit 4)}

      Total number of such cases = $C_1^5 \times C_1^5 \times C_1^3 = 75$

   C. Sum of {Boolean expression(core damage of unit 1)* Boolean expression (core damage of unit 3)* Boolean expression (core damage of unit 4)}

      Total number of such cases = $C_1^5 \times C_1^3 \times C_1^3 = 45$

   D. Sum of {Boolean expression(core damage of unit 2)* Boolean expression (core damage of unit 3)* Boolean expression (core damage of unit 4)}

      Total number of such cases = $C_1^5 \times C_1^3 \times C_1^3 = 45$

Therefore, number of ways three simultaneous core damage for the site can occur =

$$2.\left(C_1^5 \times C_1^5 \times C_1^3\right) + 2.\left(C_1^5 \times C_1^3 \times C_1^3\right) = 240$$

3. Similarly, number of two simultaneous core damage for the site =

$$\left\{\left(C_1^5 \times C_1^5\right) + 4.\left(C_1^5 \times C_1^3\right) + \left(C_1^3 \times C_1^3\right)\right\} = 94$$

4. And number of single core damage for the site =

$$C_1^5 + C_1^5 + C_1^3 + C_1^3 = 16$$

After simplification of Boolean expression for the cases of single, double, triple and quadruple core damage and quantification of the hazard and SSC failures, we get the value of corresponding site core damage frequency for a specific hazard. Repeating this process and summing CDFs for all definite external hazards of varying intensity, SCDF of a multi-unit site due to definite external hazards is obtained. Probability of multiple definite external hazards occurring simultaneously is very low and hence it is not considered.

4.5.5 Methodology for conditional external hazards

In this case also like the definite external hazards, each conditional external hazard induced initiating events are identified and corresponding ET and FT for each of the twin units are modelled together. If C_{ij} denote the probability of a conditional external hazard 'i' that directly affects unit j then C_{ijk} denote the probability that it affects unit k (k=1, 2, 3…n and k≠j) also. Then A_{ej} corresponds to conditional probability of initiating event e for the specified/particular unit k due to a direct impact of conditional external hazard. Also, c_{iG} denotes the probability of conditional external hazard i affecting shared systems group 'G' whereas p_{eGj} corresponds to conditional probability of initiating event e for unit j due to the indirect impact of corresponding conditional external hazard on shared systems group 'G'.

Case 1 & 2 below describes the analysis for single conditional external hazard and two simultaneously occurring conditional external hazards respectively, occurring at a site. Each conditional external hazard that impacts a pair of units is assumed to cause one direct

initiating event and two indirect initiating events. Tables 4.5 and 4.6 presents the Boolean expressions for conditional external hazards (Figure 4.4).

Case 1: Single conditional external hazard for any one pair of units

1. Four simultaneous core damage for the site due to a conditional external hazard = sum of all possible combinations { Boolean expression (core damage of all 4 units by the conditional external hazard)}

   Total number of ways four simultaneous core damage due to a conditional external hazards at the site = 0

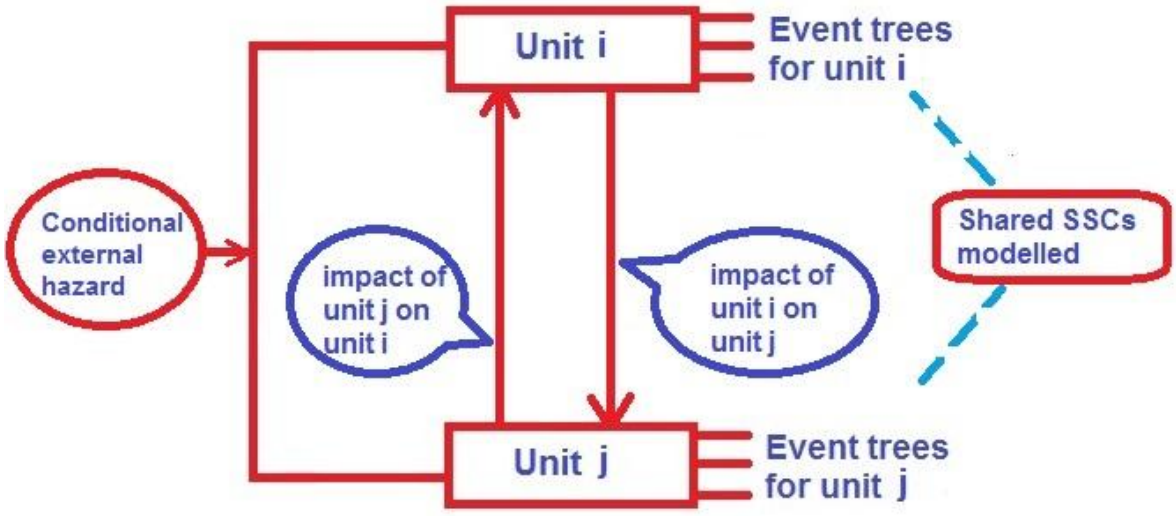

Figure 4.4: Schematic of single conditional external hazard at multi-unit site

Table 4.5: Boolean expressions for CDF due to impact of conditional external hazard on each of the units

Unit 1	Unit 2	Unit 3	Unit 4
H_1 (C_{11}.A_{11}.$BExp_{11}$)	H_1 (C_{112}. A_{12}. $BExp_{112}$)	H_2 (C_{23}. A_{13}. $BExp_{23}$)	H_2 (C_{234}. A_{14}. $BExp_{234}$)
H_1 (C_{121}. A_{11}. $BExp_{121}$)	H_1 (C_{12}. A_{12}. $BExp_{12}$)	H_2 (C_{243}. A_{13}. $BExp_{243}$)	H_2 (C_{24}. A_{14}. $BExp_{24}$)

H_i denote frequency of (conditional) external hazard i

Table 4.6: Boolean expressions for CDF due to impact of conditional external hazard on shared systems between the units

Unit 1	Unit 2	Unit 3	Unit 4
H_1 (c_{1A}.p_{1A1}.$BExp_{1A1}$)	H_1 (c_{1A}.p_{1A2}.$BExp_{1A2}$)	H_2 (c_{2B}.p_{1B3}.$BExp_{1B3}$)	H_2 (c_{2B}.p_{1B4}.$BExp_{1B4}$)
H_1 (c_{1A}.p_{2A1}.$BExp_{1A1}$)	H_1 (c_{1A}.p_{2A2}.$BExp_{1A2}$)	H_2 (c_{2B}.p_{2B3}.$BExp_{1B3}$)	H_2 (c_{2B}.p_{2B4}.$BExp_{2B4}$)

2. Three simultaneous core damage for the site due to a conditional external hazard is = sum of all possible combinations{Boolean expression(core damage of any three units by the conditional external hazard) }

   Total number of ways three simultaneous core damage due to a conditional external hazard at the site =0

3. Two simultaneous core damages for the site due to a conditional external hazard is = sum of all possible combinations {Boolean expression (core damage of any two units by the conditional external hazard)}

   Total number of ways two simultaneous core damage due to a conditional external hazard at the site = 20

4. Total number of ways single core damage for the site due to a conditional external hazard at the site = 12

Case 2: Two simultaneous conditional external hazards

Simultaneous occurrence of *conditional external hazards* is an extremely rare possibility but for the sake of completeness we consider the case of two conditional external hazards like aircraft crash and offsite explosion on twin unit pair-1 and twin unit pair-2 respectively. Same number of initiating events from each hazard are assumed and the table containing Boolean expressions for core damage remains similar for each hazard like that of Tables 4.5 and 4.6 (Figure 4.5).

1. Four simultaneous core damage for the site due to the two conditional external hazards = sum of all possible combinations {Boolean expression (core damage of all 4 units by the two conditional external hazards)}

This can occur due to all possible combinations of two CDFs from first hazard and 2 CDFs due to second hazard.

Total number of ways four simultaneous core damage due to the two conditional external hazards for the site = 124

2. Three simultaneous core damage for the site due to the two conditional external hazards is = sum of all possible combinations{Boolean expression(core damage of any three units by the two conditional external hazards)}

This can occur due to all possible combinations: one CDF from first hazard and 2 CDFs due to second hazard, two CDFs from first hazard and 1 CDF due to second hazard.

Total number of ways three simultaneous core damage due to the two conditional external hazards for the site =140

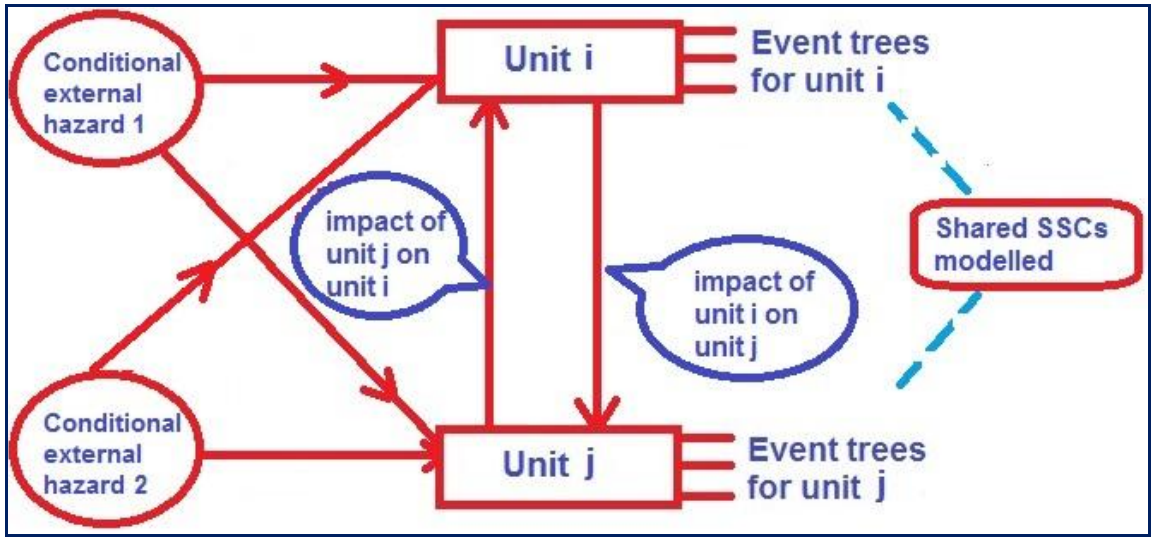

Figure 4.5: Schematic of two simultaneous conditional external hazards at multi-unit site

3. Two simultaneous core damage for the site = Sum of all possible combinations {Boolean expression(core damage of any two units by the two conditional external hazards)}

This can occur due to one CDF due to first hazard and one CDF due to second hazard or two CDF from any of the hazard.

Total number of ways two simultaneous core damage due to the two conditional external hazards for the site = 56

4. Total number of ways for single core damage due to two simultaneous conditional external hazards = 12

After simplification of Boolean expression for all possible ways of double, triple and quadruple core damage and quantification of the external hazard and SSC failures, risk for a multi-unit site due to conditional external hazards is obtained.

4.5.6 Methodology for definite internal initiating events for the site

All definite internal initiating events are to be modelled and analysed together. The event trees and fault trees are developed for these initiating events in the same manner as done for initiating events in case of definite external hazards (Figure 4.6).

