Safety Analysis of Shutdown System in Nuclear Power Plants through Petri Nets

Abhishek
Dept. of Information Technology, NIT Karnataka,
Surathkal, Mangalore
abhishek.211it001@nitk.edu.in

Ashwani Kumar
Dept. of Information Technology, NIT Karnataka,
Surathkal, Mangalore
ashwanikumar.211it013@nitk.edu.in

Prasanna Kumar
Dept. of Information Technology, NIT Karnataka,
Surathkal, Mangalore
pkrb.211it047@nitk.edu.in

Jaheer Khan
Dept. of Information Technology, NIT Karnataka,
Surathkal, Mangalore
jaheerkhan.211it026@nitk.edu.in

Madhusmita Das
Dept. of Information Technology, NIT Karnataka,
Surathkal, Mangalore
madhusmitadas.197it004@nitk.edu.in

Biju R Mohan
Dept. of Information Technology, NIT Karnataka,
Surathkal, Mangalore
biju@nitk.edu.in

***Abstract*—Addressing the critical need for rigorous safety analysis, the research focuses on the intricate shutdown mechanisms, particularly the Rod Control System and Poison Injection System. The methodology commenced with exhaustive system requirements gathering to grasp the operational nuances and emergency protocols. A meticulous Petri Net representation followed, encapsulating system components and concurrent processes within a cohesive model. The framework facilitated rigorous safety checks, formal verification, and simulation-based optimization. Through iterative design and validation against established research, the model underwent continuous refinement. The findings illuminate the robustness of safety protocols and offer a transformative outlook on shutdown procedures, laying a foundation for further research and practical implementation to secure NPP operations.**

***Index Terms*—Petri Nets, Nuclear Safety, Shutdown Procedures, Control Systems, Safety Verification, Risk Modeling, Emergency Protocols, Reliability Analysis, Criticality Management, Simulation, Optimization**

I. INTRODUCTION

Nuclear power plants need to be super safe, especially the part that controls the reactor's rods. If this control system fails, it could lead to really bad things like meltdowns or radiation leaks [1]. To understand and make sure this control system works well, we used a tool called Petri nets, which helps us create models to see how things interact.We compared this model with another one using a reliability block diagram to check how reliable and safe the system is [2]. Aside from rod control, there's another safety thing called a poison injector in the power plant. It stops the reactor in emergencies. Figuring out how well it works is vital for the plant's safety, and we're using advanced methods to model its behavior accurately.These efforts are crucial for making sure nuclear power plants are safe while generating electricity [1].

II. RELATED WORK

A. Overall Working of system

1) Rod control: The rod control system (RCS) regulates the displacement of control rods in a nuclear reactor, which absorb neutrons and control the rate of fission. The RCS consists of several components:

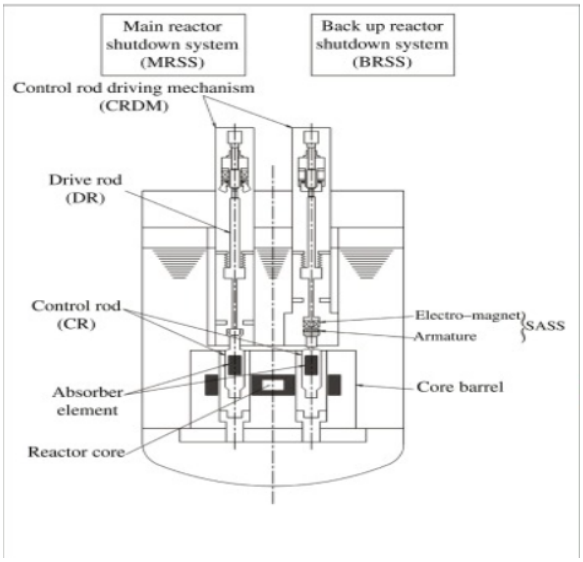

Fig. 1. Working of Rod control System

Control rod drive mechanism (CRDM): Moves the control rods and provides feedback on their position to the RCS controller. RCS controller: Monitors reactor parameters and calculates the optimal position of the control rods. It can operate in different modes. RCS power supply: Provides electrical power to the RCS controller and the CRDM. RCS instrumentation: Measures and displays the reactor parameters and the control rod positions.

