

**AN INVESTIGATION INTO THE FAIL SAFENESS OF SAFETY  
CRITICAL INSTRUMENTATION AND CONTROL IN A  
SODIUM COOLED FAST REACTOR**

*By*

**SRIKANTAM SRAVANTHI**  
(Enrollment No: ENGG02201204006)

**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**



**February, 2018.**


# Homi Bhabha National Institute

## Recommendations of the Viva Voce Committee

As members of the Viva Voce Board, we certify that we have read the dissertation prepared by Ms. Srikantam Sravanthi entitled "An investigation into the fail safeness of safety critical instrumentation & control in a sodium cooled fast reactor" and recommend that it may be accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy.

Chairman: Dr. M. Sai Baba  f Dean Academic (Engg Sci) Date: 26/2/2018

Guide / Convener: Dr. K. Devan  Date: 26/2/2018

Examiner: Prof. V. N. Achutha Naikan  Date: 26/02/2018

Member 1- Dr. B.P.C. Rao  Date: 26/2/2018


Member 2- Dr. Gopika Vinod  Date: 26.02.2018

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

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

Date:

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

  
Dr. K. Devan 26/2/2018  
(Guide)



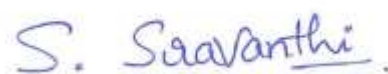
## STATEMENT BY AUTHOR

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.

Date:

Place: Kalpakkam



**(Srikantam Sravanthi)**

## 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.

Date:

Place: Kalpakkam



**(Srikantam Sravanthi)**

## **List of publications arising from the thesis**

### **JOURNALS**

1. **S. Sravanthi**, R. Dheenadhayalan, M. Sakthivel, K. Devan, K. Madhusoodanan, A Method for Online Diagnostics of Electromagnetic Relays Against Contact Welding for Safety Critical Applications in *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 5, issue 12, pp. 1734-1739, Dec. 2015.
2. **S. Sravanthi**, R. Dheenadhayalan, K. Devan, K. Madhusoodanan, An Inherently Fail-Safe Electronic Logic Design for a Safety Application in Nuclear Power Plant in *Process Safety and Environmental Protection*, vol. 111, issue C, pp. 232-243, 2017.
3. **S. Sravanthi**, R. Dheenadhayalan, K. Madhusoodanan, K. Devan, Safety Criteria and Dependability management practices: A case study with I&C systems of Prototype Fast Breeder Reactor in *Nuclear Technology*, vol. 201, pp. 180-189, Feb. 2018.

### **CONFERENCE PUBLICATION**

1. **S. Sravanthi**, R. Dheenadhayalan, Gopika Vinod, K. Madhusoodanan, K. Devan, Reliability model of a relay output card with diagnostic circuitry for safety instrumented system, in proceedings of the *IEEE conference on System Reliability and Science*, Paris, France, pp. 130-136, 2016. (DOI:10.1109/ICSRS.2016.7815851).

### **CONFERENCES**

1. **S. Sravanthi**, R. Dheenadhayalan, K. Madhusoodanan, A method for Prognostics in Electromagnetic relay for reliability improvement in a safety critical nuclear application in *International Applied Reliability Symposium*, Chennai, Tamilnadu, Aug. 19-21, 2015.

2. **S. Sravanthi**, R. Dheenadhayalan, M. Sakthivel, SLN. Swamy, K. Madhusoodanan, Life Testing of Power Contactors in 2<sup>nd</sup> *SRESA National conference on Reliability and Safety Engineering* , Chennai, Tamilnadu, Oct. 8-10, 2015.



**(Srikantam Sravanthi)**

**DEDICATED**  
**TO**  
***MY PARENTS***

## **ACKNOWLEDGEMENTS**

I take this opportunity to express 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 Shri.R. Dheenadhayalan, SO/E, EIG, IGCAR for his persistent encouragement, constant motivation, everlasting patience and insightful guidance in all the ways leading to the completion of my Ph.D work. The joy and enthusiasm he has for this research was contagious and motivational for me, even during tough times.

I sincerely thank my technology adviser Shri. K.Madhusoodanan, former group director, EIG, IGCAR and research supervisor Dr. K. Devan, Head, Reactor Neutronics Division, Reactor Design Group, IGCAR for valuable guidance and support. I convey my heartiest appreciation to my doctoral committee Chairman Dr. M. Sai Baba and committee members Dr. B.P.C. Rao and Dr. Gopika Vinod for their support and encouragement during my research work.

My sincere gratitude to, Dr. A.K. Bhaduri, Director, IGCAR and Dr. S.A.V. Satya Murty, Dr. P.R. Vasudeva Rao and Shri S.C. Chetal, former Directors, IGCAR for providing excellent environment to carry out research work.

My special thanks to Shri. A.Venkatesan Head ICD, Shri.M. Manimaran Head PIS, Ms. Somavathi, Mrs. Varuna, Mr. Pradeesh, Mr. Ananda Kumar, Mr. SLN. Swamy, Mrs. Nisha, Mr. Ankit, Mr. Subramanian, Mr. G.K. Mishra, Mr.C.P.Nagaraj, Mr.M. Saktivel, Mr. Raj Kumar and all members of ICD for their support and creating a homely environment at the work place during this period.

I specially acknowledge EID Head/EID colleagues for the inputs on card details of computer-based systems and voting logics.

I am grateful for the financial support provided by research fellowship scheme from Indira Gandhi Centre for Atomic Research, Department of Atomic Energy for the duration of the work.



I thank HBNI, CICS and CSIR for providing the international travel grant to attend the 2016 International Conference on System Reliability and Science, Paris, France.

It is my pleasure to thank all my friends and seniors Prema, Sumathi.V, Rajasekar, Balaji, Chandan Reddy, Shiva, Nagendra, Veerendra, Samba, Anand, Shivang, Santosh, Chandan Kumar, Vipin, Naveen, Sumathi.G, Naseema, Preethi, Raghavendra, Balakrishnan, Sashwat, Sanjay, Bubathi, Arun Babu, Anil, Priya, Vivek.

It has been a great honor for me to work in IGCAR and to be surrounded with some of the brightest and loving people, I have met. To all, I say Thank you from the bottom of my heart.

Finally, I would like to thank my parents Smt.S. Sulochana, Shri.S. Ramachandraiah and my siblings Mrs. Sreevani and Mrs. Sravani who have been the source of constant inspiration and motivation for me throughout my life. My heart is filled with diligent gratitude to all my family members who have created an ideal environment for me to smoothly handle my career and bring the best out of me in all the endeavors in my life.

Thank you everyone.

**(Srikantam Sravanthi)**

# CONTENTS

SYNOPSIS.....	i
LIST OF FIGURES.....	iv
LIST OF TABLES.....	vi
LIST OF ABBREVIATIONS.....	vii
1 INTRODUCTION	
1.1 Background.....	1
1.2 An Overview of Instrumentation and Control Systems in a Nuclear Power Plant...	4
1.3 Fail-safe Design .....	6
1.4 Literature Survey .....	8
1.4.1 Design principles to reduce probability of failure on demand.....	8
1.4.2 Survey on design principles used in shutdown systems.....	14
1.5 Research Objectives.....	17
1.6 Organization of the Thesis.....	20
2 STUDY OF SAFETY CRITICAL I&C SYSTEMS IN PFBR	
2.1 Introduction.....	22
2.2 Shutdown System.....	24
2.2.1 Sensors .....	24
2.2.2 Signal processing.....	27
2.2.3 Actuation system .....	34
2.3 Computer Based Systems used for Shutdown .....	39
2.3.1 Analog Input Card (AIC) .....	39
2.3.2 Digital Input Card (DIC).....	41
2.3.3 Analog Output Card (AOC) .....	42
2.3.4 Relay Output Card (ROC).....	44
2.3.5 Central Processing Unit card (CPU) .....	46
2.4 Decay Heat Removal System.....	48
2.5 Summary .....	51
3 A NOVEL ONLINE DIAGNOSTICS OF EM RELAYS AGAINST CONTACT WELD	
3.1 Introduction.....	52
3.1.1 Electromagnetic relay.....	52

3.1.2	Failure modes of EM relay .....	53
3.1.3	Arc and its consequences .....	55
3.2	Welding Concerns in Nuclear Power Plant .....	59
3.3	A Method for Online Diagnostics of EM Relay .....	61
3.3.1	Fundamental principle.....	61
3.3.2	Verification of proposed method.....	62
3.3.3	Results .....	65
3.3.4	Reliability improvement.....	67
3.3.5	Limitations and precautions .....	67
3.4	Summary .....	68
4	A RELAY OUTPUT CARD WITH WELD DIAGNOSTICS AND RELIABILITY MODELLING	
4.1	Relay Output Card with Diagnostics .....	69
4.1.1	Implementation.....	69
4.1.2	Experimental setup.....	73
4.2	Reliability Analysis.....	74
4.2.1	Markov model of the system.....	74
4.2.2	Failure rate calculation .....	78
4.2.3	Markov analysis of the ROC .....	83
4.2.4	Sensitivity analysis .....	84
4.3	Summary .....	88
5	ELECTROMAGNETIC CONTACTORS: LIFE TESTING AND FAILURE ANALYSIS	
5.1	Introduction.....	89
5.2	Reliability Demonstration Testing using Test of Hypothesis Technique .....	90
5.3	RDT Plan for a EM contactor: Application in PFBR .....	92
5.3.1	Test setup.....	93
5.3.2	Test results.....	96
5.4	Failure Analysis .....	96
5.4.1	Field driver relay .....	96
5.4.2	EM Contactors.....	98
5.5	Summary .....	102
6	INHERENT FAIL-SAFE CIRCUITS TO IMPROVE FAIL-SAFE DESIGN	
6.1	Inherent Fail-safe Design: An approach to Probability of Failure on Demand ....	103

6.2	Fail-safe AND Gate .....	105
6.3	Inherently Fail-safe Pulsating Logic Design for PFBR Safety Grade Decay Heat Removal Circuit.....	107
6.3.1	Inherently fail-safe pulsating logic design .....	109
6.3.2	Experimental Verification.....	112
6.3.3	Results .....	112
6.3.4	Failure mode effect analysis verification .....	114
6.3.5	Unsafe failure probability on demand.....	123
6.3.6	Precautions and possible improvements .....	127
6.4	Applications of Inherent Fail-safe Circuit .....	128
6.5	Summary .....	129
7	SUMMARY AND SCOPE FOR FUTURE WORK.....	130
7.1	Summary .....	130
7.2	Future Work .....	134
	REFERENCES.....	135

## SYNOPSIS

---

Nuclear power plants (NPPs) are intended to achieve the safety margins and high reliability of design features. Instrumentation and Control (I&C) systems are very crucial to achieve the desired safety function of various systems in a NPP. The stringent reliability requirements are achieved by adopting various measures like defense in depth, redundancy, independence, periodic surveillance and fail-safe design. “Fail-safe” behavior is the capability of any system to reach predefined safe state in the event of malfunction of components.

Prototype Fast Breeder Reactor (PFBR) is a sodium cooled Fast Breeder reactor Indira Gandhi Centre for Atomic Research and is being commissioned at Kalpakkam, as a part of India’s second stage nuclear energy programme. The research problem is to perform a review of the current practices, assumptions and techniques followed in design of I&C systems in a fast reactor towards achieving a fail-safe design and come out with relevant solutions for further improvement. The present study focuses on ensuring failure free performance of shutdown system and decay heat removal system. I&C for shutdown systems are to be designed “fail-safe” so that any fault in sensors, logic processors or final control elements will lead to shutdown of the reactor. Similarly, systems for decay heat removal should ensure timely initiation and sustenance of decay heat removal after reactor shutdown. Any fault in such systems should initiate unintended decay heat removal even if it leads to loss of power rather than failure to initiate safety action.

Average Probability of Failure on Demand ( $PFD_{Avg}$ ) is the quantitative parameter of interest to the safety systems considered for this study. The study of self-diagnostics and fail-safe design plays an important role in the overall goal of  $PFD_{Avg}$ . Self-diagnostics helps in detecting dangerous failure. With the aid of fail-safe design, in case of dangerous detected failures, system

can be taken to fail-safe state. Further, the system design must ensure that all detected faults lead to fail-safe state.

The quantitative effect of each of the design principle such as redundancy, independence, diversity, periodic surveillance and fail-safe design on the  $PFD_{Avg}$  is studied in this thesis. The general design principles used in a typical shutdown system and decay heat removal system are studied. From review of various design modules used in PFBR, the proposed novel solutions for the goal of reducing  $PFD_{Avg}$  are given below.

- A novel method to detect “contact weld failure” of Electro Magnetic (EM) relay is proposed which helps in online diagnostics without disturbing the load connected to the relay contact. The method uses the differences in characteristic decay of coil current during de-energization process between a healthy relay and a relay whose contacts got welded. The method works on the principle of de-energizing followed by quick re-energization of relay coil.
- The practical implementation and verification of relay contact weld detection circuit without any impact on functional circuit is verified with a relay output card. Markov model is developed to demonstrate reduction in unsafe state probability of the system. The study has been shown that failure probability of each redundant channel can be reduced by  $\approx 48$  folds with this diagnostic technique.
- Reliability demonstration testing as per MIL-HDBK-781A is carried out to confirm the failure data of EM contactor. Failure analysis of degraded contacts is performed with SEM (Scanning Electron Microscopy) and EDS (Energy Dispersive Spectroscopy). The impact of EM contactor failure on uncontrolled withdrawal of neutron absorber rods in PFBR is analyzed.



- Inherent fail-safe circuits do not require diagnostics since any of the failures in the circuit will automatically lead to a safe state of the final control element. Thus, inherent fail-safe design is studied as an alternative approach to systems with periodic self-testing. A novel inherently fail-safe AND gate is proposed. An inherent fail-safe pulsating electronic logic based valve drive circuit with the AND gate is designed for a decay heat removal system. Quantitative analysis has shown a very low  $PFD_{Avg}$  since the system fails in unsafe mode only upon combination of multiple failures.

Overall the work has proposed EM relays with online diagnostics and inherently fail-safe circuits to reduce the  $PFD_{Avg}$  of safety systems in a fast reactor.

## LIST OF FIGURES

---

Figure 1.1: Event tree.....	2
Figure 1.2: Structure of I&C in a NPP [2]. .....	5
Figure 1.3: Classification of I&C systems in a NPP.....	6
Figure 1.4: Failure rate distribution [5].....	7
Figure 1.5: $PFD_{Avg}$ of a periodically proof tested system.....	8
Figure 1.6: Schematic of shutdown system. ....	15
Figure 2.1: Flow sheet of PFBR. ....	23
Figure 2.2: Shutdown system in PFBR.....	25
Figure 2.3: Block diagram of SLFIT system. ....	29
Figure 2.4: Electromagnet coil connection diagram. ....	30
Figure 2.5: Block diagram of PCSL system. ....	32
Figure 2.6: PCSL timing diagram. ....	33
Figure 2.7: PCSL for multiple parameters. ....	34
Figure 2.8: Instrumentation in CSRDM.....	35
Figure 2.9: Block diagram of AIC. ....	40
Figure 2.10: Block diagram of AOC.....	43
Figure 2.11: Clock fail detection circuit. ....	43
Figure 2.12: Waveforms of clock fail detection circuit. ....	44
Figure 2.13: Block diagram of ROC.....	45
Figure 2.14: Block diagram of CPU card. ....	47
Figure 2.15: Dampers in SGDHR system.....	49
Figure 3.1: EM relay internal architecture. ....	53
Figure 3.2: Contact failure (a) contact material loss due to arc erosion; (b) pip and crater formation [85]. ....	56
Figure 3.3: Application of relay in nuclear power plant shutdown system. ....	59
Figure 3.4: Coil de-energization current decay curve (a)Under healthy contacts; (b)Under welded contacts. ....	61
Figure 3.5: Schematic circuit to implement EM relay diagnostics. ....	63
Figure 3.6: Experimental setup. ....	65
Figure 3.7: Results of diagnostic circuit. ....	66

---

Figure 4.1: Schematic of relay diagnostic circuitry in ROC.....	71
Figure 4.2: Detailed PCB schematic.....	72
Figure 4.3: Printed circuit board of ROC.....	72
Figure 4.4: Experimental setup.....	74
Figure 4.5: Markov state space model.....	78
Figure 4.6: Markov state space in ISOGRAPH with state probabilities.....	84
Figure 4.7: Unsafe state probability variation with test interval.....	85
Figure 4.8: Unsafe state probability variation with proof test interval.....	86
Figure 5.1: Contactor reliability testing circuit.....	93
Figure 5.2: Experimental setup.....	95
Figure 5.3: Possible interactions of electric contacts and the ambient air during arcing .....	97
Figure 5.4: Failure analysis: (a-b) SEM images of failed relay; (c-d) EDS spectrum with elemental composition of failed relay with their weight percentages in dark and bright region..	97
Figure 5.5: Surface morphology: (a-c) Deformation on C <sub>1</sub> contact; (d-f) Deformation on C <sub>2</sub> contact.....	98
Figure 5.6: EDS (a) Spots on C <sub>1</sub> contact; (b-c) Spectrum on C <sub>1</sub> with wt%.....	100
Figure 5.7: EDS (a) Spots on C <sub>2</sub> contact; (b-c) Spectrum on C <sub>2</sub> with wt%.....	101
Figure 6.1: Fail-safe AND gate (a) Design; (b) Pulse input, pulse transformer output and capacitor voltage waveforms; (c) Pulse inputs, capacitor voltage and AND output waveforms. .....	107
Figure 6.2: Logic circuit to drive solenoid valves.....	108
Figure 6.3: Schematic of fail-safe pulsing circuitry for controlling V <sub>3</sub> and V <sub>4</sub> valves.....	110
Figure 6.4: Experimental setup.....	112
Figure 6.5: During healthy operation outputs waveforms at different stages (a)Timer synchronization pulses; (b)AND gate output; (c)OR gate output; (d)24V pulse transformer output, 24V capacitor voltage output.....	113
Figure 6.6: Failure mode effect analysis results.....	114

## LIST OF TABLES

---

Table 1.1: $PFD_{Avg}$ equations for various architectures. ....	11
Table 1.2: Relation between design technique and $PFD_{Avg}$ . ....	12
Table 2.1: Design basis events. ....	23
Table 3.1: Contact failure modes [83]. ....	54
Table 3.2: Physical effects on contact reliability [83]. ....	54
Table 3.3: Failure modes and root causes [84]. ....	55
Table 3.4: Test parameters. ....	64
Table 4.1: Notations for Markov model. ....	75
Table 4.2: Notations used for functional block status in Markov model. ....	77
Table 4.3: Possible states of the system. ....	77
Table 4.4: Failure rate of TI UA-741. ....	79
Table 4.5: Failure rate of diagnostic block. ....	79
Table 4.6: Parameter values for Markov analysis. ....	83
Table 4.7: Variation of unsafe state probabilities with diagnostic block failure rate. ....	87
Table 5.1: Failure ratios of Normally Open contactor as per IEC 60947 [62]. ....	90
Table 5.2: Fixed duration test plans [94]. ....	92
Table 5.3: Contactor specifications. ....	94
Table 6.1: Comparison of logics with unsafe failure probability. ....	105
Table 6.2: Failure mode effect analysis. ....	117

## LIST OF ABBREVIATIONS

ADC	Analog to Digital Converter
AERB	Atomic Energy Regulatory Board
AI	Auto Inhibition
AIC	Analog Input Card
AOC	Analog Output Card
AS	Actuation System
CCF	Common Cause Failures
CDA	Core Disruptive Accident
CDF	Core Damage Frequency
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
CSRDM	Control and Safety Rod Drive Mechanism
CTMS	Core Temperature Monitoring System
DAC	Digital to Analog Converter
DBE	Design Basis Event
DD	Dangerous Detected
DEC	Design Extension Condition
DIC	Digital Input Card
DSL	Design Safety Limit
DSRDM	Diverse and Safety Rod Drive Mechanism
DU	Dangerous Undetected
EDAC	Error Detection and Correction
EDS	Energy Dispersive Spectroscopy
EEPROM	Electrically Erasable and Programmable Read only Memory
EM	Electro Magnetic
EOC	End of Conversion
EPROM	Electrically Programmable Read Only Memory
FBTR	Fast Breeder Test Reactor
FF	Flip Flop
FPGA	Field Programmable Gate Array
FPU	Floating Point Unit
GOT	Good Operation Trip

IA	Instrumentation Amplifier
I&C	Instrumentation and Control
IEC	International Electro technical Commission
IGBT	Gate Bipolar Transistor
IHX	Intermediate Heat exchangers
LED	Light Emitting Diode
LED	Light Emitting Diode
MI	Manual Inhibition
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
MRT	Mean Repair Time
MTTR	Mean Time to Restoration
MUX	Multiplexers
NC	Normally Closed
NO	Normally Open
NPP	Nuclear Power Plant
OGDHR	Operation Grade Decay Heat Removal
PCB	Printed Circuit Board
PCSL	Pulse coded Safety Logic
PFBR	Prototype Fast Breeder Reactor
PFD <sub>Avg</sub>	average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
PHWR	Pressurized Heavy Water Reactor
PLC	Programmable Logic Controller
PSA	Probabilistic Safety Analysis
RDT	Reliability Demonstration Testing
ROC	Relay Output Card
RPS	Reactor Protection System
r -y	reactor year
SC	Safety Class
SCRAM	Safety and Control Rods Accelerated Movement
SDS	Shut Down System
SD	Safe Detected
SEM	Scanning Electron Microscopy
SIS	Safety Instrumented System



SGDHR	Safety Grade Decay Heat Removal
SGE	SCRAM Generation Electronics
SLFIT	Safety Logic with Finite Impulse Test
SOC	Start Of Conversion
SOLC	Switch Over Logic Circuit
SPDT	Single Pole Double Throw
SRAM	Static Random Access Memory
SU	Safe Undetected
TIU	Test Interface Unit
TTL	Transistor Transistor Logic
TMR	Triple Modular Redundancy
VME	Versa Module Europa

# 1

## INTRODUCTION

---

### 1.1 Background

Nuclear power plants (NPPs) are designed to achieve high level of safety at all stages of its lifetime, including extreme natural events like earthquake, flood, tsunami etc. The design has to ensure protection of the workers, public and the environment from the harmful effects of radiations emerging from the plant. To achieve this, the 'defense in depth' philosophy in designing and operating of nuclear facilities which prevents and mitigates accidents, that release radiation or hazardous materials used. The key point is creating multiple independent and redundant layers of defense to compensate for the potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense in depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures. The Instrumentation and Control (I&C) system play a key role to ensure the safe and efficient operation of a nuclear plant and they are generally designed on the basis of their function and significance to safety. There are a number of vital functions that must be performed by I&C systems. The important safety functions that are essential to be performed for ensuring safety are (a) control of core reactivity (b) removal of heat from the core and (c) confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases. A comprehensive safety assessment, using both deterministic and probabilistic safety analysis (PSA) methods, is usually made to ensure that all safety

requirements established for the design are met and are in accordance with relevant national and international codes and standards, laws and regulations.

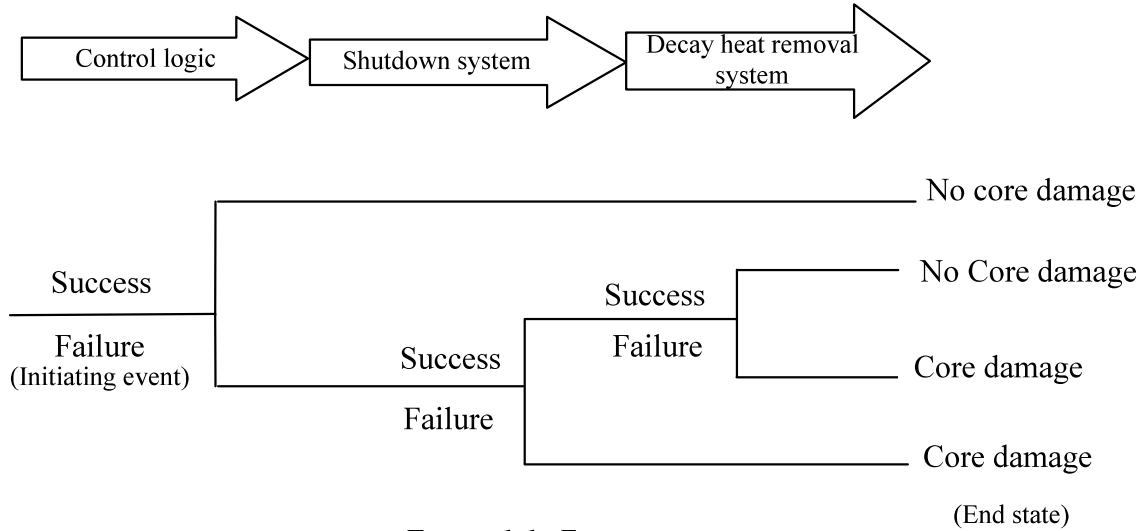


Figure 1.1: Event tree.

Figure 1.1 gives a sketch of an event tree of three systems, viz. control logic, shutdown and decay heat removal, and their failure propagation leading to the core damage. A probabilistic risk assessment parameter called the Core Damage Frequency (CDF) is generally used to quantify the probability of a Core Disruptive Accident (CDA). The three systems mentioned above are considered as “safety critical” and are necessary to be highly reliable to achieve a low value of CDF ( $\sim 10^{-6}$ - $10^{-7}$ /r-y) (reactor-year). Control system failure would cause overpower or under-cooling and can be the initiating event which has a potential for core damage in case of multiple failures. However, the failure at this stage will be handled by shutdown systems and decay heat removal systems. A list of shutdown parameters are provided in the design and their thresholds are obtained by carrying out the transient analysis of the Design Basis Events (DBEs) which challenge the Design Safety Limits (DSL) on coolant, clad and fuel. The timely action of shutdown system during any transient ensures safe shutdown such that maximum values of coolant, clad and fuel temperatures reached are limited below the DSL values. Similarly, a combination of active and passive decay heat removal circuits ensure the decay heat removal

without violating the DSL values on coolant, clad and fuel. Further, in addition to defense in depth philosophy, the concept of periodic surveillance and fail-safe design is also employed to obtain the stringent reliability requirement of very low value of CDF. The fail-safe behavior is the capability of any system or a component to reach a predefined safe state in the event of malfunction of component(s). While it would be difficult to reduce the failure probability of I&C systems beyond a lower limit, it would still be possible to reduce the “unsafe” failure probability by invoking fail-safe design. In a NPP, I&C for shutdown systems are to be designed “fail-safe” so that any fault in sensors, logic processors or final control elements will lead to shutdown of the reactor. Similarly, systems for decay heat removal should ensure timely initiation and sustenance of decay heat removal after reactor shutdown. Any fault in such systems should initiate unintended decay heat removal even if it leads to loss of power rather than failure to initiate safety action.

The fail-safe safety systems are necessary to be incorporated in the design of Fast Breeder Reactors (FBRs). Such reactors are recognized for India's second-stage nuclear energy programme, which is aimed at better utilization of its limited Uranium and abundant Thorium. Unlike thermal reactors, fast reactors are designed not in the most reactive configuration. Further, they have smaller core size with high power density. They are also characterized by very low prompt neutron life time  $\sim 10^{-7}$  seconds and low effective delayed neutron fraction ( $\beta_{\text{eff}}$ ). Hence, they require a fast acting shutdown system and coolants with high heat transfer capacity. The systems used in PHWRs like poison injection and moderator dumping are not suitable for FBRs. The designs of I&C systems for shutdown, core monitoring and decay heat removal are very challenging in sodium cooled fast reactors because they have to provide high levels of safety. There are many I&C systems working in the sodium environment at high temperatures and high radiation dose. The decay heat removal systems in a pool type FBR are typically

passive in nature depending on natural circulation of sodium with minimal intervention of I&C. Fast reactor technology has been demonstrated in an indigenously developed 40MWt sodium cooled mixed carbide fuelled Fast Breeder Test Reactor (FBTR). A 500MWe mixed oxide Prototype Fast Breeder Reactor (PFBR) with sodium coolant is in the advanced stage of commissioning at Kalpakkam. FBRs with improved safety features are also planned for the future. They have to meet the evolving Gen-IV safety criteria which demands practically eliminating the core destructive accidents by adopting the concept of Design Extension Condition (DEC) [1]. This requirement gives us the motivation for a comprehensive study of fail-safe safety system design and finding the areas requiring improvement for meeting the above design objective. In addition, the incident of uncontrolled withdrawal of one absorber rod in FBTR during criticality in the early periods of its operation also encouraged us to perform this study. The present research work is focused towards developing fail-safe safety systems for applications in future fast reactors with improved safety. A review of the current practices, assumptions and techniques followed in I&C for shutdown and decay heat removal systems of a sodium cooled fast reactor towards achieving a fail-safe design is made in the first part of this thesis with emphasize on the areas of concerns for further improvements. Remaining part gives the works carried out as part of this thesis work.

## **1.2 An Overview of Instrumentation and Control Systems in a Nuclear Power Plant**

The structure of I&C in a NPP is shown in Figure 1.2. Functions concerning overall plant performance and mode of operation are controlled and monitored at plant control level. The protection systems continuously monitor the state of the reactor and other components, initiating reactor shutdown and maintain it in a safe state during normal and accident conditions. In some NPPs, diverse systems are incorporated to monitor, control and assist in preventing operation

outside the safety margins, which would invoke the safety system. System level keeps all process variables within normal operating values. Component control level is relatively simple logic functions and interlocks, usually in connection with the actuation of single components (pumps, motors, etc).

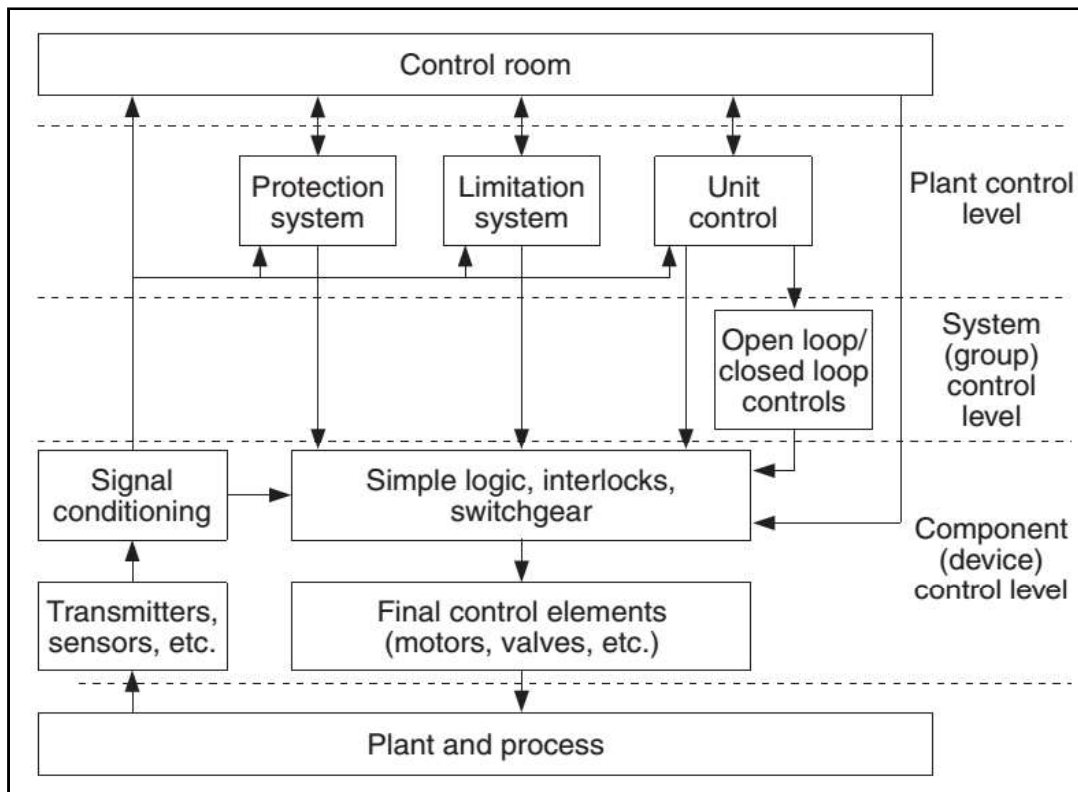


Figure 1.2: Structure of I&C in a NPP [2].

I&C systems are broadly classified into two systems; systems that perform functions important to safety and systems that perform functions that are not important to safety as shown in Figure 1.3. I&C safety systems perform the primary safety functions such as safe shutdown of the reactor or the removal of residual heat from the core, or they limit the consequences of anticipated operational occurrences and design basis accidents. Safety related I&C systems perform other functions important to safety which is not performed by safety systems.



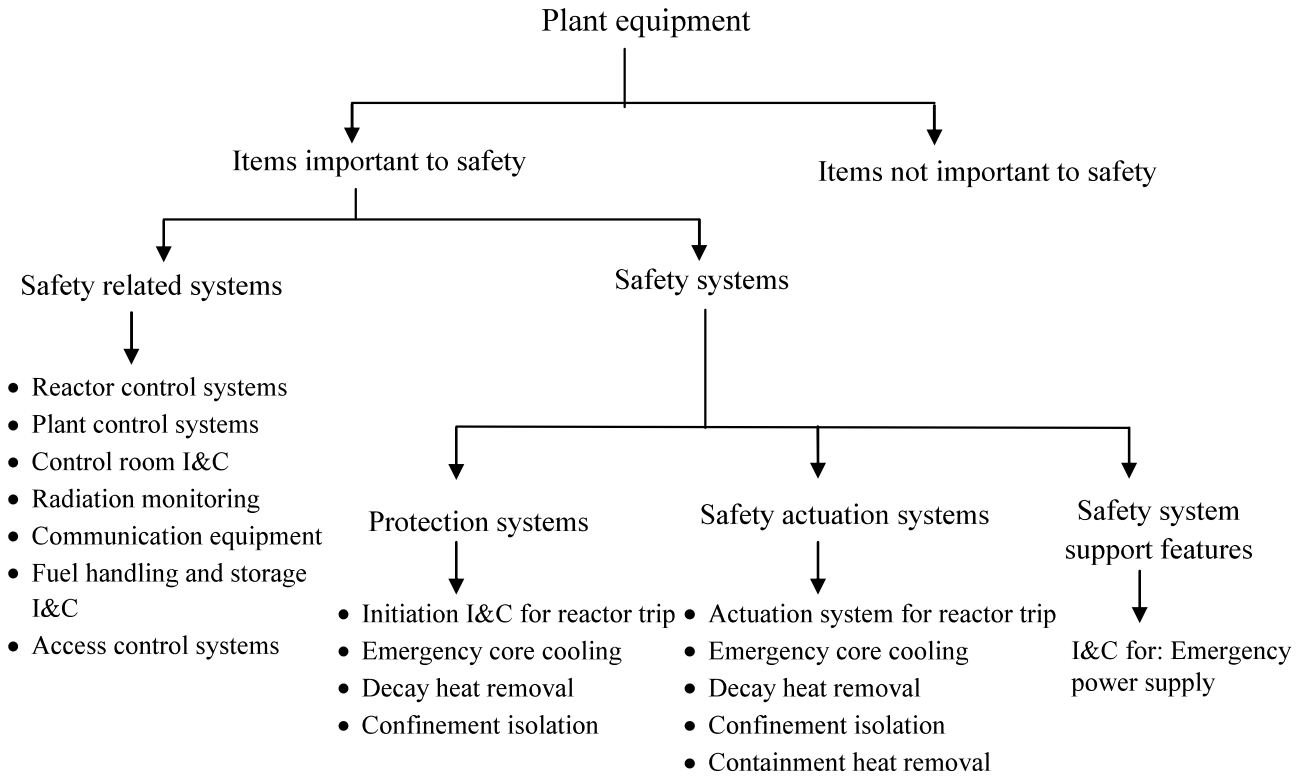


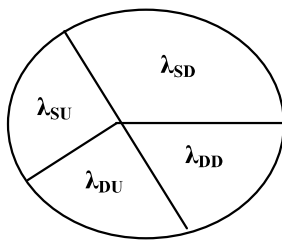
Figure 1.3: Classification of I&C systems in a NPP.

### 1.3 Fail-safe Design

The design of safety systems should ensure safety of the plant. As per the functional safety standard IEC 61508, released by International Electro-technical Commission, a dangerous failure (unsafe failure) is a failure which has the potential to put the safety system in a hazardous or fail-to-function state. This means that the safety system is not able to respond properly upon a demand. A safe failure is a failure which will not put the safety system in a fail-to-function state. It can rather result in an activation of the safety function without any demand present. A “fail-safe” design has the likelihood that the plant is put in safe state under postulated failures due to engineered design features. Fail-safe design plays an important role in enhancing the safety and achieving probabilistic reliability goals. As a quantitative reliability measure, average Probability of Failure on Demand ( $PFD_{Avg}$ ) is used to assess the fail safeness for low demand mode operation [3]. It indicates the probability of a system failing to respond upon a demand in a

specified time interval.  $PFD_{Avg}$ -unsafe, the “failure” means failure in unsafe mode and it is the parameter of interest in safety systems like shutdown systems and decay heat removal systems (Henceforth  $PFD_{Avg}$  is used to refer to  $PFD_{Avg}$  -Unsafe).

The total failure rate  $\lambda$  of a component is given by  $\lambda = \lambda_D + \lambda_S$  where  $\lambda_D$  and  $\lambda_S$  are respectively the dangerous and safe failure rates [4]. Dangerous failure is a failure which has the potential to put the safety system in a fail-to-function state. This means that the safety system is not able to respond properly upon a demand. A safe failure will result in an activation of the safety function without any demand present. Both dangerous and safe failures can further be split into detected and undetected as shown in Figure 1.4. It implies that a detected failure is revealed at the time the failure arises while an undetected failure discloses when the safety is function tested or sometimes only upon a demand.



$\lambda_{SD}$  = Safe Detected failure rate

$\lambda_{SU}$  = Safe Undetected failure rate

$\lambda_{DD}$  = Dangerous Detected failure rate

$\lambda_{DU}$  = Dangerous Undetected failure rate

Safe failure rate ( $\lambda_S$ ) =  $\lambda_{SD} + \lambda_{SU}$

Dangerous failure rate ( $\lambda_D$ ) =  $\lambda_{DD} + \lambda_{DU}$

Figure 1.4: Failure rate distribution [5].

The basic equation to calculate  $PFD_{Avg}$  is

$$PFD_{Avg} = \frac{1}{\tau} \int_0^{\tau} 1 - e^{-\lambda_{DU}t} dt \approx \frac{\lambda_{DU}\tau}{2} \quad (1)$$

For very small values of  $\lambda_{DU}$  and practical value of  $\tau$ .

where  $t$  is the mission time of the system;  $(0, \tau)$  is the first proof test interval.

Self-diagnostics helps in detecting dangerous failure. A quantitative parameter to represent self-diagnostics is the diagnostic coverage factor, which is defined as the ratio of number of dangerous failures detected to the total number of dangerous failures in the system. Proof testing

is usually manual and is more elaborative than self-diagnostic tests. Proof test interval ( $\tau$ ) is the interval between subsequent proof tests. Special test points are to be provided in the system to ensure complete fault coverage during a proof test. When the system is assumed to be as-good-as-new after each proof test, variation of PFD with time is shown in Figure 1.5. With the aid of fail-safe design, system can be taken to fail-safe state when dangerous failures are detected. Thus the study of fail-safe design is concerned about related attributes of “high safe to unsafe failure ratio”, “higher diagnostic coverage” and “reduced test interval”, each contributing to the overall reduction of  $PFD_{Avg}$ .

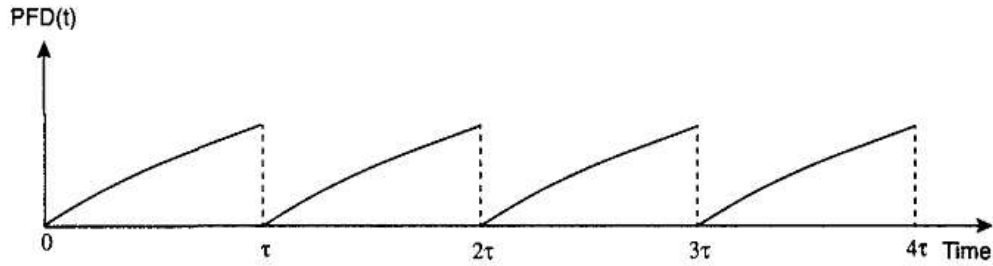


Figure 1.5:  $PFD_{Avg}$  of a periodically proof tested system.

## 1.4 Literature Survey

### 1.4.1 Design principles to reduce probability of failure on demand

From the literature survey, it is observed that the following design principles are generally used to achieve very high reliability in safety critical systems.

#### a. Redundancy and the single failure criterion

The principle of redundancy is applied as a fundamental measure for improving the reliability of systems important to safety. The design ensures that no single failure could result in a loss of the capability of a system to perform its intended safety function [6]. Shutdown systems typically use triple modular redundancy or quadruple redundancy to measure the same process variable [7], [8].

*b. Diversity*

Diverse means are used to gain sufficient protection with respect to dependent failures. Diversity is achieved by technically different functional elements of hardware to implement the same functionality, system software and by using products of different manufacturers [9]. The principle of diversity is applied to enhance reliability and to reduce the potential for common cause failures [6], [10]. Diversity between safety I&C systems and non safety I&C systems is provided for defense in depth against common cause failures [11].

Diverse computerized safety I&C system is also used in reactor protection systems to control the dependent failures [9], [12].

*c. Independence*

The principle of independence (functional isolation and physical separation by means of distance, barriers or a special layout for reactor components) is applied to enhance the reliability of systems, in particular with respect to Common Cause Failures (CCF) [6]. In any NPP, at least two shutdown systems are used and these are functionally different and physically separate [13].

*d. Fail-safe design*

Systems and components important to safety are designed for fail-safe behavior, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety function [14]. For an example, reactor protection systems are designed with passive features to the extent possible and any loss of power to shutdown systems results in drop of rods by gravity, which assures fail-safe shutdown [13], [15].

*e. Periodic surveillance*

Safety systems are designed to permit periodic testing of their functionality when the plant is in operation, including the possibility of testing channels independently for the detection of

failures and loss of redundancy. Protection system designs have all aspects of functionality testing from the sensor to the final actuator [14]. All systems important to safety include provisions that allow performance of the required testing, including built-in test facilities. These are capable of being checked at regular intervals to ensure continued correct operation [16]. Safety requirements in NPPs have motivated great interest in on-line monitoring technologies and new diagnostic and prognostic methods to anticipate, identify and resolve equipment and process problems and ensure plant safety and efficiency. Hashemian [17] has discussed the on-line monitoring technologies for sensing-line blockages, testing the response time of pressure transmitters, monitoring the pressure transmitters on-line, cross-calibrating temperature sensors, assessing equipment condition, performing predictive maintenance of reactor internals, monitoring fluid flow and extending the life of neutron detectors.

As discussed in section 1.3,  $PFD_{Avg}$  is the appropriate quantitative parameter for low demand safety instrumented systems. It is of interest to study the mathematical relation between the design principles such as redundancy, diversity, independence, fail-safe design, periodic surveillance and  $PFD_{Avg}$ . In general, safety instrumented systems employ redundant systems with voting logic. IEC 61508- Part 6 provides a set of simplified expressions for  $PFD_{Avg}$  to commonly used architectures and is shown in Table 1.1. For example 2oo3 means 2 out-of 3 voting logic, in which three systems perform a process and that result is processed by a majority voting system to produce a single output & minimum 2 systems should be healthy. In Table 1.1,

- $\beta$  is the fraction of undetected failures that have a common cause and  $\beta_D$  is of those failures that are detected by the diagnostic tests, the fraction that have a common cause.
- Mean Time to Restoration (MTTR) is the time to detect the failure by a diagnostic system and the mean down time until the system is restored.