If we consider one definite initiating event affecting units 1 & 2 and one definite initiating event affecting units 3 & 4, Boolean expression are obtained as shown in Table 4.7.

Table 4.7: Boolean expressions for CDF of each of the units for definite internal initiating events

Unit 1	**Unit 2**	**Unit 3**	**Unit 4**
Definite Initiating Event 1 affecting units 1 & 2		**Definite Initiating Event 2 affecting units 3 & 4**	
IE_1 ($BExp_{11}$)	IE_1 ($BExp_{12}$)	IE_2($BExp_{13}$)	IE_2 ($BExp_{14}$)

IE_i denote i^{th} initiating event

Further, if single initiating event is considered, two CDFs can occur in two ways and no other combination of core damage is possible. Simultaneous occurrence of multiple definite internal initiating events affecting multiple units is not considered as it is an extremely rare event.

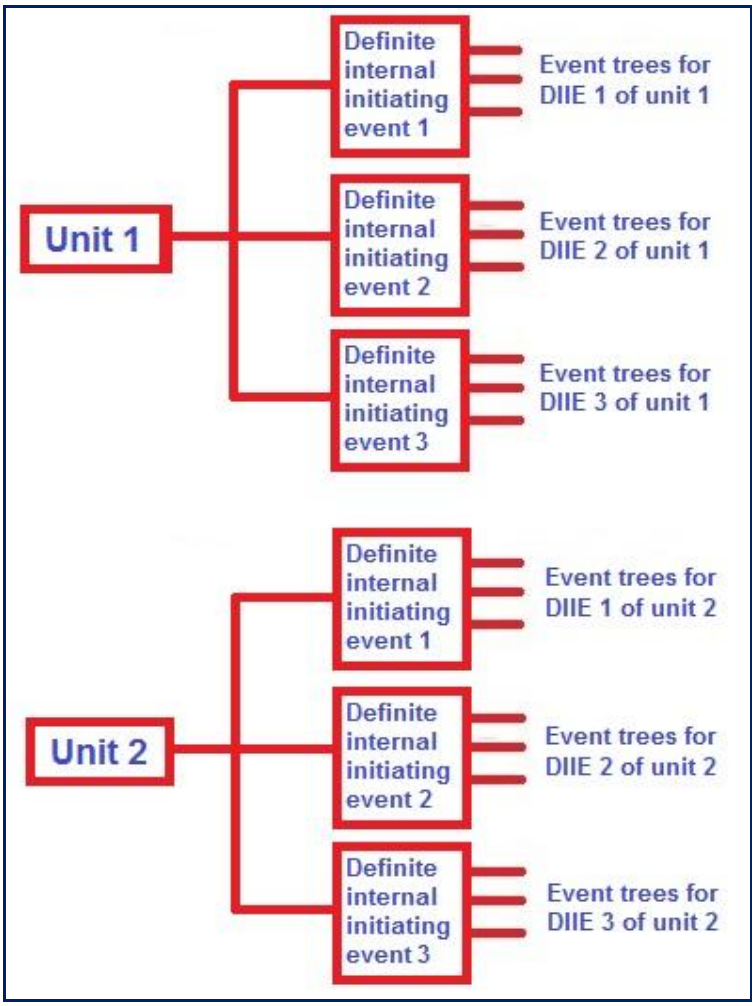

Figure 4.6: Schematic of definite internal initiating events at multi-unit site

4.5.7 Methodology for conditional internal initiating events for the site

All conditional initiating events are to be modelled together for all units. As in the earlier cases, here also number of Boolean expression for single and multiple core damage are analysed with conditional internal initiating events under both scenarios, i.e., one conditional internal initiating events occurring at the site and more than one conditional internal initiating events occurring simultaneously on the site . Methodology for obtaining various core damage configurations in this case is explained with an example.

Consider three conditional internal initiating events

1. Loss of instrument air
2. Loss of feed water

3. Loss of DC bus

As done earlier, for illustration purpose, let us consider units 1& 2 to be identical and have some sharing of resources (e.g. instrument air and feed water) and units 3 & 4 are identical and have sharing of resources (e.g. DC bus) (Figure 4.7). Case 1 describes the analysis for single conditional internal initiating event and Case 2 describes the analysis for multiple conditional internal initiating events occurring simultaneously at a site. The two variables defined are IE_{iG} denoting the frequency of conditional internal initiating event i for the shared systems group 'G' and P_{iGk} which represents the probability of conditional internal initiating event i affecting shared systems group 'G' affects unit k. The Boolean expressions for corresponding conditional internal initiating events are shown in Table 4.8.

Table 4.8: Boolean expressions for CDF of each of the units for conditional internal initiating events

Unit 1	**Unit 2**	**Unit 3**	**Unit 4**
Cond. Initiating Event 1 for Units 1&2		**Cond. Initiating Event 3 for Units 3&4**	
P_{1A1} IE_{1A} ($BExp_{1A1}$)	P_{1A2} IE_{1A} ($BExp_{1A2}$)	P_{1B3} IE_{1B} ($BExp_{1B3}$)	P_{1B4} IE_{1B} ($BExp_{1B4}$)
Cond. Initiating Event 2 for Units 1&2			
P_{2A1} IE_{2A} ($BExp_{2A1}$)	P_{2A2} IE_{2A} ($BExp_{2A2}$)		

Case 1: Single conditional internal initiating event occurring at the site

1. Four simultaneous core damages on the site due to single *conditional internal initiating event is not possible as one initiating event affects a maximum of two units only.*
2. Similarly, three simultaneous core damages on the site due to single *conditional internal initiating event is also not possible.*
3. Two simultaneous core damage for the site can occur in the following three ways
   A. Sum of all possible combinations {Boolean expression (core damage of unit 1 by the single *conditional internal initiating event*)* Boolean expression (core damage of unit 2 by the single *conditional internal initiating event*)}

      Total number of combinations = 2

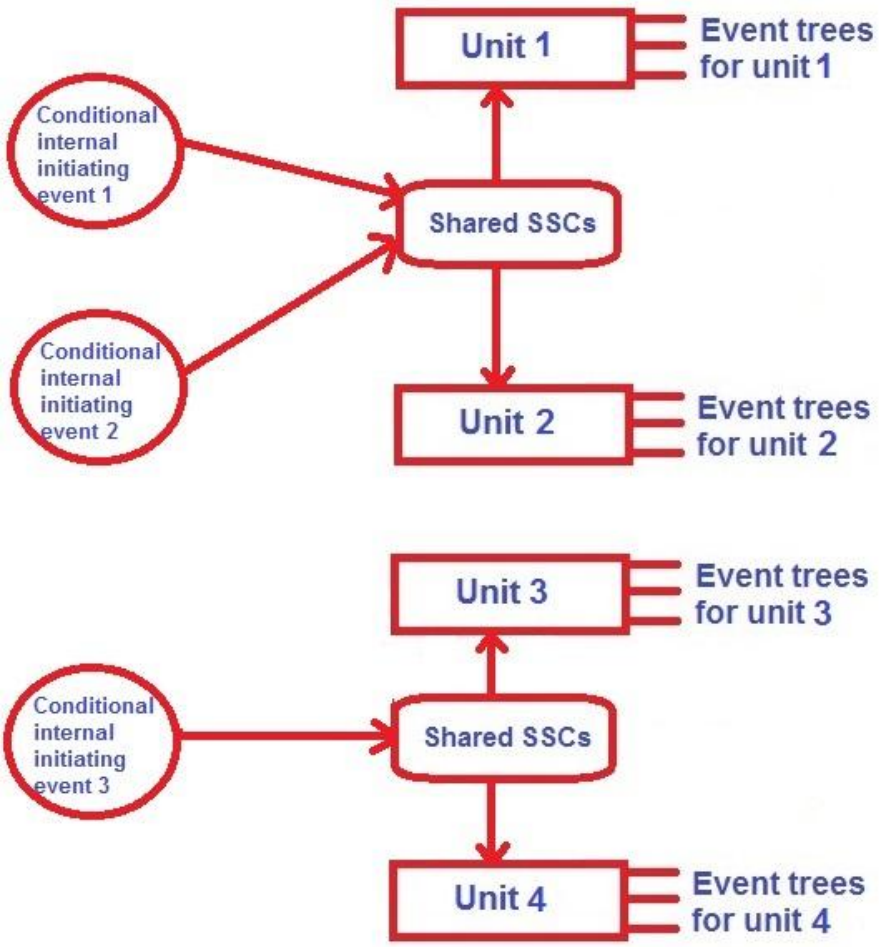

Figure 4.7: Schematic of conditional internal initiating events at multi-unit site

B. Sum of all possible combinations {Boolean expression (core damage of unit 3 by the one single *conditional internal initiating event*)* Boolean expression (core damage of unit 4 by the single *conditional internal initiating event*)}

Total number of combinations = 1

4. Single core damage on the site due to single *conditional internal initiating event* can occur in 6 ways.

After simplification of Boolean expression for the cases of single, double, triple and quadruple core damage and quantification of internal initiating event and SSC failures, risk due to conditional internal initiating events for the site is obtained.

Case 2: Multiple conditional internal initiating events occurring simultaneously on the site.

If all three IEs occur simultaneously, then

1. Four simultaneous core damages is sum of all possible combinations {Boolean expression (core damage of all 4 units by respective conditional initiating events)}

   Total number of ways four simultaneous core damages for the site = 4

2. Three simultaneous core damage for the site due to the three conditional internal initiating events is the sum all possible combinations {Boolean expression(core damage of any three units by the three conditional initiating event) }

   This can occur due to all possible combinations: one CDF from first / second IE and two CDFs from third IE or two CDFs from first/second IE and one CDF from third IE.

   Total number of ways three simultaneous core damage due to the three conditional internal events for the site = 12

3. Two simultaneous core damage for the site due to the three conditional internal initiating events is the sum all possible combinations {Boolean expression(core damage of any two units by the two conditional initiating event) }

   This can occur due to all possible combinations: Two CDFs from first / second IE or two CDFs from third IE or one CDF from first/second IE and one CDF from third IE.

   Total number of ways two simultaneous core damage due to the three conditional internal events for the site = 13

4. Total number of ways single core damage for the site due to three conditional internal events for the site = 6

After simplification of Boolean expression for the cases of single, double, triple and quadruple core damage and quantification of internal initiating events and SSC failures, risk due to multiple conditional internal initiating events for the site is obtained.

4.5.8 Methodology for internal independent events

Event Trees and corresponding fault trees developed for internal Level-1 PSA are used and the Boolean expressions are obtained (Table 4.9) to evaluate single core damage frequency only, since occurrence of multiple internal independent events is an extremely rare possibility.