The RCS performs various functions, such as reactor startup, power maneuvering, axial offset control, reactor shutdown, and emergency shutdown (SCRAM).

2) Poison Injector System: The poison injector system injects a neutron-absorbing substance into the reactor core for

emergency shutdown. It's one of two independent shutdown systems in Canadian nuclear power reactors, the other being the control rod system.

Components of the poison injector system include:
a) Poison Tanks: Store liquid poison, connected to injection tubes via pipes and valves.
b) Injection Tubes: Deliver liquid poison from tanks to the reactor core.
c) Actuation System: Triggers poison injection into the core upon receiving a signal from the reactor shutdown system.
d) Instrumentation System: Measures and displays poison injector system parameters.

The system plays a crucial role in nuclear power plant safety, performing functions like emergency shutdown and power manipulation.

B. Background

The control of a nuclear reactor involves two vital systems: the Rod Control System and the Poison Injector System. The rod control system governs the movement of control rods that regulate the fission rate within the reactor core. The poison injector system serves as an independent shutdown mechanism, injecting a neutron-absorbing substance into the reactor core during emergencies.

C. Literature Survey

The design the shutdown system of a nuclear power plant is a difficult task that ensures the safety and reliability of the reactor operation. Shutdown system consists of two subsystems: the rod control system and the poison injection system, which are responsible for inserting control rods and injecting neutron absorbers such as such as boric acid or gadolinium nitrate into the reactor core to stop the fission chain reaction.

Petri net can be used to model and analyze the shutdown system , which are a graphical and mathematical tool for describing systems that are distributed, parallel, nondeterministic,stochastic[3]. Petri nets have been widely used in various domains, such as computer science, engineering, social sciences.Petri nets to analyze the shutdown system of a nuclear power plant , which models the rod control system and the poison injection system using Petri nets and simulates their operation under normal and abnormal conditions.

A worldwide examination of pressurized water reactor (PWR) nuclear power plants (NPPs) gives us an overview, talking about how they've developed technically, been put into action, and the challenges they face [4]. Recognizing poison injectors as crucial safety systems, this review emphasizes that the Reactor Protection System (RPS) activates them based on reactor parameters [5]. The issues found in existing literature inspire our research project — to fill these gaps using hybrid Petri nets (HPNs) [6]. HPNs, an extension of Petri nets, can model both discrete and continuous dynamics. Our method aims to handle noise, disturbances, uncertainties, and failures, dealing with the limitations in current models. Additionally, the project aims to prove its effectiveness through a case study of a PWR shutdown system [6].

In summary, this literature survey points out the critical role of shutdown system design and verification in NPPs.It pinpoints the issues in existing approaches and stresses the need for a comprehensive and integrated modeling approach [6]. The proposed research using HPNs and hybrid automata aims to contribute to the progress of knowledge and practices in NPP shutdown system design and verification. The project's scope includes addressing current gaps, including realistic dynamics, and offering a more quantitative understanding of system behavior [6].

III. Methodology

In the Nuclear Power Plant(NPP) there are two major parts that work as shutdown system:
1. Rod Control System (RCS)
2. Poison Injector System (PIS)

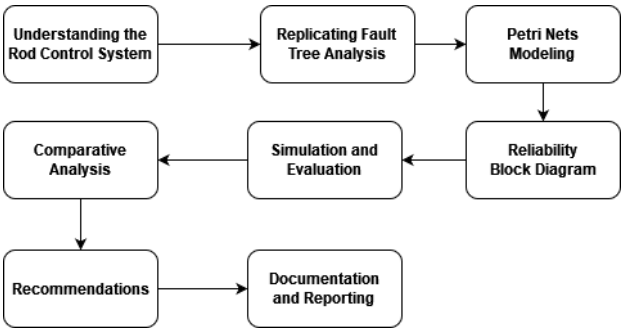

Fig. 2. Workflow of Rod control System

1. Rod Control System :
In this study, we aimed to analyze the reliability of the Rod Control System (RCS) in Advanced Pressurized Water Reactors (APWRs) by enhancing a Fault Tree Analysis (FTA) from a reference paper with additional methods such as Petri nets and Reliability Block Diagrams (RBDs). The process involved:

A. Understanding Fault Tree Structure:

We carefully examined the fault tree's structure and logic, identifying potential causes of RCS failure using basic/intermediate events and logical gates.

