ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/308733588

A review of defences against common cause failures in reactor protection systems

Conference Paper · September 2015
DOI: 10.1109/ICRITO.2015.7359232

CITATIONS
0

READS
45

4 authors, including:

Manoj Kumar
Department of Atomic Energy
21 PUBLICATIONS **54** CITATIONS
SEE PROFILE

Ashutosh Kabra
Bhabha Atomic Research Centre
11 PUBLICATIONS **38** CITATIONS
SEE PROFILE

Gopinath Karmakar
Bhabha Atomic Research Centre
18 PUBLICATIONS **42** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project Smart Energy View project

All content following this page was uploaded by Manoj Kumar on 11 May 2018.

The user has requested enhancement of the downloaded file.

A Review of Defences against Common Cause Failures in Reactor Protection Systems

Manoj Kumar, Ashutosh Kabra, G. Karmakar, P.P Marathe

Bhabha Atomic Research Centre,

Mumbai, INDIA - 400085

{kmanoj, kabra, gkarma, cnidppm}@barc.gov.in

Abstract— **Redundancy is essential for achieving fault tolerance and higher dependability attributes. Redundancy by means of replication of identical units is widely used and under the assumption of random failures, it proves to be beneficial also. But common cause failures (CCFs) are threat to such redundancy schemes. With the increasing use of computer-based/electronic programmable systems in critical applications, CCFs are becoming major contributors to systems failures.**

The paper briefly reviews the phenomena of CCFs, its potential sources, triggering mechanisms, propagation and defence measures. It also reviews CCF models and comments on their limitations.

A reactor protection system (RPS) is one of the safety critical systems in a nuclear power plant (NPP). A computer based RPS of a new NPP is taken for CCF case study. The system design is analyzed for its capability in preventing/reducing potential sources, triggering mechanisms and barriers against propagation of CCFs. The paper compares the CCF defence mechanisms employed in the new RPS along with two other recent RPSs of two reputed NPPs – AP1000 and Areva.

***Keywords*— common cause failures, common mode failures, dependent failures, diversity, reactor protection system**

I. INTRODUCTION

It is well understood, if failures of all redundant components/channel are statistically independent events, reliability can be significantly improved through the use of redundancy in the design. However, multiple dependent/common cause failures of redundant components are not rare; estimate in the nuclear power industry indicate that 1-20% of all hardware failures are of common-cause variety [1]. As CCFs nullify the redundancies, hence these affect reliability and safety of the systems. A through understanding of the phenomenon and application of preventive/defence measure is the only way to meet CCF criterion [2] for any safety system.

A common cause failure (CCF) is a failure where:

- Two or more items fail within a specified time such that the success of the system mission would be uncertain.
- Item failures result from a single shared cause and coupling factor (or mechanism)

Before proceeding further with CCF, there is a need to understand the independent, dependent and cascade failures.

Independent failures are one where failure of a component does not affect the probability of failure of another component. E.g. consider two items, 1 and 2, and let E_i denote the event that item i is in a failed state. The probability that both items are in a failed state is

$$\Pr(E_1 \cap E_2) = \Pr(E_1 | E_2) \cdot P(E_2) = \Pr(E_2 | E_1) \cdot P(E_1) \quad (1)$$

The two events, E_1 and E_2 are said to be statistically independent if

$$\Pr(E_1 | E_2) = \Pr(E_1) \text{ and } \Pr(E_1 | E_2) = \Pr(E_1 | E_2)$$

$$\text{then } \Pr(E_1 \cap E_2) = \Pr(E_1) \cdot P(E_2) \quad (2)$$

Note that when $E_1 \cap E_2 = \varnothing$, then $Pr(E_1 \cap E_2) = 0$ and $Pr(E_1|E_2) = 0$. A set of events cannot be both mutually exclusive and independent.

When failure of one component does affect the probability of failure of another component, such failures are referred as dependent failures. E.g. two items, 1 and 2, are dependent when

$$\Pr(E_1 | E_2) \neq \Pr(E_1) \, and \, \Pr(E_2 | E_1) \neq \Pr(E_2) \quad (3)$$

Example, consider two items that influence each other by producing heat. When one item fails and is "down" for repair, the other item will have an improved operating environment, and its probability of failure is reduced. The example illustrates a case where probability of failure of a component is reduced due to failure of another component. While in reliability much emphasis is on dependent failure where failure of one component increases the chance of failure of another component(s).