Total number of ways for single core damage on the site due internal independent events in all units = sum of all the Boolean expressions in Table 4.9 = 14

Table 4.9: Boolean expressions for CDF of each of the units due to internal independent events

Unit 1	Unit 2	Unit 3	Unit 4
IE_{11} ($BExp_{11}$)	IE_{12} ($BExp_{21}$)	IE_{31}($BExp_{13}$)	IE_{14} ($BExp_{14}$)
IE_{21} ($BExp_{21}$)	IE_{22} ($BExp_{22}$)	IE_{32}($BExp_{23}$)	IE_{24} ($BExp_{24}$)
IE_{31} ($BExp_{31}$)	IE_{32} ($BExp_{32}$)	IE_{33}($BExp_{33}$)	IE_{34} ($BExp_{34}$)
IE_{41} ($BExp_{41}$)	IE_{42} ($BExp_{42}$)		

IE_{ij} denote the i^{th} initiating event for unit j

4.5.9 Complete expression for Site Core Damage Frequency

The integrated approach explained in earlier sections for multi-unit safety assessment considering all categories of hazards is depicted in Figure 4.8. Extended mission time as appropriate may be used for accident sequences in case of external hazards and for internal events mission times used in internal PSA may be adopted. Thus, the integrated approach presented in this work leads to the formulation of site core damage frequency from equation (4.1) as follows:

The risk for a single unit site is the total CDF obtained from internal events and external hazards whereas the risk for twin unit site is obtained as SCDF by summing the risk from all the categories of external hazards and internal events. SCDF is expressed as:

$$\text{Site CDF for Single Unit} = \sum_{i=1}^{2}\sum_{j=1}^{m} CDF(i,j) \tag{4.2}$$

$$\text{Site CDF for Multi unit} = \sum_{i=1}^{5}\sum_{j=1}^{m}\sum_{k=1}^{n} CDF(i,j,k) \tag{4.3}$$

where

i denote the category of hazard or event

j denote the type of hazard in i^{th} category

m denote the total number of types of hazard in i^{th} category.

k denote the number of simultaneous core damages

n denotes the number of units at the site

Therefore, CDF (i, j, k) denotes the frequency of k number of simultaneous core damages due to j type of hazard in i^{th} category;

For a single unit site, i denote external and internal event whereas for multi-unit site,

i=1 refers to definite external hazards for the site

i=2 refers to conditional external hazards for the site

i=3 refers to definite internal events for the site

i=4 refers to conditional internal events for the site

i=5 refers to internal independent events considering for all units

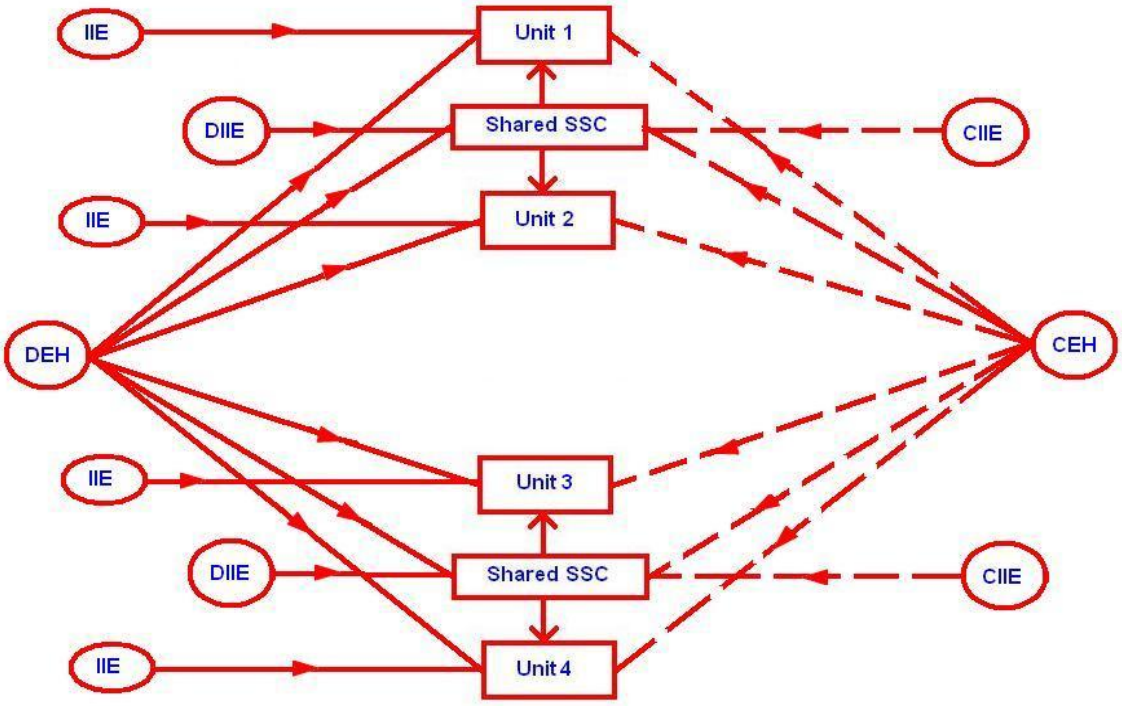

Figure 4.8: Overall schematic for multi-unit safety assessment

4.6 CONCLUSIONS

A holistic risk-informed approach is demonstrated to assess the safety of a multi-unit nuclear power plant site. It not only quantifies the frequency of multiple core damage for a multi unit site but also evaluates site CDF considering both external and internal hazards. The methodology proposed accounts for most of the dependency classes and key issues applicable for a multiple unit NPP site such as initiating events, shared connections, identical components, proximity dependencies and human dependencies.

The outcome of such integrated PSA will help in identification of those structures, systems and components (SSCs) that play important role in safety of multiple units. It will also provide additional severe accident scenarios for carrying out Level-2 PSA studies for the multi-unit site. Finally, the approach developed is expected to be useful in developing safety goals, procedures and guidelines for a multi-unit NPP site.

CHAPTER-5

INTEGRATED RISK ASSESSMENT FOR MULTI-UNIT NPP SITES – A COMPARISON

5.0 INTRODUCTION

In this chapter, the integrated approach as proposed in the previous chapter is used to estimate and compare the risk from multi unit sites housing single, double, triple and quadruple nuclear plants. The approach is realistic as it addresses all possible accident scenarios that can result from different hazards and is demonstrated with typical initiating events. Finally, the approach developed quantifies the risk for a multi-unit NPP site and evaluates the risk metric, site core damage frequency (SCDF). SCDF is overall risk associated with the site obtained by means of integrating the risk of core damage in more than one unit at the site. In other words, it is the frequency of at least single core damage per site per year with consideration of various interdependencies. The study when extended, through sensitivity analysis can form the basis to optimize the shared resources effectively at the multi-unit sites. The spin-off from such a study carried out during the design stage will provide an input to decide the optimum number of units at a site, the optimal distance between two units, layout diversity and configuration of shared systems, etc.

5.1 SAFETY GOALS

The general nuclear safety objective is to protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations effective defences against radiological hazards. This is supported by ensuring that in all operational states, the radiation exposure is kept below prescribed limits and as low as reasonably achievable and by providing reasonably practicable measures to prevent accidents in nuclear installations and to mitigate their consequence if they occur. Safety goals of an NPP arrived at based on the

above objectives from high level qualitative statements to probabilistic safety criteria such as core damage frequency (CDF) should be less than 10^{-5} per reactor year for new plants and less than 10^{-4} per reactor year for existing plant (INSAG-12, 1999).However, specific safety goal for a multi-unit site is not prescribed. In the absence of probabilistic safety goals for multi-unit risk assessment, the targets specified for a single NPP is considered applicable for a multi-unit site also irrespective of the number of units at a site. As the target for plant CDF is derived based on a comparison with risk from all other sources and with an objective to keep the doses as low as reasonably achievable for the public and environment, maintaining the target for a multiple unit site as same as that of a single unit is justified.

5.2 INTEGRATED RISK ASSESSMENT METHODOLOGY

For an integrated risk assessment at a multi-unit site, hazards are categorized as definite and conditional (Schroer and Modarres, 2013; IAEA, 2011; Zerger et al., 2013). The hazards that will always affect multiple units are called definite hazards and those which only under certain circumstances affect multiple units are called conditional hazards. After the initiating events for external hazards and internal events are identified and categorized, event tree / fault tree models are developed for each hazard category for further analysis. Schroer and Modarres (Schroer and Modarres, 2013) have identified the key issues which need to be addressed while modelling event trees and fault trees for a multi-unit site safety assessment. The issues are classified as shared systems or connections, identical components, human dependencies and proximity dependencies. The issues account for dependencies between the units arising from shared physical links, similarity in the design, installation and operational approach for a component / system, same or related environment of positioning the systems and associated dependencies for various human interactions. The schema proposed by Schroer and Modarres is further developed and an integrated approach to address both

external and internal events that can affect a single / multiple units at a site is described in this work. A pictorial representation of the proposed methodology is given in Figure 5.1. Examples of definite external hazard (DEH), conditional external hazard (CEH), definite internal initiating event (DIIE), conditional internal initiating event (CIIE) and internal initiating event (IIE) are discussed in the chapter 4 of the thesis.

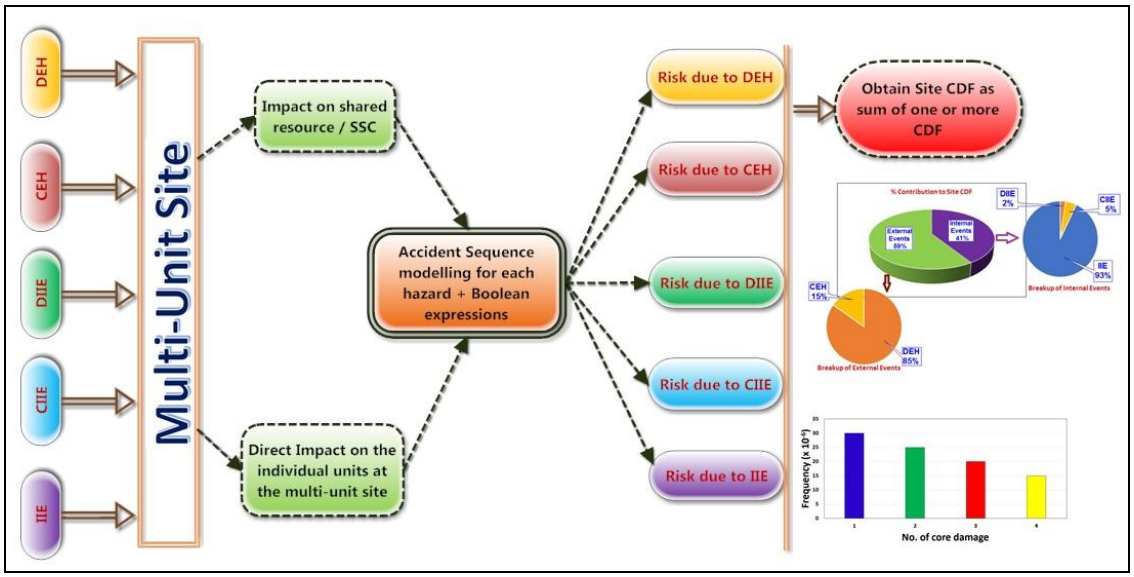

Figure 5.1: Schematic of method for multi-unit risk assessment

5.2.1 Important aspects in Multi-Unit Risk Assessment

In addition to the direct damage that may be caused to an NPP, called primary effect, there may be indirect damage by means of failure mechanisms that can propagate the damage. This indirect damage is referred to as a secondary effect (IAEA SS-50-SG-D4, 1980). The secondary effects may cause damage more than that of primary effect. To avoid secondary failures that could increase the safety-related consequences of the primary event, structures, systems and components (SSCs) important to safety are designed to accommodate the effects of accident conditions of the plant. These SSCs shall be appropriately located or protected against dynamic effects, including the effects of missiles, pipe whipping and discharging fluids and flooding that may result from equipment failures (AERB Safety Guide, 2013)

Some of the key issues that require special attention in multi-unit risk assessment include appropriate use of mission time, cliff-edge effects especially during external hazards, modelling of shared components, common cause failures of identical components and interaction effects due to proximity. Modelling of these key issues in the present study is explained in section 5.2.2.