B. Converting Fault Tree to Petri Net Model:

The fault tree was transformed into a Petri net model, a graphical tool capturing dynamic system behavior with places, transitions, arcs, and tokens.

C. Converting Petri Net Model to RBD:

The Petri net model was converted into an RBD, representing the reliability structure of the system with blocks and connectors.

D. Verification and Analysis of Models:

We verified and analyzed the models using tools like reachability analysis, simulation, and formal methods. Metrics such as failure rate and availability function were used for evaluation. Results were compared with the reference paper and other sources.

E. Data Gathering:

The datasets that were used in this study were mostly obtained from various reliable sources, including these:

- U.S. Nuclear Regulatory Commission (US NRC) Report: The datasets from their reports were selected as the base data source due to it's credibility and comprehensiveness of the data. US NRC have extensive experience in these fields of nuclear safety and related matters, making their data highly valuable for our analysis[7].
- Norman P. Cheremisinoff's Book: His book provided a lot of data and insights, making his book a helpful resource in our study. The data from this source gave a wide view on the RCS and contributed to the betterment of the analysis[8].
- M. Modarres and M. Kaminskiy's Paper: This paper published by M. Modarres and M. Kaminskiy is a great work that contains essential information on the RCS of a PWR. Academic papers and sources, like the mentioned above, provided thorugh research findings and works that are necessary in the construction of reliable models[9].

The data gathered from these sources served as the base for our reliability analysis, especially for the RCS components and it's subsystems. This data allowed us to assign accurate values to our Petri net and RBD models, enabling correct simulations and calculations based on that data.The datasets selected are directly related to the RCS of a PWR. This relation ensures that the data used is suitable for assigning values to our models, which leads accurate results.

F. Novelty:

In our group project on Rod Control System (RCS) reliability in Pressurized Water Reactors (PWRs), we introduced novel methodologies using the SHARPE tool, known for its diverse analysis features. Comparing our Petri net and Reliability Block Diagram models with fault tree results provided a comprehensive evaluation. Exploring different modeling tools' pros and cons enhanced our understanding of RCS reliability analysis in PWR reactors. Analyzing changes in data, component modifications, and failure introductions revealed insights into reliability and availability variations. Through these innovative approaches and comparisons, our project made significant contributions to RCS reliability research in PWR reactors, offering a fresh perspective within the nuclear power industry

2. Poison injection system

However, we have also found some limitations and gaps in the literature that could be addressed by our project. For example: The literature only focuses on specific poison injector systems for specific reactor types and does not compare them with other types of poison injector systems or other types of reactors. A more comprehensive comparison and evaluation of different poison injector systems for different reactor types could be useful to identify the optimal design for each case.

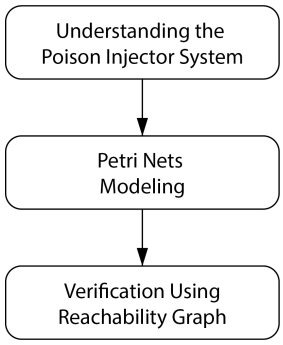

Fig. 3. Workflow of Posion Injection System

The literature does not provide much detail about the technical aspects or challenges of poison injector systems or other safety systems. A more in-depth analysis of the design principles, operational modes, failure modes, testing methods, and regulatory standards of poison injector systems or other safety systems could be helpful to improve their reliability and performance. To overcome from the given gap in literature we followed these steps:

- Step 1: Define the scope and objectives of the model. We decided to model a generic poison injector system for a PWR nuclear power plant, as it is the most common type of reactor in the world. We also decided to model the normal operation mode and two abnormal scenarios: a large break LOCA and a failure of wired shutdown systems.
- Step 2: Identify the main components and events of the system. We identified the following components and events of the poison injector system:
  Components :
  - Reactor core: The part of the reactor where the fission reaction takes place and generates heat.
  - Poison tank: The container that stores the neutron poison (such as boron) that can be injected into the reactor core to shut down the fission reaction.
  - Poison valve: The valve that controls the flow of neutron poison from the poison tank to the reactor core.
  - RPS: The system that monitors the reactor parameters (such as pressure, temperature, power level, etc.) and initiates the shutdown sequence when certain conditions are met.