Cascading failure is a sequence of item failures where the first failure shifts its load to one or more nearby items such that these fail and again shift their load to other item, and so on. Cascading failures are sometimes referred to as a Domino effect.

The dependent failures mainly comprise of CCF and cascade failures, while CCFs are due to common cause, cascade failures are due to failure of another component. In literature pertaining to modelling of dependent failures, cascaded failures are modelled as CCFs.

The common cause failures shall be accounted for during reliability, safety and risk analysis. In literature, a number of CCF models have been proposed, which are discussed in section 1.C.

Reactor protection system (RPS) plays an important role in achieving safety in a nuclear power plant (NPP), as it shuts down the plant to maintain the integrity of its core and coolant system pressure boundary in case plant parameters exceeds the specified limits.

978-1-4673-7231-2/15/$31.00 ©2015 IEEE

A new nuclear power plant (NPP) named as Indian Pressurized Water Reactor (IPWR) is being designed by BARC. RPS of this NPP is being designed in compliance with international nuclear standards, guides and practices. The aim of the paper is to analyze the CCF defence mechanisms/prevention measures employed in the design of RPS. The paper also presents a comparison of CCF defences of IPWR RPS along with other two RPSs – AP1000 and AREVA.

The paper is organized as follows: a brief discussion on CCF definitions, models, limitations and defence mechanisms is given in section II. Section III briefly describes the proposed architecture and features of RPS of IPWR, while section IV provides its comparison of defence mechanisms against CCFs with two other contemporary reactors. Summary follows up in section V.

II. Background

Despite the abundance of literature on Common Cause Failure, there are still some inconsistencies and misinterpretation over its definition. This is predominately because the definition of a Common Cause Failure and the scope of Common Cause Failure modeling within a particular system may be different. However, Smith and Watson [3] proposed that a CCF definition should include the following:

- The items affected are unable to perform as required
- Multiple failures exist within (but not limited to) redundant configurations
- The failures are "first-in-line" type of failures and not the result of cascading failures
- The failures occur within a defined critical time period (e.g., the time a plane is in the air during a flight)
- The failures are due to a single underlying defect or physical phenomenon (the "common cause")
- The effect of failures must lead to some major disabling of the system's ability to perform as required

A. Definitions

Some widely used CCF definitions, specific industry-wise, are given below:

1) Nuclear industry (NEA, 2004): [4] [5] [6] [7]

"A dependent failure in which two or more component fault states exist simultaneously or within a short time interval, and are a direct result of a shared cause."

2) Space industry (NASA PRA guide, 2002): [4] [5] [6] [7] [8]

"*The* failure *(or unavailable state) of more than one component due to a shared cause during the system mission.*"

3) Process industry (IEC 61511, 2003): [5]

"*Failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure.*"

B. Root Causes and coupling factors

Common cause failures result from the existence of two factors – failure cause and coupling factor. Failure cause is the condition that the component failure can be attributed to. The coupling factor is the propagation mechanism that enables failure of multiple components. Defences are the parts of the system that protect against the failure cause or the coupling factor.

Examples of root causes can be grouped as *pre-operational* and *operational* causes. E.g. design, manufacturing, construction, installation, and commissioning errors are example of pre-operational, while operation and maintenance-related and environmental stresses are example of operational causes.

Examples of coupling factors are same design (principles), same hardware, same function, same software, same installation staff, same maintenance & operational staff, same procedures, same system/item interface, same environment and same (physical) location for redundant units. When design diversity is applied in redundant systems, more than one coupling factors change, simultaneously.

The experience of CCF occurrences in NPPs shows that the following types of causes are dominant [7]:

- Latent faults which are related to faults in the requirement specification.
- Latent faults which are introduced during maintenance.
- The triggering of latent faults during maintenance activities by causing partly specific system states or partly invalid data which do not represent the actual plant state.