- When a DU fault has been detected during the proof test, Mean Repair Time (MRT) is the associated downtime to repair/restore the system.

Table 1.1:  $PFD_{Avg}$  equations for various architectures.

S.No.	Architecture	$PFD_{Avg}$
1	1oo1	$\lambda_D \left( \frac{\lambda_{DU}}{\lambda_D} \left( \frac{\tau}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right)$
2	1oo2	$2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 \left( \frac{\lambda_{DU}}{\lambda_D} \left( \frac{\tau}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right) \left( \frac{\lambda_{DU}}{\lambda_D} \left( \frac{\tau}{3} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right)$
3	2oo2	$2\lambda_D \left( \frac{\lambda_{DU}}{\lambda_D} \left( \frac{\tau}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right)$
4	2oo3	$6((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 \left( \frac{\lambda_{DU}}{\lambda_D} \left( \frac{\tau}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right) \left( \frac{\lambda_{DU}}{\lambda_D} \left( \frac{\tau}{3} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right) + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \left( \frac{\tau}{2} + MRT \right)$

Several studies have been made on the  $PFD_{Avg}$  formulae of IEC 61508 and the generalized form of koon (k-out-of-n) voting combinations. Jahanian [18] has proposed a generalized  $PFD_{Avg}$  formula for koon architecture and has proven that it matches with IEC 61508 by applying various values to k and n. These expressions assume 100 % proof test coverage.

By considering  $PFD_{Avg}$  of voting logic,

$$\begin{aligned}
 PFD_{Avg} = & \prod_{i=1}^{n-k+1} (n - i + 1) [(1 - \beta)\lambda_{DU} + (1 - \beta_D)\lambda_{DD}] \left( \frac{\lambda_{DU}}{\lambda_D} \left( \frac{\tau}{i+1} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right) \\
 & + \beta \lambda_{DU} \left( \frac{\tau}{2} + MRT \right) + \beta_D \lambda_{DD} MTTR + PFD_{Avg}(voting\ logic)
 \end{aligned} \tag{2}$$

and

$$PFD_{Avg}(voting\ logic) = (\lambda_{1DU} + \lambda_{1DD}) \left[ \frac{\lambda_{1DU}}{\lambda_{1D}} \left( \frac{\tau}{2} + MRT \right) + \frac{\lambda_{1DD}}{\lambda_{1D}} MTTR \right] \tag{3}$$

Equations (2) and (3) show the generalized  $PFD_{Avg}$  for a redundant safety system with voting logic. As was discussed, safety instrumented system uses various design principles to achieve

high reliability. The way in which these design principles impact  $PFD_{Avg}$  is described in Table 1.2.

Table 1.2: Relation between design technique and  $PFD_{Avg}$ .

S. No.	Design principle	Relevant Parameter in $PFD_{Avg}$
1	Redundancy	<ul style="list-style-type: none"> <li>• Coefficient term <math>(n-i+1)</math> and power term to <math>((1 - \beta)\lambda_{DD} + (1 - \beta)\lambda_{DU})</math> are the predominant factors in <math>PFD_{Avg}</math> influenced by the chosen redundancy and type of voting.</li> <li>• Triple Modular Redundancy (TMR) with 2oo3 voting is often chosen in reactor safety system since it offers a balance between safety and spurious actions. The TMR architecture also allows for taking one of the three channels for testing without shutting down the plant.</li> </ul>
2	Independence	<ul style="list-style-type: none"> <li>• Independence and diversity leads to reduction in common cause failure fraction. It is apparent from equation I that <math>\beta</math> and <math>\beta_D</math> has a strong potential to nullify the benefits from redundancy.</li> <li>• Providing dedicated sensors for redundant channels, independent power supply, placing redundant signal processing electronics in three separate rooms, following different cable routing paths are typical independence features in a NPP safety system.</li> </ul>
3	Diversity	<ul style="list-style-type: none"> <li>• Sensors with diverse working principles, different technologies in signal processing electronics and using different methods for final actuation are typically followed for diversity in a NPP.</li> </ul>

S. No.	Design principle	Relevant Parameter in $PFD_{Avg}$
4	Periodic surveillance	<ul style="list-style-type: none"> <li>• <math>\lambda_{DU}</math> is reduced by improved diagnostic coverage during periodic self-tests.</li> <li>• Effect of <math>\lambda_{DU}</math> on <math>PFD_{Avg}</math> is reduced with frequent proof tests. <math>\tau</math> is typically in days or months.</li> <li>• Effect of <math>\lambda_{DD}</math> on <math>PFD_{Avg}</math> is reduced by frequent self-tests. In digital I&amp;C systems, test interval can be in seconds or lesser.</li> <li>• Diagnostic coverage is one of the most important design parameters to measure the effectiveness of safety protection systems. The influence of diagnostic coverage, proof test interval and common cause failures on <math>PFD_{Avg}</math> is detailed in [19], [20] and [21]. The shorter proof test period and the higher proof test coverage indicate the smaller probability of failure on demand. Velten et al., [22] have studied the effect of diagnostic coverage, proof test coverage and proof test interval on <math>PFD_{Avg}</math> for different architectures. The diagnostic coverage and proof test interval have the most influence on <math>PFD_{Avg}</math> for all architectures. Proof test coverage has less significant effect on <math>PFD_{Avg}</math>.</li> </ul>
5	Fail-safe design	<ul style="list-style-type: none"> <li>• There are two aspects of fail-safe design. Firstly, <math>\lambda_D</math> is minimized by appropriate component selection and configuration. For example, consider in a shutdown system, an electromagnetic relay is kept energized normally and is de-energized to communicate a shutdown demand. This configuration depends on the fact that the</li> </ul>



S. No.	Design principle	Relevant Parameter in $PFD_{Avg}$
		<p>failure rate of relays in fail-to-open mode is low compared to fail-to-close mode.</p> <ul style="list-style-type: none"> <li>The second aspect is to ensure by design that the system is taken to safe state in case a dangerous failure is detected. This allows for the assumption that all detected failures result in safe state of the system in equation 2.</li> </ul>

#### 1.4.2 Survey on design principles used in shutdown systems

Apart from the design approaches, the general principles used in a typical shutdown system is discussed below. The purpose of the Shutdown System is to terminate the fission reaction upon any anomaly and there by ensure the safety. The three main parts in I&C loop of a shutdown system are sensor, Processing Electronics (PE) and final control element. In a sodium cooled fast reactor, redundant shutdown systems typically employ gravity drop of neutron absorber rods as a means of achieving reliable shutdown. As mentioned earlier, the methods used in Pressurized Heavy Water Reactors (PHWRs) like poison injection and moderator dumping are not suitable or difficult to design in Sodium cooled Fast Reactors. Generalized schematic of SDS is shown in Figure 1.6.

Sensors are used to measure plant parameter like neutron density, coolant temperature, flow rate, etc. All signals are typically measured with redundant and independent sensors. Typically triplicated independent sensors are used to ensure reliability [7]. To diagnose the performance of redundant sensors online, cross calibration method is widely used to detect the drift of any sensor's signal from its redundant group [17], [23]. In this method a simple average is calculated to obtain the band and then existence of each signal inside it is verified. Some other

averaging techniques are band averaging with outliers, weighted average and parity space averaging. Along with cross calibration the various diagnostic methods used in sensor stage are empirical modeling, Kalman filtering, model-based online detection technique using artificial neural networks etc., [24]–[27].

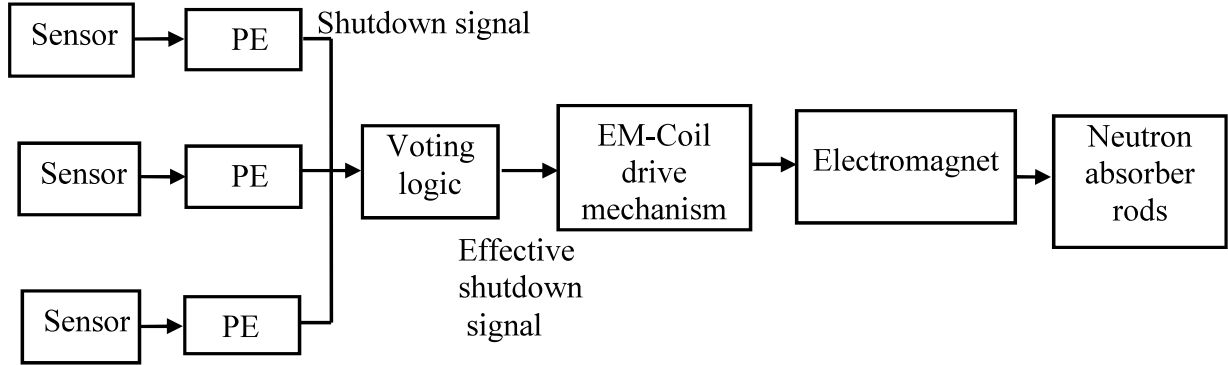


Figure 1.6: Schematic of shutdown system.

Signal processing techniques are applied on redundant sensor signals in Processing Electronics (PE) stage. PE determines whether the process variables are within their allowable band and action is taken to drop the neutron absorber rods into the core when specified conditions are violated. Sensor cable open and cable short can be detected to invalidate sensor readings. Test interface unit is often provided to inject/superimpose the test signals and the measured output parameter is compared with reference input for diagnostic purpose [28].

2oo3, 2oo4 are the generally used voting logics to prevent a single failure of the shutdown signal [7], [8], [29], [30]. Highly reliable voting logics are employed in shutdown system [2], [30], [31] since the signals from various PEs are converted into effective shutdown signal by the voting logic.

Computer systems are also used as part of shutdown systems at newly-built and upgraded NPPs. [29], [32]–[36]. For instance, Superpheonix reactor core surveillance with temperature processing using digital system is presented in [37].

Jia et al., [38] introduces the means to achieve independence in digital I&C system. The typical design measures for electrical isolation are isolation amplifier, control switch, current transformers, optical couplers, relays, circuit breakers etc. The physical separation adopts with barriers, geometry etc. Communication isolation is achieved with different safety channels. CPU is one of the important equipment of computer systems to accord with the single failure criterion and reliability requirement. Li et al., [39] detailed the different redundancy configurations for CPU such as parallel and standby.

To handle large number of field signals in NPP with high reliability and availability, two different backplane bus-based Real Time Computer (RTC) systems with switch over logic system (SOLS) is proposed [12], [40]. Shin et al., [41] have presented the advanced digital reactor protection system with diverse dual processors to prevent common mode failure. The principle of diversity is applied to both hardware design and software design. IAEA-NTR 2008 [42] gives the examples of digital I&C in various NPPs. Computer systems are easily amenable for on-line self-diagnostics [41], [43].

The final control elements are typically electromagnets which hold neutron absorber rods and are dropped into core under gravity when current to electromagnets are terminated. Predominant failures do not affect the safety of the reactor, since the reactor shutdown occurs immediately if the system fails [7], [10], [13], [15], [44]–[48]. Some of the nuclear reactors use self actuated shutdown systems. The design and testing of a simple and reliable self actuated shutdown system is given in [49], [50]. In this system a ferromagnetic Curie temperature permanent magnet holding device is used. Under increased coolant temperature or neutron flux, the magnetic holding force is reduced which leads to gravity drop of neutron absorber rods.

Bartha et al., [51] have presented the testing and diagnostic methodology of triple modular redundant system and proposed the universal test system for functionality test of reactor

shutdown system. Gaubatz [30] has discussed the four divisions of reactor protection system with quad-redundant sensors providing input to four independent microprocessor-based electronics with automated self test and diagnostics.

While general principles are discussed above, evaluation of circuit level details could not be made due to limited published literature on detailed design of reactor circuits. However, a review of various modules used in Prototype Fast Breeder reactor (a 500MWe sodium cooled fast reactor under commissioning in India) is made as part of the present study, which is detailed in Chapter-2. Fail-safe design features are studied in this reactor.

## **1.5 Research Objectives**

Based on the literature survey and from the study of safety critical I&C of PFBR,

- i. Fail safeness in absorber rods: Falling under gravity is a natural phenomenon and failure probability to insert the rods is remote. The rods drop under failures like loss of power supply, cable cut and common failures in output circuit.
- ii. The PE and voting logic employs sophisticated electronics or computer systems in which fail-safe design is adequately implemented by using techniques like finite impulse tests, test signal superimposition, discordance monitoring, etc. Very high coverage factor could be achieved due to end to end testing exploiting the simplicity in the functional requirement (the PE is basically a threshold comparator).
- iii. The sensor failures are adequately covered by discordance monitoring (comparison of readings from redundant sensors) and signal validation.

Thus the concept of fail-safe design is well applied in all three sections of the I&C loop namely sensors, PE and final control elements. However, it is observed that there is a generic assumption that EM relays fail open. Electromagnetic (EM) relays are often used to

communicate shutdown signal to voting logic [52]. EM relays are preferred over solid-state relays, IGBT etc due to their favorable failure mode. EM relays predominantly fails in contact fail-to-close mode, which is a safe failure for a design. Hence, relays are kept energized during normal operation and de-energized upon a shutdown demand to achieve a fail-safe behavior. However, literature claims that contact erosion, migration of contact materials, weld etc., are various failure modes due to arcing [53]. Contact welding (fail-to-open) is an unsafe failure mode to be carefully considered for critical application. Short time bounce cause stronger weld due to elastic deformation of the contact material [54], [55]. Morin et al., [56] claims that lamp loads has shown contact weld due to inrush current. Neuhaus et al., [57] stated that configuration of the load circuit determines the actual arc current which influences the weld. Hence it is desirable to detect weld failure in relays

From the literature it is observed that offline diagnostic methods are existing. Fang yao, et al., [58] introduced the dynamic contact resistance measurement as a weld diagnostic parameter. Zhou, et al., [59] shows that DC coil current and contactor current as diagnostic and prognostic parameters for the potential failures of contactors. The pull-in voltage, drop-out voltage and contact resistance are some of the commonly used diagnostic parameters [60]. Coil drive voltage and monitoring the contact with at least  $6V_{DC}$  and 100mA are some of the diagnostic parameters.

Currently, to detect relay failure in NPP systems, periodic opening of EM relay contact in one of the channels in a triple redundant architecture (operating in 2 out of 3 mode) is done. Contact status is checked using an auxiliary contact. This is done typically once per shift. If at all an online diagnostic method would exist, this testing could be automated and the test interval time would drastically reduce. ***Hence, it is desirable to find a new method to detect weld failure of EM relay contact online (without opening the relay contact).***

In this thesis work, a technique for online diagnostics of EM relay without affecting the contact status is proposed. The method uses the differences in characteristic decay of coil current during de-energization process between a healthy relay and a relay whose contacts got welded. The method works on the principle of de-energizing followed by quick re-energization of relay coil. The impact of diagnostic circuit on functional circuit is verified by practical implementation of printed circuit board. Further it has been shown in the study that failure probability of each redundant channel can be reduced by around 48 folds by introducing the technique.

As discussed earlier (as shown in Figure 1.1), control system failure contributes probabilistically to CDF by way of increase in demands placed on the shutdown systems. An event took place in FBTR, due to failure in reactor power regulating system. The plant has seen an uncontrolled withdrawal of one of the six absorber rods. Towards approach to criticality, 5 rods were raised to a height of 257mm. The sixth rod was being raised in steps. At about 250mm, even after the release of “raise” push button by the operator, the sixth rod continued to move upward. Investigation has found that this event was due to sluggish behavior of the raise contactor (refusing to open even after the coil supply is withdrawn) which supplied 415V power supply to the motor [61]. As per IEC-60947 [62], for high current relays (contactors), the predominant failure mode is “fail-to-open” (73%). *Hence, further studies are required to verify the reliability of EM contactor (weld failure) and its impact on uncontrolled withdrawal of neutron absorber rod.*

Reliability Demonstration Testing (RDT) is conducted to electromagnetic contactors as part of this study. The test plan is selected from MIL-HDBK-781A for fixed duration to verify the contactor failure modes. RDT has shown that failure probability of fail-to-open mode is less under the influence of cyclic stress to this particular contactor model. Surface morphology studies have shown formation of Ni precipitates due to arcing.

It is also observed that much of the circuits depend on periodic testing as a powerful defense against unsafe failures. Inherent fail-safe circuits do not require diagnostics since any of the failures in the circuit will automatically lead to a safe state of the final control element. Thus, inherent fail-safe design is a design alternative to systems with periodic self-testing. These circuits will have a lower  $PFD_{Avg}$  since the periodicity of self-test is tending to zero and the issues arising out of failures in diagnostic circuitry does not exist. However, it would be difficult to have inherently fail-safe design for complicated circuitry. *The potential for using inherently fail-safe circuits are to be explored to achieve very low  $PFD_{Avg}$  as an alternative to systems with periodic self-tests.*

In this thesis, a novel fail-safe AND gate is proposed and it is experimentally demonstrated as fail-safe under all probable failure modes. An inherent fail-safe pulsating electronic logic valve drive circuit with AND gate is designed for a decay heat removal system. This circuit consists of pulse generators, combinational logic (AND/OR) and driver. Quantitative analysis has shown a very low  $PFD_{Avg}$  since the system fails in unsafe mode only upon combination of multiple failures.

## 1.6 Organization of the Thesis

From the above listed objectives, the thesis is structured into seven chapters.

**Chapter 2** elaborates the safety critical I&C systems in PFBR such as shutdown system and decay heat removal system. Subsequently, the various design provisions in these systems to reduce  $PFD_{Avg}$  are discussed and techniques used in achieving fail-safe design of I&C loop are elaborated.

**Chapter 3** presents a novel method developed as part of this thesis work, to detect electromagnetic relay contact in fail-to-open mode failure without disturbing the load attached to

the contact. This method is online, continuous, automatic and facilitates simultaneous testing of redundant channels. Diagnostic circuit and test results are presented in this chapter.

**Chapter 4** presents the practical implementation and verification of relay contact weld detection circuit as proposed in chapter 3 using a relay output card. Markov modeling is established to verify the reliability improvement achieved with online diagnostics. Sensitivity analysis is presented by varying the test interval and proof test interval.

**Chapter 5** discusses the Reliability Demonstration Testing (RDT) of EM contactor to study the impact of uncontrolled withdrawal of neutron absorber rods. Testing was carried out based on a test plan as per Military handbook: MIL-HDBK-781A for fixed testing time method. The results of SEM (Scanning Electron Microscopy) and EDS (Energy Dispersive Spectroscopy) analysis carried out on contact surface to analyze the failure mode are also discussed.

**Chapter 6** discusses inherently fail-safe electronic logic design to lower  $PFD_{Avg}$ . A novel inherently fail-safe AND gate is proposed. Inherent fail-safe electronic logic circuit with AND gate is investigated for decay heat removal system damper control logic in PFBR.

**Chapter 7** summarizes the major conclusions drawn from the research work towards fail-safe design of safety critical I&C systems. This chapter also explains the scope for possible improvements of our works in future.



# 2

## STUDY OF SAFETY CRITICAL I&C SYSTEMS IN PFBR

---

*The present chapter provides a review of safety critical I&C systems in Prototype Fast Breeder Reactor such as shutdown system and decay heat removal system. The various design provisions in these systems to reduce  $PFD_{Avg}$  are discussed and techniques used in achieving fail-safe design of I&C are elaborated.*

---

### 2.1 Introduction

Prototype Fast Breeder Reactor (PFBR) is a 1250MWt, 500MWe, sodium cooled, Plutonium oxide-Uranium Oxide fuelled, pool type fast reactor under commissioning in India. All reactor structures, systems and components are classified systematically based on their safety functions. The events with a frequency of occurrence  $\geq 10^{-6}$ /year are considered as a Design Basis Event (DBE) and these have been further classified into categories I–IV events as shown in Table 2.1. The DBEs are the set of events that serve as the basis for the establishment of design requirements to systems, structures and components within the plant. DBEs include normal operations, operational transients and certain accident conditions under postulated initiating events considered in the design of the facility.

I&C systems of PFBR are classified as Safety Class (SC)-1 (safety-critical), Safety Class-2 (safety-related) and Non Nuclear Safety (NNS) systems. All systems which monitor shutdown parameters (SCRAM parameters) like coolant outlet temperature, neutronic flux, primary sodium pump speed, reactor inlet temperature are classified as SC-1. Additionally, I&C of Safety Grade

Decay Heat Removal (SGDHR) system and Reactor Containment Isolation Logic are classified as SC-1 systems.

Table 2.1: Design basis events.

Category	Frequency (f) (/r-y)
1	Normal operations
2	$f > 10^{-2}$
3	$10^{-2} > f > 10^{-4}$
4	$10^{-4} > f > 10^{-6}$

Chetal et al., has detailed the design features of PFBR like reactor core, reactor assembly and I&C [63]. Flow sheet of PFBR is shown in Figure 2.1. Review of shutdown system and decay heat removal system in PFBR is carried out based on [44], [64]–[76] and the internal documents. I&C design details and techniques followed in achieving fail-safe design of shutdown system and decay heat removal system in PFBR are studied in this chapter.

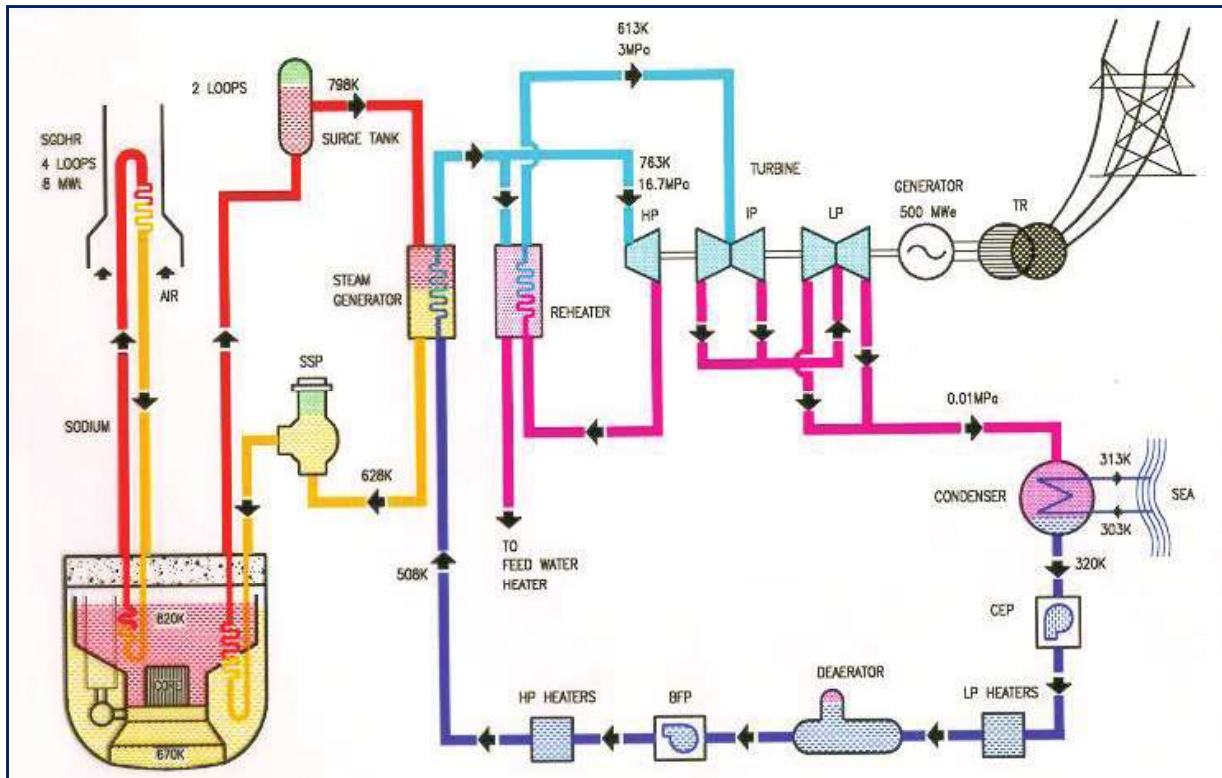


Figure 2.1: Flow sheet of PFBR.

## 2.2 Shutdown System

PFBR is provided with two redundant, independent, diverse and fast acting shutdown systems (SDS-1 and SDS-2). The failure probability requirement of each SDS system should be less than  $10^{-3}$ . The overall failure probability of SDS should be less than  $10^{-6}$  [77].

Each SDS consists of a Reactor Protection System (RPS) and Actuation System (AS). RPS consists of sensors, SCRAM Generation Electronics (SGE) and a voting logic. Signals from sensors are processed by SGE. SGE performs signal conditioning and generates a SCRAM signal in case the measured parameter crosses a configured set point. Triplicated SGEs are provided with each connected to a dedicated sensor. The resulting SCRAM signal is processed by a voting logic (2oo3 logic also known as safety logic) which produces “effective SCRAM”, leading to de-energization of electromagnets. AS consists of neutron absorber rods, electromagnet and drive mechanisms to drive the neutron absorber rods into/out of the reactor core. Schematic of SDS is shown in Figures 1.6 and 2.2. SDS-1 consists of 9 absorber rods known as Control and Safety Rods (CSR). SDS-2 consists of 3 absorber rods known as Diverse Safety Rods (DSR).

### 2.2.1 Sensors

The plant monitoring is done by functionally diverse set of sensors.

#### *1. Neutron flux sensors*

The neutronic instrumentation consists of fission chambers resistant to radiation and high temperature to monitor neutron flux in the startup, intermediate and power range. Neutronic flux is monitored in 2oo3 voting logic. SCRAM takes place when the derived parameters like logarithmic power, linear power, reactor period ( $\tau$ ) and reactivity ( $\rho$ ) thresholds are crossed in 2 of the 3 redundant channels.

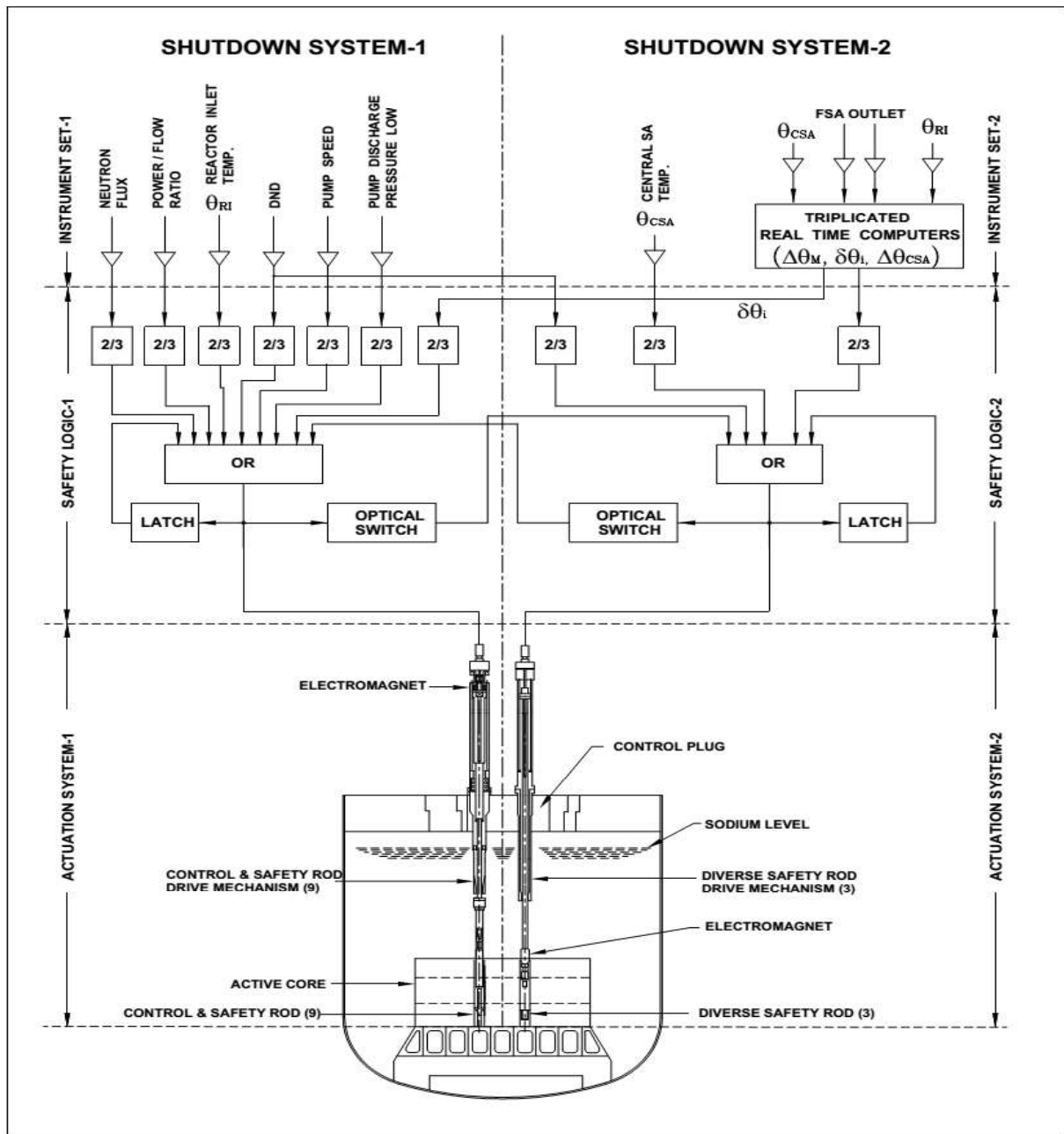


Figure 2.2: Shutdown system in PFBR.

## 2. Thermocouples

Core Temperature Monitoring System (CTMS) is provided to measure core inlet and outlet temperatures. Fast response K-type thermocouples mounted on the central canal plug monitor the central fuel sub assembly sodium outlet temperature ( $\theta_{CSA}$ ) and used in 2oo3 voting. K-type thermocouples are provided in each of the two primary sodium pump suction to monitor

the reactor inlet temperature ( $\theta_{RI}$ ).  $\theta_{RI}$  and  $\theta_{CSA}$  signals are processed through triplicated hardwired electronics. Two thermocouples provided over each of the fuel sub assemblies monitor SA sodium outlet temperature ( $\theta_i$ ) at individual SA. Parameters like the mean fuel SA sodium outlet temperature ( $\theta_M$ ), mean core sodium temperature rise ( $\Delta\theta_M$ ) and deviation of individual SA sodium outlet temperature ( $\delta\theta_i$ ) are computed online.  $\theta_{CSA}$ ,  $\Delta\theta_M$ ,  $\theta_{RI}$ ,  $\Delta\theta_{CSA}$  and  $\delta\theta_i$  cause SCRAM when their thresholds are crossed in 2 of the 3 redundant channels.

### 3. Electromagnetic flow meters

Electromagnetic flow meters measure sodium flow (Q) provided by each primary sodium pump. Each flow meter consists of three pairs of electrodes. This signal is used to obtain pressure head ( $\Delta H$ ) across the pump and power to flow ratio (P/Q) and used as SCRAM parameters with 2oo3 voting.

### 4. Delayed neutron detectors

Delayed Neutron Detectors (DND) are provided to detect and SCRAM the reactor for fuel clad rupture. DND blocks with three detectors are placed at the inlet of the four intermediate heat exchangers (IHX). The DND outputs are connected to both voting logics in both shutdown systems so that the reactor is brought automatically to a safe shutdown state in case of fuel clad failure. The system provides triplicated detection and uses 2oo3 voting logic to avoid spurious SCRAM.

Some of the salient features in design of sensors which help to achieve a low  $PFD_{Avg}$  are

- Signal validation: For any signal, apart from process range, there is a range out of which there is a large probability that sensors are at fault. For instance, though the range for coolant (liquid sodium) channel temperature measurement is 0-800°C, temperature reading cannot be below melting point of sodium. Moreover, the coolant temperature at the outlet of a fuel

assembly cannot be lesser than that measured at the inlet. Such rules are used to validate signal measurements and invalid signals are treated as “crossed the SCRAM set point”. This provision results in reducing  $\lambda_{DU}$ .

- Open sensor detection: Signal conditioning units are designed to pull HIGH for open sensors. This will result in an invalid reading. This provision results in reducing  $\lambda_{DU}$ .
- Discordance monitoring system: Each SCRAM parameter is measured using three independent and redundant sensors. A separate discordance monitoring system is provided to compare measurements from redundant channels and alert the operator in case of discrepancy between the redundant measurements. This provision helps in reducing  $\lambda_{DU}$ .
- Diverse SCRAM parameters: For each DBE, two diverse SCRAM parameters are provided; one connected to SDS-1 and the other to SDS-2. They are processed by independent sensors. The sensors used in SDS-1 and SDS-2 use diverse principles. Such features help in reducing common cause failure fraction.

## 2.2.2 Signal processing

### 2.2.2.1 SCRAM generation electronics

Signals from each sensor are processed with suitable analog signal processing circuits. Salient design features which help in achieving a low  $PFD_{Avg}$  are

- Provision for signal super imposition, check back and Good Operation Trip (GOT): An online testing provision is provided in each SGE. When triggered, an internally generated signal will superimpose on the actual signal, thus imitating a SCRAM condition. The result of such a test is reported to the operator. Since the voting logic generates effective SCRAM with 2oo3 voting, reactor operation is not hindered during such tests. A GOT is generated in case such a test fails. Since this test exercises all parts of the SGE from sensor terminal to output stage, this can be treated as a proof test with a near 100% coverage.

- Automation of periodic testing and logging: SCRAM parameters are to be tested in a sequential fashion. To avoid operator fatigue and errors, a separate “Test Interface Unit (TIU)” is provided in the plant to automate the test. TIU takes care of sequencing, logging and reporting of results. In every shift, one of the three redundant channels is tested for all SCRAM parameters.
- Discordance monitoring in set points: The “set points” registered in each SCRAM generation circuit are digitized and sent to the plant central computer periodically. An alarm is raised in case of discordance between redundant units. This provision helps in providing additional diagnostic coverage on SGEs.

#### 2.2.2.2 Voting logic (safety logic)

The voting logic for SDS-1 is known as safety logic with Finite Impulse Test (SLFIT) and for SDS-2 is known as Pulse coded Safety Logic (PCSL).

##### 2.2.2.2.1 Safety Logic with Finite Impulse Test (SLFIT)

SLFIT is based on digital logic circuits and is implemented using Field Programmable Gate Array (FPGA). It consists of two functional blocks namely safety logic and FIT Logic. Safety logic system receives SCRAM parameter signals, GOT signals, Auto Inhibition (AI) signals, Manual Inhibitions (MI), manual reset and manual SCRAM. The system also receives cross link signal from the PCSL system. To maintain fail-safe behavior, logic HIGH is treated as “NORMAL” and logic LOW is treated as “SCRAM” and 2oo3 voting is performed with reverse logic. To prevent safety logic system failing in unsafe mode, an on-line test facility i.e., Fine Impulse Test (FIT) is provided. The block diagram of SLFIT system is shown in Figure 2.3.

There are 32 triplicated SCRAM parameters, which are divided into two groups namely Group-A and Group-B. All the input signals are processed with different types of signal

conditioning circuits. These boards provide isolation and perform logic level translation to Transistor-Transistor Logic (TTL) level. 2oo3 voting logic is performed on the triplicated signals. Grouping logic performs logical AND operation among the input signals and generate output signals for electromagnet coil drive circuit. Timer and latching circuit continuously monitors the status of Grouping Logic stage output. If any one of these signals or both the signals become logic ‘LOW’ the timer operation starts i.e., the duration for which signals remains logic ‘LOW’ (continuously) is measured and if the duration is  $> 50\text{ms}$ , a latched output signal is generated. If the duration of the logic ‘LOW’ condition is  $< 50\text{ms}$ , it is ignored. IGBT (Insulated-Gate Bipolar Transistor) board consists of IGBTs and FIT pulse detection circuit.

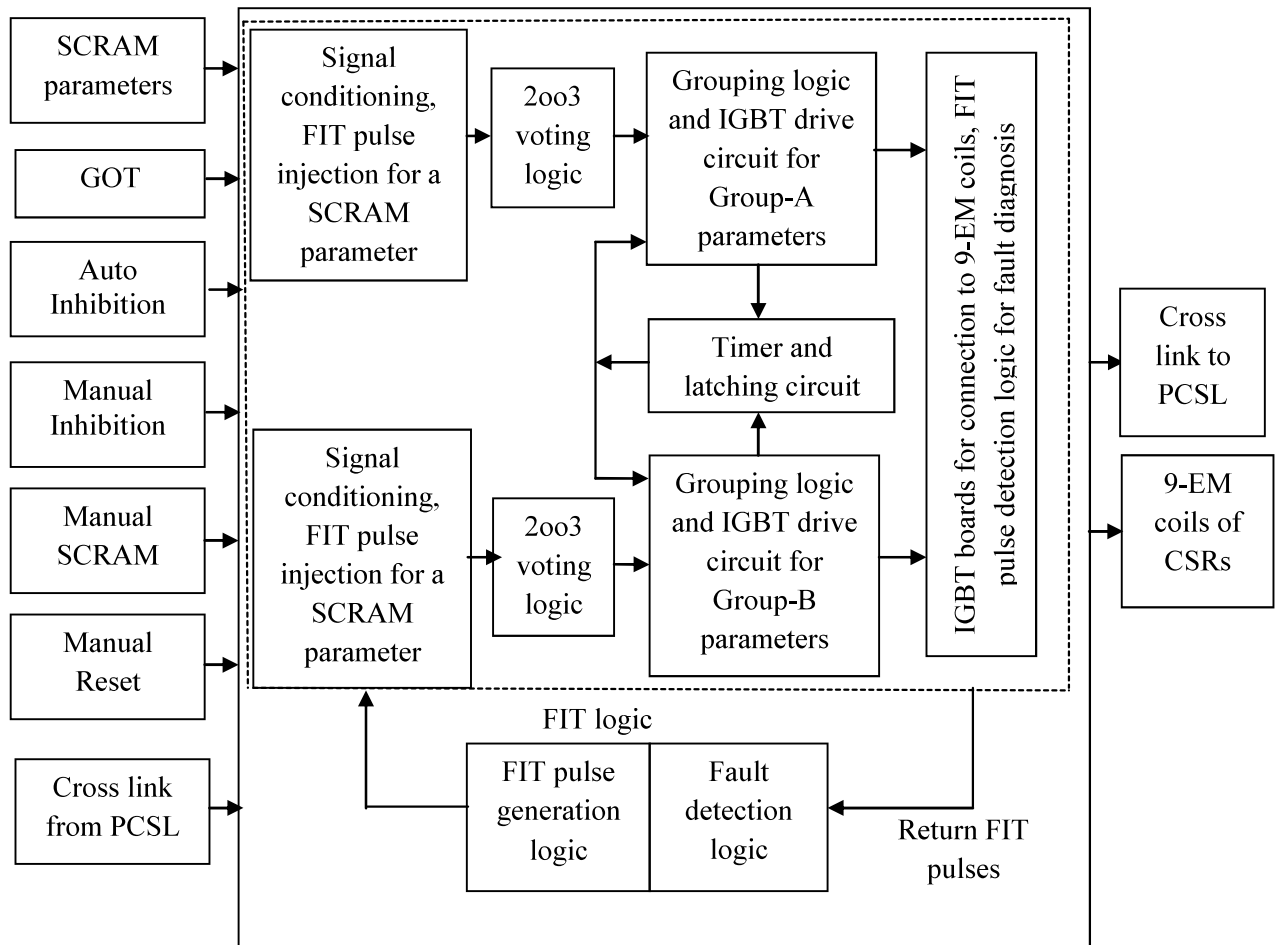


Figure 2.3: Block diagram of SLFIT system.



In order to detect stuck at 'LOW' or stuck at 'HIGH' faults, an on line test facility i.e., FIT Logic is provided. FIT Logic injects short duration trip pulses (1ms duration) in all the SCRAM parameters in a predefined order and in required combinations of trip pulses, namely, A, B, C (1oo3 mode, at a time one channel receives trip pulses), AB, BC, CA (2oo3 mode, at a time 2 channels receive trip pulses), ABC (3oo3 mode, at a time all 3 channels receive trip pulses) at the input stage of safety logic and verifies the propagation of these short trip pulses at the final stage of safety logic chain. These pulses propagate through various logic processing stages in the safety logic and traverses up to the electromagnet coil terminals. Based upon the presence or absence of pulses at coil terminals, for a given combination (1oo3, 2oo3 or 3oo3 mode), safe and unsafe faults are detected. The pulses are too short that electromagnet will not respond to de-energization signal but long enough to detect the failures.

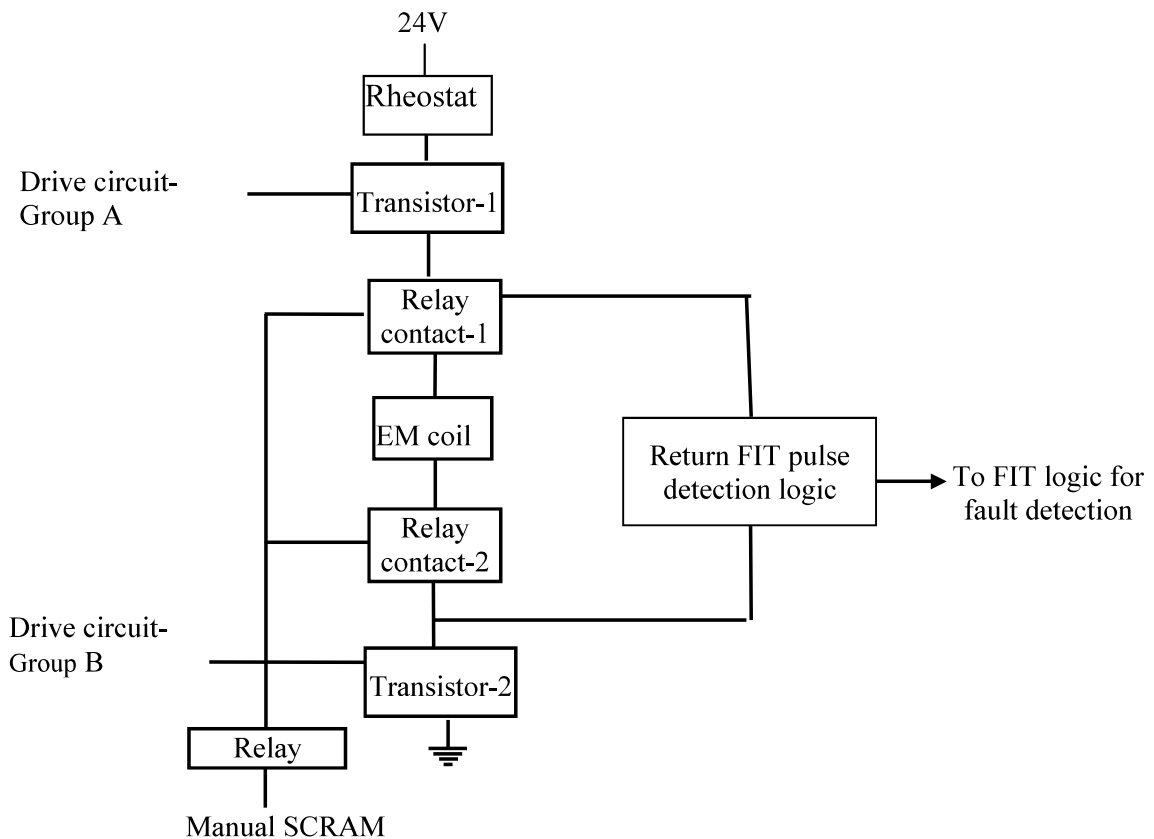


Figure 2.4: Electromagnet coil connection diagram.