  Events:
  - Normal operation: The event when the reactor operates normally under steady state conditions.
  - Shutdown signal: The event when the RPS sends a signal to activate the poison injector system.

  - Shutdown completion: The event when the reactor core reaches a subcritical state and stops the fission reaction.
  - Logical Condition: this event sends a condition that the token will wait in the LC wait condition until the valve is not closed off the control rod.
- Step 3: Construct the Petri net model using places, transitions, arcs, tokens, and markings. We used a graphical tool to draw the Petri net model. Markings are represented by the initial distribution of tokens in places.
- Step 4: Simulate the behavior of the Petri net model under normal and abnormal conditions. We used a simulation tool to run the Petri net model and observe its behavior under different scenarios. We recorded the changes in markings and transitions firing as the simulation progressed.

IV. Conversion Rules for RBD and Petri Nets

A. Conversion Rules for RBD

1) AND Gate:

a) FTA to RBD: An AND gate in Fault Tree Analysis (FTA) represents a system that fails if all of its input events fail. In Reliability Block Diagrams (RBD), an AND gate is represented by a series (logical AND) of components. The system fails if any one of the components fails.

b) RBD to FTA: An AND gate in RBD, where components are in series, can be converted to an FTA by considering each component as a separate event contributing to the top event's failure.

2) OR Gate:

a) FTA to RBD: An OR gate in FTA represents a system that fails if at least one of its input events fails. In RBD, an OR gate is represented by parallel components (logical OR). The system fails if all components fail.

b) RBD to FTA: An OR gate in RBD, where components are in parallel, can be converted to an FTA by considering each component as a separate path leading to the top event's failure.

B. Conversion Rules for Petri Nets

1) AND Gate:

a) FTA to Petri Nets: An AND gate in FTA represents a system failure when all of its input events fail. In Petri Nets, an AND gate can be represented by a transition that is enabled only when all of its input places have tokens. Create a place for each basic event contributing to the AND gate and connect them to a transition. The transition fires only when all input places have tokens.

b) Petri Nets to FTA: An AND gate in Petri Nets can be translated into FTA by considering the firing of the transition as a failure event. Each input place corresponds to a basic event in FTA, and the firing of the transition corresponds to the top event's failure.

2) OR Gate:

a) FTA to Petri Nets: An OR gate in FTA represents a system failure when at least one of its input events fail. In Petri Nets, an OR gate can be represented by multiple transitions, each associated with one of the input places. The transitions are enabled independently of each other. Tokens in any one of the input places enable the associated transition, representing the occurrence of the corresponding event.

b) Petri Nets to FTA: An OR gate in Petri Nets can be translated into FTA by considering the firing of any of the transitions as a failure event. Each transition corresponds to a basic event in FTA, and the top event fails if any one of the transitions fires.

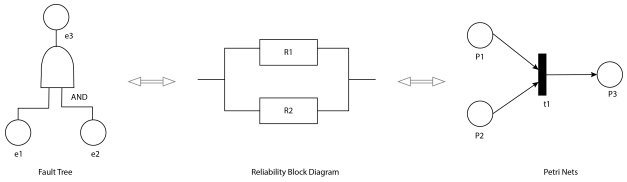

Fig. 4. Conversion Logic with AND gate

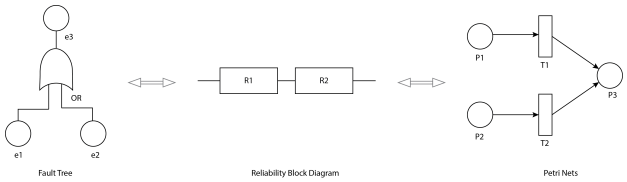

Fig. 5. Conversion Logic with OR gate

V. Results and Discussion

The following images shows FTA, RBD and Petri nets model of RCS after conversion. These were used simulated in Sharpi tool and results of those simulations and also mentioned in table below.