C. Models

The phenomena of CCFs have been recognized as a consideration in design of NPPs for quite some time. The first major use of a CCF model was in WASH 1400 probabilistic risk assessment in 1975 [6]. Since then, over 30 different CCF models have been proposed. These models can be broadly classified as follows:

- **Direct estimate** involves using the actual number of demands and number of observed failures with multiplicity, directly from the data set. E.g. Basic Parameter Model [10][11][14].
- **Ratio models** are based on the hypothesis that system specific estimates for CCF can be made by combining generic average ratio parameters with system specific single/total failure rates. An example includes Beta Factor model [9].
- **Shock models** are based on the hypothesis that each component within a common cause component group undergoes shock according to Poisson process, while failure of a component is a Beroulli trial. E.g. Binomial Failure Rate Model, Binomial with Lethal shocks.
- **Interference models** predict the number of failures by assuming random variable for component strength and load. E.g. Common Load model.

- **Other models** include Reliability Cut off method, Unified Partial method and Influence Diagram Model [15] etc.

D. Limitations of CCF models

The CCF models have focused on empirical relationships which allow the quantification of PSA (Probabilistic Safety Assessment)/PRA (Probabilistic Risk Assessment) [12][13] models without a detailed definition of failure causes and coupling mechanisms. The limitation of this approach is that very little insight can be provided into the nature of CCFs.

The CCF models mainly model dependencies with probabilistic relationship between like and non-like components. These models lack to quantify the systematic – design, interaction and stress – dependencies between components and sub-systems. The design dependency exits between systems driven by software or having programmable components. The computer based systems (driven by software) interact with other systems via communication links, which is a concern of multiple failures due to interactions.

In such scenarios, qualitative assessment by evaluating CCF preventive measures at various stage of the system life-cycle is only method to demonstrate the compliance to CCF criterion..

E. Prevention of CCFs

Diversity is an effective antidote for CCF. Diversity relies on 'independent' generation of 'different' implementations. As per [1], methods for defences against CCFs are, item diversity, isolation, shielding, containment, separation, design margin and human error prevention. Design measures to prevent coincidental failure of I&C systems in NPPs [7] are as follows:

- Principal of independence
- Design of independent I&C systems
- Functional diversity
- Avoidance of failure propagation via communication paths
- Design measures against system failure due to maintenance activities
- Integrity of I&C system hardware
- Precaution against dependencies from external dates or messages
- Assurance of physical separation and environmental robustness

III. RPS OF IPWR

RPS is used for automatic shutdown of NPP whenever NPP parameters go beyond the acceptable limit for more than acceptable time. RPS gets various parameters (nuclear as well as process) from various sensors/transducers to detect any abnormal operating condition. It initiates protection action in case of any abnormality. Initiation of the protection action results in removal of electrical power from the control cum shutoff rod drive mechanism (CSRDM) coils, allowing the rods to fall by gravity into the core. It leads to quick insertion of negative reactivity to the core, which ensures the shutting down of the reactor and safety of nuclear power plant and personnel.

A. Architecture

The proposed RPS of IPWR is a computer based system with four identical redundant trains. Architecture of RPS is shown in Fig. 1. Each train has two diverse channels (shown in two different colours) and each channel processes diverse set of parameter to provide protection against CCF. The channels in each train exchange their parameters trip information with corresponding channels of other trains. The channel generates its output based on 2-out-of-4 (*2oo4*) voting of parameters trip from all other channels. The train output is based on the 1-out-of-2 (1oo2) of outputs of both channels. The train output is used to trip the Reactor Trip Breakers (RTBs) of that particular train. Diversity is also provided for tripping reactor trip breakers (RTBs) through the under voltage trip mechanism and the shunt trip mechanism. RTBs are again configured according to *2oo4* co-incidence logic in two physically separated rooms as shown in Fig. 2.

There is also a provision for generating reactor trip signal manually for individual train by means of hardwired switch from MCR (Main Control Room) and BCR (Backup Control Room). A hardwired switch on safety panel is provided for reactor trip initiation in each train, which bypasses the RPS digital processing part.

Tripping of RTBs of any two trains cuts-off power supply to the Control Rod Drive Mechanism Control System (CSRDMS) coils. As a result, the control cum shut-off rods (CSRs) fall under gravity into the core and reactor shuts down.