5.2.2 Modelling of Key Issues

Mission Time: The mission time for accident sequences of various hazards is decided based on the nature and severity of the hazard. A mission time of 72 hr is taken for external hazards, i.e., earthquake, tsunami, clogging, etc. whereas a mission time of 24 hr is selected for all the internal events.

Cliff Edge Effect: The cliff edge effect has been modelled for all the sites while estimation of risk from the tsunami hazard. During external flooding due to tsunami, if the flood level exceeds the height of the component, the fragility of all the components located below the flood level is taken as unity and for those components above the level fragility is zero.

Shared Systems/Components:

a) **Same SSC shared between the units:** This sharing exists for diesel engines and compressors. Here, the systems/components are modelled with same identity in the fault trees/event trees of the corresponding units where they are shared (Figure 5.2).

b) **Standby System Sharing:** Sharing of resource in a multi-unit site is modelled by assigning preference probability of the component / system for a particular unit (Schroer and Modarres, 2013). For eg., if a common DG is shared between two units and the first unit is assigned with a preference probability of 0.75, DG unavailability for unit 1 (DG_{u1}) is estimated as

$$DG_{U1} = (1 - Pf_{u1}) + (Pf_{u1} * P_{DG})$$

and DG unavailability for unit 2 (DG_{u2}) is

$$DG_{U2} = Pf_{u1} + (1 - Pf_{u1}) * P_{DG}$$

where Pf_{u1} is preference probability for unit 1 and P_{DG} is the probability of DG failure.

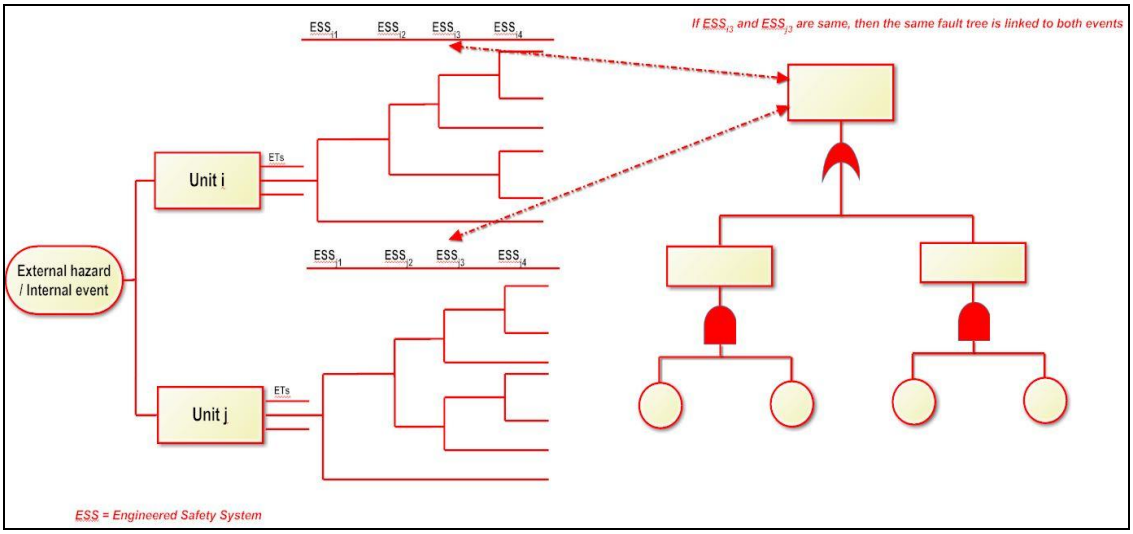

Figure 5.2: Modelling of common shared system between two units

Identical Components: The identical components in both the units like shutdown cooling pumps, emergency core cooling pumps, diesel generator and emergency process sea water pumps are grouped under common cause failures (CCF) for which beta factor model is used. The grouping of the identical components and the value of the beta factor is based on the nature and severity of the hazard. In our study, simultaneous failure of identical components for both the units is considered only for DEH.

Proximity Dependencies: The components which share the same operating environment or failure of components that can induce failure of the other nearby components are grouped together under CCF and beta factor is used. This modelling has been done for emergency process sea water pumps.

5.3 COMPLETE EXPRESSION FOR SITE CORE DAMAGE FREQUENCY

The integrated approach explained in earlier sections for multi-unit safety assessment considering all categories of hazards is depicted in Figure 5.3. Extended mission time as

appropriate may be used for external hazards and mission times used in internal PSA may be adopted for internal events.

The risk for a single unit site is the total CDF obtained from internal events and external hazards whereas the risk for twin unit site is obtained as SCDF by summing the risk from all the categories of external hazards and internal events. SCDF is expressed as:

$$\text{Site CDF for Single Unit} = \sum_{i=1}^{2}\sum_{j=1}^{m} CDF(i,j) \tag{5.1}$$

$$\text{Site CDF for Multi unit} = \sum_{i=1}^{5}\sum_{j=1}^{m}\sum_{k=1}^{n} CDF(i,j,k) \tag{5.2}$$

where

i denote the category of hazard or event

j denote the type of hazard in i^{th} category

m denote the total number of types of hazard in i^{th} category.

k denote the number of simultaneous core damages

n denotes the number of units at the site

Therefore, CDF (i, j, k) denotes the frequency of k number of simultaneous core damages due to j type of hazard in i^{th} category;

For a single unit site, i denote external and internal event whereas for multi-unit site,

i=1 refers to definite external hazards for the site

i=2 refers to conditional external hazards for the site

i=3 refers to definite internal events for the site

i=4 refers to conditional internal events for the site

i=5 refers to internal independent events considering for all units

SCDF accounts for both single and multiple core damages occurring at the site. The proposed method for quantification is explained in the subsequent sections.

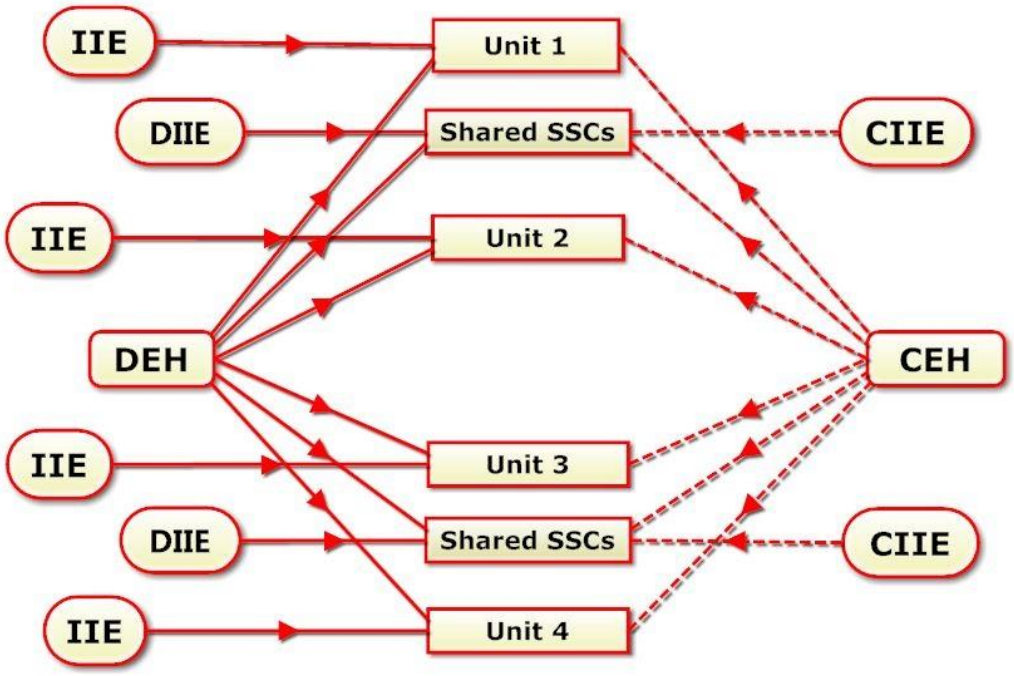

Figure 5.3: Overall schematic for multi-unit safety assessment

5.4 DESCRIPTION OF MULTI-UNIT SITES

Generally, at a multi-unit site more than one unit have identical design, for e.g., in India, multi-unit sites have more number of Pressurised Heavy Water Reactors (PHWRs). The main engineered safety systems in a typical PHWR are:

Reactor Protection System: Each unit is equipped with two diverse and independent shutdown systems:

- Primary Shutdown System: The system consists of mechanical shutoff rods which get quickly inserted in the reactor core following a reactor trip signal under the action of gravity and initially assisted by a spring thrust (Bajaj and Gore, 2005).
- Secondary Shutdown System: It consists of vertical empty tubes located in the reactor core into which liquid poison is injected whenever the system is called upon due to a trip signal (Bajaj and Gore, 2005).

Shutdown Cooling System: The shutdown cooling system of the NPP is comprised of two cooling trains. The trains take the decay heat away from the reactor core. Each train is having one shutdown cooling pump (SDCP) and one shutdown heat exchanger (SDHX) which dissipates its heat to the process water. Emergency process sea water pumps are used to circulate process sea water through the process sea water heat exchangers in once through mode to vent out the heat to the sea. A typical PHWR is equipped with two dedicated process sea water heat exchangers and three emergency process sea water pumps. Successful operation of any one heat exchanger and pump is sufficient to meet the post shutdown heat loads.

Emergency Core Cooling System: This system is deployed to remove the decay heat from the core of the reactor in order to mitigate the consequences of Loss of Coolant Accident (LOCA) in the rare event of break in primary circuit pressure boundary. The emergency core cooling system (ECCS) operates in two phases. In the first phase of operation, high pressure heavy water from accumulators is injected into the reactor core via headers whereas in the second phase (recirculation phase), water is taken up from the suppression pool and is injected into the reactor after passing it through the ECCS Heat Exchangers. The ECCS Heat Exchangers transfers its heat to the process sea water heat exchanger with the help of process water and is vent out to the sea with the help of emergency process sea water pumps.

Apart from these engineered safety systems the plant is also equipped with other safety support equipments, systems and infrastructure. The configuration of these support systems is site specific as sharing for them takes place between the units at a multi-unit site. The description of such systems and their structure/configuration in a typical Indian multi-unit site is provided as follows:

Diesel Engines: These are meant for fire water injection. Successful operation of one diesel engine will ensure sufficient supply of water for the decay heat removal of maximum two units.