To ensure the healthiness of FIT logic, self-diagnostic checks are built into the FIT Logic. Self-diagnostics in FIT detects pulse generation fault, pulse width stretched fault and address sequence fault. The superimposition pulses are fed at the input stage and the feedback is taken at input line to the electromagnet, the test can be considered as a proof test. Because of the short test pulses, a proof test interval in the order of minutes could be achieved leading to very low  $PFD_{Avg}$ . The remaining  $PFD_{Avg}$  is then decided by the inability to automatically put the system to a safe state for certain failures. FIT unavailability also contributes to  $PFD_{Avg}$ . One set of manual SCRAM contacts are processed and two sets of relay contacts are connected in series with the coil as shown in Figure 2.4. Independent IGBT circuitry is provided for each electromagnet. 300Ω resistor and freewheeling diode are connected across the coil. FIT pulses are detected on this circuit and sent to the diagnostic logic for detection of safe and unsafe faults. Electromagnet hold the CSRs when the coils are in energized condition. Any trip order > 50ms from any SCRAM parameter de-energizes all the 9 electromagnets.

#### 2.2.2.2.2 Pulse Coded Safety Logic (PCSL)

The safety logic design associated with SDS-2 is PCSL. Majority of faults in solid state logic circuit results in stuck at LOW or stuck at HIGH and hence PCSL uses dynamic pulse train which is an inherently fail-safe design. A dynamic logic signal drives the electromagnet during the normal reactor operation and in case of static failure in logic/component, dynamic signal is lost, which leads to de-energization of coil and shutdown of the reactor. The block diagram of PCSL is shown in Figure 2.5.

Signal conditioning circuits receive triplicated input from trip channels (core temperature,  $\delta\theta_i$ , DND), GOT signals, inhibition signal, signal from SLFIT and condition it from 24V to 5V level. It also injects the coded pulses from code generation logic to the channel input and

optically isolates from the core logic system. Crystal oscillator is used to generate the clock. Since the failure of clock leads to SCRAM of reactor, two crystal oscillators are used to provide redundancy. 2×1 multiplexer feeds one of the clock output. Code generation logic generates Code\_A, Code\_B, Code\_C, Code\_2003, Pulse\_D and Pulse\_E from the basic clock as shown in Figure 2.6.

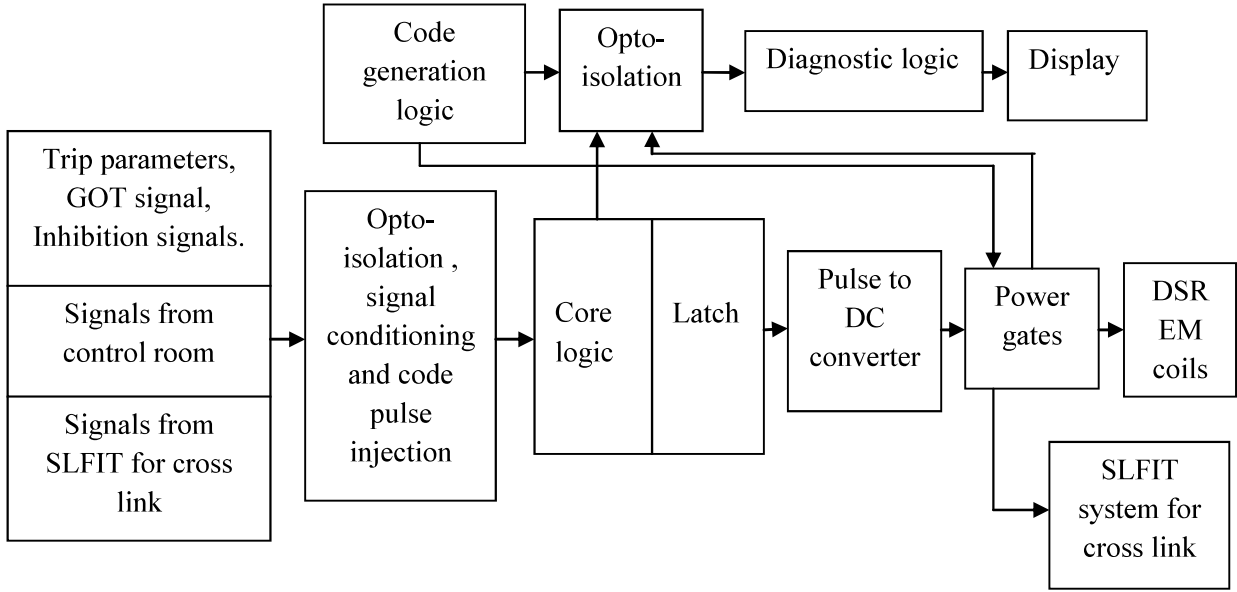


Figure 2.5: Block diagram of PCSL system.

Code\_A pulse is super-imposed along with the channel A trip parameter (CH-A). Then the trip circuit output  $A_1$  will be same as code\_A pulse when the channel A is normal and at logic LOW when CH-A is tripped. Similarly, Code\_B pulse and Code\_C pulse are superimposed along with the channel B of trip parameter (CH-B) and channel C of trip parameter (CH-C) respectively. These pulse codes repeat after every 10 clock cycles. Then, the trip circuit output B and C will be the same as Code\_B and Code\_C when the channels CH-B and CH-C are healthy. The trip circuit output A, B and C are processed by the voting logic and output is defined as:  $V_{2003} = A_1 B_1 + B_1 C_1 + C_1 A_1$ . For single parameter, output waveforms are shown in Figure 2.6.

For multiple parameters, guard line logic is used as shown in Figure 2.7 to process all the parameters. Output from one stage is fed to the succeeding guard line logic and output from the last stage is fed to pulse to DC converter, which drives the electromagnet. To energise the Coil, high current (1 to 1.5A) is required, so power MOSFET has been used to drive the high current. Each end of of coil shall be controlled independently. Each power gate is tested periodically by injecting Pulse\_D and Pulse\_E at the input of power gates.

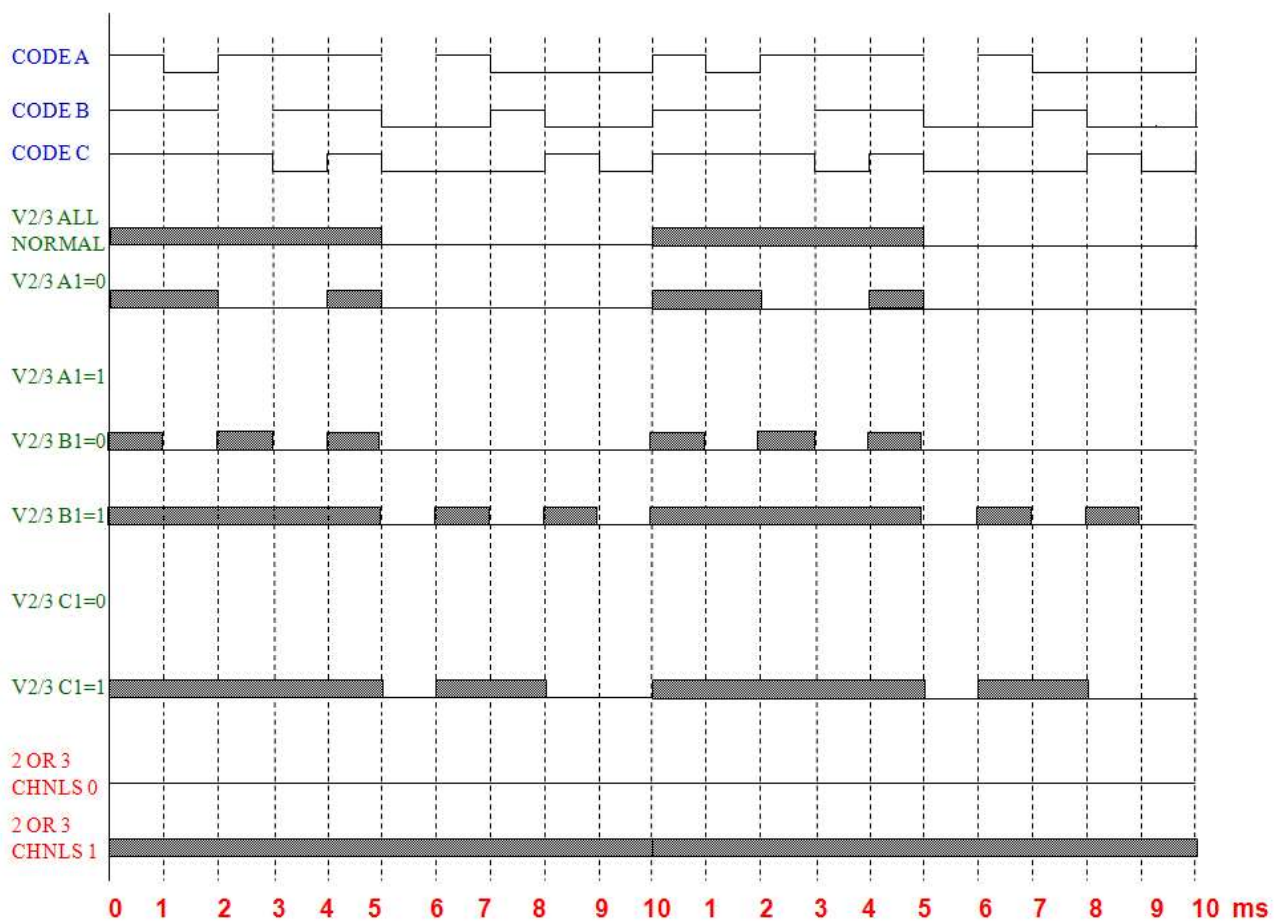


Figure 2.6: PCSL timing diagram.

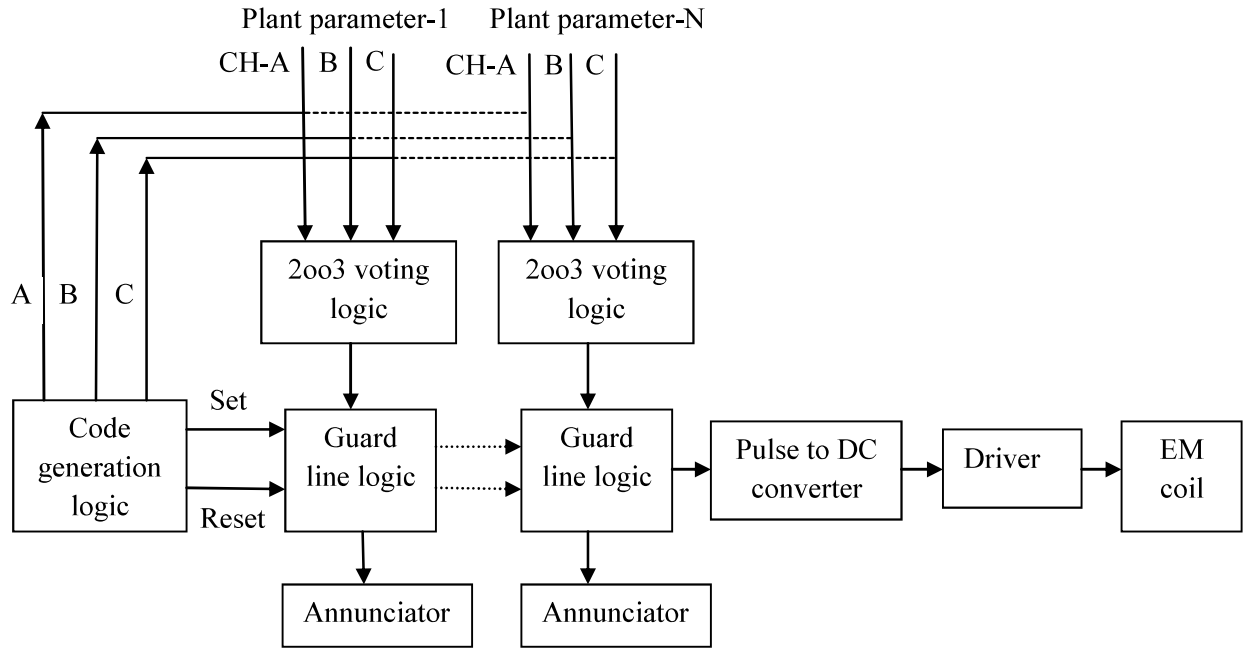


Figure 2.7: PCSL for multiple parameters.

### 2.2.3 Actuation system

Two types of mechanisms and absorber rods are provided in PFBR. SDS-1 consists of 9 neutron absorber rods known as Control and Safety Rods (CSR). Each rod is provided with a drive mechanism (CSRDM) to raise or lower the rod at a fixed speed using motors. SDS-2 consists of 3 neutron absorber rods known as Diverse Safety Rods (DSR). Each rod is provided with a drive mechanism (DSRDM) to raise or lower the rod at a fixed speed. CSRs are used for startup, power control and shutdown. DSRs are used only for shutdown. During normal operation, the DSRs will be in fully raised position and all CSRs will be at same level to achieve criticality and power operation. When a SCRAM signal is given, the mobile assembly of CSRDM along with CSR is released from the electromagnet and falls under gravity. However, in the case of DSR and DSRDM, only DSR is released from the electromagnet and falls under gravity. Motor operated drive mechanisms are provided to position the absorber rods at desired elevation.

The components involved in the control of CSR motors is shown in Figure 2.8. The position of CSRs is controlled manually from the main control room with rod selector switch and Raise/Lower push buttons. The raising of control rods is of interest with respect to the event of uncontrolled withdrawal of neutron absorber rods. A dual redundant computer system is provided to process the input signals. It consists of Digital Input (DI) card to receive raise command, CPU card to process the signals and Relay Output (RO) card to drive the output signal. Switch Over Logic Circuit (SOLC) routes one of the output signals to field driver relay coil. In case of a failure, it routes outputs from standby computer system.

Field driver relay drives  $230V_{AC}$  to the coil of an Electro Magnetic (EM) contactor.  $415V_{AC}$  is fed to a 3 phase induction motor through this contactor. The direction control of the motor is effected by changing phase sequence to the motor coils. The shaft of the motor is attached to a screw nut mechanism. An electromagnet is attached to the nut, moves the control rod either up or down.

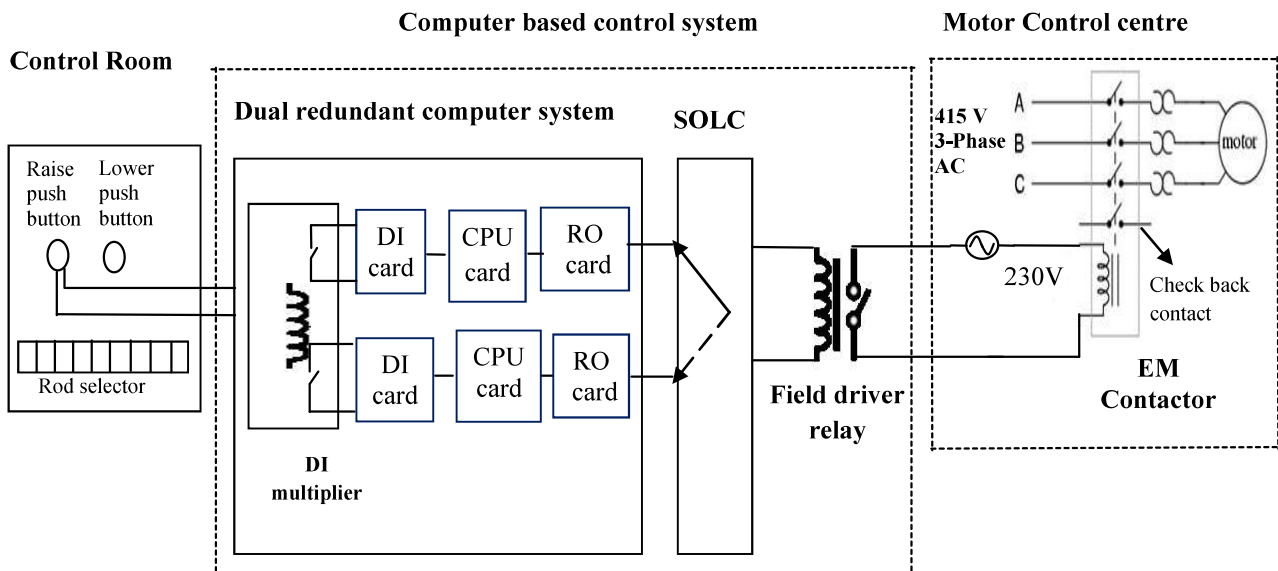


Figure 2.8: Instrumentation in CSRDM.

The I&C design for CSRDM is based on operating experience of Fast Breeder Test Reactor (FBTR), which is a 40MWt experimental test reactor at this centre, uncontrolled withdrawal event incident in FBTR and design and testing of a prototype CSRDM.

The neutronic and thermal-hydraulic effects of uncontrolled withdrawal of a neutron absorbing control rod in a thermal reactor have been well reported [78] and [79]. A fast reactor power control is typically manual, meaning that rod movements are effected only with operator commands. Devan et al., has reported the physics aspect of control rod withdrawal as part of end of life tests on the French fast reactor PHENIX [80]. Sutanto et al., has presented a study of reactivity insertion and thermal-hydraulic effects due to uncontrolled withdrawal of a control rod in a fast reactor [81]. In PFBR, continuous withdrawal of one control rod is classified as a category-2 DBE with an estimated frequency  $>10^{-2}/\text{r-y}$ . The effect of uncontrolled withdrawal of one absorber rod in PFBR is reported by Natesan et al., [82]. Continuous withdrawal of CSR at a low power level (close to 5%) does not demand shutdown action. However, the event happening at higher power level requires shutdown action from SDS based on neutronic parameters or coolant temperature at the central subassembly to meet the design safety limits.

The provisions in design to protect against uncontrolled withdrawal in PFBR are:

- Though the interlocks for raising and lowering of control rods are executed by a computer system, rod movement is manually initiated from the operator through hard wired switches and push buttons.
- Continuous withdrawal probability of more than one rod is minimized by the provision to select only one rod at a time for raising. A 10 position gang switch is provided to select the rod intended for raising. Moreover, check backs from contactor coils are taken to ensure one rod movement at a time.

- From a certain power level, continuous raise of a control rod more than 2mm/s is not permitted.
- Between two consecutive raise operations, the operator has to wait for a period of 210s.
- A difference of more than 40mm between any two of the control rods is treated as “level discordance” and an alarm is generated.
- When there is a failure in any of the components of the computer system, self-diagnostics on the system opens the relays meant to energize the motor contactors, thus leading to inoperability of the control rods. The relays predominantly fail in “open mode” and hence the chance of continuous withdrawal due to relay failure is remote.

In spite of the above provisions, EM contactor failing-to-open (contact weld) and sluggish response of the contactor upon de-energization are the instances which are out of control of the control system and the interlocks are ineffective under such circumstances.

The estimated failure frequency of unintentional withdrawal of control rod in PFBR is about 0.2/year. The system failures involved for this event are computer based system modules (DIC, CPU card, ROC), SOLC modules (SOLC, OR logic, backplane) and EM contactor. Among others, the EM contactor failure (fail-to-open mode) is dominating.

**Hence, further studies are required to verify the impact of EM contactor weld failure on uncontrolled withdrawal of neutron absorber rod in PFBR.**

The three neutron absorber rods (DSRs) of the second shutdown system are positioned outside the active core during normal operation and are used only for rapid shutdown of reactor on abnormal conditions. On receiving SCRAM signal, the electromagnet of DSRDM is de-energized and it facilitates fast shutdown of the reactor.



Salient features which help in achieving a low  $PFD_{Avg}$  in the actuation system are,

- Rod drop in case of loss of power and cable cut: Since all absorber rods are kept energized under normal operation, loss of power to electromagnet or voting logic or signal processing electronics or a cable cut in any of the interconnectivities will lead to rod drop. Since a “negative” reactivity SCRAM parameter exists, one spurious rod drop will result in all rods getting dropped subsequently. This has a major effect on reducing  $\lambda_D$ .
- Automatic and simultaneous drive down of all CSRs (upon SCRAM): Rod drop is independent of drive status and position of electromagnet. However, all electromagnets are driven down by drive mechanism motors upon a SCRAM. This feature is provided to give a push to the detached absorber rod in the remote event of rod getting stuck and failing to drop. This provision has the effect of reducing  $\lambda_D$ .
- Periodic surveillance on CSR (Rod Exercising): To check that the friction in the mobile assemblies is within limits, a set of two rods are exercised when reactor is on power. One rod is raised and the other rod is simultaneously lowered, so that reactor power is unaffected. The friction values are elucidated from load cell provisions on the mechanisms. All rods are covered cyclically. This operation is called “Rod Exercising”.
- Response time monitoring: Response time of electromagnet is in the order of 100ms. It is measured during every SCRAM. This helps in verifying the assumption that system is fully healthy upon start up.
- Drop time measurement: The time taken for the CSRs to reach the bottom is measured by actuation of a micro-switch provided for this purpose. In case of DSRs, Kalman filter based reactivity measurement is used to ensure that rods have reached the intended positions. This helps in verifying the assumption that system is fully healthy upon start up.

## **2.3 Computer Based Systems used for Shutdown**

All systems which form part of the shut down system are hardwired analog or digital electronic systems (without software) except for Core Temperature Monitoring System (CTMS). This option is preferred to avoid complications related to quantifying software reliability. However, CTMS is computer based since arithmetic operations on around 423 thermocouple channels are to be performed. These signals are monitored and processed by triple redundant Real Time Computers (RTC). RTCs are modular with Central Processing Unit card (CPU), Analog Input Card (AIC), Digital Input Card (DIC), Analog Output Card (AOC) and Relay Output Card (ROC) on VME (Versa Module European) bus backplane. This section details about the circuit details and diagnostic features in the existing design.

### **2.3.1 Analog Input Card (AIC)**

AIC accepts 37 analog input channels in which 30 are field signals and 7 are used for online calibration and diagnostics. The block diagram is shown in Figure 2.9. The AIC consists of multiplexers (MUX), Instrumentation Amplifier (IA), Analog to Digital Converter (ADC), active Low Pass Filter (LPF) and FPGA based sequencer. Multiplexer is used to time share ADC for multiple channels. 16 bit successive approximation ADC is used to convert to digital signal. Functional blocks of FPGA based sequencer are sequencing logic, VME bus interface logic and SRAM (Static Random Access Memory). Sequencing logic issues control signals for enabling and selecting a particular channel. After programmed settling period, the logic issues Start of Conversion (SOC) to ADC, waits for End of Conversion (EOC) from ADC within a programmed period. After each conversion, the digitized values are stored in SRAM memory inside Sequencer and range check performed with programmed upper and lower limits.

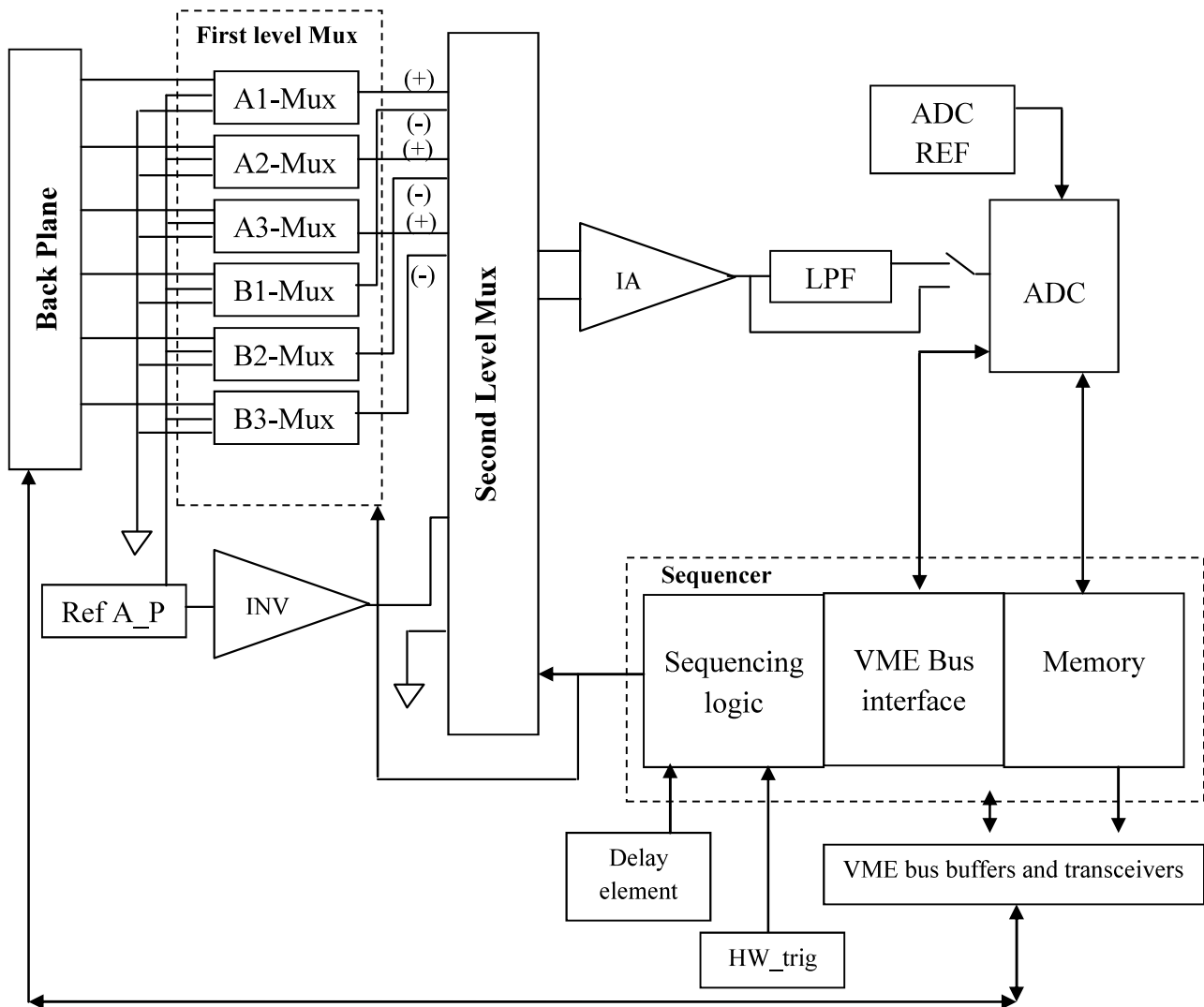


Figure 2.9: Block diagram of AIC.

### Diagnostic features

1. Multiplexer fault: One channel connected to +2.5V reference and the other channel is connected to ground reference in first level multiplexer. In the second level multiplexer one channel is connected to a fixed reference (-2.5V). This scanned data is compared with the predefined expected data to verify the healthiness.
2. ADC fault: The sequencer checks the status of ADC health by monitoring the EOC signal of ADC. If EOC is not asserted within a 15μs (3 clock cycles) (ADC conversion time is 8μs

only), then ADC health bit in sequencer remains “0”. This indicates that ADC is faulty and further scanning will be stopped. CPU reads the status register.

3. Sequencer fault: To convey the self health, sequencer maintains a trigger counter. The counter increments on every trigger. On power, the counter resets to zero. CPU has to read this count to infer the sequencer health. During continuous triggering, if the count of the two consecutive reading is matching then the sequencer is assumed to be faulty.

### 2.3.2 Digital Input Card (DIC)

VME bus based DIC receives 30 input channels. The board select logic compares the boards address to the address on the VME bus address lines and generates a board select signal when address match is obtained. The control logic generates the necessary internal read and write signal. The change of state Logic generates an internal interrupt request whenever input state changes. The transceivers block will interface with VME bus data lines. Signal conditioners block provides isolation from field inputs and converts it to TTL compatible input. The de-bounce logic provides programmable de-bounce time to the input signals. The de-bounced field inputs are read by read registers. Force 0 and Force 1 logic is used to drive the input channels 0 or 1 to find the healthiness of the card. Two diagnostic registers are provided to monitor the healthiness of data path.

#### *Diagnostic features*

1. By feeding the input with 0 or 1 through opto-coupler with Force 0 or Force 1 logic block at the input stage and checking the read digital values. When these inputs are given field inputs are masked.
2. Healthiness of registers is checked by writing and reading test data periodically.

### 2.3.3 Analog Output Card (AOC)

Number of channels connected to this card are 4. The block diagram is shown in Figure 2.10. Address data and control signals are buffered through bus buffers. Data bus is driven through bus transceivers. The functions of Bus interface/Control CPLD (Complex Programmable Logic Device) are to interface with VME, giving control signals to DAC (Digital to Analog Converter), MUX and ADC, providing the diagnostic registers for testing of bus interface and detecting clock failure. Four 12 bit voltage output DAC with 10 V is used. In output section, this voltage output is converted to 4 to 20mA and given to field. Read back section consists of isolators, analog MUX, amplifier and ADC. The current output which is given to field is converted to voltage with  $100\Omega$ . The voltage across these four resistors are isolated and fed to analog MUX which gives single output to ADC. MUX is 8:1 for this 4 are four analog outputs, one input is temperature and three are connected to ground. Isolation block provides galvanic isolation to protect the board from field signals having high amplitudes. Transformer coupling is used such that primary and secondary are magnetically coupled and electrically separated. ADC will convert analog output back to digital for diagnostic purpose and is fed back to CPLD.

#### *Diagnostic features*

1. Read back section to check healthiness of DAC.
2. Diagnostic registers: Data is written into these registers and read back from these registers and compared with written data for verifying bus interface.
3. Clock failure detection: It is designed to detect the logic stuck faults (stuck at LOW or stuck HIGH) in the system clock. When the clock fails, the delayed clock is still available for sampling the input waveform. Combined with sequential element, this circuit generates logic “1” for clock healthy condition and logic “0” for a clock fail condition. Clock failure

detection circuit and its waveforms are shown in Figure 2.11 and 2.12 in case of clock failure at stuck at LOW.

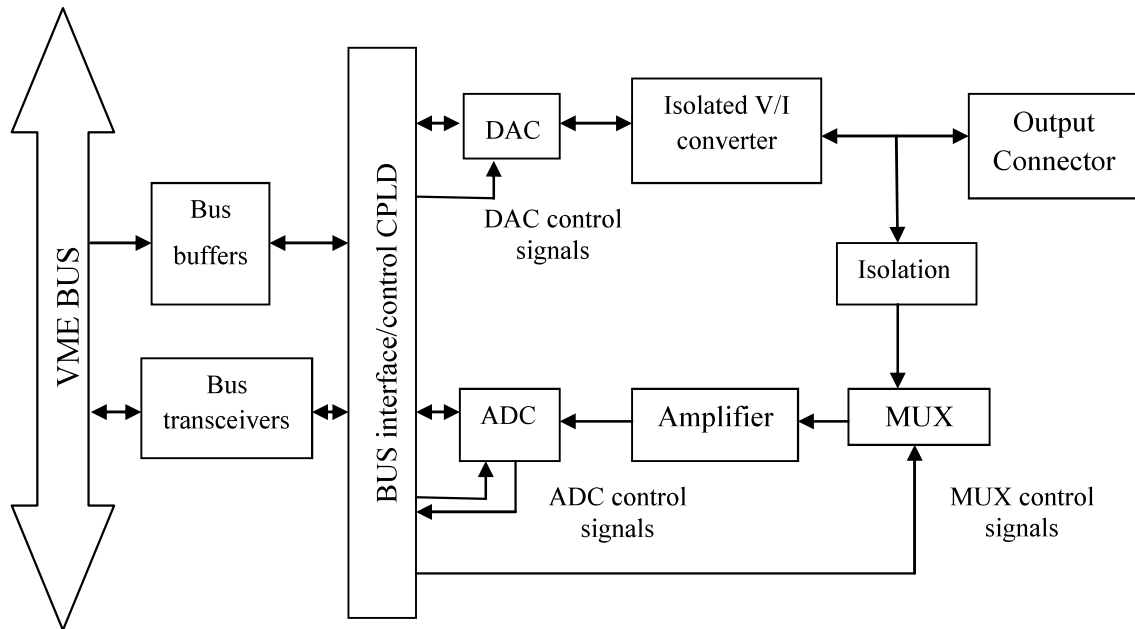


Figure 2.10: Block diagram of AOC.

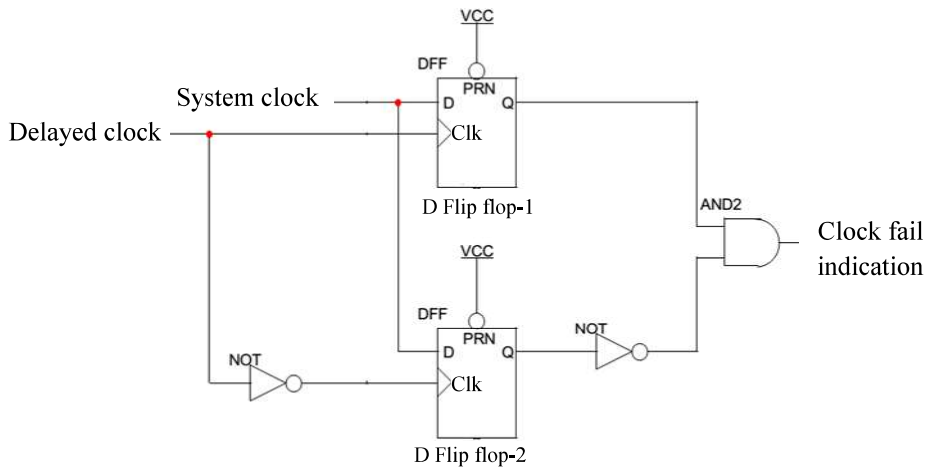


Figure 2.11: Clock fail detection circuit.

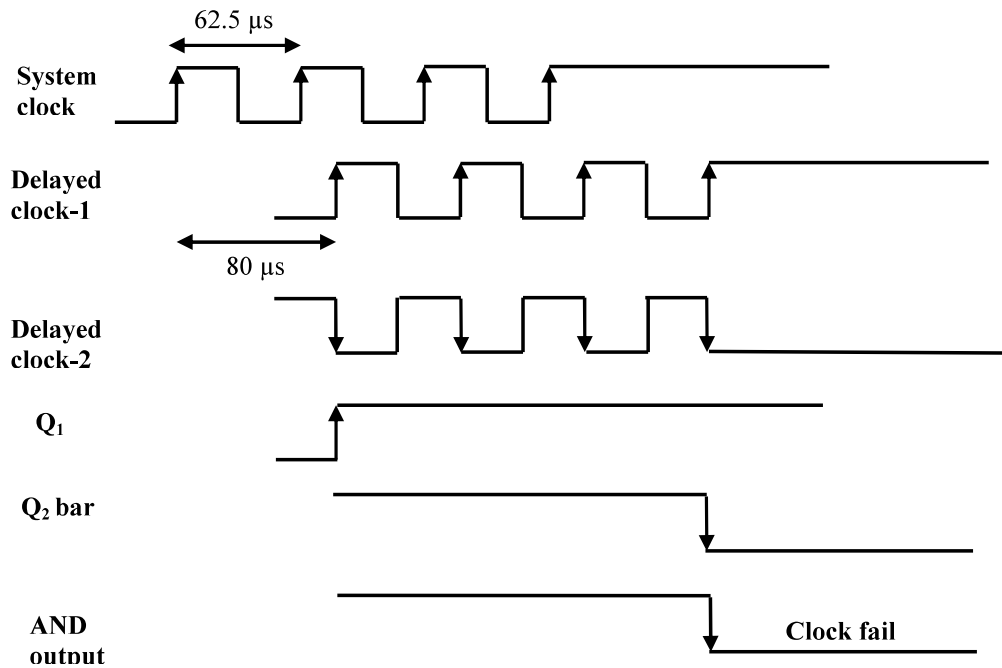


Figure 2.12: Waveforms of clock fail detection circuit.

### 2.3.4 Relay Output Card (ROC)

The block diagram of VME bus based 15 channel ROC is shown in Figure 2.13. The Transceivers & Transceiver Enable Logic block contains drivers that interface with VME bus data lines. The Board Select Logic block compares the board's address to the address on the VME bus address lines and generates a board select signal when an address match is obtained and the DTACK control logic block generates the necessary internal read and write signals. The latch block is used to latch the data on the VME bus data lines and it feeds the Inverters block which drives the relays, drivers and status LED's block. The Clock Divider block divides the system clock and feeds as a source clock to the Watchdog Timer. In case a watchdog timer times out or system clock fails, all the relays are de-energized. The Clock fail detection block generates a logical signal to indicate the failure of system clock. The Control and Status Register gives indication of board fail signal in case of mismatch between relay contact outputs versus latched data. The Relay contact read back block reads back the relay change over contact outputs.

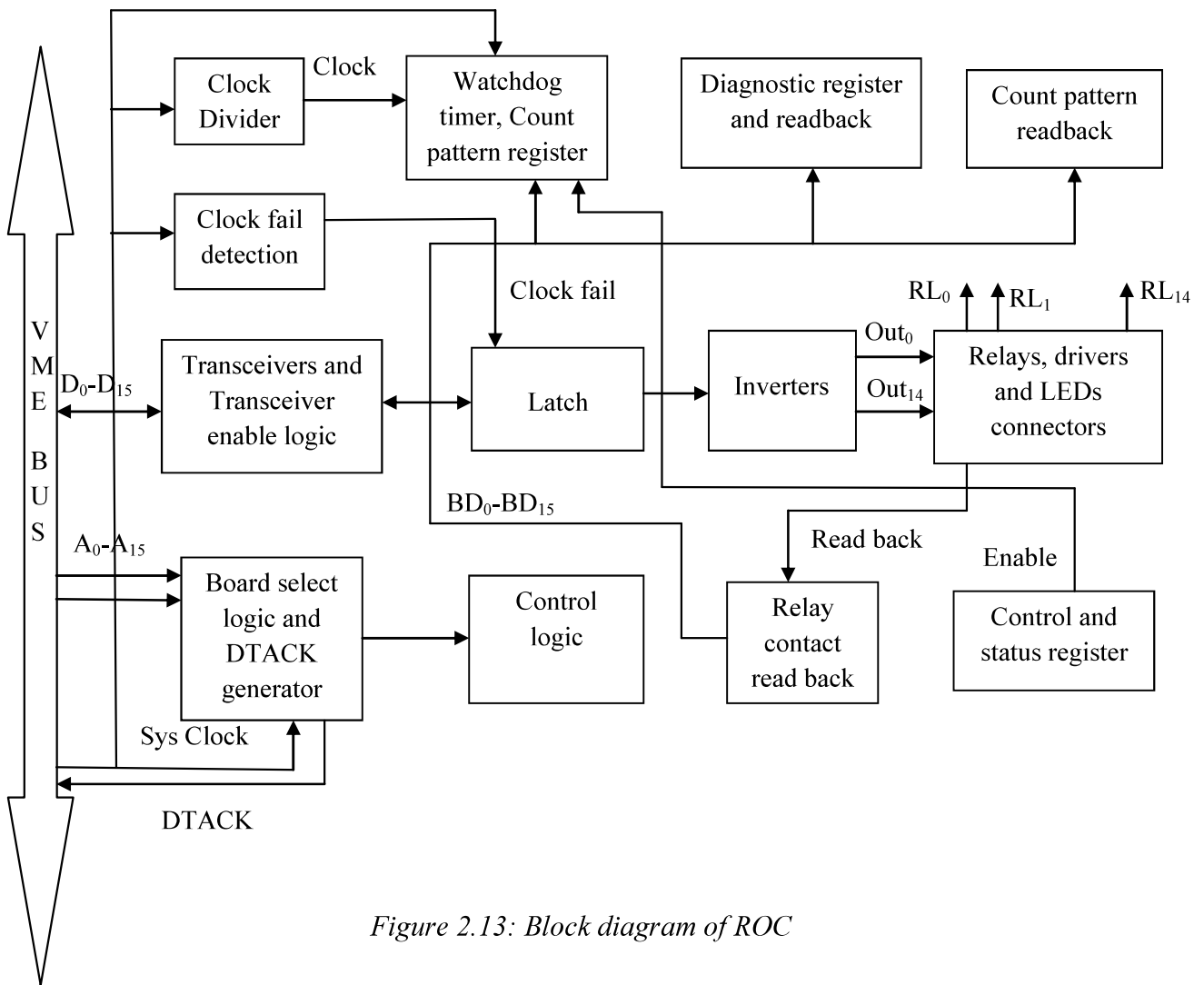


Figure 2.13: Block diagram of ROC

### Diagnostic features

1. Clock fail detection as explained in AOC diagnostic features.
2. Watch dog timer: The watch dog timer is designed using counters. Load value is set through software by loading bit patterns into count pattern registers to set the timeout value. The counters are loaded with this value periodically by the CPU card. Failure of CPU card causes the counter to decrement from the load value to zero and then generates a timeout signal.
3. Relay contact read back: Relays are kept energized under normal condition and de-energized upon SCRAM. Particular data pattern is written in relay latch register to energize or de-



energize the relay. Relay contact output are read back and compared with written data pattern. If any contact gets welded (fail-to-open mode), it is interpreted from the read-back pattern and an alarm is raised.

*Relays are kept energized since there is huge assumption that relay contacts fail in “fail-to-close” mode (contact open). To address unsafe failure mode (contact weld), current techniques allow for testing only one redundant channel at a time. Hence, it is desirable to find a new method to detect weld failure of EM relay contact online (without opening the relay contact). It has to be shown that there is no impact of diagnostic circuit on functional circuit by reliability modeling.*

4. The contacts are exercised during periodic proof testing.
5. If CPU does not refresh watchdog timers, relays are de-energized automatically.

### **2.3.5 Central Processing Unit card (CPU)**

The block diagram of VME based CPU card is shown in Figure 2.14. CPU is MC68020 and Floating Point Unit (FPU) is MC68882 based processors with hardwired TCP/IP module with Ethernet and RS-232 interface and inbuilt watchdog timer. CPU's address bus, data bus and control signals are connected directly to the FPU. The Control logic is responsible for generating the necessary signals required for the operation of the CPU card. The EPROM (Electrically Programmable Read only memory) is provided to store the program and read-only data. The EDAC (Error Detection and Correction) logic performs single bit error detection and correction and double bit error detection on the SRAM, which holds the program data. The EEPROM (Electrically Erasable and Programmable Read only Memory) is provided to store application specific configurable data.

### Diagnostic features

1. The watchdog timer is loaded with an initial count. Upon a 'software hang', clock count goes to zero.
2. EDAC on SRAM data is performed.
3. Cyclic redundancy check is done on EPROM and EEPROM to protect against memory corruption.