B. Features

The proposed architecture has two unique features, (i) dual controller (two channels) in each train and (ii) intermediate *2oo4* coincidence logic for each reactor trip parameter. This approach is followed so that each train is partitioned in both vertically and horizontally. The following features are provided in the proposed architecture of RPS in conformance with IEC Std. 62340 [7]:

- Functional independence among the redundant trains of RPS with provision of separate sensors, processing units, RTBs and power supplies for each train.
- Functional diversity is provided within a train of RPS. Diverse sensor signal and algorithm are used to detect a abnormal plant condition. This implies that both the channels shall have different software.
- Diverse controller in each train of RPS to provide equipment diversity. This implies that both the channels shall have different hardware.
- RPS equipment qualification for worst case environmental condition as per IEEE Std. 323 [16] and seismic qualification as per IEEE Std. 344 [17]. It will eliminate the possibility of CCFs due to any external event.
- Each train of RPS is located in physically separate room in the safe guard building. RTBs are also

configured according to *2oo4* co-incidence logic in two physically separated rooms as shown in Fig. 2. This arrangement ensures that fire in one room shall not prevent reactor trip actuation.

- Redundant cables are routed via different paths.
- Diverse mechanisms are provided to de-energize RTBs.
- Isolation devices are incorporated into data links and communication networks that connect redundant trains. The isolation devices ensure that credible faults, such as short circuits, open circuits, or the application of credible fault voltage do not propagate between systems. RPS logic also prevents the propagation of failures through communication links.
- Provisions like indication of bypasses, automatic removal of operating bypasses based upon plant conditions, interlocks to prevent bypassing of multiple trains at a time, identification and tagging, well defined plant operating procedures will reduce the probabilities of O&M errors.

IV. COMPARATIVE ANALYSIS

The architecture of proposed RPS is compared with 2 other contemporary RPS of Westinghouse AP1000 and AREVA. CCF defences incorporated in the design at architecture level, robustness of design, layout and operation & maintenance of these are compared and given in Table 1.

From the comparison given in Table 1, all the three RPSs seem to satisfy all the features as per the preliminary details available in literature. Although, communication within train and across train is stated to be independent, but methods to restrict propagation of failures other that isolation and data integrity checks are not clear.

Implementing equipment and functional diversity has repercussions on developmental and operation & maintenance cost. Hence, most of the architectures lack this.

V. SUMMARY

The paper consolidates information regarding CCFs to provide a better insight regarding common cause failures of C&I systems. It throws light on the limitations of CCF models in general and pertaining to computer-based systems. It also list recommended practices during design and operational phases to prevent CCFs.

A list of parameters to access a system's defence against CCF are given. These parameters are based on literature survey. Three RPS of contemporary reactors (AP1000, Areva and IPWR) are compared for these parameters.

The comparison given here is in binary form, a more detailed comparison on a scale of 3 or 5 will be better. This will help in indicating relative conformance of one system compared to other. This will indeed require more information about the systems as well.

ACKNOWLEDGMENT

We thankfully acknowledge Shri C. K. Pithawa, Director, E&IG and Shri Y. S. Mayya, Associate Director, E&IG for encouraging us and extending support to pursue this work. We also thank Dr. A. P. Tiwari, Head, RCSDS, BARC for his continuous support and guidance for this work.

REFERENCES

[1] P. J. Rutledge and A. Mosleh, "Dependent-Failures in Spacecraft: Root Causes, Coupling Factors, Defenses, and Design Implications," in *Annual Reliability and Maintainability Symposium*, 1995, pp. 337-342.

[2] IEEE Std. 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, 2009, IEEE.

[3] A. M. Smith and I. A. Watson, "Common cause failures – a dilemma in perspective," *Reliability Engineering*, vol. 1, no. 2, pp. 127-142, 1980.

[4] P. Hokstad and M. Rausand, , K. B. Mishra, Ed.: Springer, 2012, ch. Common Cause Failure Modeling: Status and Trends, pp. 621-640.

[5] M.A. Lundteigen and M. Rausand, "Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing," *Journal of Loss Prevention in the process industries*, vol. 20, no. 3, pp. 218-229, 2007.

[6] A.N. O'Connor, "A general cause based methodology for analysis of dependent failures in system risk and reliability assessments," 2013.

[7] IEC Std. 62340, Nuclear Power Plants - instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF), 2007, IEC.

[8] J.E. Stott, B.T. Britton, R.W. Ring, F. Hark, and G.S. Hatfield, "Common cause failure modeling: aerospace vs. nuclear," in *Proceedings of the 10th International Conference on Probabilistic Safety Assessment and Management*, 2010.