Diesel Generators: These are deployed to take the emergency loads of the NPP like Decay Heat Removal (DHR), emergency lighting, egress lighting system lamps and for charging AC UPS System and DC control power supply systems. Operation of one diesel generator is sufficient for meeting all the emergency loads of a single unit.

Sea Water Pump house: The sea water pump house deployed at the site houses condenser cooling water, process sea water and emergency process sea water pumps for both the units. The five condenser cooling water pumps and the three process sea water pumps which are installed for each NPP are driven by class 4 power supply. But the three dedicated emergency process sea water pumps are driven by class 3 power supply and availability of any one of them will ensure sufficient supply of water for DHR of a single unit.

Switchyard: The NPP is connected to the electrical grid system for class 4 power through a switchyard which also facilitates export of plant generated electric power to the grid.

Sea Water Intake tunnel: This tunnel provides sea water to the NPPs which serves as the ultimate heat sink.

Compressed Air System: The site has a compressed air station for supplying compressed air to the NPPs. Operation of one compressor ensures sufficient supply of all air (Instrument, Service and Mask air) for a single unit.

In this work, a case study of one, two, three and four unit sites is carried out. Event trees and fault trees are developed to estimate site core damage frequency for each of the four sites. The configuration of the critical infrastructure for the multiunit site housing up to four units is described in Table 5.1 and a schematic of multi-unit sites is given in Figures 5.4a-

5.4d. When a system with n redundant component requires at least k out of the n component to successfully function for the system to function, the success criteria is denoted as k/n:S.

Table 5.1: Various Systems, Structures and Components / Safety Support Systems for the multi-unit sites

Systems, Structures and Components / Safety Support Systems	Success Criteria			
	Single Unit Site	**Twin Unit Site**	**Three Unit Site**	**Four Unit Site**
Diesel Generators	1/3:S	1/3:S for each of the two units	1/3:S for each of the two units and 1/3:S for the third unit	1/3:S for each of the first two units and 1/3:S for each of the next two units
Diesel Engines	1/2:S	1/4:S	1/4:S for the two units and 1/2:S for third unit	1/4:S for the first two units and 1/4:S for the next two units
Switchyard Buses	1/2:S	2/3:S	2/3:S for the two units and 1/2:S for the third unit	2/3:S for the first two units and 2/3:S for the next two units
Compressors	1/2:S	2/4:S	2/4:S for the two units and 1/2:S for the third unit	2/4:S for the first two units and 2/4:S for the next two units
Sea Water Intake Tunnel	1	1	1 for the two units and 1 for the third unit	1 for the first two units and 1 for the next two units

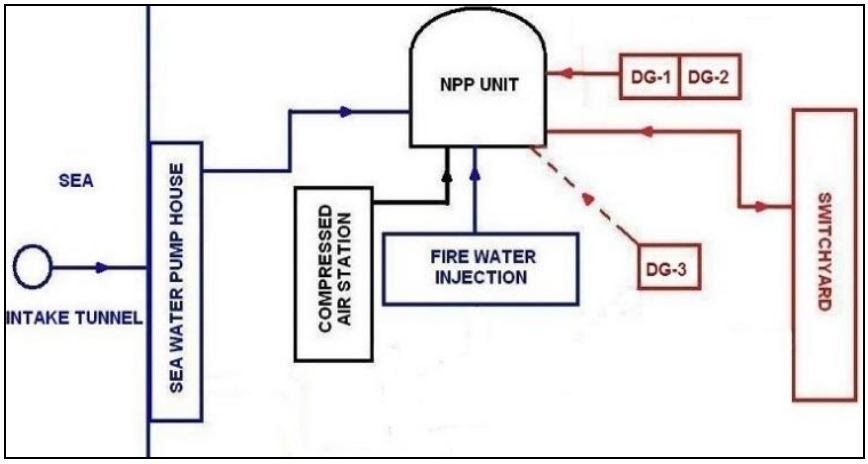

Figure 5.4a: Schematic of single unit PHWR site

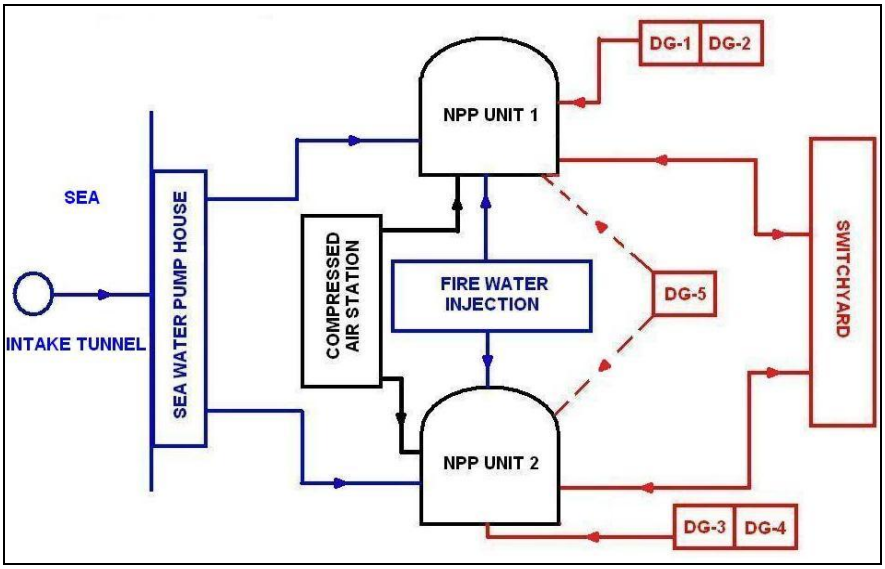

Figure 5.4b: Schematic of single unit PHWR site

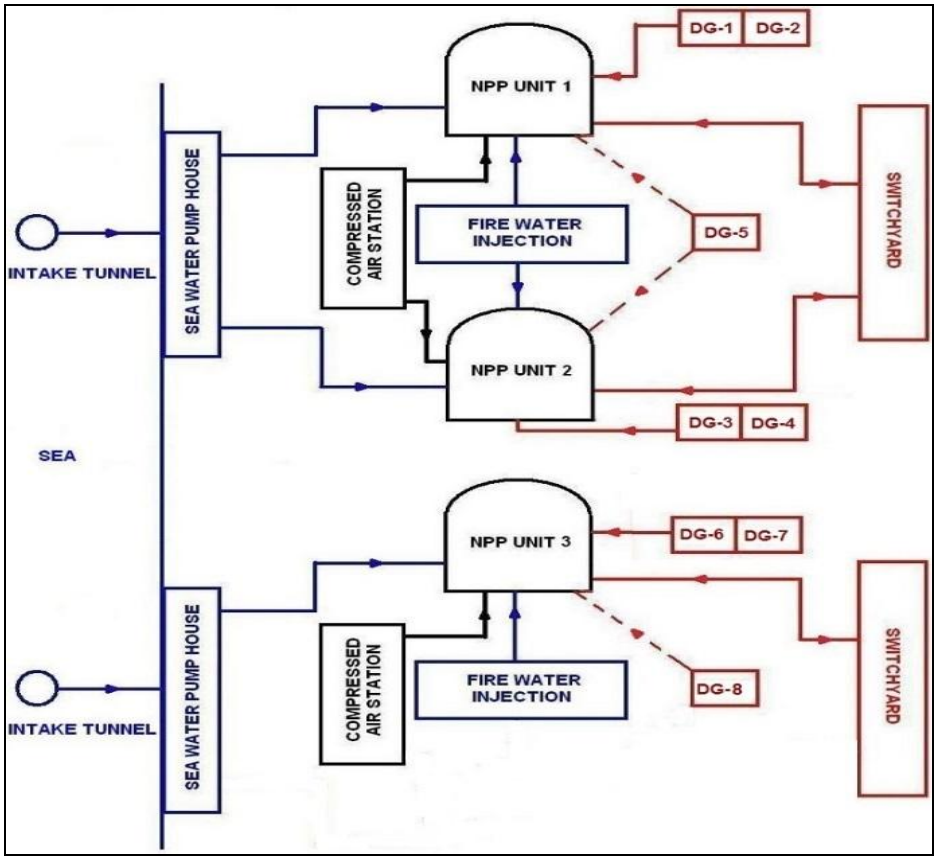

Figure 5.4c: Schematic of three unit PHWR site

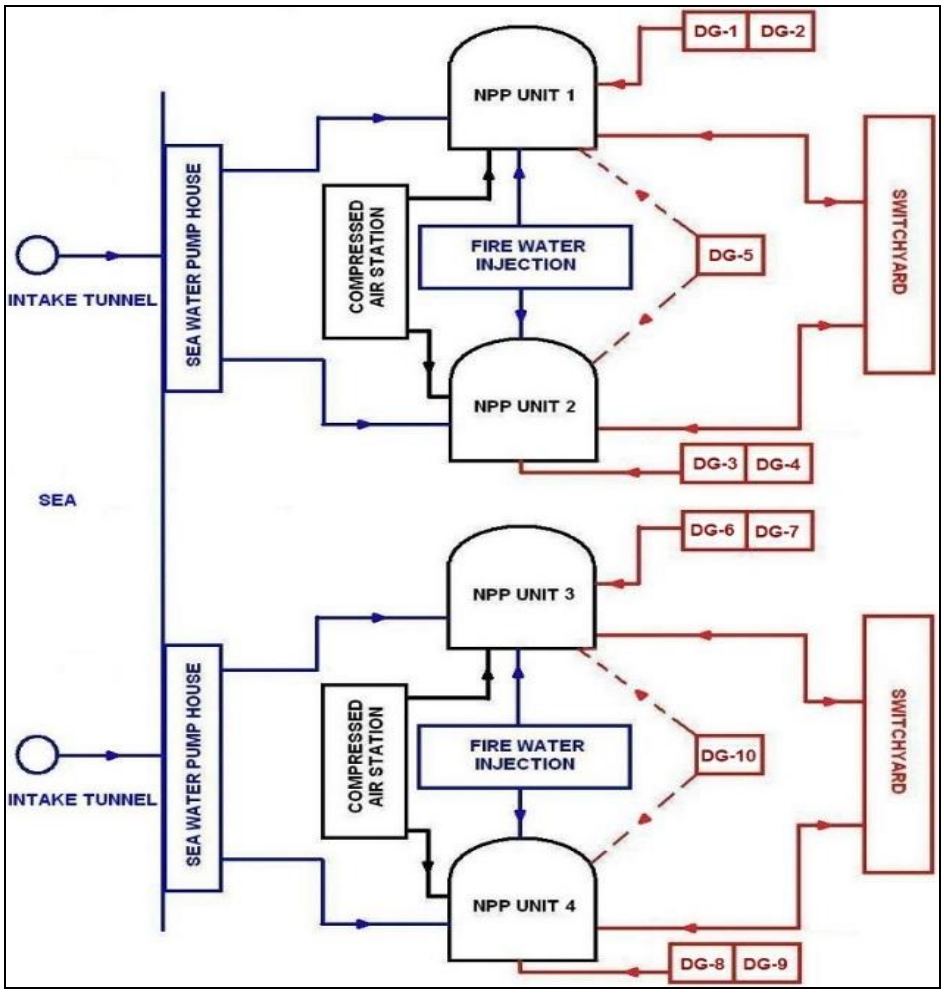

Figure 5.4d: Schematic of four unit PHWR site

5.5 MULTI UNIT RISK ASSESSMENT

5.5.1 Estimation of component failures

Hazards, initiating events and key issues modelled are listed in Table 5.2. The list is not comprehensive as only selected representative events considered in the study for demonstration of the methodology are shown.