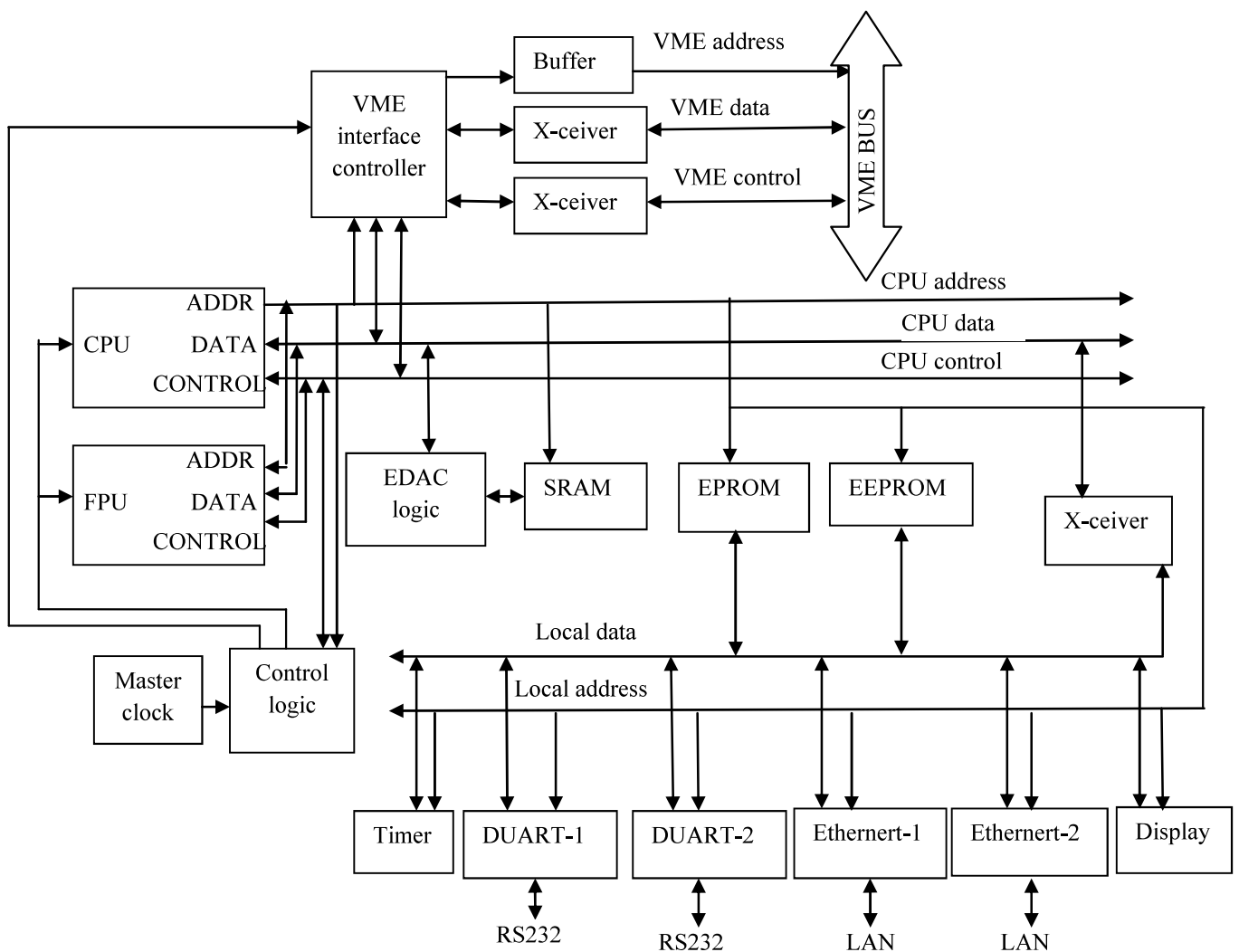


Figure 2.14: Block diagram of CPU card.

## 2.4 Decay Heat Removal System

During normal operation, the heat generated in the core is removed by the primary sodium flowing through the core and is transported to the IHX where it transfers heat to secondary sodium. The secondary sodium in turn transfers the heat to water in the steam generators to produce steam to run the turbine. After reactor is shutdown, the residual heat (mainly fission product decay heat) is removed with Operation Grade Decay Heat Removal (OGDHR) System predominantly using normal heat removal path. When the secondary sodium system, steam–water system and power supply are available, the DHR operation is carried out by OGDHRS. But, dependence of the OGDHRS on power supply makes the system less reliable. Whenever the OGDHRS is not available, the DHR is carried out by more reliable Safety Grade Decay Heat Removal (SGDHR) system. In an NPP, decay heat removal function after reactor shutdown demand very low failure frequency in the order of  $10^{-6}$  to  $10^{-7}$ /r-y. For instance, John Arul et al., shows reliability analysis of SGDHR in PFBR [76].

SGDHR consists of four sodium loops each with  $8\text{Mw}_t$  capacity. In each loop, the heat transfer from sodium pool to the SGDHR loop takes place through a sodium to sodium heat exchanger dipped into the pool (DHX). This heat will be dissipated to atmosphere (ultimate heat sink) through sodium to air exchangers (AHX). To achieve very high reliability, the sodium flow in the SGDHR loop and air flow through AHX are designed to be driven by natural circulation. Dampers are employed to control air flow to AHX so as to minimize energy loss during power operation of the reactor. When the reactor shuts down, the dampers are to be designed to reliably open. The opening action is to be automatic and should have very low  $\text{PFD}_{\text{Avg}}$ . Both inlet and outlet air flow path has two sections each controlling one half of the available flow area. The damper in one section is pneumatically driven and the damper in second section is electrically driven as shown in Figure 2.15. This arrangement is provided for diversity in design.

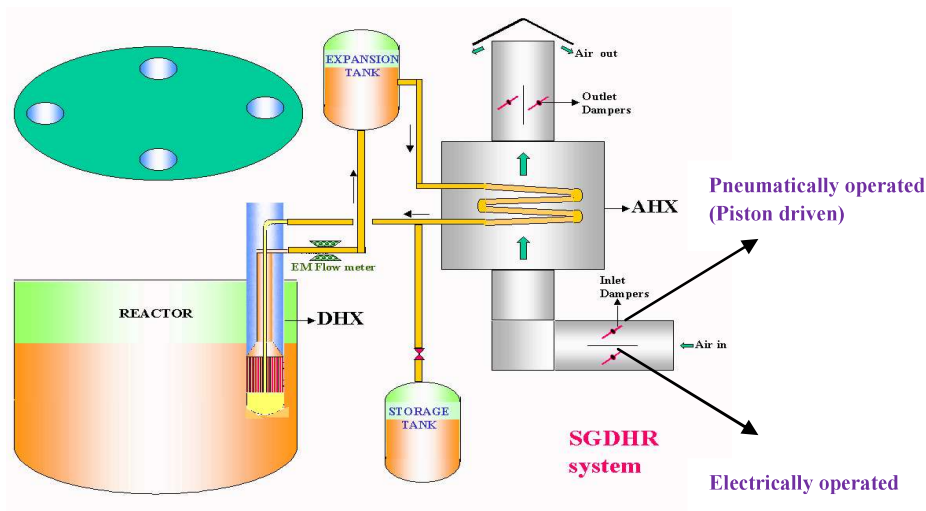


Figure 2.15: Dampers in SGDHR system.

Both the damper systems deploy relay logic to control opening and closing of dampers. Solid state electronics was not preferred due to their possible failure in unsafe mode. **Since both pneumatic and electrical damper control is through relay logic, the inherent fail-safe design possibilities are to be explored to lower  $PFD_{Avg}$  and to improve diversity.**

Salient features in SGDHR to reduce  $PFD_{Avg}$  are

- The control of dampers is segregated from monitoring function. Thus, conventional EM relay logic built with ladder diagram is used to control dampers whereas a computer based system is used for monitoring sodium flow, temperature, etc. This helps in simplification of safety circuit and usage of minimum number of components in the system.
- EM relays are used to implement the logic rather than solid state circuits. Relays are kept energized during normal condition and are de-energized to indicate a demand condition (since EM relays predominantly in fail-to-close mode). Additionally, “Normally Open”

contacts are used. Thus, dampers will open upon loss of control power supply, failures in EM relays and cable cut.

- “De-energize to OPEN” type solenoid valves are used in pneumatic dampers so that upon failure of control power supply, dampers will fully open.
- A counter-weight is provided on pneumatically operated dampers. Pneumatic pressure is required to close the dampers. Thus, loss of pressure will lead to an opening of dampers.

## **2.5 Summary**

- The various design principles, techniques, and methods used to achieve the fail-safe design in safety critical I&C systems of PFBR are studied.
- There are sufficient fail-safe features in sensor stage such as discordance monitoring, open sensor detection etc. Self testing and periodic testing are fail-safe design features in SCRAM generation electronics. SDS-1 voting logic has online testing by injecting short duration pulses. SDS-2 voting logic has inherent fail-safe design. Absorber rods are dropped into core under gravity during loss of coil power supply to electromagnets. Falling under gravity is a natural phenomenon, thus unsafe failure probability is insignificant.
- In decay heat removal systems, fail-safe behavior is achieved with passive features wherein natural circulation of coolant guarantees removal of decay heat. I&C is limited to the opening/closing of the dampers. I&C failures results in opening of dampers.

# 3

## A NOVEL ONLINE DIAGNOSTICS OF EM RELAYS AGAINST CONTACT WELD

---

*This chapter elucidates the application of electromagnetic relays in nuclear power plant shutdown system and concerns on contact weld failure mode. Online diagnostics is an important aspect of fail-safe design. A novel method for online diagnostics of contact weld failure in electromagnetic relays without affecting the contact status is described. Diagnostic circuit and test results are presented in this chapter.*

---

### 3.1 Introduction

#### 3.1.1 Electromagnetic relay

An Electro Magnetic (EM) relay is an electrically operated mechanical switch that uses a low voltage input signal to control a circuit. They play an important role in nuclear, automotive, aerospace, military, communication switching and industry automation where reliability of the relay is critical.

Relay consists of an electromagnetic coil (inductor), spring, and switch contacts as shown in Figure 3.1. In order to switch, a low power circuit, typically 12 or 24V<sub>DC</sub>, energizes an inductor coil that creates a magnetic field. The magnetic field attracts the metal plate by overcoming the spring force, thus closing the circuit between the contacts on the side that is Normally Open (NO). When the coil is de-energized, the spring force overcomes the magnetic force and the contact switch returns to its position on the side that is Normally Closed (NC).

A single pole double throw relay as shown in Figure 3.1, left represents the NC side which is in contact when the coil is de-energized, and the right contact is NO. The primary contact seen in the middle has two sides and moves to the NO side when the coil is energized.

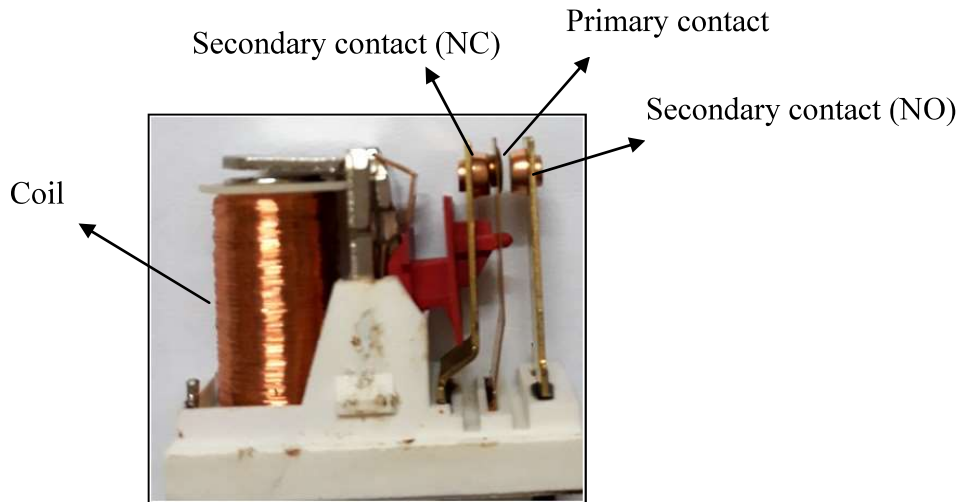


Figure 3.1: EM relay internal architecture.

Mechanical life of a relay is defined as the number of no-load operating cycles. A relay's mechanical life is relatively long, typically up to 10,00,000 operations. The electrical durability of a relay is the expected number of on-load operations it will achieve. A relay's electrical life of contact range from 1,00,000 to 5,00,000 cycles. Datasheet specifies electrical durability at rated load (resistive/inductive), rated current and maximum switching voltage. Electrical durability depends on many factors such as the type of load, switching frequency, load current, ambient temperature, rated temperature etc. In practice, electrical durability will greatly vary because of load and environmental conditions. The next section explains literature review on failure modes and mechanisms.

### 3.1.2 Failure modes of EM relay

For relays, the reliability is often expressed in terms of the number of switching operations and the principal requirement is consistency of contact resistance. The most common



failure modes are latch-up and bridging of contacts and high contact resistance due to erosion and contamination. Other modes include wear-out of structural parts such as the spring, failure to make contact closure and damage to the enclosure. Table 3.1 shows a list of these failure modes and Table 3.2 lists that parameters influence relay degradation [83]. Behrens et al., [84] has studied field failures; the failure modes are listed in Table 3.3.

Table 3.1: Contact failure modes [83].

Cause	Failure	Effect
Arc	Contact weld	Contact material composition changes
	Contact erosion	
	Material transfer	
	Inorganic layer formation (Oxide, Sulphide)	Contact resistance changes
	Organic layer formation (oil, grease, vapour)	
Particle	Abrasion	Contact reliability reduction
	Dust	

Table 3.2: Physical effects on contact reliability [83].

Influences	Parameters	Effect
Electrical	Current Voltage	Heating, melting, material migration, chemical reactions, fritting, electrical discharge, contact resistance.
Thermal	Arc	Melting of contact material, material migration.
Mechanical	Friction Pressure	Deformation, wear, cold welding, contact resistance.
Ambient conditions	Dust Gases	Increased wear, particles, formation of chemical layers and corrosion.
Chemical	Oxidation	Contact resistance, inorganic and organic layers, corrosion.

Table 3.3: Failure modes and root causes [84].

Failure	Root cause
Elevated over temperature/ contact resistance	<ul style="list-style-type: none"><li>• Too low contact force</li><li>• Surface layers on the contact surfaces caused by corrosion</li><li>• Particles on the contacts</li><li>• Changes of the contact material due to arcing</li><li>• Insufficient electrical conductivity of the contact material</li><li>• Impurities in or on the contact materials</li></ul>
Reduced electrical service life	<ul style="list-style-type: none"><li>• Failures in the contact material as wrong composition or microstructure</li><li>• High amount of porosity or crack formation</li><li>• Bad joining of the contact tip with contact carrier resulting in reduced heat flow from tip to carrier</li></ul>
Welding of contacts	<ul style="list-style-type: none"><li>• High short circuit current through contact cause melting of contacts spots</li><li>• Bouncing of contact during make operation</li><li>• Contact tips will mate after complete erosion of surfaces</li></ul>

### 3.1.3 Arc and its consequences

Arcing is the main cause of contact erosion, migration of contact materials and weld. Electrical arc is neutral plasma consisting of ionized species coming from the contact material and from the surrounding environment. It is a dynamic and unstable phenomenon. The main characteristics of this arc (arc duration, arc voltage and arc current) depend on the parameters of the electrical circuit, the parameters of the opening system and the nature of the elements close to the arc plasma which are able to come into the plasma and modify its composition (contact material, nitrogen or oxygen from atmosphere or materials from the case) [53].

As the contact begins to open contact resistance increases, the voltage drop across contacts also increases. Contact spot temperature ( $T_C$ ) depends on contact voltage and hence  $T_C$  will increase. A stage will be reached where  $T_C$  meets  $T_m$  (melting temperature) of metal. Once the contact spot melts, it forms molten metal bridge between contacts. When bridge ruptures it releases metal vapor into the contact gap. This metal vapor will have high velocities because of high temperatures just after rupture of the molten bridge. After rupture of molten metal bridge, when voltage is greater than minimum voltage across the contact, an arc will be formed. Contact arcing results in shortened contact life. The formation of arc during the contact closing is also of great practical importance. Once the voltage is impressed across the contacts and the first electron is initiated, an arc will be established between them even if the contacts are apart and it burns for few  $\mu s$  before they actually touch [53].

Depending on the severity and duration of the arc,

- Much material will be lost from the contacts that they fail to electrically close the load circuit as shown in Figure 3.2a.
- If one contact loses much material to the other contact, it results in pip and crater formation as shown in Figure 3.2b.

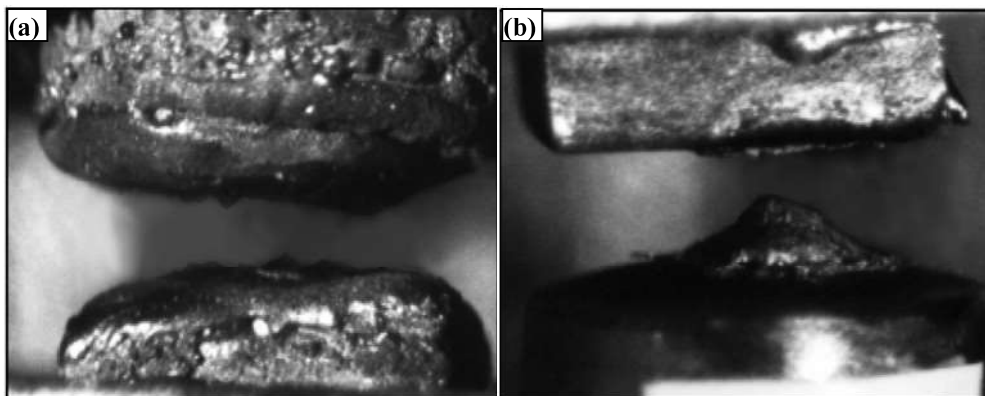


Figure 3.2: Contact failure (a) contact material loss due to arc erosion; (b) pip and crater formation [85].

Another result of severe arcing is “contact welding”. As the contacts come together, the first high spot to make contact is subject to full load current. Even if load current is a fraction of an ampere, the  $I^2R$  heat generated in this high spot instantly causes the high spot to melt. As the contacts move forcefully, this liquefied metal may spatter, resulting in a loss of material. As the molten metal between the contacts cools, the contacts are frozen together. This weld is weak and easily broken by the action of the relay spring force when the relay is de-energized. Contacts may fail-to-open if the force to break the weld is higher than the maximum opening force provided by the spring.

A weld can happen in similar manner upon contact break also. As the contacts begin to separate, less and less contact area carries load current. Load current begins to funnel into this constricted area and  $I^2R$  heat begins to increase. The last point of contact melts and as the contacts continue to separate, a thin bridge of molten metal is stretched between the contacts. Literature claims various reasons for contact weld.

Rieder et al., [86] claims that contact welding is influenced by bounce pattern at make. Short time bounce cause stronger welds due to elastic deformation of the contact material. Chen and Witter [55] have also mentioned that strong welds are always associated with very short time bounces during make or break, normally less than  $100\mu s$ , that produce a larger amount of molten metal from a constriction resistance and solidify when contact touches. Bounces with longer duration, has more contact impact force for spattering the molten metal due to the larger gap and arc area. So, the weld strength of longer bounces is generally weak. Zhao et al., [87] investigated the relationship between arc duration and occurrence of contact welding. Welding has occurred on both the make and break operation; however, probability of welding during the make operation was much higher than that during break operation under same test conditions. Out of

29 incidents of welding in the study, 27 occurred during make operations while only 2 were during break. It is considered that increasing the number of operations will result in increased contact erosion, a decrease in contact force and overtravel. This causes a marked increase in arc duration which is used as an indication of imminent welding. From the experimental results, it is concluded that welding may occur suddenly or randomly in the electrical lifetime test without any prior changes indication in the make and break arc durations. A group of make or break arcs with longer duration causes imminent welding. It also claims that, welded area and welding strength in each break operation helps in predicting the occurrence of welding.

Morin et al., [56] investigated arc erosion and weld experiments with various loads. Testing with lamp loads has shown highest material transfer due to inrush current. When the contacts begin to separate, the rupture of the molten bridge initiates arcing. This arc has two effects, which together lead to contact welding:

- It initiates contact constriction
- It induces a sudden current fall which cools this contact constriction. These simultaneous effects induce a solidification of the contact surface, and welding occurs.

Contact fail-to-open can occur during the break operation of motor with shorter duration arc. This arc forms crater on anode and cathode. Accumulated molten material around anodic crater forms as a rim. With the formation of rim, actual contact gap reduces which results as contact welding [88]. It was found by Doublet et al., [89] that extension of the power supply from  $14V_{DC}$  to  $42V_{DC}$  increases arc current and so the arc duration which covers the total bounce time. At higher current the amount of material transfer is more. Along with this welding is also noticed. Neuhaus et al., [57] stated that configuration of the load circuit determines the actual arc current which influences the weld force. In ohmic load, arc durations of the bounce arcs are

longer than the duration of the pre-strike arcs and thus the welds caused by bounce arcs are stronger. In ohmic/inductive load, weld caused by bounce is stronger than a prestrike arc because of higher current. In ohmic/capacitive load, prestrike arcs are major cause for welds because of high inrush current. Mechanical parameters which influence the weld are impact velocity and static contact force.

From the literature, it can be concluded that contact welding is a failure mode to be carefully investigated for a safety critical application.

### 3.2 Welding Concerns in Nuclear Power Plant

In a Nuclear Power Plant (NPP), EM relays are often used to communicate shutdown signal to voting logic as shown in Figure 3.3. Relays are kept energized during normal operation and de-energized upon a shutdown demand to achieve a fail-safe behavior.

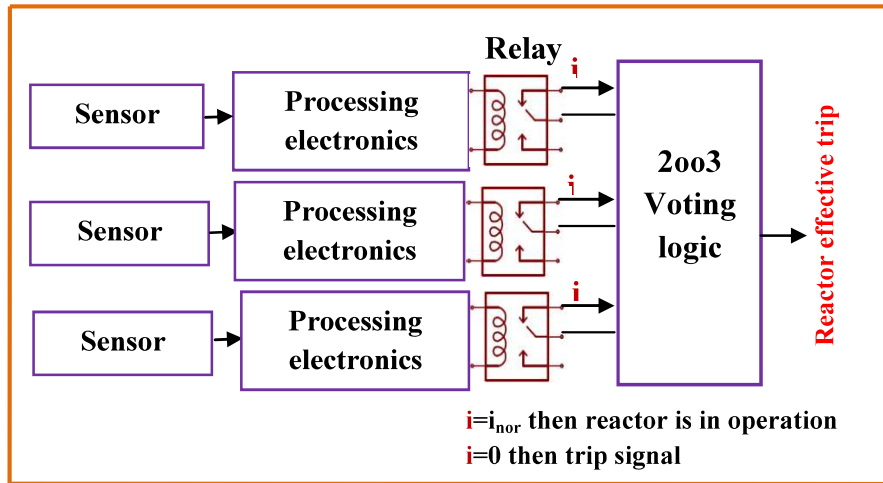


Figure 3.3: Application of relay in nuclear power plant shutdown system.

EM relays are preferred over solid state relays since they predominantly fail-to-close. Failures detected in processing electronics lead the system to fail-safe by de-energizing the coil. If relay contacts get welded, it will not respond to a de-energization command. However, from literature survey contact welding cannot be ruled out.

Safety criteria for NPPs demand online testing of shutdown systems right from the sensor to final control elements. In current practice, contact weld failure in EM relays is detected by periodic opening in one of the channels in a triple redundant architecture (operating in two out of three mode) and checking the status of auxiliary contact.

Various authors have claimed different parameters for failure diagnostics of EM relays. Yao, et al., [90] introduced the dynamic contact resistance measurement device to capture the contact resistance in the process of contact being closed or open. From this, contact bounce time, maximal contact resistance and contact resistance in the close state are extracted as diagnostic parameters. Xin Zhou, et al., [59] shows that DC coil current and contactor current as diagnostic and prognostic parameters for the potential failures of contactors. Contact over travel time, armature pull-in time and coil current differential are derived parameters used for diagnostics. Contact over-travel time provides information on the remaining life of contacts and coil current differential provides indication of contact weld. The armature pull-in time gives the information on contact closing speed. The test results agree well with contactor failure. The pull-in voltage, drop-out voltage and contact resistance are some of the commonly used diagnostic parameters [60]. Measuring the coil resistance and monitoring the contact with at least  $6V_{DC}$  and 100mA are some of the diagnostic parameters when relay is out of circuit. Coil drive voltage and monitoring the contact with at least  $6V_{DC}$  and 100mA are some of the diagnostic parameters when relay is in circuit.

Most of these methods are offline and use contact side measurement (healthiness is verified by opening the relay contact) for diagnostics of contact weld failure. Hence, it is desirable to develop a new method to detect EM relay contact weld failure in online (without opening the relay contact). Based on detailed investigation of EM relay, a novel online

diagnostic method is proposed in this study by interpreting coil current decay curve. It detects relay contact in fail-to-open condition without disturbing the load attached to the contact. This method is online, continuous, automatic and facilitates simultaneous testing of redundant channels. The relays considered for testing are of SPDT type; however this method can be applied for any type of contact.

### 3.3 A Method for Online Diagnostics of EM Relay

#### 3.3.1 Fundamental principle

During de-energization of a healthy EM relay, the coil current decay curve takes a characteristic shape as shown in Figure 3.4(a). It is observed that when contacts get welded, the coil current decay curve follows a distinctly different shape as depicted in Figure 3.4(b). Coil current decay waveforms are captured across the series resistor in freewheeling diode path.

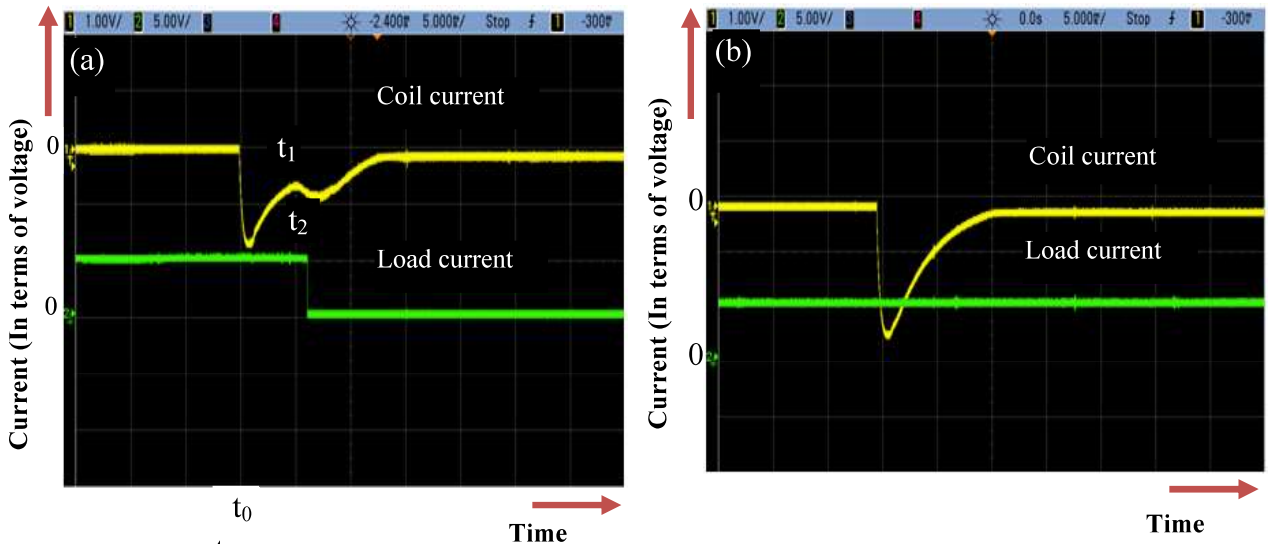


Figure 3.4: Coil de-energization current decay curve (a) Under healthy contacts; (b) Under welded contacts.

In case of a healthy relay referred in Figure 3.4(a), when de-energization is triggered at  $t_0$ , coil current is given by,



$$i_d = I_0 e^{(-t(R/L_1))}$$

where,  $I_0$  is initial current,  $R$  is the summation of coil and freewheeling diode series resistances and  $L_1$  is coil inductance.

However, at time instant  $t_1$ , the decay curve starts taking a different locus given by,

$$i_d = I_1 e^{(-t(R/L_2))}$$

where,  $L_2$  is new coil inductance.

This change in decay curve is due to inductance change which in turn is indicative of start of armature detachment. Actual opening process of the relay contact starts after a few ms from  $t_1$  ( $\sim 1.6$ ms) as depicted in Figure 3.4(a) with the indication of  $t_2$  in load current.

In case of a welded contact referred in Figure 3.4(b), there is no change in decay curve and is given by,

$$i_d = I_0 e^{(-t(R/L))}$$

This is because there is no change in  $L$  since the armature never detach. “Absence of a second minimum can be used to detect a welded contact. The time between  $t_1$  and  $t_2$  ( $\sim 2$ ms) can be utilized for re-energizing the coil before the contact starts moving”.

### 3.3.2 Verification of proposed method

A re-energizing circuit shown in Figure 3.5 is designed to verify that it is indeed possible to re-energize a de-energized relay before the contact starts opening. Diagnostic circuitry is used to annunciate a relay failed with a welded contact. Experimental setup is shown in Figure 3.6.

#### a) Re-energization circuit

A test signal (TS) is fed to CLK of D-Flip Flop-1 ( $D_{FF-1}$ ). This triggers  $\bar{Q}$  to go low, thus initiating de-energization of the relay shown at  $t_0$  in Figure 3.7(a). The current decay curve is

captured using a differential amplifier. The information embedded in the waveform is extracted using a differentiator followed by a zero crossing detector as shown in Figures 3.7(b) and (c). Thus, the two local minima express themselves as two short rectangular pulses. The second pulse is used to trigger re-energization of the coil by passing through  $D_{FF-3}$  and  $D_{FF-2}$ . Results are shown in Figures 3.7(d), (e), and (f). By this process, the diagnostic information is extracted without any change in load current as shown in Figure 3.7(g).

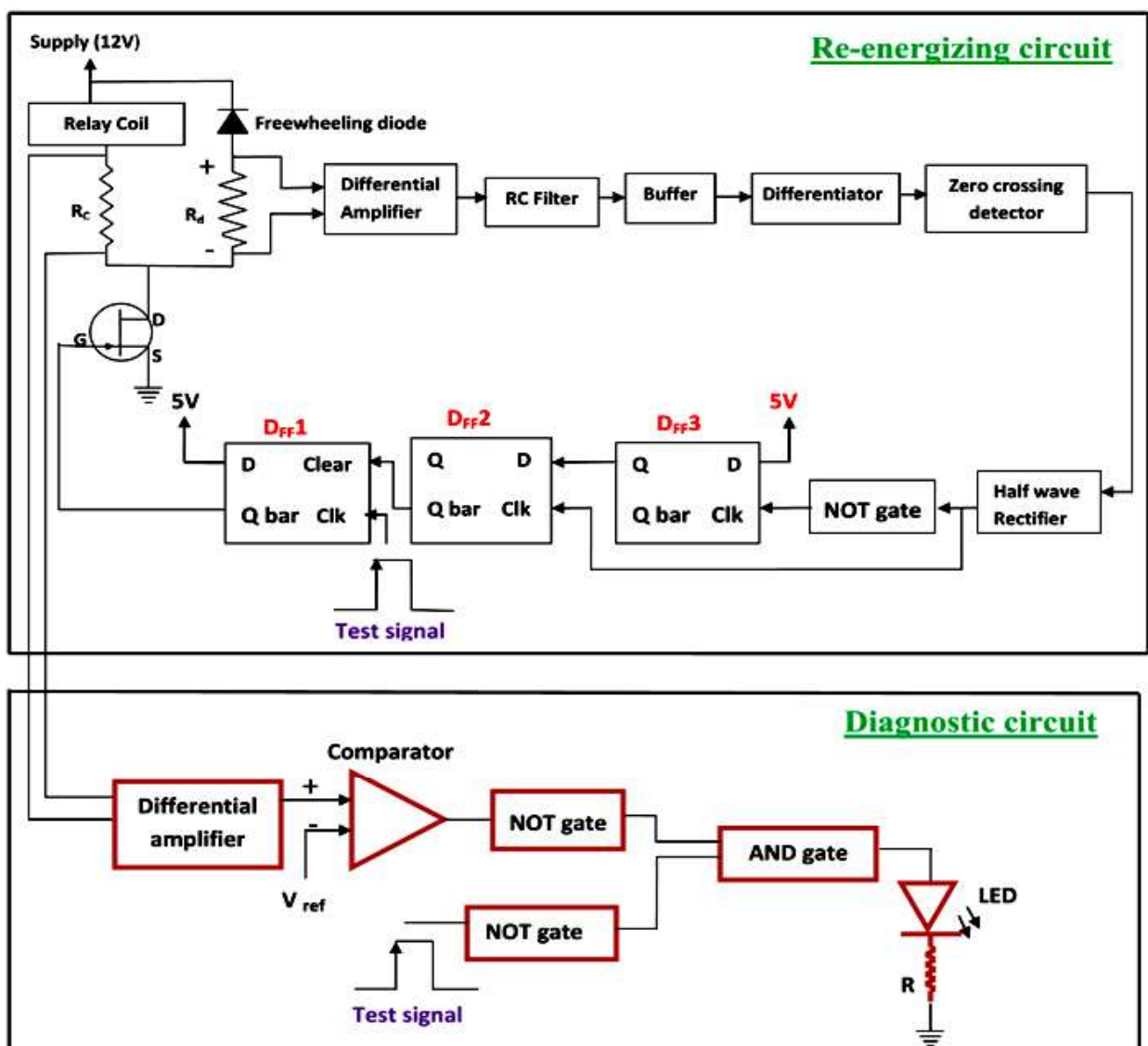


Figure 3.5: Schematic circuit to implement EM relay diagnostics.

b) Diagnostic circuit

As shown in Figure 3.5, diagnostic circuit will verify whether re-energization of coil has taken place or not. LED will give the indication if test (re-energization) fails.

Coil re-energization before the start of contact opening is also verified with voltage waveform of a resistor in series with the coil. Re-energization point is shown in Figure 3.7(i). There is no re-energization point for welded contact as shown in Figure 3.7(j).

Coil voltage waveform is compared with  $V_{ref}$  (0.2V).  $\overline{TS}$  and complement of comparator output are performed AND operation, which drives low (LED off), if relay contact is healthy. If relay contact is welded, due to failure in re-energization, the inverted comparator output remains HIGH even after test pulse is withdrawn. This makes LED ON which can be used for annunciating a relay failure.

Table 3.4: Test parameters.

Relay type	O/E/N 58
Contact type	Form c(Change over)
Coil voltage	12V
Coil resistance	285 $\Omega$
Coil current drawn	40mA
Coil suppressors	Diode and 100 $\Omega$ resistor
Load condition	Resistive load

The advantage achieved in this method is detecting contact weld failure online, without disturbing load circuit. This method is immune to coil voltage variation. Experimental test parameters are listed in Table 3.4.

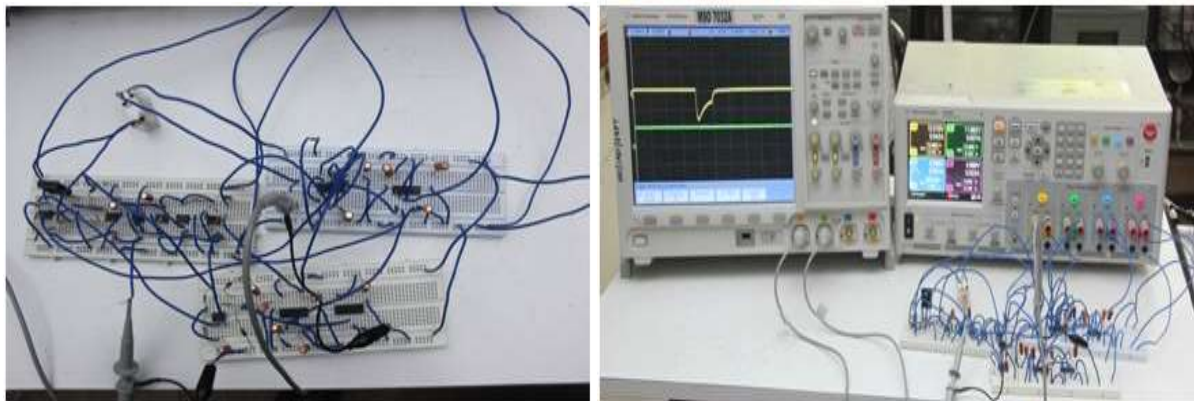
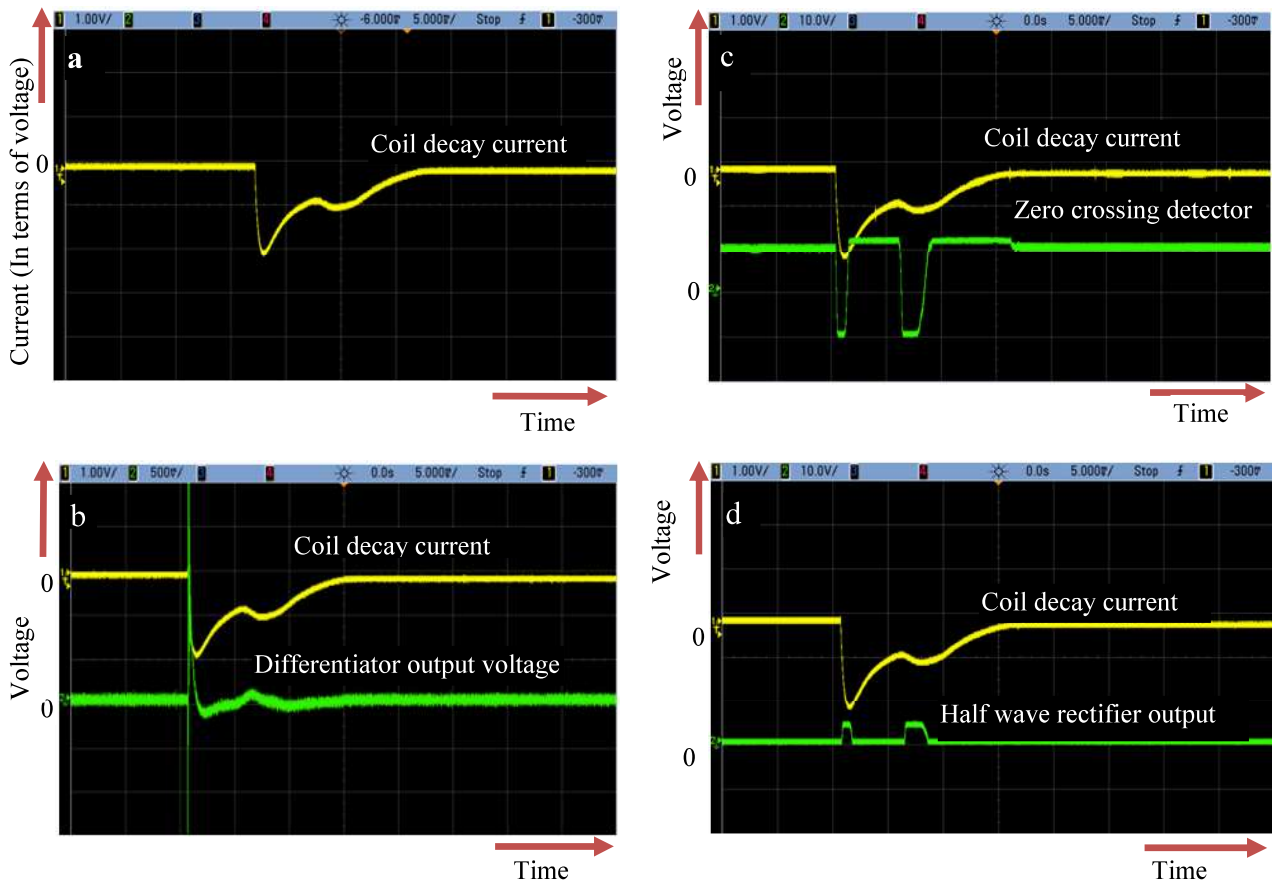


Figure 3.6: Experimental setup.

3.3.3 Results



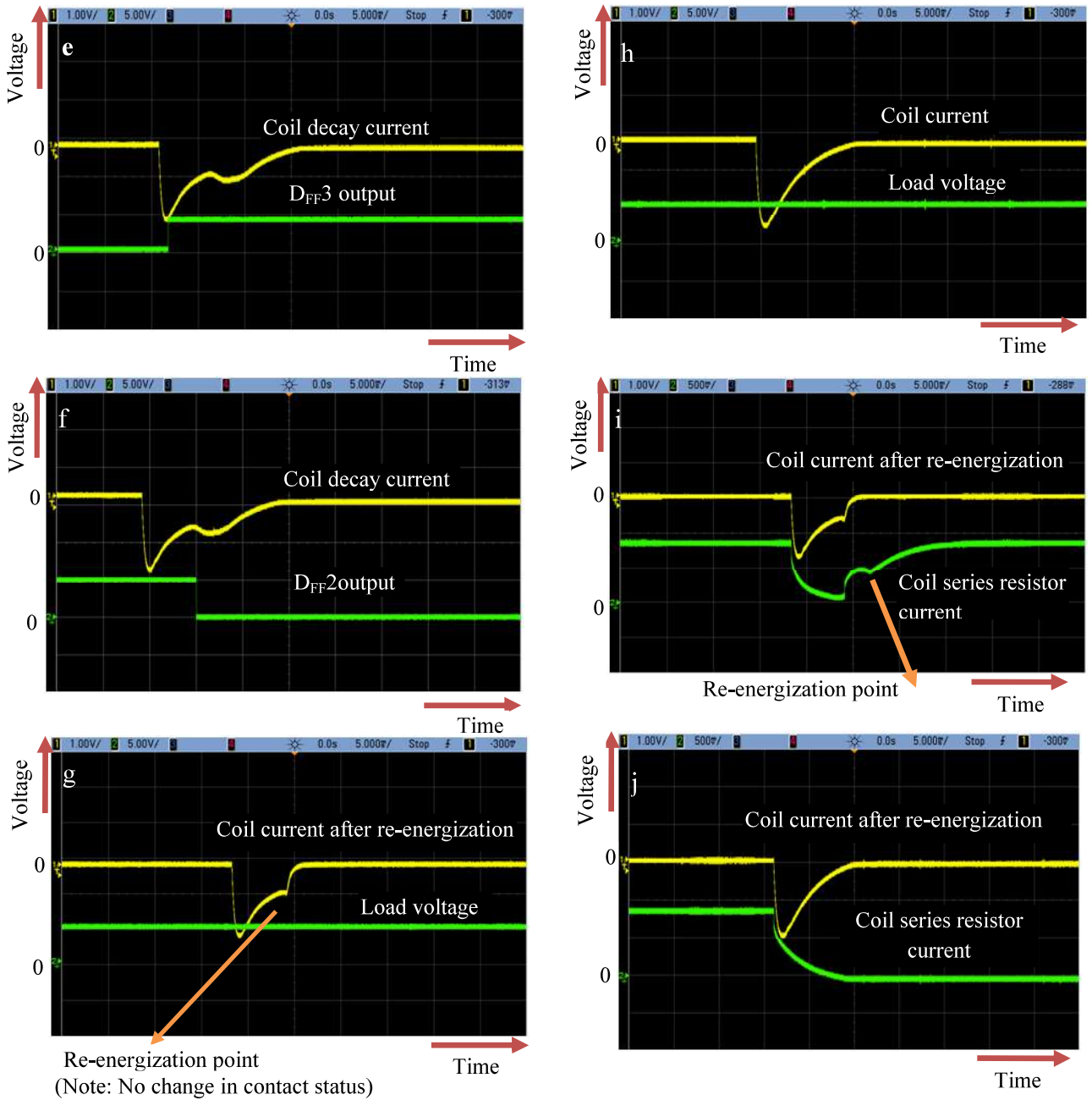


Figure 3.7: Results of diagnostic circuit (a)LPF output; (b)Differentiator output; (c)Zero crossing detector output; (d)Half wave rectifier output; (e) $D_3$  flip flop output; (f) $D_2$  flip flop output; (g)Coil re-energization current with load voltage for healthy relay; (h)Coil re-energization current with load voltage for welded relay; (i)Coil series resistor voltage waveform for healthy relay; (j) Coil series resistor voltage waveform for welded relay.

### **3.3.4 Reliability improvement**

By deploying this method for online diagnostics; test interval can be drastically reduced. This is because load is not disturbed during the test. Moreover, simultaneous testing of multiple redundant channels is possible. Therefore, by reducing test interval, failure probability can be decreased, which leads to reliability improvement of relay. Reliability improvement achieved by incorporating this method is discussed in Chapter 4.

This apart, the confidence on the systems is also improved since dependency on auxiliary or mirror contact is removed. Thus diagnostic becomes more robust.