[9] P. Hokstad, A. Maria, and P. Tomis, "Estimation of common cause factors from systems with different numbers of channels," *IEEE Transactions on Reliability*, vol. 55, no. 1, pp. 18-25, 2006.

[10] T. Lilleheier, "Analysis of commom cause failures in complex safety instrumented systems," 2008.

[11] P.H. Kvam and J.G. Miller, "Common cause failure prediction using data mapping," *Reliability Engineering & System Safety*, vol. 76, no. 3, pp. 273-278, 2002.

[12] M. Stamatelatos et al., "Probabilistic risk assessment procedures guide for NASA managers and practitioners," 2011.

[13] I.A. Watson, "Analysis of dependent events and multiple unavailabilities with particular reference to common-cause failures," *Nuclear Engineering and Design*, vol. 93, no. 2, pp. 227-244, 1986.

[14] L. Xie, J. Zhou, and X. Wang, "Data mapping and the prediction of common cause failure probability," *Reliability, IEEE Transactions on*, vol. 54, no. 2, pp. 291-296, 2005.

[15] A. Zitrou, T. Bedford, and L. Walls, "An influence diagram extension of the unified partial method for common cause failures," *Quality Technology & Quantitative Management*, vol. 4, no. 1, pp. 111-128, 2007.

[16] IEEE Std. 323, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, 2003, IEEE.

[17] IEEE Std. 344, Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, 2004, IEEE.

[18] Westinghouse AP1000 Design Control Document. (2005, Jan.) USNRC. [Online]. http://pbadupws.nrc.gov/docs/ML1117/ML11171A465.pdf

[19] AREVA Design Control Document. (2007, Mar.) USNRC. [Online]. http://pbadupws.nrc.gov/docs/ML1322/ML13220A734.pdf

TABLE 1
COMPARISON OF DEFENSES AGAINST CCFS

Criteria	**Parameter**		**AP1000** [18]	**AREVA** [19]	**IPWR**
Architecture	within a train	Independence (Communication)	√	√	√
		Independence (Functional)	√	√	√
		Functional diversity	√	√	√
		Equipment Diversity	X	X	√
	Among trains	Independence (Communication)	√[1]	√[1]	√
		Independence (Sensors)	√	√	√
		Independence (RTBs)	√	√	√
		Functional diversity	X	X	X
		Equipment Diversity	X	X	X
		Diversity in RTBs	√	X	√
		Power Supply independence	√	√	√
Robustness	Environmental robustness		--	--	√
	EMI/RFI qualification		--	--	√
	Integrity of I&C system hardware		--	--	√
	Integrity of I&C system Software		--	√	√
Layout	Physical separation		√	--	√
	Elevation		--	--	√ (+10.5m)
Operation & Maintenance	Cope with operator error		√	√	√
	Cope with failure due to maintenance activities		√	√	√

√: Yes (available); X: No (not available); -- Information not available

[1]: Nuclear instrumentation systems (NIS) sensors for start-up and intermediate ranges are only two. One sensor is shared between trains A & B, while other is shared between trains C & D.