Table 5.2: Hazards, initiating events and key issues modelled

Category of Hazard in		Hazard	Initiating Event	Key Issues Modelled	
Single Unit	**Multi Unit**			**Single Unit**	**Multi Unit**
External Hazards	Definite External Hazards (DEH)	Earthquakes	Loss of offsite power	• Mission Time • Proximity Dependencies	• Mission Time • Proximity Dependency • Shared SSC • Identical Components
		Tsunami	Loss of offsite power	• Cliff Edge Effect • Mission Time • Proximity Dependencies	• Cliff Edge Effect • Mission Time • Proximity Dependency • Shared SSC • Identical Components
	Conditional External Hazards (CEH)	Clogging in intake tunnel	Loss of ultimate heat sink	• Mission Time • Proximity Dependencies	• Mission Time • Proximity Dependency • Shared SSC
Internal Events	Definite Internal Initiating Events (DIIE)	--	Loss of offsite power	• Mission Time • Proximity Dependencies	• Mission Time • Proximity Dependency • Shared SSC
	Conditional Internal Initiating Events (CIIE)	--	Loss of instrument air		• Mission Time • Proximity Dependency • Shared SSC
	Internal Independent Events (IIE)	--	Primary-LOCA		• Mission Time • Proximity Dependency • Shared SSC
		--	TOPA / LORA		• Mission Time • Proximity Dependency • Shared SSC

5.5.2 Estimation of fragility for external hazards

External events have emerged as significant risk contributors to NPPs and Fukushima accident has revealed the potential of an extreme external event to damage redundant and diverse safety systems. A list of external events to be considered for NPP is given in (NUREG/CR-2300, 1983) For external hazards like earthquake and tsunami, independent accident sequences are to be developed to model failures due to external hazard. The modelling must also include internal random failures in addition to seismic / tsunami fragility. The fragility of all the SSC at a multi-unit is estimated as per the nature and severity of the hazard and is discussed below.

Seismic Fragility: For earthquakes, the entire spectrum of magnitude applicable for the site is divided into several ranges of magnitude and risk is calculated for each range. The objective of fragility evaluation is to estimate the PGA value for which the seismic response of a given component located at a specified point in the structure exceeds the component capacity resulting in its failure. Estimation of this ground acceleration value, called the ground acceleration capacity of the component, is accomplished using information on plant design bases, responses calculated at the design and analysis stage, and as-built dimensions and material properties. Because there are many sources of variability in the estimation of this ground acceleration capacity, the component fragility is described by means of a family of fragility curves. A probability value is assigned to each curve to reflect the uncertainty in the fragility estimation, usually in terms of non-exceedance probability (USNRC, 1983). The mean fragility of the component is estimated using:

$$P(A \leq a) = \varphi\left(\frac{1}{\beta_c}\ln\left(\frac{a}{A_m}\right)\right) \tag{5.3}$$

where A_m is the median ground acceleration capacity, 'a' is the peak ground acceleration (PGA) value for which probability of failure (P) is determined and $\beta_C = \sqrt{\left(\beta^2{}_R + \beta^2{}_U\right)}$

(Kennedy et al., 1984, Reed et al., 1994) where β_r and β_u represent the logarithmic standard deviations of aleatory and epistemic uncertainty respectively.

Tsunami Fragility: A probabilistic approach is necessary for evaluating tsunami hazard due to the inherent uncertainties associated with the estimation of run-up heights along the coastal areas and the random behaviour of nature. The maximum run-up height at the site is estimated based on historical data and the site specific bathymetry. Fragility analysis requires a clear understanding of what constitutes failure of the structure / element / component. A methodology of tsunami PSA was developed by (Kim et al. 2012). Several modes of failure may have to be considered and fragility curves may have to be developed for each of these modes. For a detailed analysis, failure modes such as Loss of structural integrity through collapse, sliding, overturning, excessive impact, submergence due to flooding, sprays, flow through openings are studied. For simplicity, submergence and failure of support structure are considered for our study:

a) Failure of the component due to submergence: In this case, if the component is fully submerged, the component fragility is taken as unity. If the flooding level is equal to component height then the fragility is taken as 0.1 (Takeshi M., 2011) and for the case when the component is above the flooding level, its fragility is taken to as zero.
b) Failure of the component due to loss of support structure: In this case for a given run-up height, the equipment failure probability is taken as the fragility of the support structure.

Clogging of the intake tunnel: Although the phenomenon of clogging of intake tunnel is external, the components of the NPP may become unavailable only due to internal random failures during that time. Hence, internal event data is used for this hazard.

Internal Events: In the case of internal events, random failure probabilities of the components are only considered.

5.5.3 Comparison of risk in multi-unit sites

Following the approach explained in previous sections event trees and fault trees are developed for multi-unit sites housing one, two, three and four NPPs. Site core damage frequency for each of the four sites is estimated and compared.

Assumptions:

- Each of the site is equipped with identical PHWR.
- The plant is equipped with the following engineered safety systems as described.
    - Shutdown system comprising of two redundant paths
    - Decay heat removal system
    - Power supply system
    - Other auxiliary support systems such as sea water pump house, fire water injection system, switchyard, compressed air system, sea water intake tunnel.

These assumptions are made considering the system configuration present in a typical multi-unit site.

Applying the method explained in earlier sections and by using generic component failure probabilities and frequencies of external and internal events, the core damage frequency of each of a four unit site is obtained and shown in Table 5.3 & Figure 5.5. The results indicate that a simple aggregation of single unit CDF do not represent the multi-unit CDF. It is also clear that single unit risk metrics do not capture the correlation effects and cannot be manipulated to capture integrated risk of multi-unit site.

Table 5.3: Comparison of Site CDF

	No. of units in the site			
	One	**Two**	**Three**	**Four**
SCDF	2.86E-05	1.78E-04	2.24E-04	4.03E-04
Single CDF	2.86E-05	1.66E-04	1.95E-04	3.32E-04
Double CDF		1.18E-05	2.23E-05	4.27E-05
Three CDF			6.53E-06	2.38E-05
Four CDF				4.93E-06

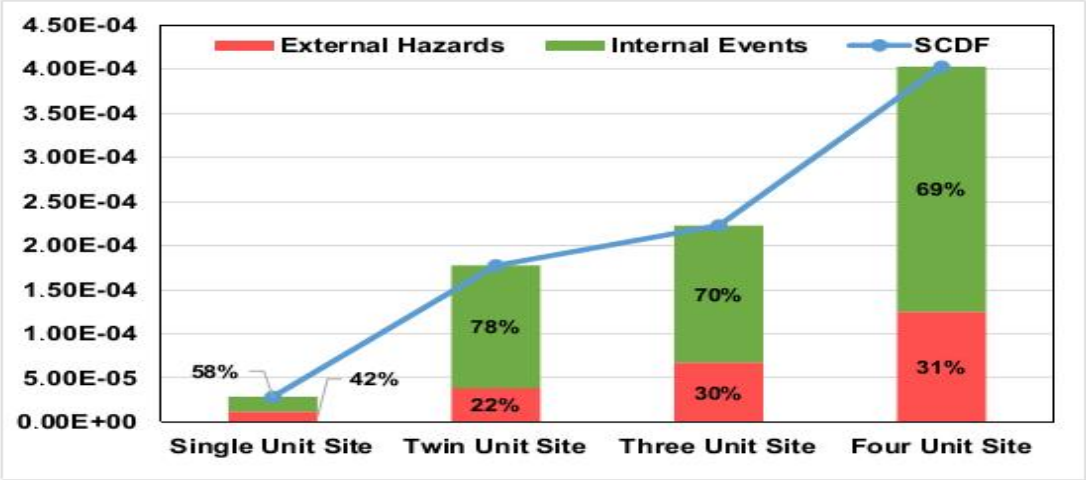

Figure 5.5: Distribution of multiple core damages

Site CDF is defined as the cumulative sum of single and multiple core damages. The breakup of multiple core damages in multi-unit site is depicted in Figure 5.6.

Figure 5.6: Site CDF in multi-unit NPPs

The site core damage frequency increases with increasing number of units located at the site. As expected, the major contributors are the shared resources and common cause failures of identical components. For the sites with more than 1 unit, the contribution of external hazards to site CDF show an increasing trend.

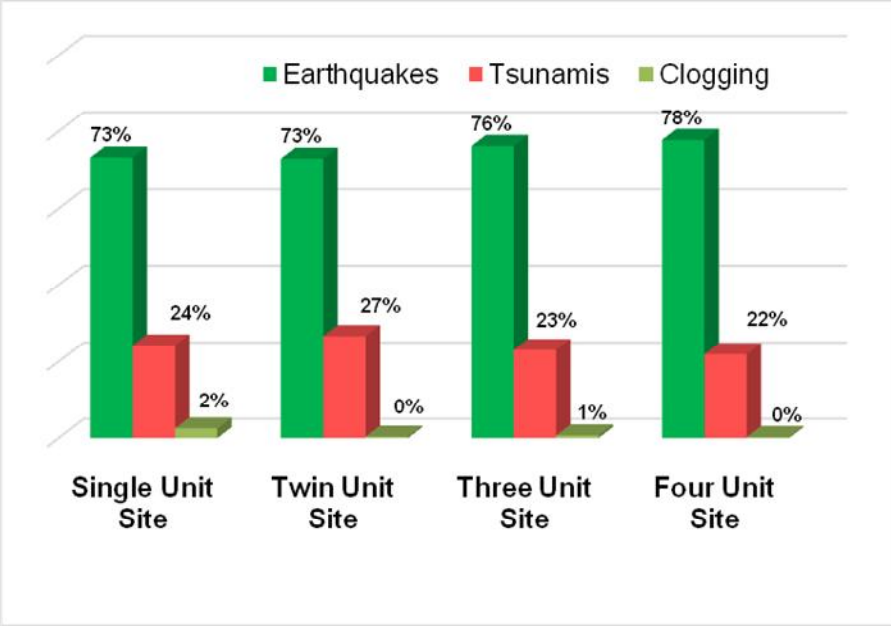

Figure 5.7: Distribution of external hazards in multi-unit sites

Among the external hazards considered, risk from earthquakes is about 75% and Tsunamis contribute the rest (Figure 5.7). Among the internal events considered, DIIEs contribute about 99% in all multi-unit sites.