### **3.3.5 Limitations and precautions**

- This method is developed keeping in mind the requirements in nuclear regulatory codes mandating periodic testing of final control elements. It is assumed that the system developer has choice for relay selection.
- The proposed method will work only when a diode with series resistor is chosen in parallel to the relay. However, this may not have an optimized effect on relay opening time.
- The proposed method is verified with SPST and SPDT types of relay. For some relay constructions, the armature may move slightly even with a welded contact in which case the method is ineffective. Moreover, the timing between  $t_1$  and  $t_2$  is a function of relay geometry. The chosen relay has to be tested before selecting the same for an application.
- Detailed microscopic investigation may be carried out on any possibility of contact degradation due to minor mechanical movement of contacts as a result of applying this method with a short test interval.

### **3.4 Summary**

- A novel online, continuous and automated method is proposed to perform online diagnostics of electromagnetic relay for a safety critical application.
- Diagnostic method works on the principle of de-energizing followed by quick re-energization of relay coil before the contact starts moving apart. Test results are satisfied and welded contact detected successfully.
- The significance of the current work is that it facilitates diagnostics without any impact on the load. Isolation of the load is thus intact. Simultaneous testing of redundant channels becomes possible.
- Reliability improvement is possible due to reduction in “test interval” and robustness of the method.

# 4

## A RELAY OUTPUT CARD WITH WELD DIAGNOSTICS AND RELIABILITY MODELING

---

*This chapter presents practical implementation and verification of relay contact weld detection circuit proposed in chapter 3 using a relay output card. Markov modeling is developed to verify the reliability improvement achieved with online diagnostics. Sensitivity analysis is carried out by varying the test interval and proof test interval.*

---

### 4.1 Relay Output Card with Diagnostics

#### 4.1.1 Implementation

A novel method has been proposed and presented in Chapter 3 to detect a weld failure of relay contacts without disturbing the load. In this method, healthiness of relay contact is monitored by interpreting the coil current decay curve of the relay. When a de-energization signal is given to a relay, a diagnostic circuit gives the re-energization signal before the contacts start to open if it is healthy. This method is implemented in a Relay Output Card (ROC) to demonstrate the method in a practical application. A ROC is a Printed Circuit Board (PCB) populated with Electro Magnetic (EM) relays and forms part of a final control element in a typical Safety Instrumented System (SIS) loop. Figure 4.1 shows the simplified representative schematic of relay weld detection circuit in ROC. The circuit has two blocks namely functional block (shown in red border) and diagnostic block (shown in blue border). Relay is connected to  $12V_{DC}$  and drain of MOSFET ( $Q_1$ ). In this, “Relay energize” is the control signal, controlled by



an external controller (logic solver of SIS). “Relay Enable” is the diagnostic block control signal which will be HIGH. Both “Relay energize” and “Relay enable” signals have to be held HIGH to energize the relay. The controller gives a “Test trigger” to the Clk of D-Flip Flop ( $D_{FF}$ )-1. This triggers Q-bar (Relay enable) to go Low. The LOW signal at “Relay Enable” de-energizes the relay. The diagnostic circuit reverts back it to HIGH (to re-energize relay) if contact is healthy. The re-energization takes place before the relay contact starts moving. “Test status” is indicated with Relay enable, Test trigger and Relay energize signals. Test status is read back by the controller to infer the health of the contact. This method facilitates healthiness monitoring without affecting contact status (contacts does not move during the diagnostic test). Detailed PCB schematic is shown in Figure 4.2 and the PCB is shown in Figure 4.3.

ROC is interfaced with Central Processing Unit (CPU) card on I2C bus (Inter-Integrated Circuit) backplane. CPU card is microcontroller based with STELLARIS LM3S2965 with ARM CORTEX M3 core from Texas Instruments. This card has two numbers of built in I2C ports for controlling I2C0 and I2C1 bus, built in JTAG port for debugging and programming and supports programming in C. CPU sends the command on backplane I2C0 bus to each card in the slot. After this, the I2C0 buffer (LTC4304) is enabled on a particular ROC in order to open that card for I2C0 data communications. Bi-directional Serial Data line (SDA) and Serial Clock (SCL) lines from the buffer is connected to register (PCA9556), consists of 8-bit input port and 8-bit output port to control further. The CPU enables the PCA9556’s I/Os as either inputs or outputs by writing to the configuration register. “RELENERGIZE” signal is kept HIGH by writing at output port-1 ( $O_1$ ). HIGH to LOW transition “TESTRESET” signal connected at  $O_4$  is used to reset the  $D_{FF}$ -3 to get the initial conditions before diagnostic test. “TESTTRG” signal is given to clock of  $D_{FF}$ -1 ( $U_2$ ) through  $O_2$ . This triggers Q-bar to go Low. The LOW signal at “Relay



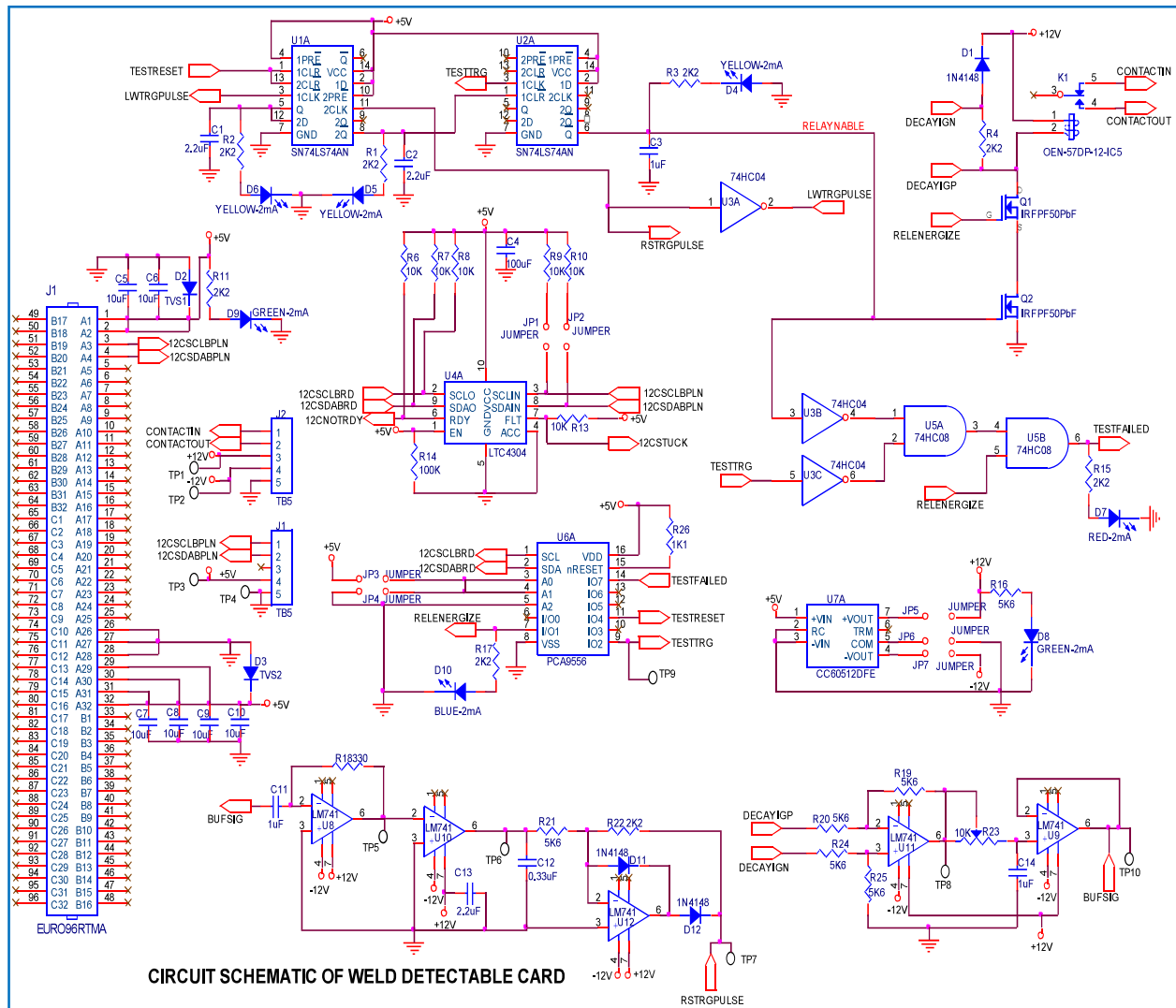


Figure 4.2: Detailed PCB schematic.

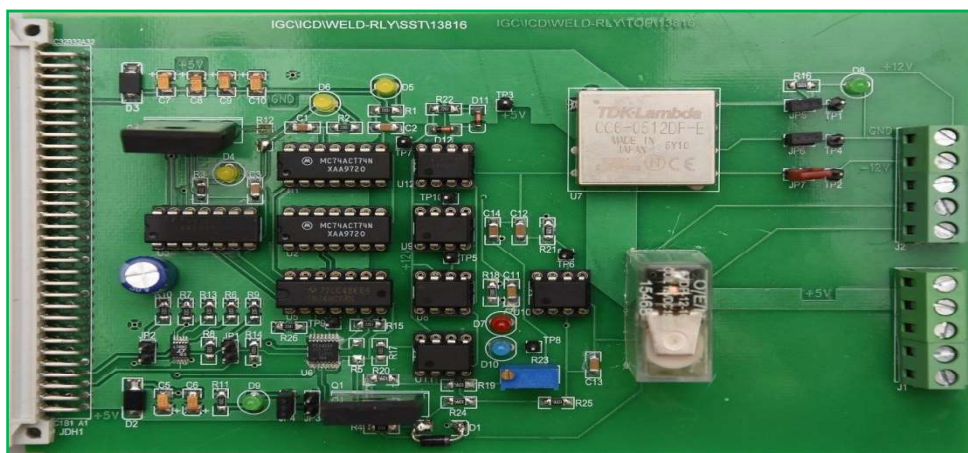
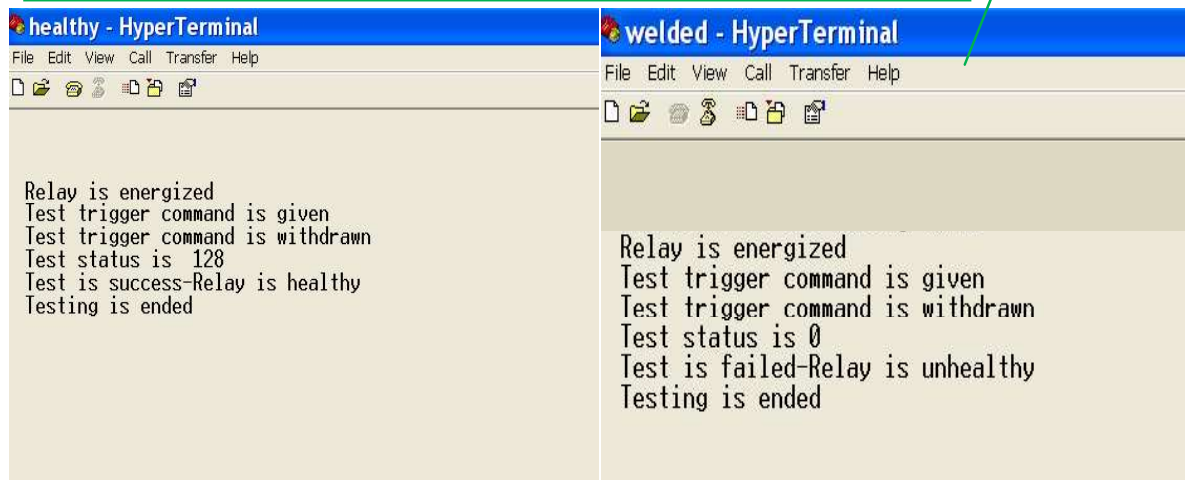
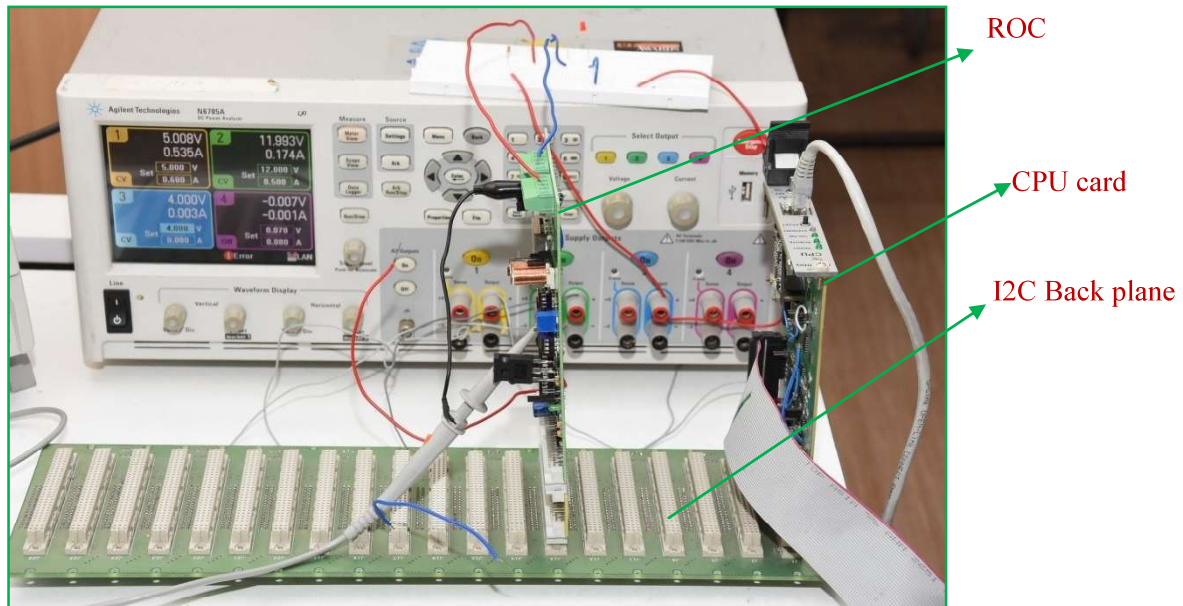
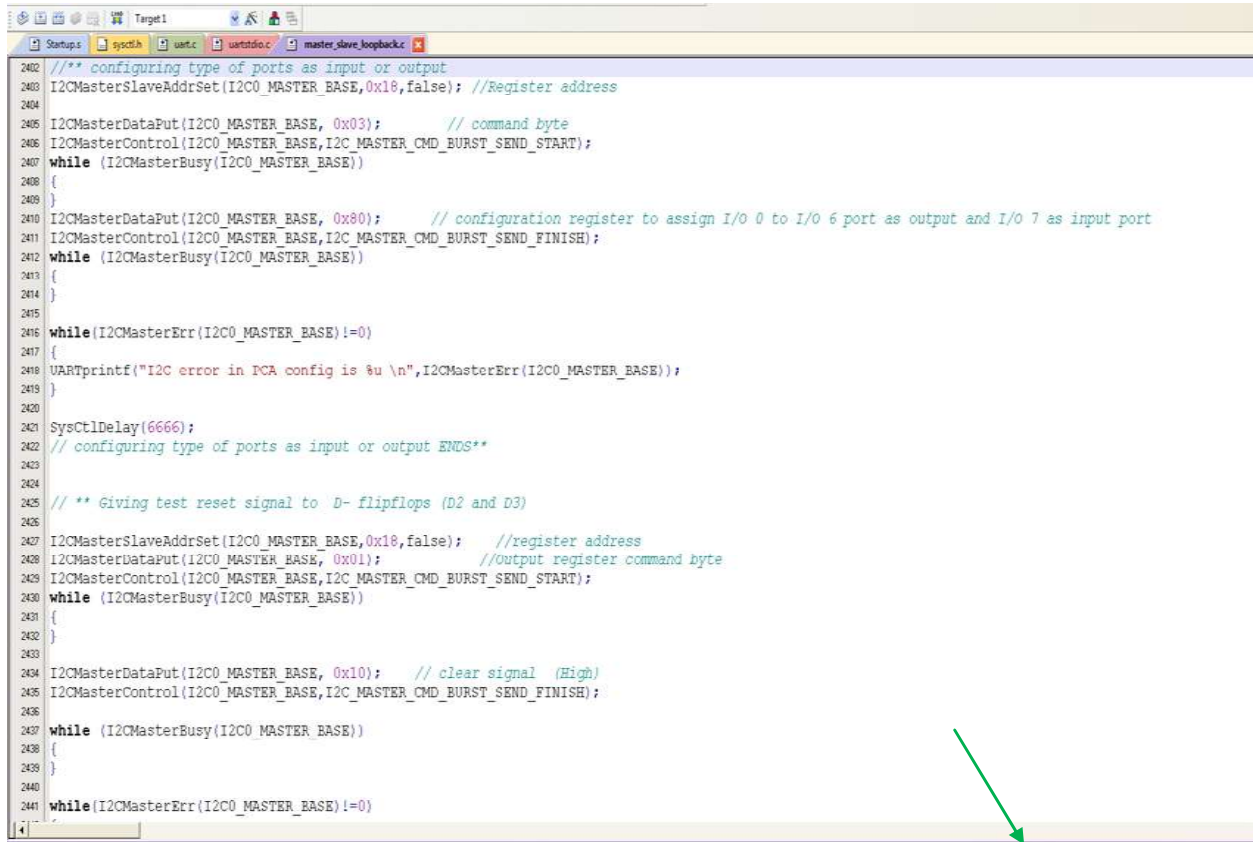


Figure 4.3: Printed circuit board of ROC.

### 4.1.2 Experimental setup





```

2402 /** configuring type of ports as input or output
2403 I2CMasterSlaveAddrSet(I2C0_MASTER_BASE,0x18,false); //Register address
2404
2405 I2CMasterDataPut(I2C0_MASTER_BASE, 0x03); // command byte
2406 I2CMasterControl(I2C0_MASTER_BASE,I2C_MASTER_CMD_BURST_SEND_START);
2407 while (I2CMasterBusy(I2C0_MASTER_BASE))
2408 {
2409 }
2410 I2CMasterDataPut(I2C0_MASTER_BASE, 0x80); // configuration register to assign I/O 0 to I/O 6 port as output and I/O 7 as input port
2411 I2CMasterControl(I2C0_MASTER_BASE,I2C_MASTER_CMD_BURST_SEND_FINISH);
2412 while (I2CMasterBusy(I2C0_MASTER_BASE))
2413 {
2414 }
2415
2416 while(I2CMasterErr(I2C0_MASTER_BASE)!=0)
2417 {
2418     UARTPrintf("I2C error in PCA config is %u \n",I2CMasterErr(I2C0_MASTER_BASE));
2419 }
2420
2421 SysCtlDelay(6666);
2422 /** configuring type of ports as input or output ENDS**
2423
2424
2425 // ** Giving test reset signal to D- flipflops (D2 and D3)
2426
2427 I2CMasterSlaveAddrSet(I2C0_MASTER_BASE,0x18,false); //register address
2428 I2CMasterDataPut(I2C0_MASTER_BASE, 0x01); //output register command byte
2429 I2CMasterControl(I2C0_MASTER_BASE,I2C_MASTER_CMD_BURST_SEND_START);
2430 while (I2CMasterBusy(I2C0_MASTER_BASE))
2431 {
2432 }
2433
2434 I2CMasterDataPut(I2C0_MASTER_BASE, 0x10); // clear signal (High)
2435 I2CMasterControl(I2C0_MASTER_BASE,I2C_MASTER_CMD_BURST_SEND_FINISH);
2436
2437 while (I2CMasterBusy(I2C0_MASTER_BASE))
2438 {
2439 }
2440
2441 while(I2CMasterErr(I2C0_MASTER_BASE)!=0)

```

Figure 4.4: Experimental setup.

Keil programming

## 4.2 Reliability Analysis

### 4.2.1 Markov model of the system

Markov model is established to study the effect of various parameters like the failure modes of diagnostic circuitry and its possible unintended impact on the functional block.

The ROC circuit forms part of shutdown system to communicate shutdown signal. The probability that the shutdown signal is not communicated when actual demand arises (relay contact not opening even when coil is de-energized) will be extremely small. This mode of failure is called “dangerous” or “unsafe failure”. When the relay contact used to communicate shutdown signal opens without any actual demand, it is called as “spurious failure”. For effective model of the system dynamics, the notations are introduced in Table 4.1.



Table 4.1: Notations for Markov model.

$\lambda_{RL-D}$ = Failure rate of functional block (relay block) in dangerous mode	Those failures in the functional block which are unsafe like welding of relay contacts, driver transistor stuck at HIGH, etc.
$\lambda_{RL-S}$ = Failure rate of functional block (relay block) in spurious mode	Those failures in the functional block which will result in an opening of relay contacts. These are safe failures and are immediately detectable.
$\lambda_{D-UD}$ = Failure rate of diagnostic block in undetected mode (mode 0)	Those failures in the diagnostic block which remain dormant. When a test is done, the controller will assume that the test is being performed, but the test trigger will not actually go through the functional block. These failures are not unsafe until the relay contact gets welded and when the real need of diagnostic circuitry arises.
$\lambda_{D-S}$ = Failure rate of diagnostic block in spurious mode (mode 1)	Those failures in the diagnostic block which will result in an opening of relays. These are safe failures and are immediately detectable.
TI-Test Interval	The time interval between two subsequent automatic tests done on the relay to reveal welded contacts.
$T_s$ - Mean time for safe restoration	The time taken to remove the ROC or put the system in a safe state after detection of weld/spurious failure. In safe state, the system will not perform its function but will remain in safe state.
$\mu_{TIS}$ = Repair rate with respect to corective action taken when the diagnostic circuitry detects an unsafe failure.	The inverse of the sum of test interval and the mean time taken to remove the PCB or put the system in safe state. Thus $\mu_{TIS} = \frac{1}{(TI+T_s)}$
$\mu_{RL}$ = Repair rate of relay output card	The inverse of the mean time to restore the system to healthy state.
$\tau$ - Proof test interval	The time interval between subsequent proof tests. Proof test is conducted manually where all undetected failures

	in the diagnostic block are revealed. Special test points are to be provided in the circuit to ensure complete fault coverage. This may involve monitoring of signal transitions using an oscilloscope. Thus, these tests are done typically in the order of weeks or months.
$\mu_{PT}$ = Repair rate - proof test	The inverse of the Mean Time To Detect and Repair (MTTDR). Any faults in the diagnostic block which remain dormant are revealed only during a proof test. $MTTDR = \tau + (\text{Time to restore the system back to healthy state})$ . Thus $\mu_{PT} = \frac{1}{MTTDR}$
$\mu_S$ = Repair rate- safe restoration	The inverse of the mean time for safe restoration. Thus $\mu_S = \frac{1}{T_S}$

The system described in above section is modeled in Markov state space. The possible states of the functional block are ‘functional block is healthy’, ‘relay contact fail-to-open’ and ‘fail-to-close’ represented with two binary bits as shown in Table 4.2. The possible states of the system with functional and diagnostics block is shown in Table 4.3 with 4 binary bits (first two bits indicate the functional block status and rest of the two are status of diagnostic block).

The possible states listed in Table 4.3 will have transitions to other states as shown in Figure 4.5. The state 1111 is the initial state where the functional block and diagnostic block are healthy. The state 0111 is relay functional block failure in dangerous mode, but diagnostic block is healthy. This is unsafe for the short duration, since this failure will be detected within the test interval. When the failure is detected the system, it is reasonable to assume that the system is put quickly in safe state 0000 without actually knowing the cause of the failure (by removing the PCB from its slot in the enclosure). Thus the system is in safe but spuriously failed state until the actual repair action is completed. Before detection of the unsafe failure, there may be a chance to

go to state 0101 (relay functional block failure in dangerous mode and diagnostic block mode 0 failure) at a rate of  $\lambda_{D-UD}$ . State transitions from 1101 to 1100, 1001 to 1000 and 0101 to 0100 are neglected since they are not numerically significant. Hence, 0111, 0101 are the unavailable states for this system, the state probabilities are  $P_1$  and  $P_2$  respectively. Thus, unsafe state probability (steady state) of the system is  $P_1 + P_2$ .

The state 1110 is reached when the functional block is healthy, but the diagnostics block has failed in mode 1. This state is transitory. So the state transition from 1111 to 1110 is shown as 1111 to 1010.

Table 4.2: Notations used for functional block status in Markov model.

1	1	Functional block is healthy
1	0	Relay fail-to-close (spurious)
0	1	Relay fail-to-open (dangerous state)

Table 4.3: Possible states of the system.  
(other states either do not exist or numerically insignificant)

State	Functional block		Diagnostics block 1-No failure in mode 0, 0-mode 0 failure	Diagnostics block 1- No failure in mode 1, 0-mode 1 failure
1	1	1	1	1
2	1	1	0	1
3	1	0	1	1
4	1	0	0	1
5	1	0	1	0
6	0	1	1	1
7	0	1	0	1



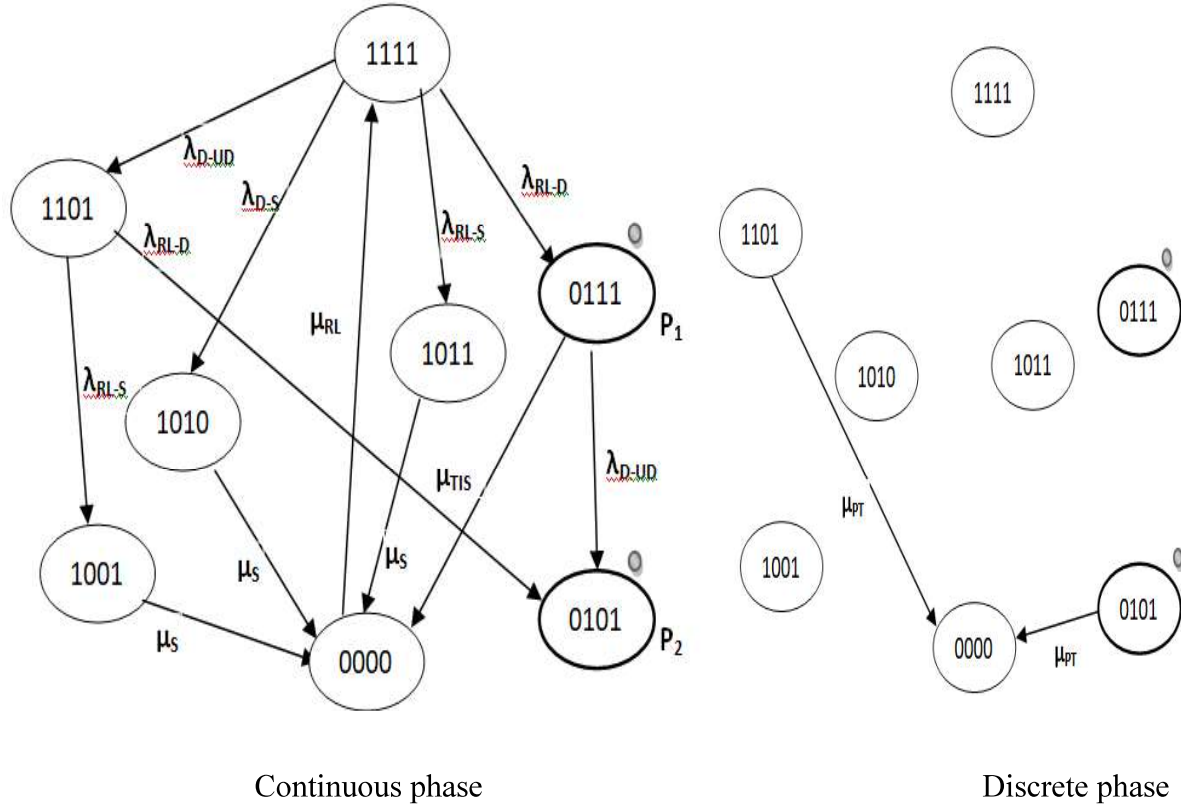


Figure 4.5: Markov state space model.

#### 4.2.2 Failure rate calculation

The failure rates required for the system model described in the above are calculated in this section. Failure rates required for calculation are taken from MIL-HDBK 217F Notice 2 [91] as per parts count method, with the assumptions of environment is considered as ground, benign, diode is considered as general purpose analog diode, resistor composition is considered as RCR style, capacitor is considered as paper type. The mode probability distribution values are from RIAC FMD-91 [92].

##### 1. Failure rate of diagnostic block

The diagnostic block consists of re-energization circuitry and feedback circuitry. The feedback circuitry does not contribute to the spurious failure of relays. Thus the re-energization circuitry alone is considered in this sub-section. The failure rate of an op-amp is calculated based

on the data available in the datasheet of TI UA-741, MIL-HDBK-217F and is shown in Table 4.4. The re-energization circuit in diagnostic block failure rate is shown in Table 4.5.

Table 4.4: Failure rate of TI UA-741.

Micro circuits, hybrid failure rate $\lambda_p = (\sum N_c \lambda_c)(1 + 0.2 \pi_E) \pi_F \pi_Q \pi_L$ failures/ $10^6$ hours		
Transistor failure rate, $\lambda_c$ (failures/ $10^6$ hours)	$N_c = 22$	0.00015
Resistor failure rate, $\lambda_c$ (failures/ $10^6$ hours)	$N_c = 11$	0.0005
Diode failure rate, $\lambda_c$ (failures/ $10^6$ hours)	$N_c = 1$	0.0036
Capacitor failure rate, $\lambda_c$ (failures/ $10^6$ hours)	$N_c = 1$	0.0036
Overall failure rate $\lambda_c$ (failures/ $10^6$ hours)	$\sum N_c \lambda_c$	0.016
Environment factor, $\pi_E$	Ground Benign	0.5
Quality factor $\pi_Q$	Class S category	0.25
Learning factor $\pi_L$	Years in production is $>2$	1.0
Circuit function factor $\pi_F$	Linear	5.8
<b>Failure rate rate <math>\lambda_p</math> (failures / <math>10^6</math> hours)</b>		<b>0.02552</b>

Table 4.5: Failure rate of diagnostic block.

Stage	Component	Failure rate (failures / $10^6$ hours)	Quantity	Stage Failure rate (failures / $10^6$ hours)
Differential amplifier	Resistors	0.0005	4	0.002
	Op-Amp	0.02552	1	0.02552
LPF	Resistor	0.0005	1	0.0005
	Capacitor	0.0036	1	0.0036
Buffer	Op-Amp	0.02552	1	0.02552
Differentiator	Capacitor	0.0036	1	0.0036

Stage	Component	Failure rate (failures / $10^6$ hours)	Quantity	Stage Failure rate (failures / $10^6$ hours)
	Resistor	0.0005	1	0.0005
	Op-Amp	0.02552	1	0.02552
Zero crossing detector	Op-Amp	0.02552	1	0.02552
Half wave rectifier	Resistors	0.0005	2	0.001
	Diode	0.0036	2	0.0072
	Op-Amp	0.02552	1	0.02552
NOT gate	SN74HC04	0.0057	1	0.0057
D-Flipflop	SN74LS74AN	0.0057	3	0.0171
Kick back voltage	Free wheeling diode	0.0036	1	0.0036
	Free wheeling diode resistor	0.0005	1	0.0005
MOSFET	MOSFET	0.014	1	0.014
	Resistor	0.0005	1	0.0005
		<b>Total</b>		<b>0.1874</b>

The failure rate of diagnostic circuit is 0.1874 failures/ $10^6$  hours includes both mode 0 and mode 1 failures.

Calculation of mode specific failure rates are as follows:

Note: The mode probability distribution values are taken from RIAC FMD-91 [92].

- a) Failure rate of diagnostic block in spurious mode (mode 1) ( $\lambda_{D-S}$ )
  - i. D<sub>1</sub> flip flop contribution (m): Output stuck at low: This failure will result in fail to re-energize after de-energization by test trigger. Thereafter, relay will not be energized even when demand arises.

Thus  $m = (P_{\text{output stuck at low}} + P_{\text{output open}} + P_{\text{supply open}}) \times D_1 \text{ failure rate}$

$$= (0.09 + 0.36 + 0.12) \times 0.0057 = 0.003249 \text{ failures}/10^6 \text{ hours.}$$

- ii. D<sub>2</sub> flip flop contribution (n): When Q bar output fails to transit from HIGH to LOW; it does not give “clear” input to D<sub>1</sub>. All the failure modes of D<sub>2</sub> lead to this event.

Thus  $n = 0.0057 \text{ failures}/10^6 \text{ hours.}$

- iii. D<sub>3</sub> flip flop contribution (o): When Q output fails to give HIGH; it will fail to give “D” input to D<sub>2</sub> flip flop.

Thus  $o = (P_{D_3 \text{ output stuck at low}} + P_{\text{input open}} + P_{\text{output open}} + P_{\text{supply open}}) \times D_3 \text{ failure rate}$

$$= (0.09 + 0.36 + 0.36 + 0.12) \times 0.0057 = 0.005301 \text{ failures}/10^6 \text{ hours.}$$

- iv. Q<sub>2</sub> transistor failure rate (p): MOSFET fail to respond as per D<sub>1</sub> output.

Thus  $p = (P_{\text{open}} + P_{\text{output LOW}} + P_{\text{output HIGH}} + P_{\text{parameter change}}) \times \text{FET transistor failure rate}$

$$= (0.05 + 0.22 + 0.05 + 0.17) \times 0.014 = 0.00686 \text{ failures}/10^6 \text{ hours.}$$

- v. Others (q): All the failure modes of a NOT gate, half wave rectifier, zero crossing detector, differentiator, buffer, RC filter and differential amplifier contribute to spurious failure rate.

Thus  $q = 0.1558 \text{ failures}/10^6 \text{ hours.}$

Thus, spurious failure rate ( $\lambda_{D-S}$ ) =  $m + n + o + p + q = 0.17691 \text{ failures}/10^6 \text{ hours.}$

**The failure rate of diagnostic block in spurious mode ( $\lambda_{D-S}$ ) = 0.17691 failures/10<sup>6</sup> hours.**

Thus, 94.4% of diagnostic block failure rate lead to spurious failure of the functional board.

- b) Failure rate of diagnostic block in undetected mode (mode 0) ( $\lambda_{D-UD}$ )

- i. 5.6% of re-energization circuitry in diagnostic block failure rate (0.01049 failures/10<sup>6</sup> hours) contributes to undetected failure rate (100%-94.4% as discussed above).

- ii. The feedback circuitry normally gives a LOW output. Upon a test, the output remains low if the test passes. If a weld is detected, the output turns HIGH. A “Stuck at LOW” output will be interpreted by the controller as “Test passed” irrespective of relay status. Thus this failure remains dormant and will be revealed only in the proof test.

The failure rate contribution from feedback circuitry is detailed below:

- Contribution from AND gate =  $(P_{\text{output stuck LOW}} + P_{\text{input stuck at LOW}} + P_{\text{power supply open}} + P_{\text{output open}}) \times \text{AND gate failure rate}$   
 $= (0.09 + 0.36 + 0.12 + 0.36) \times 0.0057 = 0.005244 \text{ failures}/10^6 \text{ hours.}$
- Contribution from NOT gate =  $(P_{\text{output stuck LOW}} + P_{\text{power supply open}} + P_{\text{output open}}) \times \text{NOT gate failure rate}$   
 $= (0.09 + 0.12 + 0.36) \times 0.0057$   
 $= 0.003249 \text{ failures}/10^6 \text{ hours.}$

**The failure rate of diagnostic block in undetected mode ( $\lambda_{D-UD}$ ) = 0.01898 failures/ $10^6$  hours.**

## 2. Functional block failure rate

### a) Failure rate of functional block in dangerous mode ( $\lambda_{RL-D}$ )

- i.  $Q_1$  transistor failure rate =  $P_{\text{Short mode}} \times \text{MOSFET failure rate}$   
 $= 0.51 \times 0.014 = 0.00714 \text{ failures}/10^6 \text{ hours.}$
- ii. Relay failure =  $P_{\text{Relay contact short mode}} \times \text{relay failure rate}$   
 $= 0.19 \times 0.13 = 0.0247 \text{ failures}/10^6 \text{ hours.}$

**Therefore, the functional block failure rate in dangerous mode ( $\lambda_{RL-D}$ ) = 0.03184 failures/ $10^6$  hours.**

### b) Failure rate of functional block in spurious mode ( $\lambda_{RL-S}$ )

The functional block failure rate in spurious mode ( $\lambda_{RL-S}$ ) is assumed to be four times the relay block dangerous failure rate ( $\lambda_{RL-D}$ ).

Therefore, the functional block failure rate in spurious mode ( $\lambda_{RL-S}$ ) = 0.12736 failures/ $10^6$  hours.

#### 4.2.3 Markov analysis of the ROC

The following assumptions are made in the analysis:

- The functional block failure rate in spurious mode ( $\lambda_{RL-S}$ ) is considered to be four times the relay block dangerous failure rate ( $\lambda_{RL-D}$ ) by assuming all other failure modes which are not considered for functional block failure in dangerous mode leads to spurious mode.
- TI is assumed as 15minutes since the proposed diagnostic method is online and automatic.
- $T_s$  is assumed as 15minutes by considering the typical time taken by operator to reach the signal processing cabinet.
- $\tau$  is assumed as 168hours (1week) keeping in view that manual intervention and work load.

The various parameters required for Markov analysis is summarized in Table 4.6.

Table 4.6: Parameter values for Markov analysis.

Parameter	Value
$\lambda_{D-S}$	0.17691 failures/ $10^6$ hours
$\lambda_{D-UD}$	0.01898 failures/ $10^6$ hours
$\lambda_{RL-D}$	0.03184 failures/ $10^6$ hours
$\lambda_{RL-S}$	0.12736 failures/ $10^6$ hours
$\mu_{RL}$	0.125/hour
$\mu_{PT}$	0.005952/hour
$\mu_{TIS}$	2/hour
$\mu_S$	4/hour

Markov analysis is done with ISOGRAPH Reliability Software [93]. Markov analysis is performed to the ROC state space model as shown in Figure 4.5 with the listed values in Table 4.6. Markov model with state probabilities is shown in Figure 4.6. When the failure is detected,

the system is put in a spurious state by removing ROC PCB.  $P_1$  and  $P_2$  are the probabilities for the system to be in dangerous unavailable states. The state probabilities are  $1.59 \times 10^{-8}$  and  $1.71 \times 10^{-11}$ .

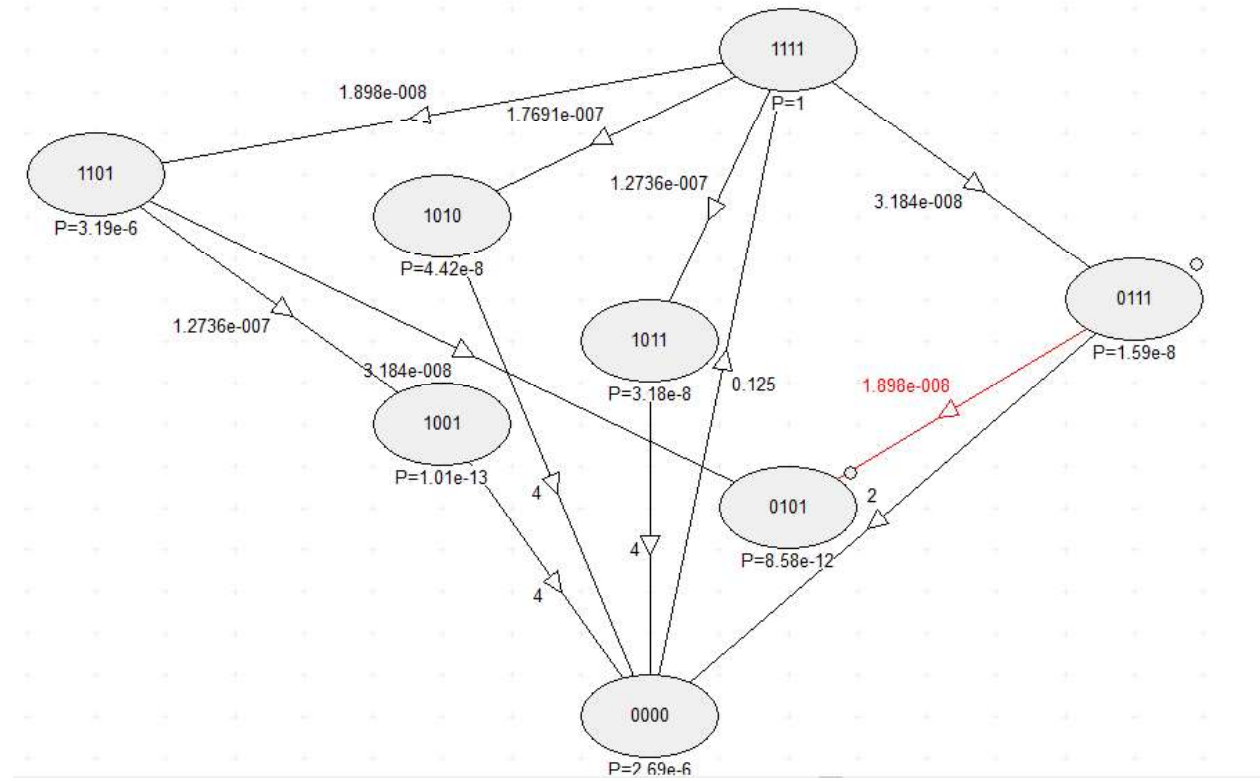


Figure 4.6: Markov state space in ISOGRAPH with state probabilities.

#### 4.2.4 Sensitivity analysis

##### 1. Reduction in unsafe state probability with test interval variation

In general, as part of periodic testing, a relay will be tested every shift (8hours) in a redundant channel (2oo3 voting logic) and hence the test interval is 24hours. This is because relay contacts open during the test, and the load is disturbed. Since, the proposed method of weld detection can be online (without opening the contacts), the test interval can be reduced from hours to minutes. The Figure 4.7 shows the comparison of unsafe state probability (steady state) between 24hours

and 15minutes. This shows that unsafe state probability of ROC is reduced by around 48 folds by introducing the technique.

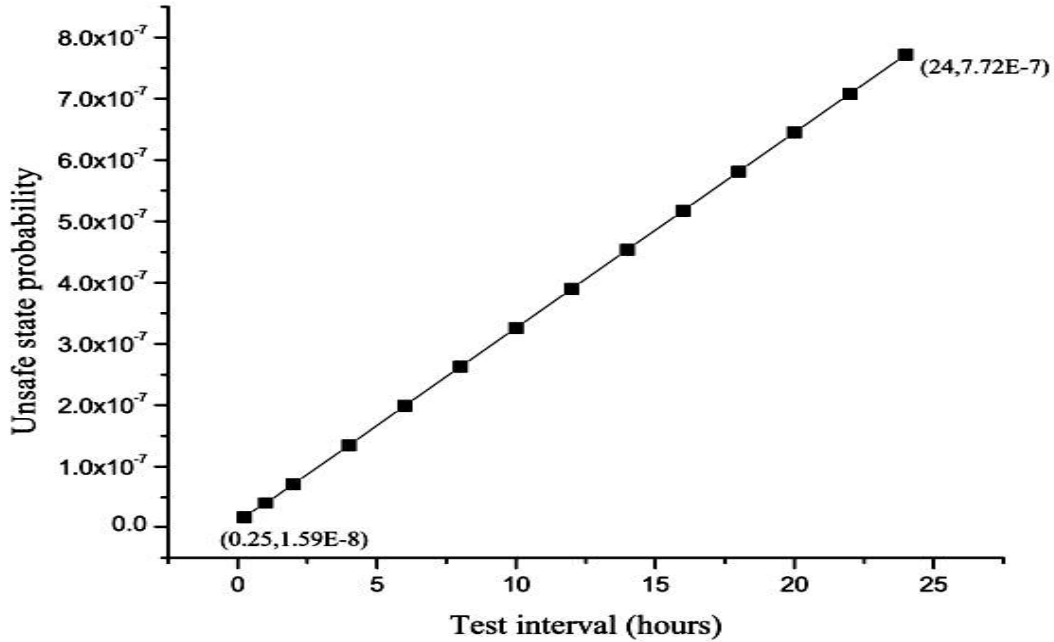


Figure 4.7: Unsafe state probability variation with test interval.