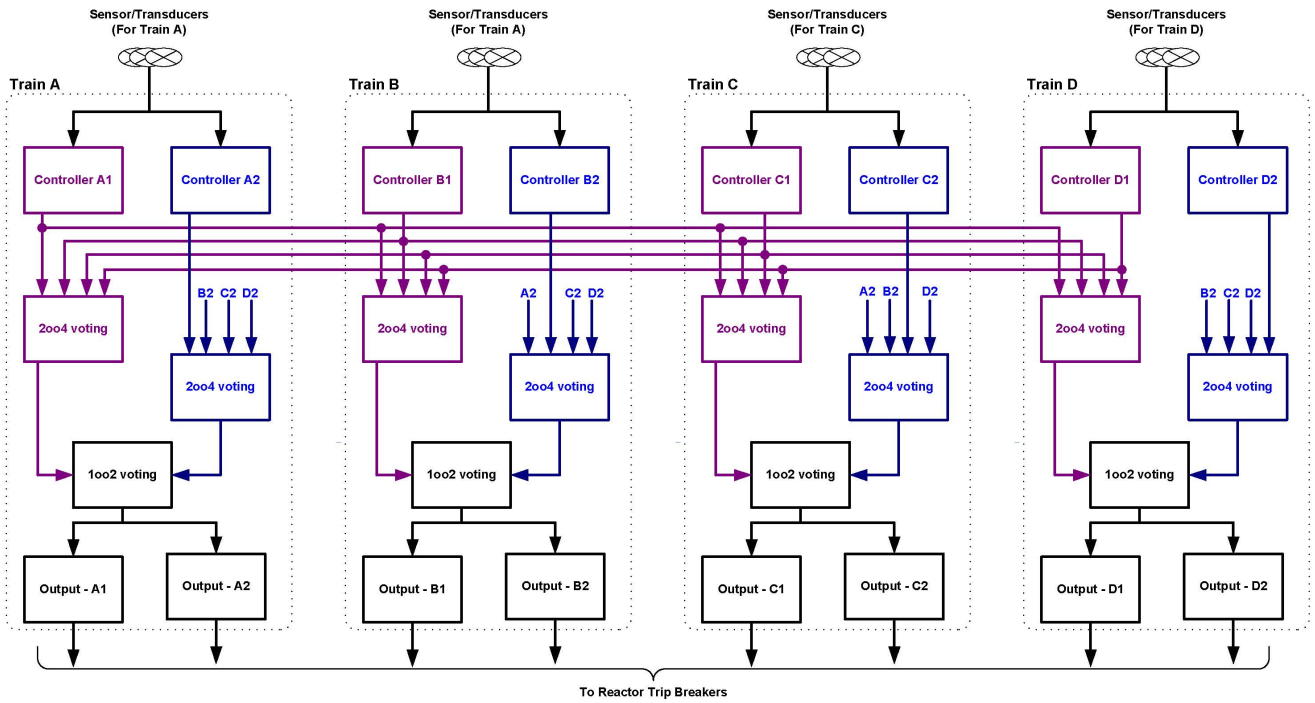

Fig. 1: Architecture of Reactor Protection System (RPS). All the four trains are identical. Each train has two diverse channels (shown in two different colours) and each channel processes diverse set of parameter. The channels in each train exchange their output with corresponding channels of other trains. The channel generates its output based on 2oo4 voting of parameters from all other channels. The train output is based on the 1oo2 of outputs of both channels.

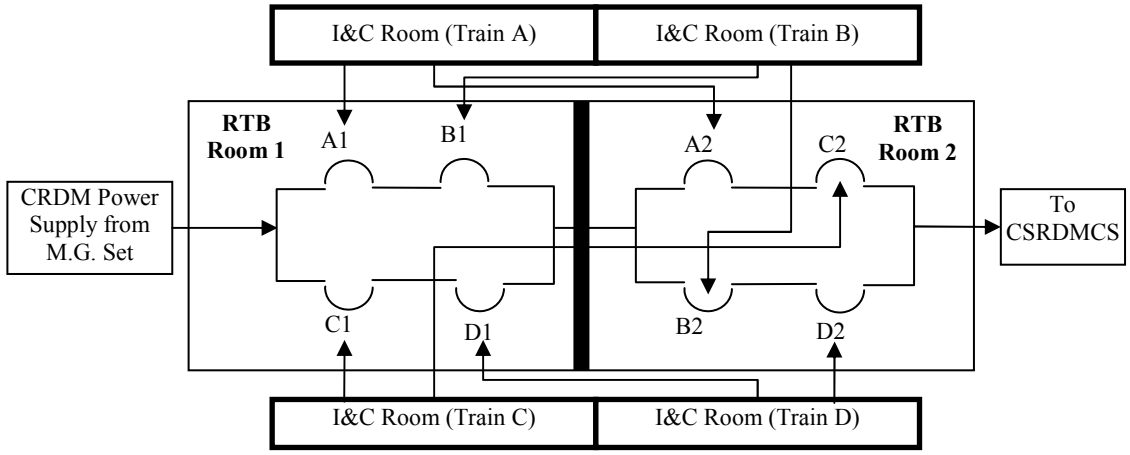

Fig. 2: Configuration of Reactor Trip Breakers (RTBs). Outputs of RPS trains (A1, A2, B1, B2, etc) are used for controlling power supply to CSRDMCS based on 2oo4 voting.

View publication stats