5.6 RESULTS AND CONCLUSIONS

A comprehensive approach is proposed for risk assessment in a multi-unit site and demonstrated with a case study. The methodology proposed accounts for most of the dependency classes and key issues applicable for a multiple unit NPP site such as initiating events, shared connections, cliff edge effect, identical components, proximity dependencies, mission times and human dependencies. The methodology made it quite apparent that simple aggregation of single unit CDF fails to capture the true risk for a multi unit site. For the external events considered in the case study, the seismic and the tsunami events are found to have high potential for multi-unit risk. However, a good interface of the shared resources with the plant can reduce the multi-unit site risk to a greater extent. This method helps in identification of critical structures, systems and components important for safety in multi-unit

sites which are otherwise overlooked by carrying out individual unit risk assessment. Further, quantification of risk with this methodology will enable the regulatory authority to make risk informed decisions in a realistic manner. The proposed method is expected to be useful in developing safety goals, procedures and guidelines for a multi-unit NPP site. The outcome of such integrated PSA will also help in identification of those structures, systems and components that play important role in safety at multiple units and in regulatory decisions such as optimum number of units at a site, distance between two units, layout diversity and configuration of shared systems, etc. to minimize risk to the public and environment. Future work will address risk assessment in multi-unit sites that houses other fuel cycle facilities including spent fuel storage facility along with nuclear power plants.

CHAPTER-6

SUMMARY & SCOPE OF THE FUTURE WORK

6.0 INTRODUCTION

The fundamental objective of nuclear safety is to ensure that the risk from the operation of nuclear power plant (or nuclear facilities) is acceptably low and thereby guarantee the safety of plant, plant personnel, public at large and the environment. To ensure and demonstrate the safety of nuclear power plants, safety analysis is an essential element of overall safety assessment which is used over a broad range of operating and accident conditions in a comprehensive manner. The present research in the domain of Probabilistic Safety Assessment (PSA) is focussed towards common cause failure analysis for engineered safety systems using alpha factors obtained by mapping technique, dynamic modelling of the scenarios with time dependent success criteria and development of an integrated approach to assess the risk from a multi unit nuclear power plants site with consideration of both external and internal hazards. The developed integrated approach is demonstrated by estimating the risk for various sites housing single, double, triple and quadruple nuclear plants. The accomplished research work is expected to play an important role in estimating the risk from various nuclear power plant sites and assessing options to reduce it. It is also expected to be instrumental in future utilization of nuclear energy by supporting the deployment of Generation III and Generation IV nuclear power plants at various sites in the world with high safety levels as the utmost priority.

6.1 ALPHA FACTOR MODEL FOR COMMON CAUSE FAILURE ANALYSIS OF ENGINEERED SAFETY SYSTEMS USING MAPPING TECHNIQUE

The nuclear power plants are deployed with many engineered safety systems for ensuring nuclear safety. In these systems, redundancy is the fundamental technique adopted for fault

tolerance. However, common cause failures (CCF) can cause them to fail and are considered as a major contributor to the risk. Therefore, it is imperative to quantify the CCF in order to demonstrate the reliability of the safety systems. Various methods such as Beta factor, Multiple Greek Letter, Binomial Failure Rate and Alpha factor have been developed for estimating the risk from CCF (Mosleh et al., 1989). Among the available CCF models, alpha factor model is considered to be more realistic as it can model the real scenario to a greater extent. The main strength of this method is its ability to analyze various CCF events of different intensities as applicable to plant/system specific requirements. As a part of research work to exhibit the technique of mapping up of event impact vectors to determine alpha factors for high redundant systems has been demonstrated. Taking insights from the case studies of safety systems of the Indian Nuclear Power Plants a critical comparison of Alpha factor method with Beta factor method is performed and the following important conclusions are made:

1. The alpha factor model realistically assesses the contribution of each of the CCF event based upon subjective assessment of a constant ρ, conditional probability of each component failure given a shock.
2. Alpha factors are found to be less sensitive to change in the value of mapping up beta and this sensitivity further reduces as more number of components are added to the system.
3. Contribution of CCF events to total failure probability is found to be less sensitive to the value of mapping up beta. However, it is found to be highly sensitive to the change in success criterion for the system.
4. The use of alpha factors is found to be highly suitable, especially for large redundant configuration and with stringent success criteria. In such cases, the use of beta factor model yields highly repressed estimates, thereby underestimating the risks imposed by common cause events.

6.2 MARKOV ANALYSIS FOR TIME DEPENDENT SUCCESS CRITERIA OF PASSIVE DECAY HEAT REMOVAL SYSTEM

The engineered safety systems employed in the nuclear power plants are required to accomplish the specified tasks with varying mission times depending on the requirement and are subjected to different operating and environmental conditions. The configuration of these systems and the success criteria changes with time and therefore they are known as phased mission systems. A realistic reliability analysis of such systems must take into account the above described dynamics in system configuration and success criteria. In this thesis, Markov model technique is applied on Safety Grade Decay Heat Removal (SGDHR) system of Indian fast breeder reactor PFBR to efficiently model time dependent success criteria and estimate the unavailability of the system. The system has been modelled exhaustively under continuous and periodic monitoring schemes with and without the consideration of common cause failures. The estimates of the upper and lower bounds for the mean unavailability of SGDHR system over the mission time have been determined. The work aims in demonstrating the dynamic modelling of the scenarios with time dependent success criteria and also studies the factors affecting the availability of such system. Major findings of the study are:

1. The change in the value of time across which success criteria (t1) is changed and its effect on the system unavailability are more comprehensively captured by the Markov analysis while such effects cannot be observed by other methods such as Fault tree analysis.
2. Significant difference in system unavailability is observed between the two cases, viz., with CCF and without CCF under both continuous and periodic monitoring schemes.
3. On detailed analysis with two repair crews, not much significant improvement in the system availability is observed since the failure rates are very low and number of states is large.

6.3 INTEGRATED RISK ASSESSMENT OF MULTI-UNIT NUCLEAR POWER PLANT SITES

Most of the nuclear power producing sites in the world are housing multiple units. Such sites are faced with hazards generated from external events like earthquake, tsunami, flood, etc. which can threaten the safety of nuclear power plants. Further, risk from a multiple unit site and its impact on the public and the environment was apparent during the Fukushima nuclear disaster in March 2011. Hence, it is imperative to evolve a methodology to systematically assess the safety of a multi-unit site. In this work, unique features to be addressed in multi-unit safety assessment are discussed and an integrated approach is developed to assess the risk contribution of multiple nuclear plants at the site. The highlights of the proposed methodology are:

1. Inclusion of risk from both external and internal hazards.
2. Quantification of the frequency of multiple core damage for a multi unit site along with evaluation of site CDF which is the frequency of at least single core damage per site per year.
3. Comprehensive account for most of the dependency classes and key issues applicable for a multiple unit NPP site, viz., initiating events, cliff edge effect, shared connections, identical components, proximity dependencies and human dependencies.

The proposed approach leads to identification of structures, systems and components (SSCs) which play important role in safety of multiple units. Further, it is useful in developing safety goals, procedures and guidelines for multi-unit NPP sites. Towards demonstration of the method, it is applied to estimate the risk from various sites housing single, double, triple and quadruple nuclear plants and the risk is compared against each other. The major findings of the study are:

1. The methodology reveals that simple aggregation of single unit CDF fails to realistically estimate the risk for a multi unit site.
2. External events such as seismic and tsunami pose high threat for multi-unit NPP sites. However, a good interface of the shared resources with the plant can reduce the multi-unit site risk to a greater extent.
3. The study helps in identification of those structures, systems and components that play important role in safety at multiple units and in regulatory decisions such as optimum number of units at a site, distance between two units, layout diversity and configuration of shared systems, etc. to minimize risk to the public and environment.
4. The quantification of risk with this methodology will enable the regulatory authority to make risk informed decisions in a realistic manner for the multi unit sites.

6.4 SCOPE FOR FUTURE RESEARCH

The future research areas identified from the thesis are:

1. Extension of the developed multi unit risk assessment methodology to account the risk from
    i. Organizational dependencies
    ii. Human dependencies
2. Enhancing the scope of the methodology to account the risk from spent fuel storage bays located inside the nuclear power plant or its vicinity.
3. Further enhancement in the methodology to account the risk from other fuel cycle facilities like conversion, fabrication, enrichment, reprocessing and waste treatment plants present at the site. This is expected to provide a comprehensive risk assessment for the sites housing various nuclear facilities along with power plants.

REFERENCES

AERB Technical report, 2005. Glossary of terms for nuclear and radiation safety, India.

AERB Safety Guide, 2013. Protection against internally generated missiles in nuclear power plants, AERB/NPP/SG/D-3, India.

Apostolakis G., 2012. A Regulator's Perspective on Nuclear Power Plant Safety for the Future, International Forum on Safe Nuclear Power Plants, Korea Advanced Institute of Science & Technology.

Alam M., Ubaid M. A, 1986. Quantitative reliability evaluation of repairable phased-mission systems using Markov approach, IEEE Transactions on Reliability, R-355, 498-503.

Andrews J.D., Clifton A, 2000. Fault Tree and Markov Analysis Applied to Various Design Complexities, Proceedings of the 18th International System Safety Conference.

Arendt, J.S., Lorenzo, D.K., 2000. Evaluating process safety in the chemical industry: A user's guide to quantitative risk analysis.

Arul A. J., Kumar C. S., Athmalingam S., Singh O. P., Rao K. S., 2006. Reliability analysis of safety grade decay heat removal system of Indian prototype fast breeder reactor, Annals of Nuclear Energy 33, 180–188.

Athmalingam, S., Vijayakumaran, 2000. Operation Note for Safety Grade Decay Heat Removal Circuit, PFBR/3400/ON/ 1001.

Bajaj, S. S., Gore, A. R., 2005. The Indian PHWR, Nuclear Engineering and Design, 236, 701–722.

BARC, Safety of nuclear reactors, design level safety.
http://www.barc.gov.in/pubaware/snr_dls.html.

Berg, H. P., Görtz, R., Kesten, J., 2008. Methods for the treatment of Common Cause Failures in redundant systems, Journal of Reliability & Risk Analysis: Theory & Applications, Vol.1, 8-18.

Bhardwaj S. A., (2013)., "Indian Nuclear Power Programme - Past, Present and Future," Sadhana 38, Part B, 775–794.

Čepin, M., 2008. DEPEND-HRA—A method for consideration of dependency in human reliability analysis, Reliability Engineering & System Safety, 93, 1452-1460.

Dave D. K., Sharma B. M., Kumar S., Nuclear Power Plant Safety-Nuclear Engineering-301, Pandit Deendayal Petroleum University.

Deterministic or probabilistic analysis? RISKworld, Issue 1, 2002.

Ebeling C. E., 2011. Reliability and Maintainability Engineering.

Ebisawa, K., Fujita, M., Iwabuchi, Y., & Sugino, H., 2012. Current issues on PRA regarding seismic and tsunami events at multi units and sites based on lessons learned from Tohoku earthquake/tsunami, Nuclear Engineering and Technology, 44, 437-452.

FaultTree + for Windows, Isograph Software manual version 11.2.

Fleming, K.N., 2005. On the issue of integrated risk-A PRA practitioner's perspective. In: Proceedings of the ANS international topical meeting on probabilistic safety analysis. San Francisco, CA.

Fleming, K. N., 2011. Markov models for evaluating risk-informed in-service inspection strategies for nuclear power plant piping systems, Reliability Engineering and System Safety, 83, 27–45.