## 2. Variation of unsafe state probability with proof test interval

Proof testing will involve manual intervention to ensure complete fault coverage. Thus, the proof test interval has to be as large as possible in view of operator convenience. However, proof test interval has to be fixed without significant effect on unsafe state probability. Figure 4.8 shows unsafe state probability variation with proof test interval. Unsafe state probability shows a significant effect when proof test interval is greater than 40days. Thus, a proof test interval of 40days can be selected.



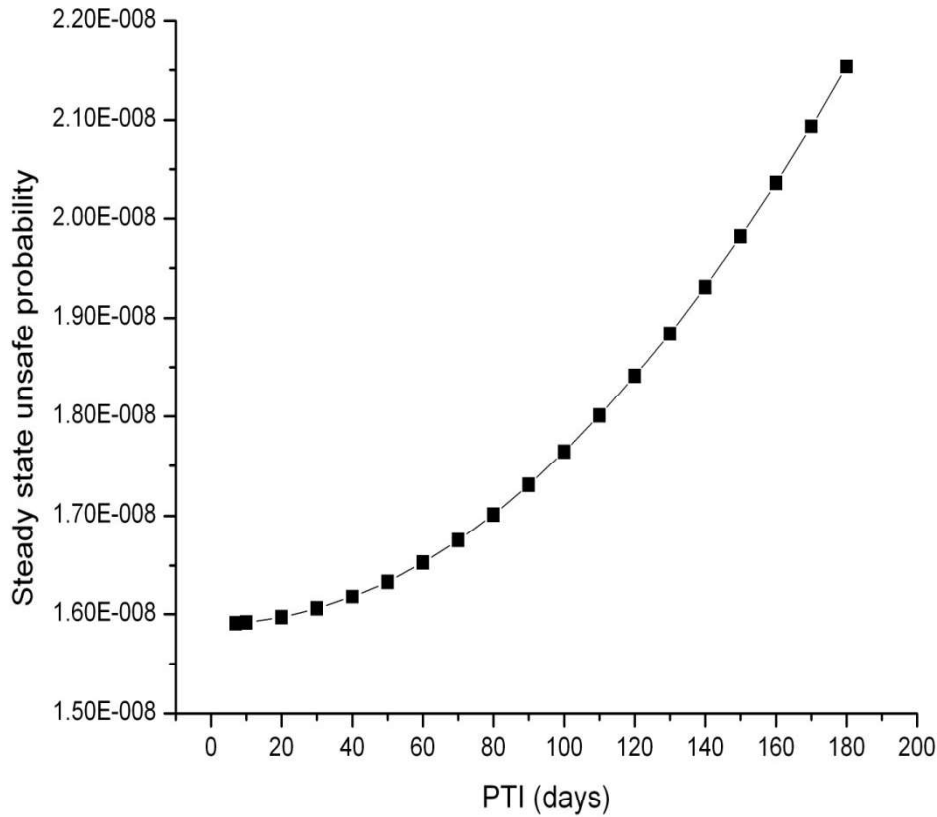


Figure 4.8: Unsafe state probability variation with proof test interval.

### 3. Diagnostic block dormant failure rate

The dormant failure of diagnostic block results in unavailability of testing provision. This subsequently can result in an unsafe state of the system (state  $P_2$  in Markov model). However, the unsafe state probability is dominated by  $P_1$ . Thus a significant margin in designing diagnostic circuit still exists when the proof test interval is one week. Unsafe state probability (steady state) is calculated for various values of  $\lambda_{D-UD}$  and shown in Table 4.7. Thus,  $\lambda_{D-UD}$  can be as high as  $0.3796 / 10^6$  hours without significant impact on unsafe state probability.

Table 4.7: Variation of unsafe state probabilities with diagnostic block failure rate.

$\lambda_{D-UD}$ (failures/ $10^6$ hours)	$P_1$	$P_2$	Unsafe state probability
0.01898	$1.59 \times 10^{-8}$	$1.71 \times 10^{-11}$	$1.59 \times 10^{-8}$
0.03796	$1.59 \times 10^{-8}$	$3.42 \times 10^{-11}$	$1.59 \times 10^{-8}$
0.07592	$1.59 \times 10^{-8}$	$6.84 \times 10^{-11}$	$1.59 \times 10^{-8}$
0.11388	$1.59 \times 10^{-8}$	$1.03 \times 10^{-10}$	$1.60 \times 10^{-8}$
0.15184	$1.59 \times 10^{-8}$	$1.37 \times 10^{-10}$	$1.60 \times 10^{-8}$
0.1898	$1.59 \times 10^{-8}$	$1.71 \times 10^{-10}$	$1.60 \times 10^{-8}$
0.3796	$1.59 \times 10^{-8}$	$3.42 \times 10^{-10}$	$1.62 \times 10^{-8}$
0.7592	$1.59 \times 10^{-8}$	$6.84 \times 10^{-10}$	$1.65 \times 10^{-8}$

### **4.3 Summary**

- It is possible to implement an online diagnostic circuitry for a relay output card to detect contact weld failures without any impact on functional circuit using the method proposed in Chapter 3.
- From the reliability analysis, it can be seen that the incorporation of diagnostic circuit reduces the unsafe state probability of the system by around 48 folds. The significant reduction in unsafe state probability is achieved through very low test interval which is turn has been possible because the proposed method is amenable for online implementation.
- Failures in diagnostic circuit have very less significance on the unsafe state probability of the system.
- It is possible to fix the test interval and proof test interval based on the target unsafe state probability requirement.

# 5

## **ELECTROMAGNETIC CONTACTORS: LIFE TESTING AND FAILURE ANALYSIS**

---

*The studies performed on EM contactor to understand its impact on uncontrolled withdrawal of neutron absorber rod in PFBR is reported. In this chapter, introduction to reliability demonstration testing of electromagnetic contactors is given. The test plan is chosen from MIL-HDBK-781A for fixed duration to verify the contactor failure modes. It also presents the surface morphology and composition analysis of degraded contacts carried out by scanning electron microscopy and energy dispersive spectroscopy.*

---

### **5.1 Introduction**

As seen from the Chapter 1 and 2, in spite of the fail-safe design provisions, Electro Magnetic (EM) contactor fail-to-open (contact weld) and sluggish response of the contactor upon de-energization are the instances leading to uncontrolled withdrawal of neutron absorber rods. Thus, there is a need to study the failures in contactors in detail. To verify the weld failure probability of contact, reliability demonstration test is performed. Failure analysis using Scanning Electron Microscopy (SEM) and Energy Dispersive Spectroscopy (EDS) is done and results are discussed.

An EM contactor is an electrically controlled switch used for switching higher current. EM contactors are the preferred final control elements to switch power to three phase AC motor. It consists of power contacts, auxiliary contacts, contact springs and an electromagnet. The electromagnet provides the driving force to close the contacts. The mechanical durability and

electrical durability of a contactor are assigned by the manufacturer, and this can be verified by statistical analysis with the test procedure given in IEC-60947 [62]. Electrical durability depends on many factors such as the type of load, switching frequency, switching phase, load current, ambient temperature, rated temperature, number of ON/OFF cycles, quality factor, contact form factor and construction factor. The datasheet specifies electrical durability at rated load (resistive/inductive), rated current and maximum switching voltage.

Table 5.1: Failure ratios of Normally Open contactor as per IEC 60947 [62].

Failure mode	Failure ratio with electrical durability test	Failure ratio with mechanical durability
Failure-to-open	73%	50%
Failure-to-close	25%	50%
Short circuit between poles	1%	0%
short circuit between pole and any adjacent part	1%	0%

IEC-60947 lists failure-to-open, failure-to-close, short circuit between poles and short circuit between pole and any adjacent part as failure modes of contactors. Table 5.1 lists typical failure ratios for NO contactors. It can be seen that failure-to-open (contact weld) is the most dominant mode of failure. This is of concern when such contactors are used for absorber rod movement.

## 5.2 Reliability Demonstration Testing using Test of Hypothesis Technique

Reliability Demonstration Testing (RDT) is performed in order to evaluate the reliability of a selected component. In order to evaluate the reliability level, the failure rate is selected from the manufacturer datasheet or practical field experience.

RDT plan is chosen from MIL-HDBK-781A for this study [94]. In fixed duration MTBF demonstration test, component will be tested as per calculated operating time. The reliability

parameter selected for this testing is Mean Time Between Failure (MTBF). Producer's risk ( $\alpha$ ) is the probability of rejecting a component with true MTBF equal to the upper test MTBF ( $\theta_0$ ). The probability of rejecting the component with true MTBF greater than upper test MTBF will be less than  $\alpha$ . Consumer's risk ( $\beta$ ) is the probability of accepting the component with a true MTBF equal to the lower test MTBF ( $\theta_1$ ). The probability of accepting the component with true MTBF less than the lower test MTBF will be less than  $\beta$ . Discrimination ratio (D) is the ratio of upper test MTBF to the lower test MTBF. The symbols used in fixed duration test plan are

T= Test termination time

k= Number of failures

a= Accept number

r= Reject number

c= Confidence

As per MIL-HDBK-781A [94] fixed duration, time terminated tests conducted with replacements, the termination time, the accept and reject numbers are calculated from,

$$\beta = \sum_{k=0}^a \frac{(T/\theta_1)^k e^{-T/\theta_1}}{k!}$$
$$1 - \alpha = \sum_{k=0}^{r-1} \frac{(T/\theta_0)^k e^{-T/\theta_0}}{k!}$$

Twelve of the most frequently used test plans derived from these equations are summarized in Table 5.2. During fixed operating time, if the total number of failures is equal to or less than the accept number of failures specified in the selected test plan, the component is accepted. If total number of failures is equal to or greater than reject number of failures corresponding to the selected test plan, the component is rejected.

Table 5.2: Fixed duration test plans [94].

Plan	$\alpha$	$\beta$	D	T ( $\times\theta_1$ )	R ( $\geq$ )	A ( $\leq$ )
IX-D	12.0	9.9	1.5	45.0	37	36
X-D	10.9	21.4	1.5	29.9	26	25
XI-D	19.7	19.6	1.5	21.5	18	17
XII-D	9.6	10.6	2.0	18.8	14	13
XIII-D	9.8	20.9	2.0	12.4	10	9
XIV-D	19.9	21.0	2.0	7.8	6	5
XV-D	9.4	9.9	3.0	9.3	6	5
XVI-D	10.9	21.3	3.0	5.4	4	3
XVII-D	17.5	19.7	3.0	4.3	3	2
XIX-D	29.8	30.1	1.5	8.1	7	6
XX-D	28.3	28.5	2.0	3.7	3	2
XXI-D	30.7	33.3	3.0	1.1	1	0

### 5.3 RDT Plan for a EM contactor: Application in PFBR

As part of this study, fixed duration RDT is carried out from MIL-HDBK-781A for the EM contactor used for control rod movement in PFBR.

Estimated use of raise contactor in plant life (in CSRDM) = 80,000 times in reactor life (PFBR reactor life is 40years).

The estimated use is derived based on contactor raise operations during approach towards criticality, start-up and burn up calculations. There are 9 absorber rods used for control function and hence 9 such contactors are used.

The intention is to demonstrate the contactor failure is limited to 0.5 in reactor life (With the assumption that contactor is not replaced when no failure is seen).

To achieve this, contactor failure rate should be

$$\lambda = (0.5 / (80000 \times 9)) \sim 7 \times 10^{-7} / \text{cycle}$$

Fail-to-open when coil is de-energized is the failure mode of concern. Assuming exponential distribution, MTBF ( $\theta_0$ ) = 14,28,572 cycles.

To verify this, test plan-XV-D is selected from MIL-HDBK 781A.

Total test duration =  $9.3 \times \theta_1 = 9.3 \times (\theta_0/D) = 44,28,573$  cycles.

Test plan-XV-D with  $9.3 \times \theta_1$  is chosen based on the time required to complete the test as well as optimizing the risk involved in the conclusion going incorrect.

With this test plan, if the number of failures is less than or equal to 5, then the test can be accepted with a 9.9% risk of true MTBF being equal to the lower test MTBF. The probability of accepting a component with a true MTBF less than the lower test MTBF will be still lesser than 9.9%.

### 5.3.1 Test setup

Testing circuit for MTBF of EM contactor is shown in Figure 5.1. Ten contactors of same make and model as in reactor are used for testing. Specifications of contactors are listed in Table 5.3. The contactor panel has indications for voltages in each phase, current drawn in each phase and ON/OFF status of each contactor. Contactors are placed in motor control center without air conditioning and hence similar environment is chosen for testing [typical temperature is 30°C].

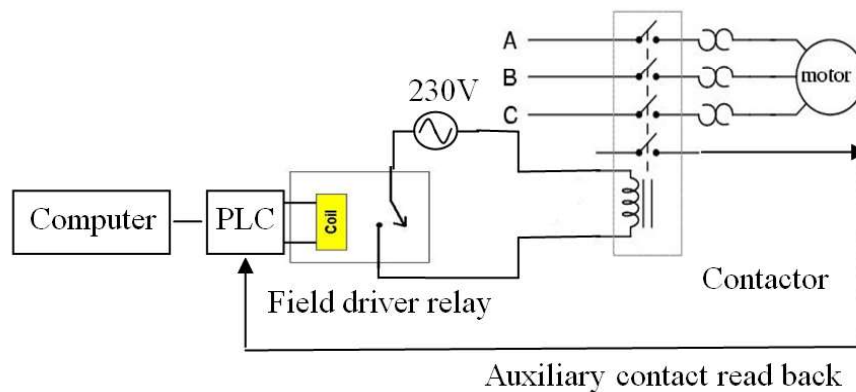


Figure 5.1: Contactor reliability testing circuit.



Table 5.3: Contactor specifications.

Make	Schneider Electric
Model	LC1D12
Coil voltage	240V <sub>AC</sub> , 50/60Hz
Number of poles	3NO
Rated operational voltage	$\leq 690V_{AC}$
Rated operational current	12A max
Auxiliary contacts	1NO + 1NC mechanically linked as per IEC 60947-5-1
Closing time	12-22ms
Opening time	4-19ms
Ambient temperature	-50 <sup>0</sup> C to 600 <sup>0</sup> C

CSRDM motor is simulated using an inductive load bank with adjustable load current and power factor. Testing is automated using a Programmable Logic Controller (PLC) using Unity Pro software, and human-machine interface is provided using Vijeo Citect SCADA software. The test setup is shown in Figure 5.2.

Contactors are tested at 1.5A based on field conditions. A power factor of 0.8 is set to simulate induction motor loading conditions. Inrush current as in a motor is also experienced by the contactor. Motors will take inrush current of 5-10 times the steady state current. Lesser the time spent in contactor ON and OFF states, shorter the testing time. As per datasheet, the time for transition from OFF to ON of the contactor is specified as 22ms max. Due to inrush, the current will be many times larger during first few AC cycles. This is measured using an oscilloscope, and it is noticed that the inrush dies down in 5 cycles max. Considering time for field driver relay, an ON duty of 120ms is chosen. The datasheet time for transition from ON to OFF of the contactor is 19ms max. The OFF duty of 180ms is chosen considering the ability of the load bank to remove heat generated by heavy inrush current.

The health of the contactors is continuously monitored using an auxiliary contact attached with the contactor. These contacts are mechanically linked to the main contacts and can be reliably used to infer main contactor status (verified by breaking the casing). Feedback from auxiliary contact should arrive within 50ms from the instant ON command is issued (including the time consumed by field driver relay). Similarly, feedback from auxiliary contactor should arrive within 50ms from the instant OFF command is issued. The entire process of cycling and health monitoring is automated using a PLC. Moreover, manual indication for ON/OFF status of the contactor is also provided by lamp through redundant auxiliary contacts. The ON/OFF status of the load is also indicated using lamps.

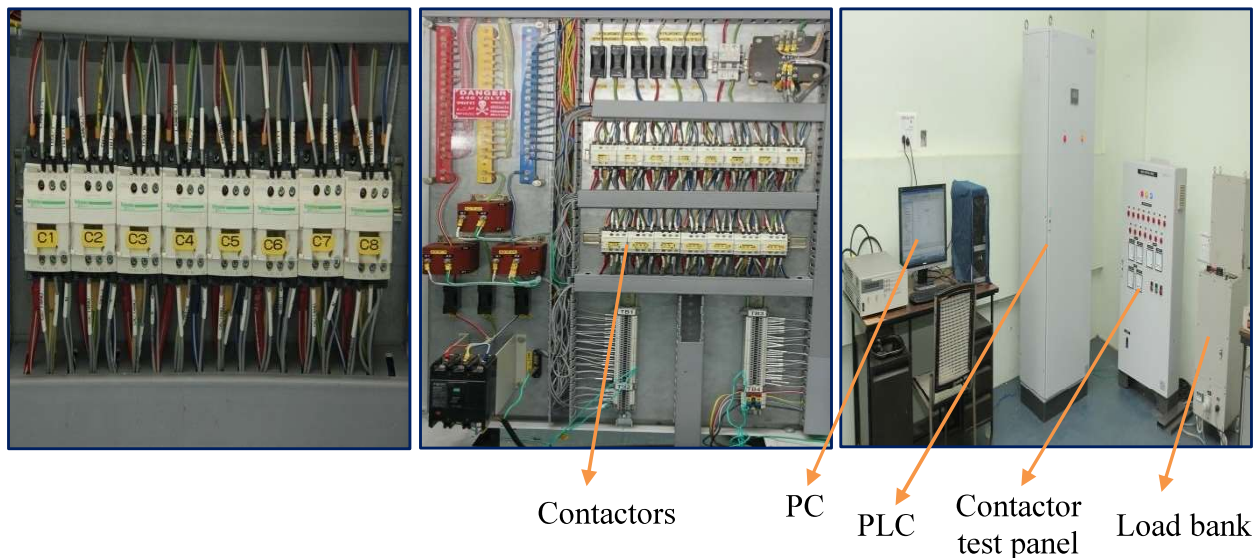


Figure 5.2: Experimental setup.

It is assumed that the number of cycles is the only possible mechanism for damage accumulation and life consumption. Since the degradation mechanisms are vital when current is actively passing through contacts, it is assumed that test time between the cycles has no effect on the estimation. Field conditions will see more resting time and the influence of rest time on the failure mechanism, if any, will only lead to conservative results.

### **5.3.2 Test results**

Testing is done as per test plan for 44,28,573 cycles using 10 specimen contactors and fail-to-open mode failures are not observed under the influence of cyclic stress. Hence, it can be concluded that the contactor true MTBF is equal to the lower test MTBF with a risk of 9.9%. So, the component can be accepted. However, contactors welding due to other stresses like temperature, humidity etc., are not taken account in this test.

## **5.4 Failure Analysis**

Due to the limitations in the assumptions made in the RDT and considering the importance of “weld failure”, failure analysis of the field driver relay and EM contactors is performed using Scanning Electron Microscopy (SEM) and Energy Dispersive Spectroscopy (EDS) (SEM, FEI Inspect F50, Cold FEG).

### **5.4.1 Field driver relay**

Arcing event will change the structure of the contact surfaces. The arc melts the contact surface and when the surface solidifies, its composition will change. There are many possible interactions between the arc, the contact surface and the constituents of the air. Hot contact surface and the air will form oxides, nitrides and carbonates. If the air has industrial pollution such as SO<sub>2</sub>, H<sub>2</sub>O, chlorine compounds and dust, it is possible to form sulfides and chlorides. The possible interactions of arc with contact surface is shown in Figure 5.3.

During the test, one field driver relay has failed (safe mode) at 65,00,000 cycles and is replaced with a new one. Secondary electron micrograph of the failed relay sample is given in Figure 5.4(a). Magnified image is shown in Figure 5.4(b). Micrographs show two contrast regions such as dark and bright. This is due to the formation of the corrosion products on the surface.

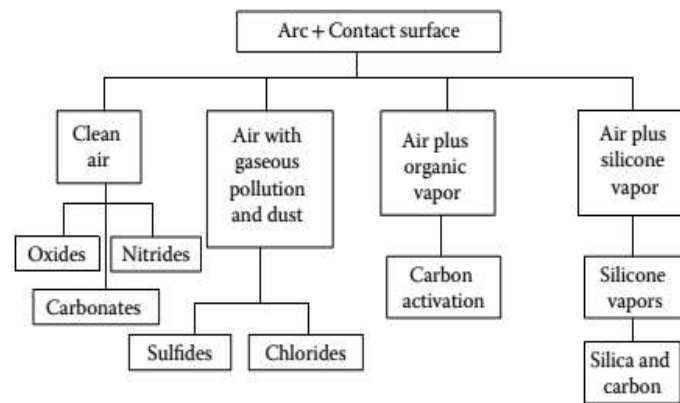


Figure 5.3: Possible interactions of electric contacts and the ambient air during arcing [53]

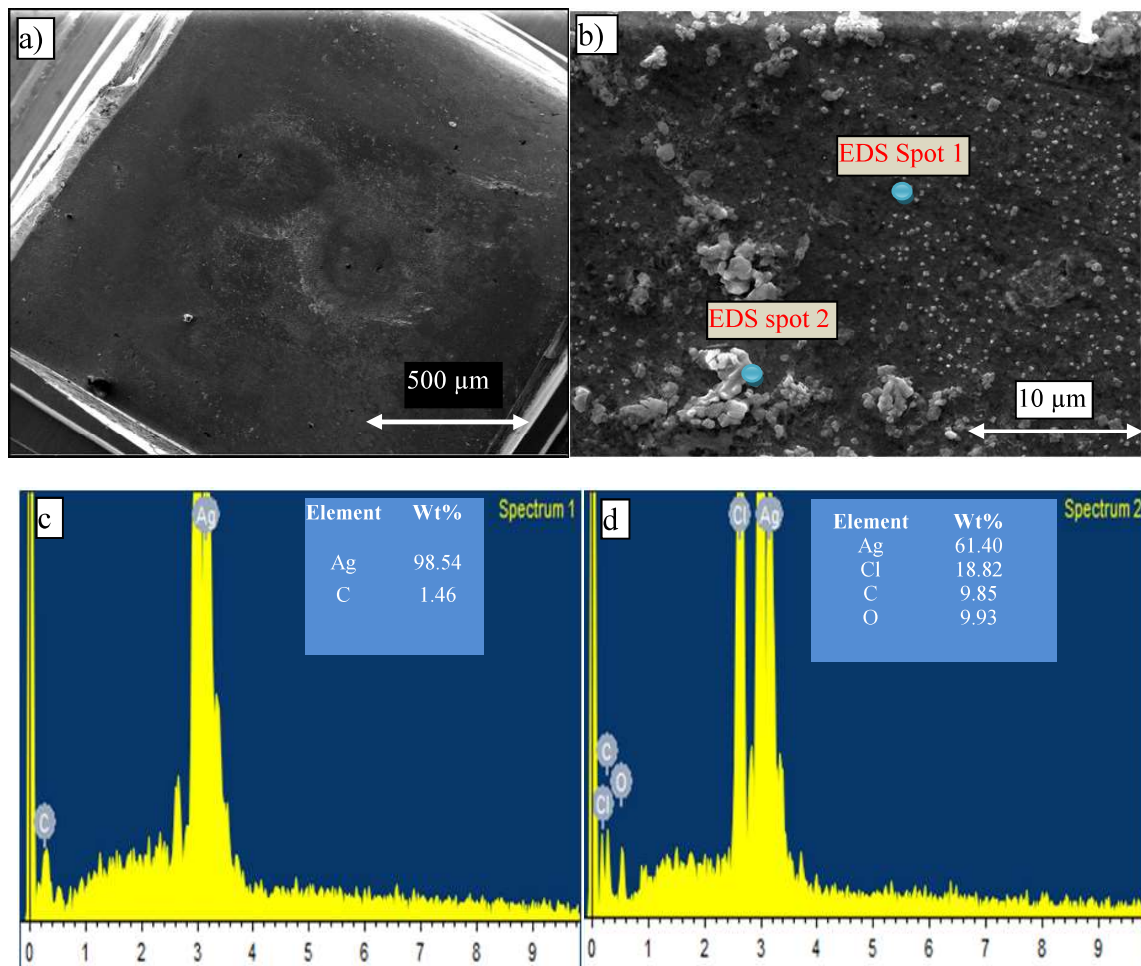


Figure 5.4: Failure analysis: (a-b) SEM images of failed relay; (c-d) EDS spectrum with elemental composition of failed relay with their weight percentages in dark and bright region.

EDS analysis is performed in dark and bright regions of Figure 5.4(b) and spectrum with weight percentages are shown in Figure 5.4(c) and 5.4(d) respectively. Dark region shows the matrix composition of contacts (Ag-98.54%). Bright region shows the presence of the corrosion products (Cl, C and O) along with reduced percentage of Ag. These corrosion products can form AgCl and Ag<sub>2</sub>O on the surface. AgCl is the common corrosion product leading to failure of relay [53]. The presence of these corrosion products may increase the contact resistance, which ultimately leads to weld failure of the relay.

#### 5.4.2 EM Contactors

After the reliability demonstration testing, there were no failures in unsafe mode. The testing was further continued for two specimens envisaging failures. Contactor-1 ( $C_1$ ) is tested up to 11,01,047 cycles without failure. Contactor-2 ( $C_2$ ) has failed at 29,07,327 cycles in safe mode.

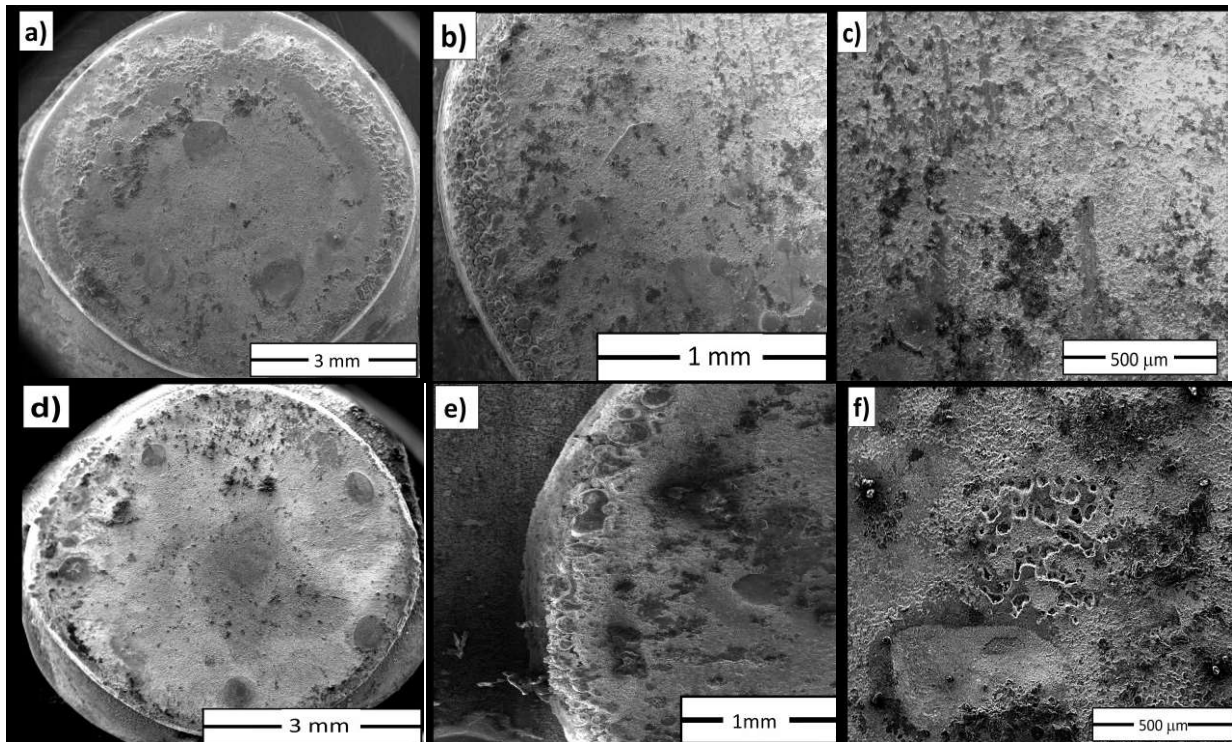


Figure 5.5: Surface morphology: (a-c) Deformation on  $C_1$  contact; (d-f) Deformation on  $C_2$  contact.

SEM and EDS has been performed to understand the morphological and chemical composition changes of contacts after different number of cycles. Figure 5.5(a-c) shows the degradation on C<sub>1</sub> contact and Figure 5.5(d-f) shows that on C<sub>2</sub> contact. It can be seen from SEM images that degradation is apparent on the surface of the contacts with formation of pips and craters due to changes in mechanical and electrical parameters. Figure 5.5(a) and 5.5(d) shows that deformation is more on boundary of the contact and the magnified images of the contacts are shown in Figure 5.5(b-c) and (e-f). From the morphology of the contacts it can be seen that C<sub>2</sub> has undergone more deformation compared to C<sub>1</sub> and the precipitates are formed irregularly. The formation of these precipitates is probably due to arcing of the contacts.

Ni (10-40%) is usually added to Ag to improve the hardness allowing the contact to retain good mechanical properties after undergoing an electrical arc (welding resistance). The high electrical conductivity of the material and easy handling makes it ideal for intense applications. This added nickel might melt during the arcing and form precipitates at the surface which ultimately changes the morphology. This reduces the effective contact area and decreases the conduction with increasing number of cycles.

Further, EDS analysis of contacts with different number of cycles was carried out and EDS spectrum is shown in Figure 5.6 and 5.7. Analysis shows that Ni content in precipitates is found to be growing with increase in number of cycles as shown in wt% table. It is also found that density of precipitates is more with higher number of cycles. Along with Ni, considerable amount of oxygen and carbon elements (corrosion products) also exist in the surface. As per Slade [53], electrically insulating films stem from the formation of oxide or corrosion products. These films are mechanically brittle. However, nickel oxide is more difficult to fracture because it is mechanically stiffer than other contact materials. Electrical contact is established only after

the films are fractured and metal-to-metal contact spots are formed. In these conditions, constriction resistance is determined by fracture mode of insulating corrosion products.

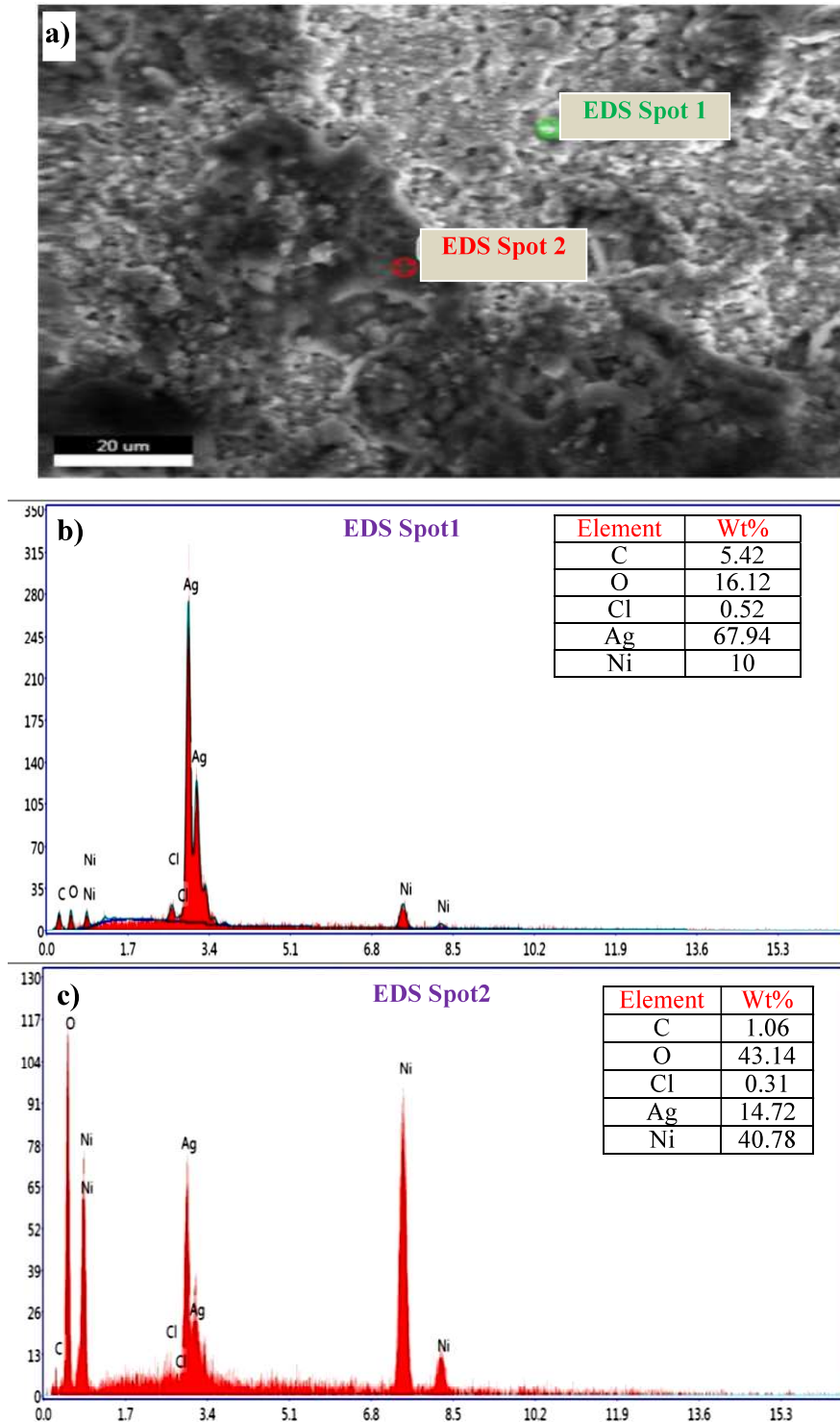


Figure 5.6: EDS (a) Spots on  $C_1$  contact; (b-c) Spectrum on  $C_1$  with wt%.



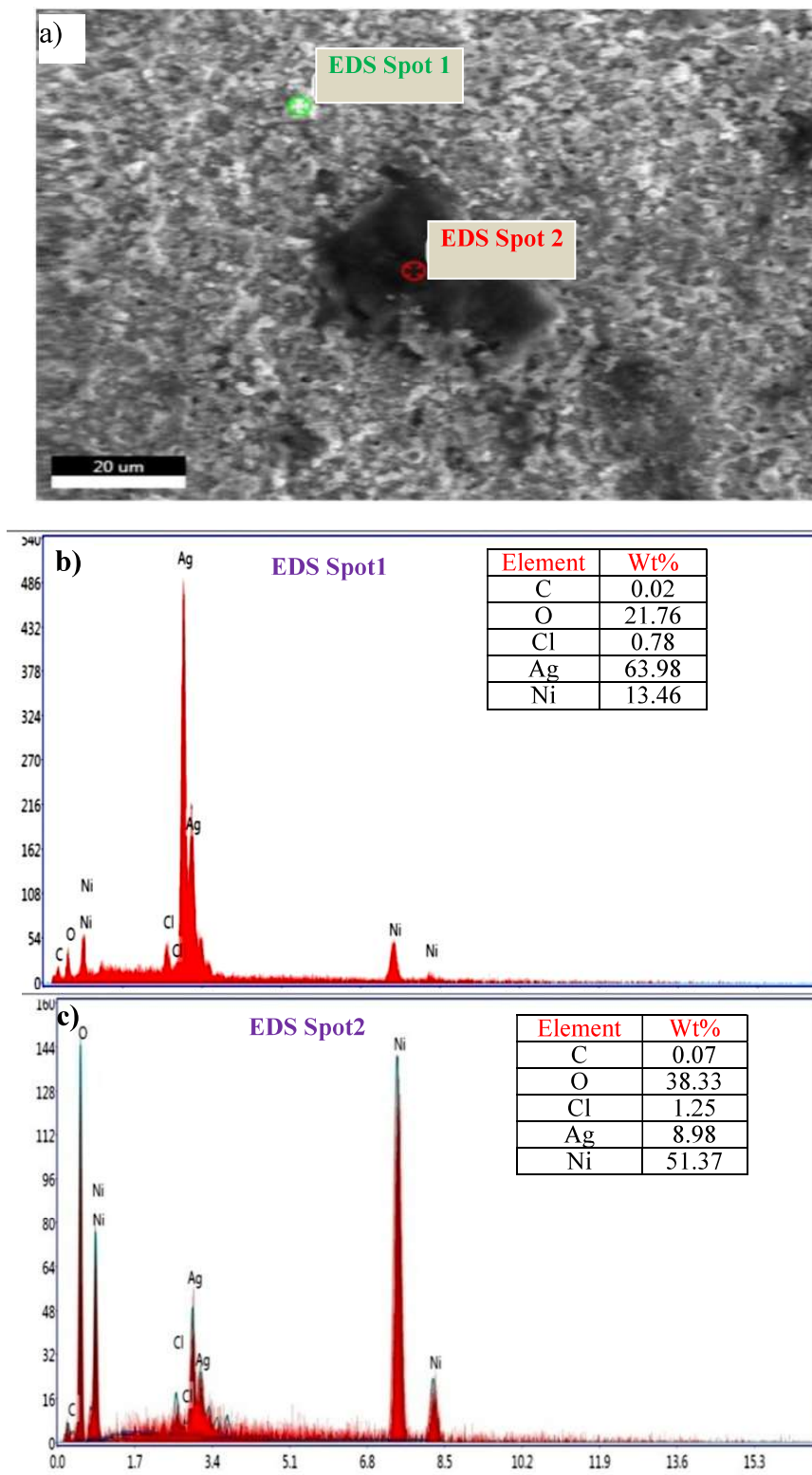


Figure 5.7: EDS (a) Spots on  $C_2$  contact; (b-c) Spectrum on  $C_2$  with wt%.



## **5.5 Summary**

- Reliability demonstration test of sufficiently de-rated contactors has shown that failure probability of fail-to-open mode is less under the influence of cyclic stress.
- SEM and EDS images of contacts depict surface morphology degradation with the formation of Ni precipitates due to arcing. Ni precipitates is found to be growing with the increasing number of cycles. This may decrease the effective contact area and conductivity which may ultimately lead to failure of the contactors. However, contactor fail-to-open is not noticed probably due to higher rating of contactor when compared to field condition.
- From the instrumentation provisions and EM contactor studies, it can be concluded that the chance of uncontrolled withdrawal of control rod in Prototype Fast Breeder Reactor is remote.

# 6

## INHERENT FAIL-SAFE CIRCUITS TO IMPROVE FAIL-SAFE DESIGN

---

*In this chapter, an inherently fail-safe electronic logic circuit is proposed. Further, the logic is investigated for safety grade decay heat removal system damper control logic of PFBR with a very low unsafe failure probability requirement. The inherently fail-safe electronic logic circuit consists of pulse generators, combinational logic (AND/OR) and driver. Failure mode effect analysis presented here shows that all the perceivable failure modes are fail-safe. Quantification of  $PFD_{Avg}$  for this design is also presented in this chapter. A very low  $PFD_{Avg}$  is achieved since the system fails in unsafe mode only upon combination of multiple failures.*

---

### 6.1 Inherent Fail-safe Design: An approach to Probability of Failure on Demand

The nuclear industry has seen a slow transition from relay based logics to solid state electronics and then computer based logic execution [2]. However, relay logics are still in use for important safety applications like the execution of voting logic in shutdown systems and actuation of final control elements in decay heat removal systems [95]–[97]. Relay logics are desired for their very low failure probability in unsafe mode (stuck close) (19% as per RAC FMD-91) [92], immunity to EMI/EMC disturbances and a very rich industrial experience. However, they are not amenable for built in self testing, and only a periodic black-box type testing is done as part of surveillance.

When solid state electronics is employed for such applications, they are designed with continuous online self-diagnostics and a provision to drive final control elements to the fail-safe state to achieve the desired level of unsafe failure probability. In solid state electronics, time delays are much shorter than conventional systems employing relays.

Fail-safe is one of the important design attribute that causes the SIS to go to a predetermined safe state in the event of specific failure. Nuclear Power Plant (NPP) reliability requirements can only be achieved with a fail-safe design. Inherent fail-safe circuits do not require diagnostics since any of the failures in the circuit will automatically lead to a safe state of the final control element. These circuits will have a lower unsafe failure probability since the periodicity of self-test is tending to zero and the issues arising out of failures in diagnostic circuitry does not exist.

Practices of inherent safety have also been developed in the chemical industry. These designs will eliminate adverse events even though their probabilities are small. Some of the factors considered in inherent safety designs are higher loads than those foreseen, worse properties of materials, imperfect theory of the failure mechanism and possibly unknown failure mechanism and human error [98]. Kletz [99] gives a brief summary of major accidents such as Bhopal, Chernobyl and Spads etc. It says that inherent safer designs are not easily adopted as other process safety features. Srinivasan et al., [100] has reviewed progress in inherent safety and basic concepts and its incorporation into regulation and accident investigation are introduced.

A comparison of the  $PFD_{Avg}$  between relay logic, solid state electronics with diagnostics and inherent fail-safe design is shown in Table 6.1. From this, it can be seen that relay logic relies on the low unsafe mode failure of EM relays (contacts weld), whereas  $PFD_{Avg}$  is reduced in solid state electronics by incorporating periodic testing. This helps in detection of dangerous

failures.  $PFD_{Avg}$  can also be reduced with inherent fail-safe logic by designing a circuit with  $\lambda_{DNI}$  as minimal as possible. Option-3 has the potential to deliver very low  $PFD_{Avg}$  compared to option-2 since periodicity of self test is tending to zero and the issues arising out of failures in diagnostic circuitry does not exist. However, option-2 is ubiquitous in NPP safety systems since it is not easy to design complex systems with very low  $\lambda_{DNI}$ .

The general industry trend is moving towards FPGA/CLPD based designs and option-2 is the natural choice for performing self-diagnostics. However, for nuclear industry with emphasis on very low PFD and simplicity in specific applications, option-3 can be considered in this study.

Table 6.1: Comparison of logics with unsafe failure probability.

Option	Logic	$PFD_{Avg}$	Explanation
1	Relay	$\lambda_D \left( \frac{\tau}{2} + MRT \right)$	$\lambda_D$ is small for relays.
2	Solid state electronics	$(\lambda_{DU} + \lambda_{DD}) \left[ \frac{\lambda_{DU}}{\lambda_D} \left( \frac{\tau}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right]$	$\lambda_{DU}$ is minimized by improved diagnostic coverage.
3	Inherent fail-safe	$\lambda_{DNI} \left( \frac{\tau}{2} + MRT \right)$	$\lambda_{DNI}$ has to be shown to approach zero

In inherent fail-safe designs, the improved reliability comes with increased spurious actions. Moreover, it has to be proved that circuit is fail-safe under all permissible failure cases. A novel inherently fail-safe electronic logic circuit is proposed as part of this study.

## 6.2 Fail-safe AND Gate

Conventional commercially available AND gate is not fail-safe because a short circuit in a transistor produce output without input signals and this is a very dangerous condition.

Businaro et al., [101] and Tsunoda et al., [102] presents various fail-safe logic blocks for safety systems. Fail-safe performance is achieved by converting clock pulse to high frequency oscillation and reshaping back to pulse in every stage. A high frequency pulse (in MHz) will be generated during ON pulse duration. However, the AND logic is not completely fail-safe.

A perfect fail-safe AND logic gate is proposed in this chapter and it is designed with continuous pulse input (KHz). Pulse with  $T_{ON}$  of  $50\mu s$  and  $T_{OFF}$  of  $150\mu s$  is chosen. A fail-safe AND gate should prevent transmission of pulses to downstream stages when anyone of the input is not pulse, even under one or more of its input stuck at LOW/HIGH/OPEN and under the failure of its internal components. This cannot be achieved using commercially available gates.