Fullwood, R.R., 2000. Probabilistic Safety Assessment in Chemical and Nuclear Industries, New Delhi.

Hayns, M., 1999. The evolution of probabilistic risk assessment in the nuclear industry. Trans IChemE, 77, Part B, 117-142.

Holmberg, J.E., & Knochenhauer, M., 2010. Guidance for the definition and application of probabilistic safety criteria.

IAEA, 2011. A methodology to assess the safety vulnerabilities of nuclear power plants against site specific extreme natural hazards.

IAEA Report GC56/INF/2, 2012. Nuclear Safety Review for the Year 2012.

IAEA Specific Safety Guide No. SSG-3, 2010. Development and application of level 1 probabilistic safety assessment for nuclear power plants.

IAEA Safety Series No. 50-SG-D4, 1980. Protection Against Internally Generated Missiles and Their Secondary Effects in Nuclear Power Plants– A safety guide.

IAEA Specific safety Guide No. SSG-2. 2009. Deterministic safety analysis for nuclear power plants.

IAEA Specific Safety Guide No. SSG-2, 2009. Deterministic Safety Analysis for Nuclear Power Plants.

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

IAEA Safety Series No. 50-P-8, 1995. Procedures for Conduction Probabilistic Safety Assessments of Nuclear Power Plants (Level 2).

IAEA Safety Series No. 50-P-12, 1996. Procedures for Conduction Probabilistic Safety Assessments of Nuclear Power Plants (Level 3).

IAEA-TECDOC-648, 1992. Procedures for conducting common cause failure analysis in probabilistic safety assessment.

IAEA-TECDOC-1200, 2001. Application for Probabilistic Safety Assessment PSA for nuclear power plants.

IAEA-TECDOC-1341, 2003. Extreme external events in the design and assessment of nuclear power plants.

IAEA-TECDOC-1511, 2006. Determining the quality of probabilistic safety assessment PSA for applications in nuclear power plants.

IAEA-Technical Report, 1991. The International Chernobyl Project Technical Report, Assessment of Radiological Consequences and Evaluation of Protective Measures, Report by an International Advisory Committee.

IAEA Training Course on Safety Assessment of NPPs to Assist Decision Making, Safety Analysis: Event Classification.

INSAG-10, 1996. Defence in depth in nuclear safety, International Atomic Energy Agency.

INSAG-12, 1999. Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev.1, International Atomic Energy Agency

Jain, S. K., 2010. Nuclear Power in India – Past, present and future. http://www.npcil.nic.in/pdf/CMD_paper_07dec2010.pdf

Katiyar, S. C., Bajaj, S. S., 2005. Tarapur Atomic Power Station Units-1 and 2: Design features, operating experience and license renewal, Nuclear Engineering and Design, 236, 881–893.

Kennedy R., Ravindra, M., 1984. Seismic fragilities for nuclear power plant risk studies, Nuclear Engineering and Design, 79, No. 1, 47 - 68.

Khan, F. I,, Abbasi, S. A., 1998. Techniques and methodologies for risk analysis in chemical process industries. Journal of Loss Prevention in the Process Industries, 11, 261–277.

Kim M.K., Choi I.K., 2012. A tsunami PSA methodology and application for NPP site in Korea, Nuclear Engineering and Design, 244, 92 - 99.

Kumar, C. S., Arul A. J., Singh O. P., Rao K. S., 2005. Reliability analysis of shutdown system, Annals of Nuclear Energy, 32, 63-87.

Kumar S. L., Natesan K., John Arul A., Balasubramaniyan V., Chetal S.C., 2011. Design and evaluation of Operation Grade Decay Heat Removal System of PFBR, Nuclear Engineering and Design, 241, 4953–4959.

Muhlheim, M.D., Wood, R.T., 2007. Design strategies and evaluation for sharing systems at multi-unit plants phase-I, ORNL/LTR/INERI-BRAZIL/06-01. Oak Ridge National Laboratory.

NUREG/CR-2300,1983. PRA procedures guide: a guide to the performance of probabilistic risk assessment for NPP, Technical report, USNRC.

Lasitha, A., Kumar, A., Kumar, M., Singh, M.K, Srivastava, S., Babu, R. M. S., Mahapatra, U., 2006. Test and Monitoring system 1 TMS1 for shutdown system 1 for TAPS 3 &4, BARC Newsletter, Issue 272.

Lowe, P., Garrick, Inc., 1983. Seabrook Station Probabilistic Safety Assessment Section 13.3 Risk of Two Unit Station, Prepared for Public Service Company of New Hampshire, PLG-0300.

Mathews, T.S., Arul, A.J., Parthasarathy, U., Kumar, C.S., Ramakrishnan, M., Subbaiah, K.V., 2009. Integration of functional reliability analysis with hardware reliability: An application to safety grade decay heat removal system of Indian 500 MWe PFBR, Annals of Nuclear Energy, 36, Issue 4, 481–492.

Mosleh, A. , Fleming, K. N., Parry, G.W., Paula, H.M., Worledge D.H., Rasmuson, D.M., 1989. Procedures for analysis of common cause failures in probabilistic safety analysis, NUREG/CR-4780, Vol.1.

Mosleh, A., 1991. Common cause failures: an analysis methodology and examples, Reliability Engineering & System Safety, 343, 249-292.

Mosleh, A., Rasmuson, D. M., Marshall, F.M., 1998. NUREG/CR-5485, Guideline on modeling Common-Cause Failures in Probabilistic Risk Assessment.

Muhlheim, M.D., & Wood, R.T., 2007. Design strategies and evaluation for sharing systems at multi-unit plants phase-I ORNL/LTR/INERI-BRAZIL/06-01. Oak Ridge National Laboratory.

OECD, 2009. Probabilistic risk criteria and safety goals. Technical Report NEA/CSNI/R200916, Organization for Economic Co-operation and Development.

Pages, A., Gondran, M., 1986. System Reliability: Evaluation & Prediction in Engineering.

Papazoglou, I. A., Nivolianitou, Z., Aneziris, O., Christou, M., 1992. Probabilistic safety analysis in chemical installations, Journal of Loss Prevention in the Process Industries, 5, 181-191.

Parthasarathy ,U., Selvaraj, P., Velusamy, K., Chellapandi, P., 2003. Criteria for successful DHR through Safety Grade Decay Heat Removal System, PFBR/34000DN/1014/Revision A.

Paul Scherrer Institute, 2013. Reconstruction of the Fukushima nuclear accident. https://www.psi.ch/media/reconstruction-of-the-fukushima-nuclear-accident

Reed, J.W., Kennedy, R., 1994. Methodology for developing seismic fragilities, Final Report TR-103959, EPRI.

Rouvroye, J.L., Brombacher, A.C., 1999. New quantitative safety standards: different

techniques, different results?, Reliability Engineering and System Safety, 66, 121-125.

RiskSpectrum Analysis Tools, Theory Manual, Version 3.0.0.

Sakthival, M., Swamy, S.L.N., Athmalingam, S., Madhusoodanan, K., 2012. Design of control logic for dampers of AHX in SGDHR circuit, PFBR/63400/DN/1003/Rev-D.

Saleh, J.H., Marais, K.B., Favaró, F.M. 2014. System Safety Principles: A Multidisciplinary Engineering Perspective, Journal of Loss Prevention in the Process Industries, 29, 283-294.

Samaddar, S., Hibino, K., Coman, O., 2014. Technical approach for safety assessment of multi-unit NPP sites subject to external events, PSAM12, Hawaii.

Sanyasi Rao, V.V.S., 2010. Probabilistic Safety Assessment of Nuclear Power Plants –Level 1, International Conference on Reliability Safety and hazard.

Schroer, S., Modarres, M. 2013. An event classification schema for evaluating site risk in a multi-unit nuclear power plant probabilistic risk assessment. Reliability Engineering and System Safety, 117, 40 – 51.

Seth, V. K., 1988. Design Features of Reactor Assembly and Structures of Indian 500 MWe PWHR stations, Nuclear Engineering and Design , 109, Issues 1–2, 163-169.

Solanki, R.B., Prasad M., 2007. Probabilistic Safety Assessment of Nuclear Power Plants -A Monograph, AERB.

SNETP Fukushima Task Group report, 2013. Identification of Research Areas in Response to the Fukushima Accident.

Tang, Z., Dugan, J. B., 2004. An integrated method for incorporating common cause failures in system analysis, Reliability and Maintainability, 2004 Annual Symposium - RAMS ,610-614.

Takeshi, M., 2011. Discussions of Fukushima nuclear power plant accidents by a viewpoint of PSA. Nuclear Safety and Simulation, 2(3), 226-235.

Tixier, J., Dusserre, G., Salvi, O., Gaston, D., 2002. Review of 62 risk analysis methodologies of industrial plants, Journal of Loss Prevention in the Process Industries, 15, 291-303.

U.S. Nuclear Regulatory Commission SECY-05-0130 2005. Policy issues related to new plant licensing and status of the technology-neutral framework for new plant licensing.

Wierman, T. E., Beck, S. T., Calley, M. B., Eide, S. A., Gentillon, C. D., William, E. K., 2001. Reliability Study: Combustion Engineering Reactor Protection System, NUREG/CR-5500, 1984–1998, Vol.10.

Wierman, T. E., Rasmuson, D.M., Mosleh, A., 2007. Common-Cause Failure Database and Analysis -System: Event Data Collection, Classification, and Coding, NUREG/CR-6268, Rev. 1.

World Nuclear Association, Nuclear Fuel Fabrication, (Updated June 2016). http://www.world-nuclear.org/information-library/nuclear-fuel-cycle/conversion-enrichment-and-fabrication/fuel-fabrication.aspx

World Nuclear Association, Radioactive Waste Management, (Updated March 2015). http://www.world-nuclear.org/info/nuclear-fuel-cycle/nuclear-wastes/radioactive-waste-management/

World Nuclear Association, The Economics of Nuclear Power, (Updated April 2015). http://www.world-nuclear.org/info/Economic-Aspects/Economics-of-Nuclear-Power/

Xing, L., Fleming, K. N., Loh W. T., 1996. Comparison of Markov model and fault tree approach in determining initiating event frequency for systems with two train configurations, Reliability Engineering and System Safety, 53, 17-29.

Xing, L., Dugan, J. B., 2000. Reliability analysis of static phased mission systems with imperfect coverage, Proceedings of the Second International Conference on Mathematical Methods in Reliability.

Yang, J. E., Han, S. H., Ahn, K., Jung, W. S., Lim, H. G., 2009. Development of A New Framework for the Integrated Risk Assessment of All Modes/All Hazards, Korean Nuclear Society 2009 Autumn Meeting, Gyeongju, Korea.

Yang, J.E. 2012. Development of an integrated risk assessment framework for internal/external events and all power modes. Nuclear Engineering and Technology, 44, 459-470.

Zerger, B., Ramos, M.M., Veira, M.P. 2013. European Clearinghouse: Report on External Hazard related events at NPPs, Joint Research Centre of the European Commission.

Zhang, T., Long, W., Sato, Y., 2003. Availability of systems with self-diagnostic components—applying Markov model to IEC 61508-6, Reliability Engineering and System Safety, 80, 133–141.