Figure 6.1 depicts fail-safe design of 2-input AND gate. The basic idea is that energy is extracted from first input (A) pulses through a pulse transformer and stored as DC in a capacitor (C). This, in turn, provides required current for the second input (B) pulses to get transmitted further. A pulse transformer  $PT_1$  with VT product of  $50V\cdot\mu s$  ( $5V \times 10\mu s$ ) and  $PT_2$  with VT product of  $250V\cdot\mu s$  ( $5V \times 50\mu s$ ) is chosen in AND stage. This variation in VT product is chosen to achieve fail-safe features during some of the failure modes. Truth table of AND logic is verified with this design and results are shown in Figure 6.1(b-c).

A stuck at HIGH in A will not pass through the pulse transformer ( $PT_1$ ) because of absence of pulses which gives a zero at AND output, whereas a stuck at HIGH in B will only switch a DC and hence does not pass through the pulse transformer ( $PT_2$ ), gives a zero at output. During the open mode of failure of C,  $PT_1$  output is fed  $PT_2$ . AND output (Y) is  $10\mu s$  ON (as against  $50\mu s$  when normal), which is a very low short duration pulse. All other failures like transistor short and open are automatically taken care by  $PT_1$  and  $PT_2$ . Failures (like timer resistor or timer

diode failures) which lead change in to pulse duty cycle are seized by pulse transformers with appropriate VT product.

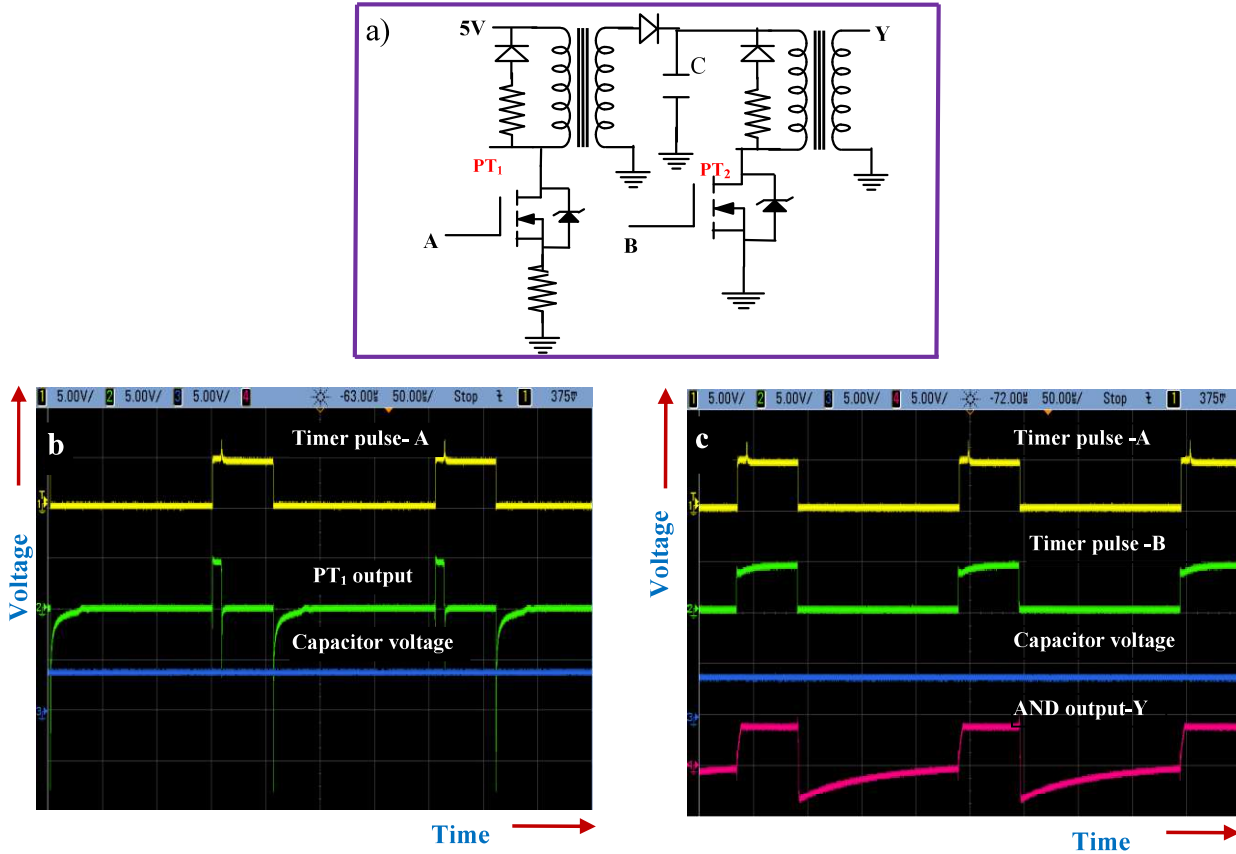


Figure 6.1: Fail-safe AND gate (a) Design; (b) Pulse input, pulse transformer output and capacitor voltage waveforms; (c) Pulse inputs, capacitor voltage and AND output waveforms.

### 6.3 Inherently Fail-safe Pulsating Logic Design for PFBR Safety Grade

#### Decay Heat Removal Circuit

In Safety Grade Decay Heat Removal (SGDHR) system, heat will be dissipated to the atmosphere through sodium to air exchangers (AHX). To achieve very high reliability, the sodium flow in the SGDHR loop and air flow through AHX is by natural circulation. Dampers are provided to control air flow through AHX to control the heat removal from the reactor core as shown in Figure 2.15.

Both inlet and outlet air flow path have two dampers, each controlling one half of the available flow area. One damper is pneumatically driven and the other damper is electrically driven (motor operated). This arrangement is provided for diversity in design. The pneumatic damper is controlled using a set of solenoid valves. Both the damper systems deploy relay logic to control opening and closing of dampers. Solid state electronics was not preferred due to unsafe mode failure.

The control logic for pneumatic dampers receives seven digital inputs and drives six solenoid valves. The equivalent combinational logic circuit is shown in Figure 6.2. In Figure 6.2,  $I_1$  to  $I_7$  are digital inputs;  $V_1$  to  $V_6$  are solenoid valves;  $V_3$  and  $V_4$  de-energization ensures opening of dampers. Without having control of all other valves, the opening of valves  $V_3$  and  $V_4$  will drive the dampers to open fully. Thus, de-energization of valves  $V_3$  and  $V_4$  are crucial in ensuring fail-safe operation of the dampers. In this case study, relay control logic is implemented with pulse circuit and inherently fail-safe AND gate. This solution also serves the purpose of diversity in control logic with same/equal unsafe failure probability for future fast breeder reactor designs.

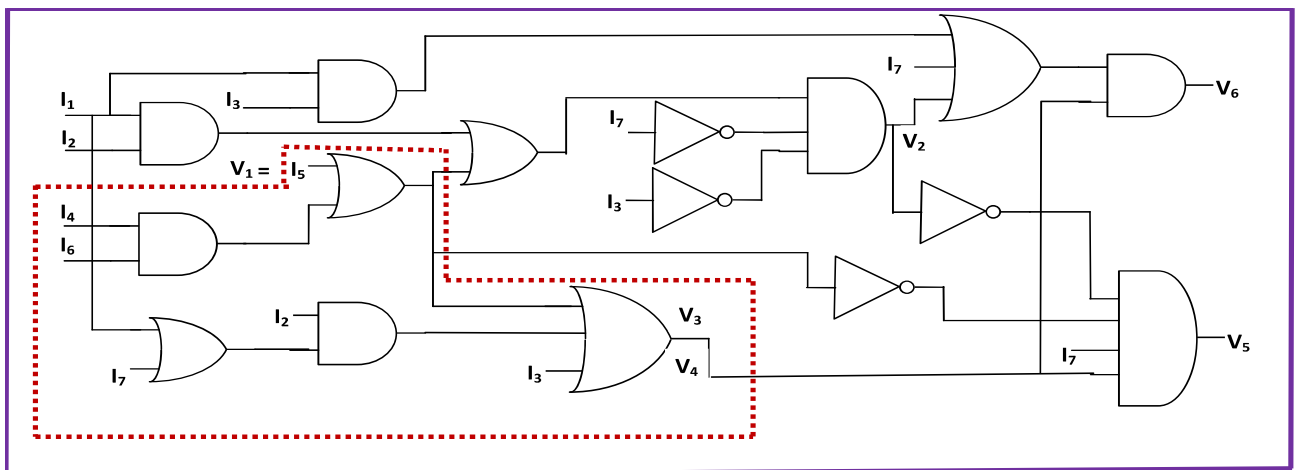


Figure 6.2: Logic circuit to drive solenoid valves.

The inherent fail-safe design is achieved by processing the inputs in terms of synchronized pulses rather than static digital levels. Pulse transformers are used at specific locations in the circuit, so that energy transition to subsequent stages is seized in case of a failure in the previous stage. Such pulse processing is selectively applied only to those parts of the circuit for which fail-safe behavior of final control elements is expected. The proposed method, with due modifications, can be extended to similar industrial control involving combinational circuits.

### 6.3.1 Inherently fail-safe pulsating logic design

A fail-safe valve driver circuit for controlling valve energization and de-energization comprising of pulse generators, combinational logic and driver circuit is shown in Figure 6.3. The idea is to generate synchronized pulses from static digital inputs, perform AND, OR operations on pulses and charging the capacitor to the holding voltage of solenoid valves.

#### 6.3.1.1 Pulse generator

Each digital input from the field has a corresponding pulse generator with a common charging and discharging circuit. The pulse generator generates 5V rectangular pulses at its output. Based on remote switch position ( $SW_1$ - $SW_7$  in the field) output of pulse generators are connected to further stages. Pulses from pulse generators have to be time synchronized, for correct truth table execution. The frequency and duty cycle of rectangular pulses have to be chosen in line with the Voltage-Time (VT) product of pulse transformers and the charging/discharging capacities used in subsequent stages.

Pulse circuit has been built with conventional 555 timers in astable multivibrator mode. Pulses are fed to next stage in control with remote switches ( $SW_1$ - $SW_7$ ). The multivibrators share a common charging and discharging circuit as shown in Figure 6.3 for time synchronization. Timer output pulse with  $T_{ON}$  of  $50\mu s$  and  $T_{OFF}$  of  $150\mu s$  is chosen to match pulse transformer VT



product. Pulse transformers allow the pulses and blocks DC.

Minor trigger voltage variations in 555 timers can drive the multivibrators out of synchronization. Hence, a low magnitude inductor (L) in series with the charging path is used. L will not allow sudden changes in current direction and this time gap allows all timers to come into trigger level during a charging cycle.

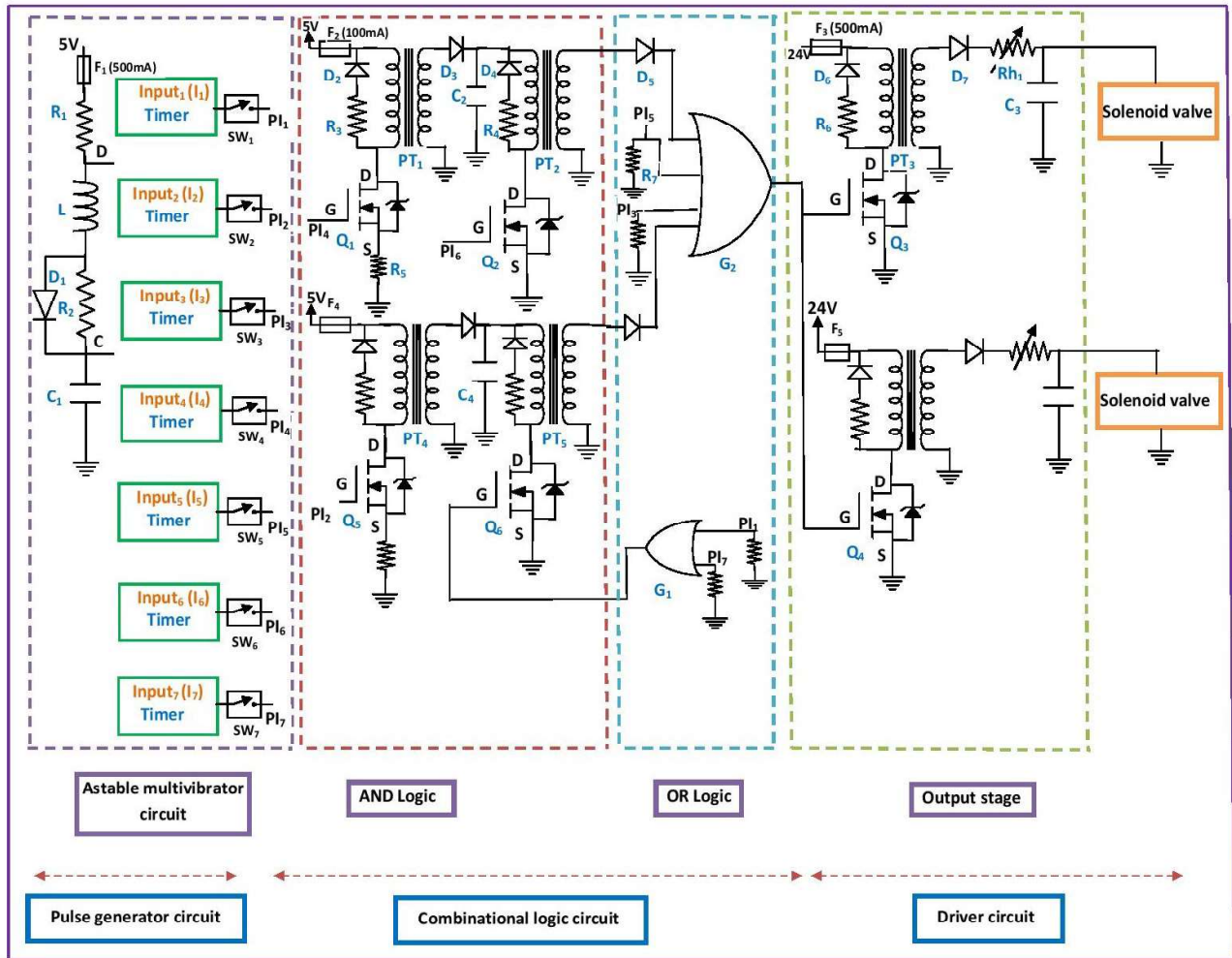


Figure 6.3: Schematic of fail-safe pulsing circuitry for controlling  $V_3$  and  $V_4$  valves.

### 6.3.1.2 Combinational logic circuit

In this stage is AND, OR operations are performed on timer pulses as shown in Figure 6.3.

### 1. Fail-safe AND gate

A 2-input fail-safe AND gate is described in section 6.2, takes the pulse from pulse generator and drives the next stage. During the open mode of failure of  $C_2$  AND gate output is 10 $\mu$ s ON (as against 50 $\mu$ s when normal), which is not sufficient to charge a 24V capacitor ( $C_3$  in Figure 6.3).

### 2. OR gate

A fail-safe OR gate should not produce pulses at the output when none of its input receive pulses. Thus, fail-safe is achieved inherently by pulse logic execution and no special OR gate circuitry is required. Hence, commercially available OR gate is used. A logic family which treats any OPEN input as LOW is preferable so as to accommodate signals which are directly connected to OR gate. Alternatively a pull down resistor can be connected to input pins when a logic family which treats any OPEN input as HIGH is used. Pull down resistor SHORT or OPEN does not affect safety, since in both cases output is static and hence cannot pass through subsequent stage.

### 3. Valve driver stage

An output driver stage is required to meet the higher current requirements of a DC solenoid valve. The pulse transformer with a current capacity of  $\sim 1$ A is chosen for the purpose. Power MOSFET is used to convert 5V pulse trains into 24V pulse train. The charging capacitor ( $C_3$ ) delivers the required DC to the solenoid valve. Output transistor short or open will lead to de-energization of solenoid valves. Pulse transformer of 1200V- $\mu$ s ( $24\text{V} \times 50\mu\text{s}$ ) is used at driver stage. Initial inrush in charging the capacitor ( $C_3$ ) is limited with a variable resistor ( $R_{h1}$ ), and it is adjusted manually to reach the required capacitor voltage during startup. Thereafter it remains in the same position throughout the steady state operation.

### 6.3.2 Experimental Verification

The fail-safe circuit shown in Figure 6.3 is designed on PCB to verify that it is possible to energize the valve with pulsating logic. Prototype board and experimental setup are shown in Figure 6.4.

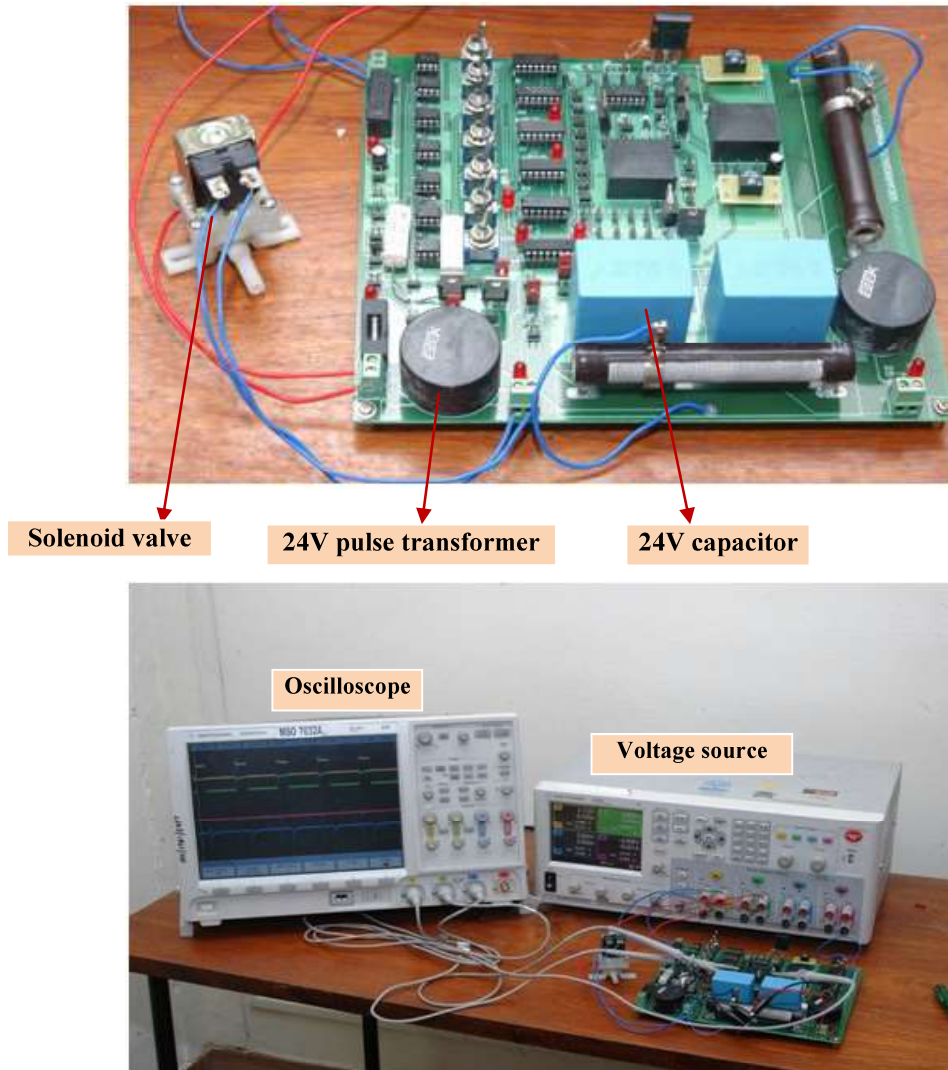


Figure 6.4: Experimental setup.

### 6.3.3 Results

Synchronized output pulses are shown in Figure 6.5(a). Figure 6.5(b) shows the output waveforms of pulse transformers corresponding to  $PI_4$  and  $PI_6$  with respect to pulse input. OR

gate output is shown in Figure 6.5(c). The Figure 6.5(d) depicts the output of pulse transformer and output capacitor voltage which holds the solenoid valve in energized condition. Voltage of capacitor is shown as 15V, which keeps the solenoid valve in energized, the holding voltage of solenoid being  $\sim 13V$ .

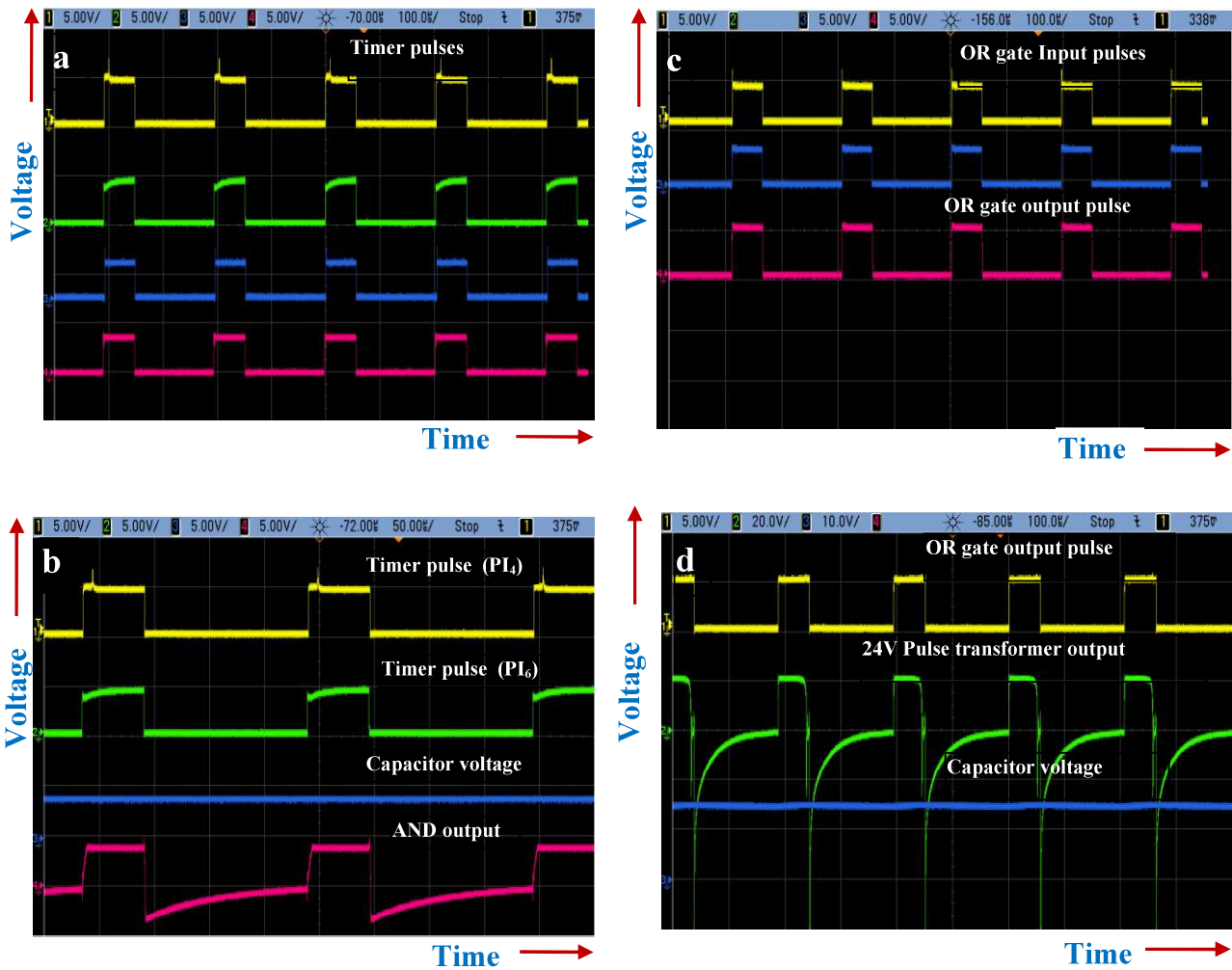


Figure 6.5: During healthy operation outputs waveforms at different stages (a)Timer synchronization pulses; (b)AND gate output; (c)OR gate output; (d)24V pulse transformer output, 24V capacitor voltage output.

#### 6.3.4 Failure mode effect analysis verification

A test circuit has been designed to implement inherent fail-safe circuit as shown in Figure 6.3 with sufficient provision of jumpers to simulate the failure of every component such as stuck high/low and open/short. Detailed failure mode effect analysis listed in Table 6.2 is carried out by considering the different modes as in [92]. Graphs captured upon failure simulations are selectively shown and referred in Table 6.2. To handle failures leading to over current, the verification is done with an upper current limit on the power source. Protective fuse is blown wherever this limit is observed. From the FMEA table it can be inferred as all perceivable failure modes are shown to result in fail- safe state, the proposed circuitry can be used as a diverse method for damper control in PFBR system.

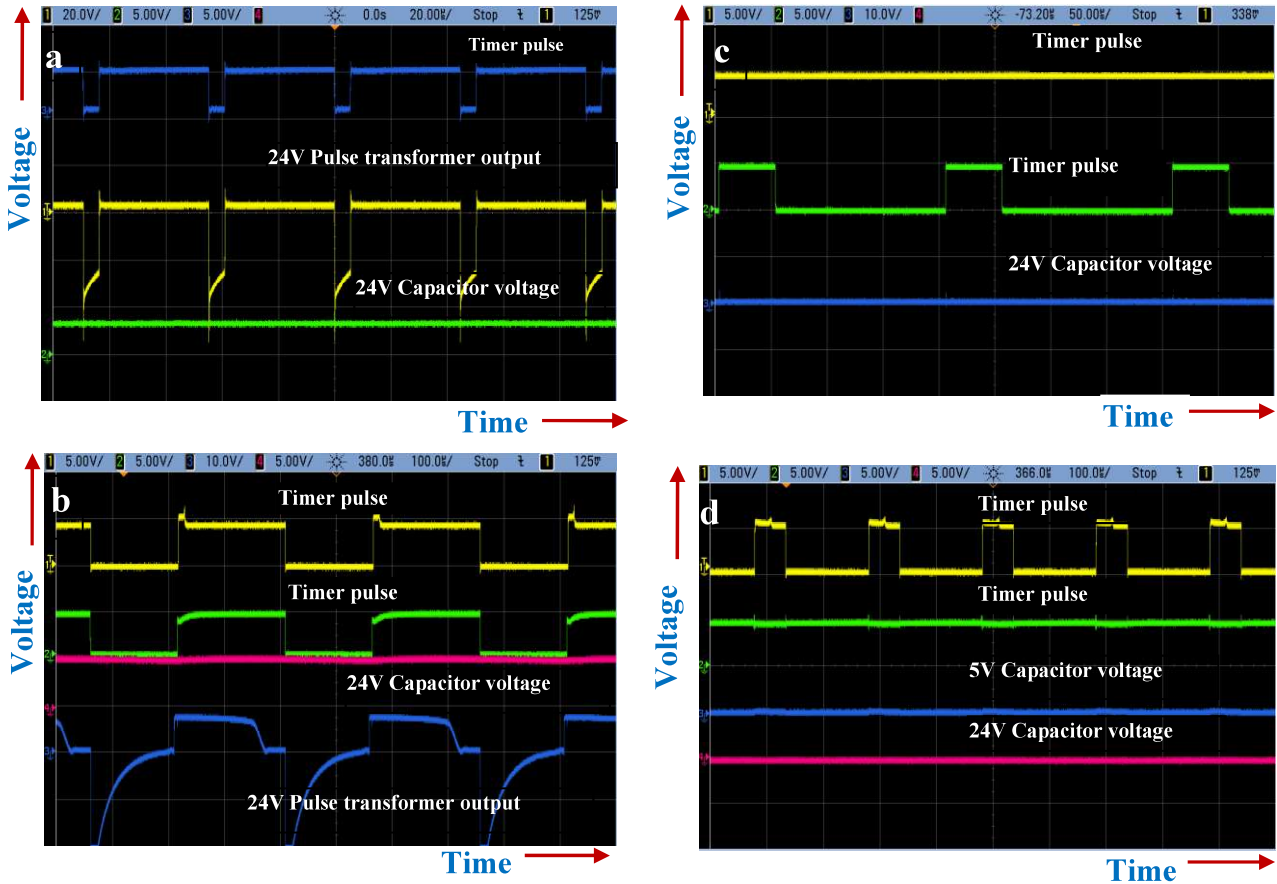


Figure 6.6: Failure mode effect analysis results.



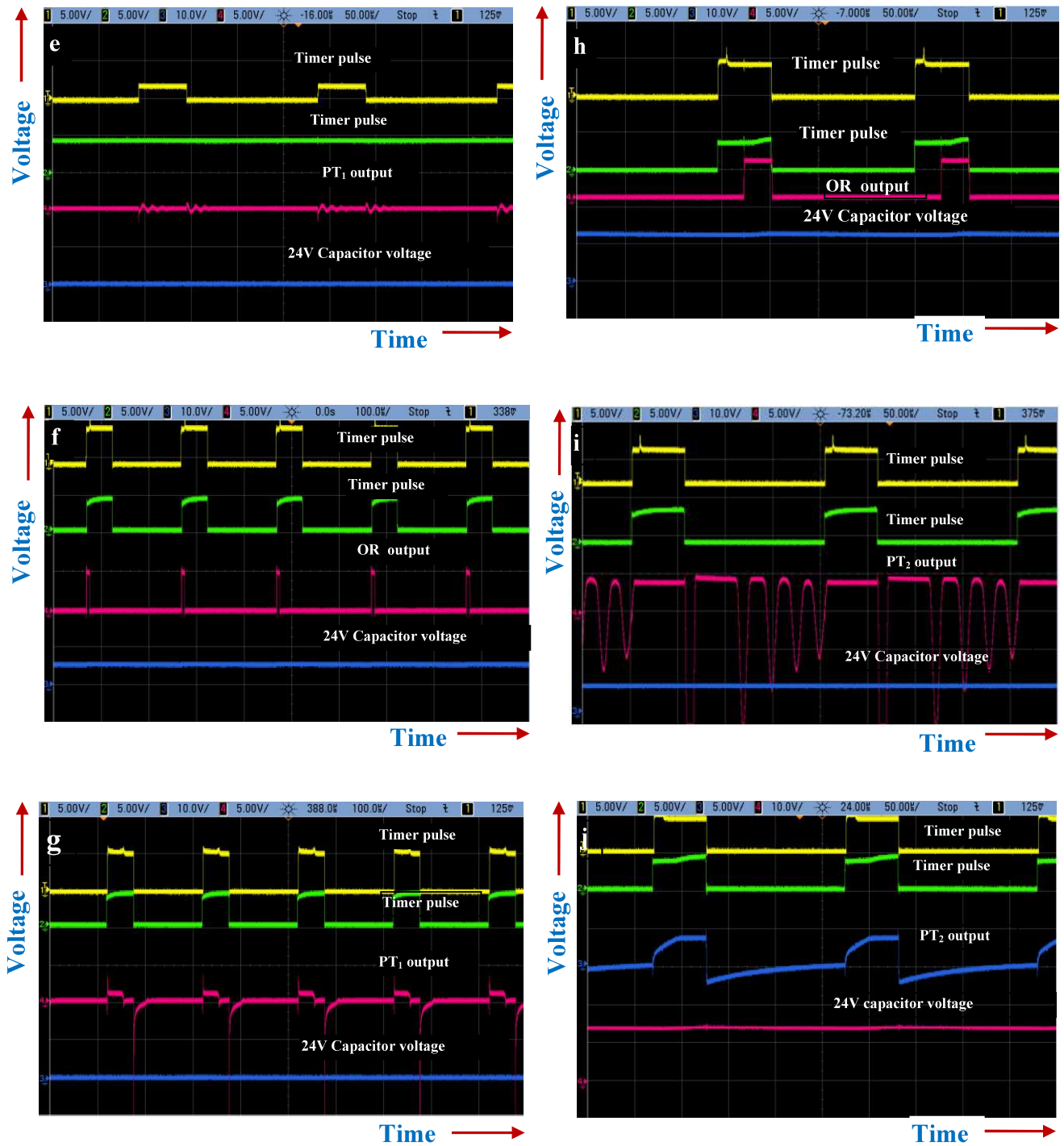


Figure 6.7: Failure mode effect analysis results.

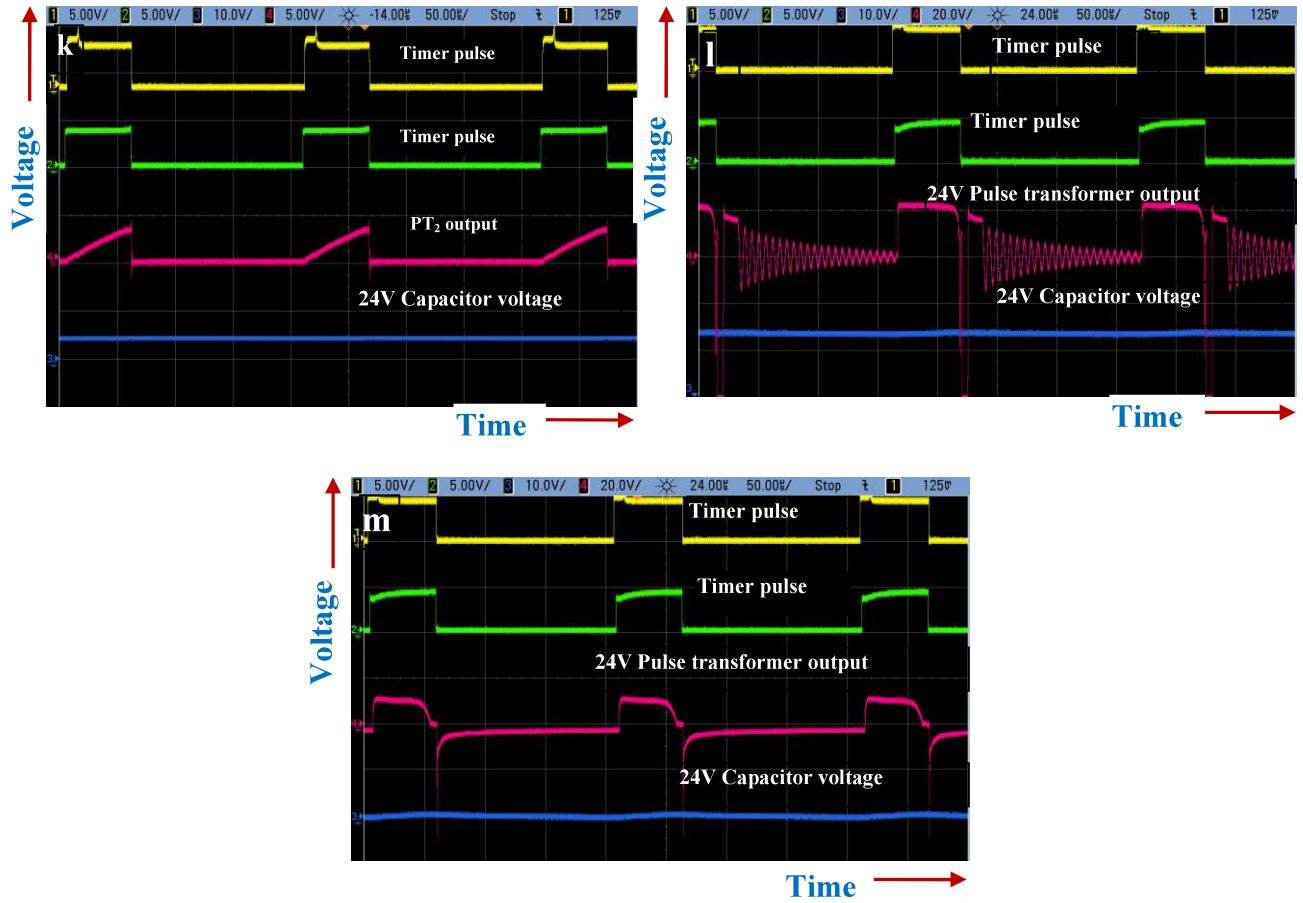


Figure 6.8: Failure mode effect analysis results.

- (a) Timer discharging resistor ( $R_2$ ) short; (b) Timer diode ( $D_1$ ) open; (c)  $PI_4$  stuck at high; (d)  $PI_6$  stuck at high; (e) MOSFET ( $Q_1$ ) Gate to Source short; (f) Capacitor ( $C_2$ ) open; (g) Capacitor ( $C_2$ ) short; (h) Rectifying diode ( $D_5$ ) short; (i) Freewheeling diode ( $D_4$ ) open; (j) Freewheeling diode ( $D_4$ ) short; (k) Freewheeling diode resistor ( $R_4$ ) short; (l) Freewheeling diode ( $D_6$ ) open; (m) Rectifying diode ( $D_7$ ) short.

Table 6.2: Failure mode effect analysis.

	Component	Failure mode	Effect	Consequence
<b>T I M E R</b>	Capacitor (C <sub>1</sub> )	Short	Timer output is LOW.	De-energization of solenoid valves takes place due to absences of pulses.*
		Open		
	Resistor (R <sub>1</sub> )	Short	Timer output is LOW.	De-energization of solenoid valves takes place due to absences of pulses.*
		Open	Timer output is HIGH.	
	Resistor (R <sub>2</sub> )	Short	Duty Cycle approaching 1. Pulse transformers are unable to follow the pulse. Results are in Figure 6.6(a).	De-energization of solenoid valves takes place because of insufficient capacitor voltage.*
		Open	Duty cycle is approaching to 0.	De-energization of solenoid valves takes place due to absences of pulses.*
	Diode (D <sub>1</sub> )	Short	Same as R <sub>2</sub> short.	De-energization of solenoid valves takes place because of insufficient capacitor voltage. *
		Open	Increase in timer pulse duty cycle. Pulse transformers are unable to follow the pulse. Results are in Figure 6.6(b).	
	Inductor (L)	Open	Output of timers is HIGH.	De-energization of solenoid valves will not takes place until one of the input to OR gate (G <sub>2</sub> ) is high. *
		Short	Loss in pulse synchronization between timers.	
<b>A N D</b>	Timer-4 (Timer output connected to Q <sub>1</sub> Gate)	Stuck at LOW	Output of PT <sub>2</sub> is LOW.	De-energization of solenoid valves takes place if all the inputs to G <sub>2</sub> are low. **
		Stuck at HIGH	Output of PT <sub>2</sub> is LOW. Output of PT <sub>2</sub> is LOW. Results are in Figure 6.6(c) when current limiting is enforced in power source. In the absence of current limiting, fuse (F <sub>2</sub> ) will blow.	
	Timer-6(Output	Stuck at LOW	Output of PT <sub>2</sub> is LOW.	De-energization of solenoid valves takes place if all the



	Component	Failure mode	Effect	Consequence
	connected to Q <sub>2</sub> Gate)	Stuck at HIGH	Capacitor (C <sub>4</sub> ) is overloaded; it's not able to charge to 5V. Output of PT <sub>2</sub> is LOW. Results are in Figure 6.6(d).	inputs to G <sub>2</sub> are low. **
	Timer-3 (Timer output connected to G <sub>2</sub> )	Stuck at LOW	Output of G <sub>2</sub> depends on other inputs.	De-energization of solenoid valves takes place if all the inputs to G <sub>2</sub> are low. **.
		Stuck at HIGH.	Output of G <sub>2</sub> is HIGH.	De-energization of solenoid valves takes place.
	MOSFET (Q <sub>1</sub> )	Gate/Source open	Output of PT <sub>1</sub> is LOW.	De-energization of solenoid valves takes place if other inputs to G <sub>2</sub> are low. **
		Gate to source short	It leads to the reduction in voltage level of timer pulse driving Q <sub>1</sub> due to overloading which in turn causes loss in pulse synchronization between timers. Results are in Figure 6.6(e). This failure will cause 5V fuse to blow.	Absence of pulses is causing valve de-energization.
		Drain to source short	This failure draws extra current. Circuit can be protected by having internal fuse. Internal fuse (F <sub>2</sub> ) in AND stage will blow.	De-energization of solenoid valves takes place if all the inputs to G <sub>2</sub> are low. **.
	MOSFET source to ground resistance (R <sub>5</sub> )	Open	MOSFET remains in OFF state. Output of PT <sub>2</sub> is LOW.	De-energization of solenoid valves takes place if all the inputs to G <sub>2</sub> are low. **.
		Short	It will follow the expected results except that an extra current drawn. Internal fuse in AND stage (F <sub>2</sub> ) will blow.	
	Pulse transformer freewheeling	Open	This failure over the time may cause damage to MOSFET due to kick back voltage.	This failure does not cause any change in functionality.

	Component	Failure mode	Effect	Consequence
	diode ( $D_2$ )	Short	This failure does not affect the circuit due to freewheeling diode resistance ( $400\Omega$ ) in series except that an extra working current drawn.	
	Pulse transformer freewheeling diode resistor ( $R_3$ )	Open	Same as $D_2$ open	This failure will not cause any change in functionality.
		Short	Minor distortion in kick voltage transient is observed.	
	Rectifying diode ( $D_3$ )	Open	Capacitor $C_2$ cannot be charged since path is open.	De-energization of solenoid valves takes place if other inputs to $G_2$ are low. **
		Short	Capacitor voltage will discharge through pulse transformer ( $PT_1$ ). So capacitor cannot hold 5V. Output of $PT_2$ is LOW.	
	Capacitor ( $C_2$ )	Open	$PT_1$ short duration pulse ( $10\mu s$ ) is directly fed to $PT_2$ . If $PI_6$ is present, $PT_2$ gives $10\mu s$ pulse output. This pulse duration is not enough to hold the 24V charge on capacitor. Results are in Figure 6.6(f).	De-energization of solenoid valves takes place if other inputs to $G_2$ are low. **
		Short	It overloads the pulse transformer. No voltage is developed across capacitor. Output of $PT_2$ is LOW. Results are in Figure 6.6(g).	
	MOSFET ( $Q_2$ )	Gate/Source open	Output of $PT_2$ is LOW.	De-energization of solenoid valves takes place if other inputs to $G_2$ are low. **
		Gate to source short	Same as $Q_1$ Gate to source short.	Absence of pulses is causing valve de-energization.

	Component	Failure mode	Effect	Consequence
O R		Drain to source short	Capacitor cannot charge to 5V. Output of PT <sub>2</sub> is LOW. Internal fuse (F <sub>2</sub> ) in AND stage will blow.	De-energization of solenoid valves takes place if all the inputs to G <sub>2</sub> are low. **.
	Rectifying diode (D <sub>5</sub> )	Open	Output of PT <sub>2</sub> is not connected to OR.	De-energization of solenoid valves takes place if other inputs to G <sub>2</sub> are low.**
		Short	Over the time it will affect OR gate due to negative voltage at OR input pin. Pulse shape changes to OR gate input. Reduction in OR gate pulse output duration. Results are in Figure 6.6(h).	
	Pulse transformer freewheeling diode(D <sub>4</sub> )	Open	This failure changes the pulse shape and increase in ON time. This lead to reduction in voltage level from PT <sub>3</sub> output. Results are in Figure 6.6(i).	De-energization of solenoid valves takes place.
		Short	Slight reduction in capacitor (C <sub>2</sub> ) voltage. Minor distortion in PT <sub>2</sub> output. Pulse ON time to PT <sub>3</sub> is reduced. Results are in Figure 6.6(j).	This failure may not cause any change in valve status. Valve may de-energize if ON time sufficiently reduced. **
	Pulse transformer freewheeling diode resistor (R <sub>4</sub> )	Open	Same as D <sub>4</sub> open	De-energization of solenoid valves takes place.
		Short	Change is pulse shape and duration. C <sub>3</sub> will not be charge sufficiently. Results are in Figure 6.6(k).	De-energization of solenoid valves takes place if other inputs to G <sub>2</sub> are low. **
	OR gate (G <sub>2</sub> )	Input open	CMOS family considers open input as logic LOW. Even when input is taken as HIGH, PT <sub>3</sub> will block energy transfer to solenoid valve.	De-energization of solenoid valves takes place if other inputs to G <sub>2</sub> are low. **
		Output stuck at LOW	MOSFET Q <sub>3</sub> remains OFF. PT <sub>3</sub> output is zero.	De-energization of solenoid valves takes place.

	Component	Failure mode	Effect	Consequence
		Output stuck at HIGH	It will cause 24V fuse ( $F_3$ ) to blow.	
	Input pin to ground resistor ( $R_7$ )	Open	This failure will not cause any affect on circuit. This resistor is an extra provision to treat open input as logic low. By design itself proper logic family can be chosen to achieve this.	De-energization of solenoid valves takes place if other inputs to $G_2$ are low. **
		Short	This failure overloads timer. It causes 5V fuse ( $F_1$ ) to blow.	Loss of 5V supply to board.
D R I V E R	MOSFET ( $Q_3$ )	Gate/ Source open	Output of $PT_3$ is LOW.	Absence of pulses causes solenoid valves de-energization.
		Gate to source short		
		Drain to source short	It causes 24V ( $F_3$ ) fuse to blow.	De-energization of solenoid valves takes place.
	Pulse transformer freewheeling diode ( $D_6$ )	Open	Output pulse distortion. Failure over the time may cause damage to MOSFET due to kick back voltage. Results are in Figure 6.6(I).	No immediate loss of functionality. De-energization of solenoid valves takes place if input is driven low at gate of $Q_3$ .
		Short	Output pulse distortion.	
	Pulse transformer freewheeling diode resistor ( $R_6$ )	Open	Same as $D_6$ open.	No immediate loss of functionality. De-energization of solenoid valves takes place if input is driven low at gate of $Q_3$ .
		Short	Capacitor voltage is not sufficient to hold solenoid valve.	De-energization of solenoid valves takes place.

	Component	Failure mode	Effect	Consequence
	Rectifier diode (D <sub>7</sub> )	Open	Pulse transformer output is not connected to charge the capacitor C <sub>3</sub> .	De-energization of solenoid valves takes place.
		Short	Capacitor cannot hold the 24V since it discharges through pulse transformer as well as valve. Results are in Figure 6.6(m).	
	Capacitor (C <sub>3</sub> )	Open	Output pulse of PT <sub>3</sub> is directly fed to solenoid valve.	De-energization of solenoid valves takes place.
		Short	No voltage is developed across solenoid valve.	
	Rheostat (Rh <sub>1</sub> )	Open	Pulse is not connected to charge capacitor.	De-energization of solenoid valves takes place.
		Short	Very sharp rise time for capacitor charging when powered ON. Stress on power MOSFET and PCB traces.	No immediate loss of functionality. This failure de-energization of valves.
P U L S E  T R A N S F O R M E R	PT <sub>1</sub> , PT <sub>3</sub>	Primary to secondary short	This shorts power source to ground. This failure blows corresponding source fuse (F <sub>1</sub> / F <sub>3</sub> ).	De-energization of solenoid valves takes place.
		Primary short	Same as Primary to secondary short.	
		Secondary short	This failure is similar to capacitor in short mode failure.	
	PT <sub>2</sub>	Primary to secondary short	Capacitor is unable to charge to 5V. Output of PT <sub>2</sub> is LOW.	De-energization of solenoid valves takes place if other inputs to G <sub>2</sub> are low. **
		Primary short	Output of PT <sub>2</sub> is not 5V pulse. Based on number of windings shorted peak of pulse will be decided.	
		Secondary short		

	Component	Failure mode	Effect	Consequence
	PT <sub>1</sub> ,PT <sub>2</sub> ,PT <sub>3</sub>	Primary/ Secondary Coil Open	Pulse cannot be transmitted to next component	De-energization of solenoid valves takes place provided the particular transformer is involved in energization.

### 6.3.5 Unsafe failure probability on demand

This section shows the PFD (unsafe) calculation for the inherent fail-safe circuit. PFD values are compared to relay logic and inherent fail-safe circuit.

#### *i. Unsafe failure probability quantification of inherent fail-safe circuit*

Quantification of PFD for an inherently fail-safe circuit is quite complicated. This is because it is an attempt to systematically analyze the remote chances of failure modes which are not considered in FMEA or combination of those modes which contribute to  $\lambda_{\text{DNI}}$  (Dangerous Non Inherent failure rate). In pulsating circuit, it has been verified that all single component failures are fail-safe. However, some failures are not immediately detectable, and they are revealed only under certain input combinations. This gives opportunity for multiple failures to accumulate over time and then possibly leading to an unsafe scenario. With this viewpoint, those combinations of failures which have the potential to cause unsafe output is analyzed. To prevent these failures, which contribute to significant unsafe failure probability, the circuit has to be tested with selected test points every proof test interval. During proof testing, the entire truth table has to be checked. Over and above this, a suspected failure like parameter change in transformers which may remain dormant has to be checked. Because of complexity involved,  $\tau$  is assumed as six months.

The combinations of failures which lead to unsafe output are analyzed and quantified below. In this calculation failure mode probability distribution is considered from RIAC-91 [92]. Failure rates of components are taken from MIL-HDBK-217F [91]. Though this standard is not updated, for simple components such as transistors, resistors, etc., this will suffice.

Case I:

(PT<sub>1</sub> parameter change) AND (C<sub>2</sub> open) AND (PI<sub>6</sub> stuck at HIGH [OR] Q<sub>2</sub> drain to source short)

The increase in VT product of PT<sub>1</sub> will give output with high duty cycle. Open mode failure of C<sub>2</sub> will result in the output of PT<sub>1</sub> to appear as an input of PT<sub>2</sub>. Along with this failure combination, if Q<sub>2</sub>-drain to source short occurs, then irrespective of PI<sub>6</sub>, AND stage gives output of PT<sub>1</sub>. This output is unsafe.

- a. Mode probability of “transformer parameter change” is 16%. Failure rate of Low power pulse transformer is 0.0035 failures/ 10<sup>6</sup> hours. Thus, “PT<sub>1</sub> parameter change” failure rate is

$$\lambda_1 = 0.00056 \text{ failures}/10^6 \text{ hours} \quad (1)$$

- b. Mode probability of “capacitor open” is 35%. Failure rate of Aluminum oxide capacitor is 0.024 failures/ 10<sup>6</sup> hours. Thus, “C<sub>2</sub> open” failure rate is

$$\lambda_2 = 0.00084 \text{ failures}/10^6 \text{ hours} \quad (2)$$

- c. Failure rate calculation of PI<sub>6</sub> stuck at HIGH and Q<sub>2</sub> drain to source short is

1. Mode probability of “Micro circuit digital”, Bipolar output stuck at HIGH is 28%. Failure rate of timer is 0.032 failures/10<sup>6</sup> hours. Thus, “PI<sub>6</sub> stuck at HIGH” failure rate is

$$0.00896 \text{ failures } /10^6 \text{ hours} \quad (3)$$

2. Mode probability of “FET short” is 51%. Failure rate of Si FET is 0.014 failures/10<sup>6</sup> hours. Thus, “Q<sub>2</sub> drain to source short” failure rate is

$$0.00714 \text{ failures } /10^6 \text{ hours} \quad (4)$$

Thus, (PI<sub>6</sub> stuck at HIGH) OR (Q<sub>2</sub> drain to source short) failure rate is (3) + (4).

$$\lambda_3 = 0.0161 \text{ failures}/10^6 \text{ hours} \quad (5)$$

$$\begin{aligned} \text{Unsafe failure probability} &= (1 - e^{-\lambda_1\tau})(1 - e^{-\lambda_2\tau})(1 - e^{-\lambda_3\tau}) \\ &= 0.6104 \times 10^{-15} \end{aligned} \quad (6)$$

Along with the specified test cases, a special case to be tested for determining this combination of failure is by providing pulse input to PI<sub>4</sub> and static LOW to PI<sub>6</sub>. If this test case leads to energizing the valve then it can be concluded that this combination of failures have occurred.

Case II:

(PT<sub>4</sub> parameter change) AND (C<sub>4</sub> open) AND (G<sub>1</sub> output at stuck at HIGH [OR] Q<sub>6</sub> drain to source short [OR] PI<sub>1</sub> stuck at HIGH [OR] PI<sub>7</sub> stuck at HIGH)

a. “PT<sub>4</sub> parameter change” failure rate is

$$\lambda_4 = 0.00056 \text{ failures} / 10^6 \text{ hours (from 1)} \quad (7)$$

b. “C<sub>4</sub> open” failure rate is

$$\lambda_5 = 0.00084 \text{ failures} / 10^6 \text{ hours (from 2)} \quad (8)$$

c. Failure rate calculation of G<sub>1</sub> output at stuck at HIGH, Q<sub>6</sub> drain to source short, PI<sub>1</sub> stuck at HIGH and PI<sub>7</sub> stuck at HIGH is

1. Mode probability of “Micro circuit, Digital” MOS output stuck at HIGH is 8%. Failure rate of MOS technology gate is 0.0057 failures/10<sup>6</sup> hours. Thus, “G<sub>1</sub> output at stuck at high” failure rate is

$$0.000456 \text{ failures} / 10^6 \text{ hours} \quad (9)$$

2. “Q<sub>6</sub> drain to source short” failure rate is

$$0.00714 \text{ failures} / 10^6 \text{ hours (from 4)} \quad (10)$$



3. “PI<sub>1</sub> stuck at HIGH” failure rate is

$$0.00896 \text{ failures} / 10^6 \text{ hours (from 3)} \quad (11)$$

4. “PI<sub>7</sub> stuck at HIGH” failure rate is

$$0.00896 \text{ failures} / 10^6 \text{ hours (from 3)} \quad (12)$$

Thus, (G<sub>1</sub> output at stuck at HIGH) OR (Q<sub>6</sub> drain to source short) OR (PI<sub>1</sub> stuck at HIGH) OR (PI<sub>7</sub> stuck at HIGH) is (9) + (10) + (11) + (12).

$$\lambda_6 = 0.02551 \text{ failures} / 10^6 \text{ hours} \quad (13)$$

$$\begin{aligned} \text{Unsafe failure probability} &= (1 - e^{-\lambda_4 \tau})(1 - e^{-\lambda_5 \tau})(1 - e^{-\lambda_6 \tau}) \\ &= 0.9671 \times 10^{-15} \end{aligned} \quad (14)$$

**Thus, PFD (unsafe) for inherent fail-safe circuit is (6) + (14) = 0.158 × 10<sup>-14</sup>**

The PFD result seems to be unrealistic. It can be easily seen that this is achieved because the actual system failure happens only upon a combination of multiple failures (at least three). The components involved are diverse in nature, and hence Common Cause Failures (CCF) is not considered in this calculation. However, the components reside on the same board, and there could be multiple failures in the board which would ultimately dictate the effective PFD. Quantification of CCF is not attempted since it would depend on factors external to the system like power supply, environment, etc. However, the quantitative result serves the purpose of gaining an in-depth insight into the system reliability.

Another aspect is that the very low PFD (unsafe) is achieved with additional spurious actuation (opening of dampers when not intended). However, increase in flow can take place only when both inlet and outlet dampers are spuriously opened. Manual overriding options are

provided in the dampers when decay heat removal is in progress. These options are utilized by operators to close the failed damper from the field.

ii. *Unsafe probability quantification of relay logic (existing logic)*

Combinational equation of relay logic (as in Figure 6.2) is  $I_5 + I_4 \times I_6 + I_3 + I_2 \times I_1 + I_2 \times I_7$ . Minimal cutset to unsafe failure event is  $I_5 + I_3$ . Mode probability of “relay contact” in short is 19%. Failure rate of relay is 0.13 failures/ $10^6$  hours. Therefore failure rate of relay in short mode is 0.0247 failures/ $10^6$  hours. Failure rate of relay logic  $\lambda_7 = 0.0494$  failures/ $10^6$  hours. A proof test interval ( $\tau$ ) of one week is assumed for relay logic due to simplicity in exercising the system as against six months assumed for an inherent fail-safe circuit.

$$\text{Unsafe failure probability} = (1 - e^{-\lambda_7 \tau})$$

Thus, **PFD (unsafe) for relay logic is  $0.8299 \times 10^{-5}$**

This comparison shows that it is possible to build inherent fail-safe solid state circuits with very high confidence level on unsafe failure probability on demand.

### 6.3.6 Precautions and possible improvements

The pulse transformers are to be designed and tested so that any duty cycle increase or decrease leads to loss of energy transmissions. Though PT<sub>3</sub> primary to secondary short will lead to fuse blowing in 24V stage, it has the potential to transmit DC to solenoid valves if secondary is burnt open before fuse, due to improper fuse design. As an additional precaution measures such as isolating PT<sub>3</sub> primary and secondary and geometrical separation of primary and secondary with shared core (core being grounded) can be adopted. Internal fuse can be used in every stage to protect the circuit. The fuses have to be carefully rated and response times well tested. The effect of noise on the circuitry has to be further investigated.

## **6.4 Applications of Inherent Fail-safe Circuit**

Inherent fail-safe design can achieve equivalent or lesser unsafe failure probability compared to combinational logic designs implemented with relays. Hence, the suggested method can be adapted to any industrial application where the relay control logic is implemented. Some of the relay logic applications are nuclear, space, railways, telecommunications etc. Relay logics are used in routing control and signaling on railways. Large relay circuits are employed in elevators for control, but progressively superseding with modern solid state circuits. It is also used for controlling and automation purposes in electro-hydraulics and electro-pneumatics. Relay logic is used to implement the shutdown system trip logic in CANDU-PHW reactor. The proposed inherent fail-safe design can be easily extended to similar industrial control involving combinational circuits with modifications.

## **6.5 Summary**

- A novel fail-safe AND gate is proposed to reduce the unsafe failure probability and it is experimentally proven as fail-safe under all probable failure modes.
- An inherent fail-safe pulsating electronic logic valve drive circuit with AND gate for a safety critical nuclear application is proposed. A detailed failure mode effect analysis for the proposed design is presented and verified empirically. Since all perceivable failure modes are shown to result in the fail-safe state, the circuitry can also be used as a diverse method for damper control in SGDHR of FBRs.
- The method can achieve equivalent or lesser unsafe failure probability compared to relay logic being currently used in PFBR. The suggested method can be adapted to any industrial application where combinational circuit is employed.

# 7

## SUMMARY AND SCOPE FOR FUTURE WORK

---

*The present chapter summarizes the research work carried out in the field of fail-safe design of safety critical instrumentation and control systems for applications to medium sized sodium cooled fast reactors. The study is performed in a 500MWe Prototype Fast Breeder Reactor, which is in the advanced stage of commissioning at Kalpakkam, India. The conclusions derived from this study are briefly outlined. Further, the scope for future works in this field is mentioned.*

---

### 7.1 Summary

Instrumentation and Control (I&C) systems are very crucial to achieve the desired safety function of various systems in a Nuclear Power Plant (NPP). The design of “fail-safe” safety critical I&C systems are made to achieve a low value of average Probability of Failure on Demand ( $PFD_{Avg}$ ). The fail-safe behavior is the capability of a system to reach a predefined safe state in the event of malfunction of components. Shutdown systems and decay heat removal systems play a key role in a NPP towards achieving CDF targets. As a first step, the various design principles used in I&C of these systems to reduce  $PFD_{Avg}$  namely, redundancy, independence, diversity, periodic surveillance and fail-safe design are studied. The quantitative effect of each of the design principle on the  $PFD_{Avg}$  is clearly brought out.

The design principles and techniques in shutdown and decay heat removal systems of a 500MWe sodium cooled Prototype Fast Breeder Reactor (PFBR) are studied. There are three

parts of I&C chain namely sensors, processing electronics and final control elements. Sensor failures are addressed using discordance monitoring, signal validation etc. The processing electronics and voting logic employs sophisticated electronics or computer systems in which fail-safe design is adequately implemented by using techniques like finite impulse tests, test signal superimposition, discordance monitoring, etc. In shutdown systems, absorber rods are dropped into core under gravity due to loss of power supply and cable cut to shutdown of the reactor. In decay heat removal systems, fail safe behavior is achieved by invoking passive features, wherein natural circulation of coolant guarantees removal of decay heat. However, a few active components are involved to allow for initiation of decay heat removal when required. Relay logic is used to initiate flow in decay heat removal systems. Failures in power supply, relays and pneumatic supply lead to spurious initiation of decay heat removal action (fail safe action). Thus adequate design provisions are provided in safety systems of PFBR to achieve fail-safe design and consequently a very low  $PFD_{Avg}$ .

The evolving safety requirements demand practically eliminating the core disruptive accident. Thus there is still a need to further decrease  $PFD_{Avg}$  of safety systems. The potential areas identified to be strengthened are listed below.

1. The EM relays used in the safety systems are assumed to be “fail-to-close”. To address unsafe failure mode (contact weld), current techniques allow for testing only one redundant channel at a time. Hence, it is desirable to find a new method to detect weld failure of EM relay contact online (without opening the relay contact). It has to be shown that there is no impact of diagnostic circuit on functional circuit by reliability modeling.
2. Uncontrolled withdrawal of absorber rods could be caused by failures in EM contactors in reactor power control system. Further studies are required to verify the reliability of

EM contactor (weld failure) and its impact on uncontrolled withdrawal of neutron absorber rod.

3. Much of the circuits depend on periodic testing as a powerful defense against unsafe failures. Inherent fail-safe circuits do not require diagnostics since any of the failures in the circuit will automatically lead to a safe state of the final control element. Thus, inherent fail-safe design as an alternative to systems with periodic self-testing is to be explored.

The present research is focused to address the above mentioned potential areas. Following are the important achievements of this research work:

A novel online, continuous and automated method is proposed to perform online diagnostics of Electro Magnetic (EM) relay for a safety critical application. The diagnostic method works on the principle of de-energizing followed by quick re-energization of the relay coil before the contact starts moving apart. Test results are satisfactory and welded contact is detected successfully. The significance of the current work is that it facilitates diagnostics without any impact on the load. Isolation of the load is thus intact. Simultaneous testing of redundant channels becomes possible.

The practical implementation and verification of relay contact weld detection circuit without any impact on functional circuit is verified with a relay output card. From the reliability analysis, it is noticed that the diagnostic circuit incorporation reduces the unsafe state probability of the system in each redundant channel by around 48 folds. The significant reduction in unsafe state probability is achieved through very low test interval which is turn has been possible because the proposed method is amenable for online implementation. Diagnostic circuit failures

have very less significance on the unsafe state probability of the system. It is possible to fix the test interval and proof test interval based on the target unsafe state probability requirement.

Reliability demonstration test on sufficiently de-rated contactors has shown that failure probability of fail-to-open mode is less under the influence of cyclic stress. SEM and EDS images of contacts depict surface morphology degradation with the formation of Ni precipitates due to arcing. Ni precipitates is found to be growing with the increasing number of cycles. This may decrease the effective contact area and conductivity which may ultimately lead to failure of the contactors. However, contactor fail-to-open is not noticed probably due to higher rating of contactor when compared to field condition. From this study, it is seen that the chance of uncontrolled withdrawal of control rod in PFBR is remote.

A novel fail-safe AND gate is proposed in this study to reduce the unsafe failure probability and it is experimentally proven to be fail-safe under all postulated failure modes. An inherent fail-safe pulsating electronic logic valve drive circuit using the AND gate for decay heat removal system. A detailed failure mode effect analysis for the proposed design is presented and verified empirically. Since all perceivable failure modes are shown to result in fail-safe state, the circuitry can also be used as a diverse method for damper control in SGDHR of FBRs. The method achieved lesser unsafe failure probability compared to relay logic being currently used in PFBR. The suggested method is suitable to any industrial application where the combinational circuit is employed.

Overall the work has proposed EM relays with online diagnostics and inherently fail-safe circuits to reduce the  $PFD_{Avg}$  of safety systems in a fast reactor.



## **7.2 Future Work**

Based on the investigation, the following are recommended for future studies:

- Absorber rods held by electromagnets are de-energized when there is a demand to shutdown the reactor. Electromagnets play a pivotal role in ensuring fail-safe behavior of shutdown systems. Not only the de-actuation, but also the de-actuation within given time is to be ensured as part of fail-safe design. Response time of electromagnets is verified during actual drop (during SCRAM). The EM relays and electromagnets operate with similar principles. Thus, the online method to detect relay contact weld described in chapter 3 can be explored to measure the response time of electromagnet.
- Though, chapters 3 and 4 deal extensively with relay diagnostics, a method for early prediction (prognostics) of relay failure will be helpful in lowering the dangerous failure probability. This can be further explored.
- SGDHR circuit in PFBR has two types of dampers to control air flow through sodium to air heat exchanger namely pneumatic and electrical. Electrical dampers are typically stay put upon power failure due to inherent difficulties. Possibilities can be explored to come out with a fail-safe arrangement for future FBRs.

## REFERENCES

- [1] Safety Design Criteria for Generation IV Sodium-cooled Fast Reactor System, Generation IV International Forum, 2013.
- [2] Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, IAEA Tech. reports, No.387, International Atomic Energy Agency, Vienna, 1999.
- [3] IEC 61511, Functional Safety –Safety Instrumented Systems for the process industry sector, part 1-3, International Electrotechnical Commission, Geneva, Switzerland, Geneva, 2003.
- [4] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related- systems, International Electrotechnical Commission, Geneva, Switzerland, 2010.
- [5] ISA-TR84.00.02-2002-Safety Instrumented Functions (SIF)-Safety Integrity Level (SIL) Evaluation Techniques-Introduction, The Instrumentation, Systems, and Automation Society, North Carolina, USA, 2002.
- [6] Safety of Research Reactors, Safety requirements, No. NS-R-4, International Atomic Energy Agency, Vienna, 2005.
- [7] H.A. Gabbar, L. Xia, M.U. Isham and V. Ponomarev, Signal processing system design for improved shutdown system of CANDU® nuclear reactors in large break LOCA events, Nuclear Engineering and Design, vol. 298, pp. 255–263, Mar. 2016.
- [8] D.Y. Lee, J B. Han and J. Lyou, Reliability Analysis of the Reactor Protection System with Fault Diagnosis, Key Engineering Materials, vol. 270-273, pp. 1749-1754, 2004.
- [9] H.D. Fischer and L. Piel, Diversity in computerized reactor protection systems, Reliability Engineering and System Safety, vol. 63, issue 1, pp. 91-97, 1999.
- [10] Manoj Kumar, A. Kabra, G. Karmakar and P.P. Marathe, A review of defences against common cause failures in reactor protection systems, 4<sup>th</sup> IEEE International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), pp. 1-6, Sept. 2015.
- [11] H.Y. Chung and D.W. Kim, Design of Advanced Power Reactor (APR1400) I&C System, IFAC Power Plants and Power Systems Control, vol. 36, issue 20, pp. 729-734, Sep. 2003.

- [12] R.P. Behera, N. Murali and S.A.V. Satya Murty, Designing fault-tolerant real-time computer systems with diversified bus architecture for nuclear power plants, *Journal of Nuclear Science and Technology*, vol. 51, issue 4, pp. 521-525, Apr. 2014.
- [13] RS. Hart and RA. Olmstead, *CANDU Passive Shutdown Systems*, IAEA Tec. Doc. No.920, International Atomic Energy Agency, 1996.
- [14] *Safety of Nuclear Power Plants: Design, Specific Safety Requirements*, No. SSR-2/1, International Atomic Energy Agency, Vienna, 2016.
- [15] S. Bakhri, Investigation of Rod Control System Reliability of PWR Reactors, *KnE Energy*, vol. 1, issue 1, Sep. 2016.
- [16] *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*, Safety Standards Series No.NS-G-1.3, International Atomic Energy Agency, Vienna, 2002.
- [17] H.M. Hashemian, On-line monitoring applications in nuclear power plants, *Progress in Nuclear Energy*, vol. 53, issue 2, pp. 167-181, Mar. 2011.
- [18] H. Jahanian, Generalizing PFD formulas of IEC 61508 for KooN configurations, *ISA Transactions*, vol. 55, pp. 168–174, March 2015.
- [19] F.E. Nadir, I.H. Baraka, M. Bsiss and B. Amami, Influence of failure modes and effects analysis on the average probability of failure on demand for a safety instrumented system, 4<sup>th</sup> IEEE International Colloquium on Information Science and Technology, pp. 867-871, Oct. 2016.
- [20] J. Jin, L. Pang, B. Hu and X. Wang, Impact of proof test interval and coverage on probability of failure of safety instrumented function, *Annals of Nuclear Energy*, vol. 87, issue 2, pp. 537-540, 2016.
- [21] İ. Üstoğlu, Ö. T. Kaymakçı and J. Börcsök, Effects of varying diagnostic coverage on functional safety, 2014 IEEE International Symposium on Fundamentals of Electrical Engineering (ISFEE), pp. 1-6, Nov.2014.
- [22] W. Velten Philipp and M. Houtermans, The effect of diagnostic and periodic proof testing on the availability of programmable safety systems, 10<sup>th</sup> IEEE WSEAS International Conference on Communications, pp. 180-186, July 2016.
- [23] M.K. Khan and G. Heo, A benchmarking study on online cross calibration techniques for redundant sensors, 2017 European Safety and Reliability Conference, in proceedings of Safety and Reliability-Theory and Applications, CRC Press, p. 127, Slovenia, June 2017.

- [24] J.W. Hines and R.E. Uhrig, Trends in computational intelligence in nuclear engineering, *Progress in Nuclear Energy*, vol. 46, issue. 3-4, pp. 167-175, Jan. 2005.
- [25] J. Ma and J. Jiang, Applications of fault detection and diagnosis methods in nuclear power plants: A review, *Progress in Nuclear Energy*, vol. 53, issue 3, pp. 255-266, Apr. 2011.
- [26] S. Mandal, Sensor Fault Detection in Nuclear Power Plant Using Artificial Neural Network, *Journal of Mathematics and Informatics*, vol. 4, pp. 81–87, Dec. 2015.
- [27] A.S. Erbay, B.R. Upadhayaya and S. Seker, A PC-Based Signal Validation System For Nuclear Power Plants, *Proceedings of IAEA Technical Committee meeting, Diagnostic Systems In Nuclear Power Plants, Turkey*, pp. 163–180, June 1998.
- [28] P. Saritha Menon, N. Sridhar and D. Thirugnana Murthy, FPGA based pump speed measurement system for Prototype Fast Breeder Reactor, 3<sup>rd</sup> IAEA National symposium on advances in control and instrumentation, Mumbai, pp. 118–125, Nov. 2014.
- [29] C. Guo, D. Li and H. Xiong, Preliminary Study on Reliability Analysis of Safety I&C System in NPP, 2<sup>nd</sup> International Congress on Computer Applications and Computational Science in proceedings of *Advances in Intelligent and Soft Computing*, pp. 303–310, 2011.
- [30] D.C. Gaubatz, Reactor protection system with automatic self-testing and diagnostic, *Google Patents*, 1996.
- [31] G. Dragffy, The design of a highly reliable safety critical emergency shutdown system, *Reliability Engineering and System Safety*, vol. 61, issue 3, pp. 215-227, 1998.
- [32] F. Li, Z. Yang, Z. An, and L. Zhang, The first digital reactor protection system in China, *Nuclear Engineering and Design*, vol. 218, issue 1, pp. 215-225, 2002.
- [33] N. Hayashi, Replacement of the control & instrumentation system with the microprocessor based system in Japanese PWR plants, *Proceedings of IAEA Technical Committee meeting, Computerized Reactor Protection and Safety Related Systems in Nuclear Power Plants, Hungary*, pp. 185–197, 1997.
- [34] MC. Popescu, Shutdown Systems computer monitoring for Cernavoda NPP, *Proceedings of IAEA Technical Committee meeting, Computerized Reactor Protection and Safety Related Systems in Nuclear Power Plants, Hungary*, pp. 207–209, 1997.
- [35] W.Y. Yun, Applications of Computer Based Safety Systems in Korea Nuclear Power Plants, *Proceedings of IAEA Technical Committee meeting, Computerized Reactor*

- Protection and Safety Related Systems in Nuclear Power Plants, Hungary, pp. 199–205, 1997.
- [36] Y.G. Oh, J.K. Jeong, C.J. Lee, Y.H. Lee, S.M. Baek and S.J. Lee, Fault-Tolerant Design for Advanced Diverse Protection System, Nuclear Engineering and Technology, vol. 45, issue 6, pp. 795-802, Nov. 2013.
- [37] J.P. Trapp and A. Lebran, Computerized reactor surveillance and control system: An FBR example, Proceedings of IAEA Technical Committee meeting, Computerized Reactor Protection and Safety Related Systems in Nuclear Power Plants, Hungary, pp. 55–64, 1997.
- [38] X. Jia, Z.Q. Wang, Y.B. Zhang and Y.H. Guo, The Independence of Safety Digital I&C System in Nuclear Power Plant, The International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection of Nuclear Power Plant, Proceedings in Lecture Notes in Electrical Engineering 400, China, pp. 201–208, June 2016.
- [39] Y. Li, W. Sun, L. Zhou, and L. Zhang, Analysis of CPU Redundant Configuration for the Safety DCS of NPP, The International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection of Nuclear Power Plant, Proceedings in Lecture Notes in Electrical Engineering 400, China, pp. 33–40, June 2016.
- [40] M. Manimaran, A. Shanmugam, P. Parimalam, N. Murali and S.A.V. Satya Murty, Fault tolerant distributed real time computer systems for I&C of Prototype Fast Breeder Reactor, Nuclear Engineering and Design, vol. 268, pp. 96-103, Mar. 2014.
- [41] H.K. Shin, S.K. Nam, S.D. Sohn and H.S. Chang, Development of an Advanced Digital Reactor Protection System Using Diverse Dual Processors to Prevent Common-Mode Failure, Nuclear Technology, vol. 141, issue 1, pp. 33-44, Jan. 2003.
- [42] Instrumentation and Control (I&C) Systems in Nuclear Power Plants: A Time of Transition, 52<sup>nd</sup> IAEA General Conference (2008), NTR 2008 Supplement, International Atomic Energy Agency, 2008.
- [43] Z. Ma, H. Yoshikawa and M. Yang, Reliability model of the digital reactor protection system considering the repair time and common cause failure, Journal of Nuclear Science and Technology, vol. 54, issue 5, pp. 539-551, May 2017.
- [44] V. Rajan Babu, R. Veerasamy, Sudheer Patri, I.S. Raj, S.C.S.P.K. Krovvidi, S.K. Dash, C.M. Murthy, K.K. Rajan, P.Puthiyavinayagam, P.Chellapandi, G. Vaidyanathanan, S.C.

- Chetal, Testing and qualification of control & safety rod and its drive mechanism of Fast Breeder Reactor, Nuclear Engineering and Design, vol. 240, pp. 1728–1738, Jul. 2010.
- [45] D. Favet, B. Carlucci and D.S., Third Shutdown level for EFR Project, Proceedings of IAEA Technical Committee meeting, Absorber materials, control rods and designs of shutdown systems for advanced liquid metal fast reactors, Russia, pp. 173–188, 1995.
- [46] K.D. Badgajar, System science and control techniques for harnessing nuclear energy, System Science and Control Engineering, vol. 4, issue 1, pp. 138164, Jan. 2016.
- [47] E. Ramesh and S. Usha, Reliability analysis of control rod drive mechanisms of FBTR for reactor startup and power control, IEEE 2<sup>nd</sup> International Conference on Reliability, Safety and Hazard (ICRESH), pp. 431–435, 2010.
- [48] Y.P. Chyou, D.D. Yu and Y.N. Cheng, Performance validation on the prototype of control rod driving mechanism for the TRR-II project, Nuclear Engineering and Design, vol. 227, issue 2, pp. 195-207, Jan. 2004.
- [49] S. Nakanishi, T. Hosoya, S. Kubo, S. Kotake, M. Takamatsu, T. Aoyama, I. Ikarimoto, J. Kato, Y. Shimakawa and Kiyoshi Harada Development of Passive Shutdown System for SFR, Nuclear Technology, vol. 170, issue 1, pp. 181-188, Apr. 2010.
- [50] J. Josephson and E. S. Sowa, The Design and Testing of a Self-Actuated Shut down System for the Protection of Liquid Metal Fast Breeder Reactors (LMFBRS), IEEE Trans. Nuclear Science, vol. 24, issue 2, pp. 919-930, 1977.
- [51] T. Bartha, I. Varga, A. Soumelidis and G. Szabe, Implementation of a Testing and Diagnostic Concept for an NPP Reactor Protection System, 5<sup>th</sup> European dependable computing conference, Budapest and in proceedings of Dependable computing-EDCC-5, LNCS-3463, pp. 391-402.
- [52] A.S. Bartu, A dual-channel reactor protection system for nuclear power plants, Transactions of the American Institute of Electrical Engineers, Part-1: Communication and Electronics, vol. 79, issue 4, pp. 358-362, 1960.
- [53] P.G. Slade, Electrical contacts: Principles and applications, 2<sup>nd</sup> edition, CRC Press, 2014.
- [54] W.F. Rieder and A.R. Neuhaus, Contact welding influenced by anode arc and cathode arc, respectively, 50<sup>th</sup> IEEE Holm Conference on Electrical Contacts, pp. 378-381, Sep. 2004.

- [55] Z. Chen and G. Witter, Dynamic welding of silver contacts under different mechanical bounce conditions, 45<sup>th</sup> IEEE Holm Conference on Electrical Contacts, pp. 1-8, Oct. 1999.
- [56] L. Morin, N.B. Jemaa, D. Jeannot, J. Pinard and L. Nedelec, Make arc erosion and welding in the automotive area, IEEE Transactions on Components and Packaging Technologies, vol. 23, issue 2, pp. 240-246, June 2000.
- [57] A.R. Neuhaus, W.F. Rieder and M.H. Schmidt, Influence of electrical and mechanical parameters on contact welding in low power switches, IEEE Transactions on Components and Packaging Technologies, vol. 27, issue 1, pp. 4-11, March 2004.
- [58] F. Yao, J. Lu, J. Zheng and Z. Huang, Research on the failure diagnostics parameters and the reliability prediction model of the electrical contacts, 52<sup>nd</sup> IEEE Holm conference on Electrical Contacts, pp. 69–72, 2006.
- [59] X. Zhou, L. Zou and R. Briggs, Prognostic and Diagnostic technology for DC actuated contactors and motor starters, IEICE Transactions on Electronics, vol. E92–C, issue 8, pp. 1045-1051, 2009.
- [60] Technical note on Verification and Diagnosis of Suspected Relay Failures, TE Connectivity.
- [61] G. Shanmugam, A. Babu and K.S. Kumar, Operating Experiences of FBTR, IAEA International Conference on Fast Reactors and Related Fuel Cycles: Next Generation Nuclear Systems for Sustainable Development, June 2017.
- [62] IEC 60947-4-1: Contactors and motor-starters-Electromechanical contactors and motor-starters, International Electrotechnical Commission, Geneva, 2012.
- [63] S.C. Chetal, V.B. Subramaniyan, P.Chellapandi, P. Mohanakrishnan, P. Puthiyanayagam, C.P. Pillai, S.Raghupathy, T.K. Shanmugham and C. Sivathanu Pillai, The design of the Prototype Fast Breeder Reactor, Nuclear Engineering and Design, vol. 236, pp. 852-860, Apr. 2006.
- [64] M. Sakthivel and K. Madhusoodanan, Core temperature monitoring system for Prototype Fast Breeder Reactor, Nuclear Science and Engineering, vol. 170, pp. 290-293, March 2012.
- [65] G.K. Mishra, M. Sakthivel, S.L.N. Swamy and K. Madhusoodanan, Instrumentation for Sodium-Cooled Fast Breeder Reactors, Nuclear Science and Engineering, vol. 174, pp. 96–102, May 2013.

- [66] M.K. Misra, N. Sridhar and D.T. Murthy, Design and implementation of safety logic with fine impulse test system for a nuclear reactor shutdown system, 27<sup>th</sup> International Conference on VLSI design and 13<sup>th</sup> International Conference on Embedded systems, IEEE, pp. 198-203, Jan. 2014.
- [67] M.K. Misra, N. Sridhar, B. Krishnakumar, S.A.V. Satya Murty and P. Swaminathan, Reliability analysis of safety logic with fine impulse test system of Indian Prototype Fast Breeder Reactor, 2<sup>nd</sup> International Conference on Reliability, Safety and Hazard, IEEE, pp. 412–417, Dec. 2010.
- [68] M. Anwer, N. Satheesh, C.P. Nagaraj and B. Krishnakumar, Pulse coded safety logic for PFBR, 1<sup>st</sup> National Conference on Nuclear Reactor Technology, IAEA, p. 421, Nov. 2002.
- [69] N. Satheesh, M. Anwer, D. Thirugnanamurthy and B.K. kumar, Reliability assessment of pulse coded safety logic system for PFBR, 4<sup>th</sup> National Conference on Nuclear Reactor Technology: Emerging trends in Nuclear Safety, IAEA, p. 208, March 2011.
- [70] R. Dheenadhayalan, A. Venkatesan, K. Madhusoodanan and P. Chellapandi, Design of instrumentation for control and safety rod drive mechanisms of Prototype Fast Breeder Reactor, International Journal of Nuclear Energy Science Technology, vol. 7, issue 4, pp. 380–395, 2013.
- [71] R. Vijayashree, R. Veerasamy, Sudheer Patri, P. Chellapandi, G. Vaidyanathan, S.C. Chetal and Baldev Raj, Design, development, testing and qualification of diverse safety rod and its drive mechanism for a Prototype Fast Breeder Reactor, Journal of Engineering for Gas Turbines and Power, vol. 132, issue 10, p. 102921, 2010
- [72] C.S. Kumar, A. John Arul, O. Pal Singh and K. Suryaprakasa Rao, Reliability analysis of shutdown system, Annals of Nuclear Energy, vol. 32, pp. 63–87, Jan. 2005.
- [73] U. Parthasarathy, T. Sundararajan, C. Balaji, K. Velusamy, P. Chellapandi and S. C. Chetal, Decay heat removal in pool type Fast Reactor using passive systems, Nuclear Engineering and Design, vol. 250, pp. 480–499, Sep. 2012.
- [74] L.S. Kumar, K. Natesan, A. John Arul, V. Balasubramaniyan and S. C. Chetal, Design and evaluation of operation grade decay heat removal system of PFBR, Nuclear Engineering and Design, vol. 241, 4953–4959, Dec. 2011.
- [75] L. Srivani, K. Kameswari, R. Dheenadhayalan, A. John Arul, K. Palani Sami, D.T. Murthy, K. Madhusoodanan and S.A.V Satya Murty, Initiator frequency analysis for



- PFBR control and safety rod system, 2<sup>nd</sup> SRESA National Conference on Reliability and Safety Engineering, p. 56, Oct. 2015.
- [76] A. John Arul, C.S. Kumar, S. Athmalingam, O.P. Singh and K. Suryaprakasa Rao, Reliability analysis of safety grade decay heat removal system of Indian Prototype Fast Breeder Reactor, *Annals of Nuclear Energy*, vol. 33, pp. 180-188, Jan. 2006.
  - [77] Safety systems for Pressurized Heavy Water Reactors, Guide No. AERB/NPP-PHWR/SG/D-10, Atomic Energy Regulatory Board, Mumbai, 2005.
  - [78] W.T. Kouidri, F. Letaim, A. Boucenna and M.H. Boulhaouchet, Safety analysis of reactivity insertion accidents in a heavy water nuclear research reactor core using coupled 3D neutron kinetics thermal-hydraulic system code technique, *Progress in Nuclear Energy*, vol. 85, pp. 384-390, Nov. 2015.
  - [79] T. Abou EL Maaty, Uncontrolled withdrawal of a control rod without scram, *Annals of Nuclear Energy*, vol. 35, pp. 11-17, Jan. 2008.
  - [80] K. Devan, A. Batchchan, M. Alagan and P. Chellapandi, Analysis of control rod withdrawal end-of-life tests in the PHEONIX reactor at IGCAR, The role of reactor physics toward a sustainable future, IAEA, p.15, Oct. 2014.
  - [81] Sutanto and Y. Oka, Analysis of anticipated transient without scram of a Super Fast Reactor with single flow pass core, *Annals of Nuclear Energy*, vol. 75, pp. 54-63, Jan. 2015.
  - [82] K. Natesan, N. Kasinathan, K. Velusamy, P. Selvaraj and P. Chellapandi, Plant dynamics studies towards design of plant protection system for PFBR, *Nuclear Engineering and Design*, vol. 250, pp. 339-350, Sep. 2012.
  - [83] Application note on Contact System, TE Connectivity. (URL: <http://www.te.com/us-en/home.html>)
  - [84] V. Behrens, T. Honig, O. Lutz, W. Schmitt, D. Spath and B. Worle, Failure of arcing contacts in low voltage switching devices-Examples, root causes, counter measures, 56<sup>th</sup> IEEE Holm Conference on Electrical Contacts, pp. 1-7, Oct. 2010.
  - [85] Application note on Contact arc phenomenon, Picker Components.
  - [86] W.F. Rieder and A. R. Neuhaus, Contact welding influenced by anode arc and cathode arc, respectively, 50<sup>th</sup> IEEE Holm Conference on Electrical Contacts, pp. 378-381, Sep. 2004.

- [87] L. Zhao, Z. Li, H. Zhang and M. Hasegawa, Random Occurrence of Contact Welding in Electrical Endurance Tests, IEICE Transactions on Electronics, vol. E94-C, issue 9, pp. 1362-1368, 2011.
- [88] T.J. Schoepf, R. Rowlands and G. Drew, Contact welding at break of motor inrush current, IEEE Transactions on Components and Packaging Technologies, vol. 29, issue 2, pp. 278-285, June 2006.
- [89] L. Doublet, N.B. Jemaa, F. Hauner and D. Jeannot, Make arc erosion and welding tendency under 42V<sub>DC</sub> in automotive area, 49<sup>th</sup> IEEE Holm Conference on Electrical Contacts, pp. 158-162, 2003.
- [90] F. Yao, J. Lu, J. Zheng and Z. Huang, Research on the failure diagnostics parameters and the reliability prediction model of the electrical contacts, 52<sup>nd</sup> IEEE Holm conference on Electrical Contacts, pp. 69–72, 2006.
- [91] Military Handbook: Reliability prediction of electronic equipment: MIL-HDBK-217F, Department of Defense, 1995.
- [92] Failure Mode/Mechanism distributions, Reliability Analysis Center, 1991.
- [93] Isograph Reliability Workbench; Version 10.1.
- [94] MIL-HDBK-781A: Reliability test methods, plans and environments for engineering, development qualification and production, Department of Defense, 1996.
- [95] Research Reactor Modernization and Refurbishment, IAEA Tech. reports, No.1625, International Atomic Energy Agency, Vienna, 2009.
- [96] S. Tikku, G. Raiskums, J. Harber and P. Foster, Safety system and control system separation requirements for ACR-1000<sup>TM</sup> and operating CANDU reactors, 18<sup>th</sup> International Conference on Nuclear Engineering, ASME, pp. 883-892, May 2010.
- [97] G. Bereznai, Nuclear Power Plant Systems and Operation. University of Ontario Institute of Technology, Oshawa, Canada, 2005.
- [98] S.O. Hansson, Promoting inherent safety, Process Safety and Environmental Protection, vol. 88, issue 3, pp. 168-172, May 2010.
- [99] T.A. Kletz, Inherently safer design-its scope and future, Process Safety and Environmental Protection, vol. 81, issue 6, pp. 401–405, 2003.
- [100] R. Srinivasan and S. Natarajan, Developments in inherent safety: A review of the progress during 2001-2011 and opportunities ahead, Process Safety and Environmental Protection, vol. 90, issue 5, pp. 389-403, Sep. 2012.

- [101] T. Businaro, I.L. Conti and I.M. Conti, Fail-Safe circuits for nuclear protective systems, IEEE Transactions on Nuclear Science, vol. 11, issue 2, pp. 64-70, 1964.
- [102] T. Tsunoda, S. Gotoh and E. Suzuki, A fail-safe reactor safety system, Journal of Nuclear Science Technology, vol. 4, issue 12, pp. 614–622, 1967.