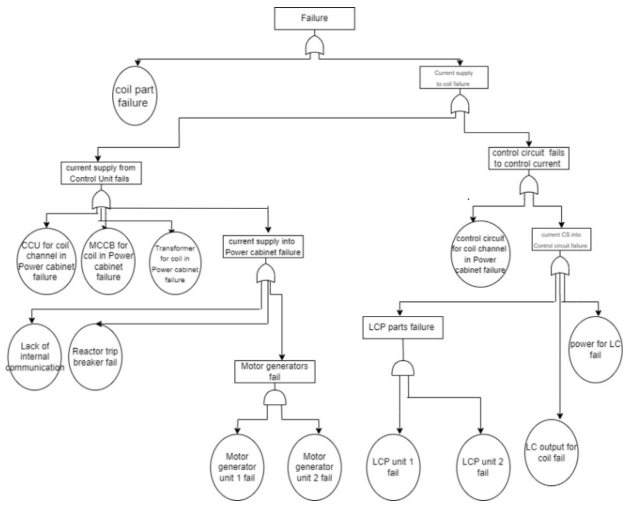

Fig. 6. FTA of Rod Control System [10]

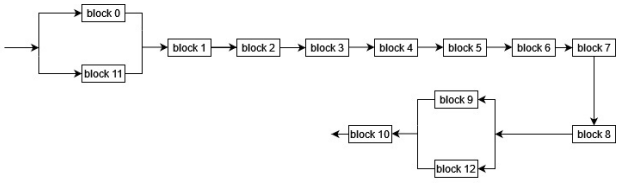

Fig. 7. RBD of Rod Control System

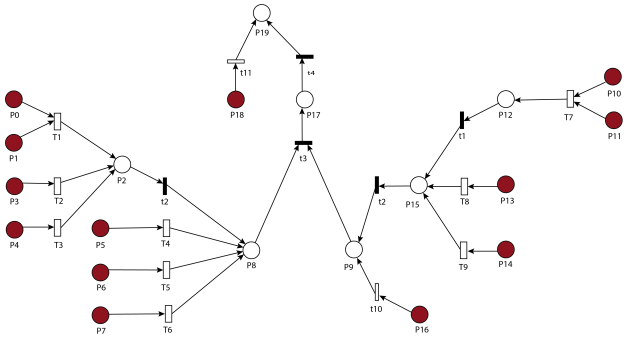

Fig. 8. Petri Net of Rod Control System

TABLE I
METRIC PERFORMACES OF RCS

	Mean Time To Failure	Variance
Fault Tree	1.53666151e+002	2.28243224e+004
RBD	1.53786795e+002	2.28591843e+004
Petri Nets	6.79386757e+005	3.54847968e+011

TABLE II
DESCRIPTION OF PETRI-NETS PLACES OF RCS

Places	Description
P0	Motor Unit 01 started.
P1	Motor Unit 02 started.
P2	Electrical supply into power cabinet
P3	Distribution panel for CRDM working
P4	Reactor trip working
P5	Control unit for gripper is working
P6	MCCB in power cabinet is working
P7	Transformer in coil is working
P8	Electrical supply from current control unit is supplied
P9	Circuit successfully controls electrical current being supplied
P10	Logical cabinet processing part 01 working
P11	Logical cabinet processing part 02 working
P12	Logic cabinet is working
P13	Power is being supplied to it
P14	Logic cabinet output part is working
P15	Current control system is working
P16	Control circuit from coil channel in power cabinet is working
P17	Electrical current supplied to coil
P18	Coil part is working
P19	System working successfully

TABLE III
DESCRIPTION OF PETRI-NETS TRANSITIONS OF RCS

Transitions	Description
T1	Motor successfully started
T2	Distribution panel activated
T3	Reactor trip worked
T4	Control gripper worked
T5	MCCB in power cabinet worked
T6	Transformer in coil worked
T7	Logical cabinets processed
T8	Power supplied
T9	Logic cabinet output given
T10	Control circuit in power cabinet worked
T11	Coil part worked
t0	Electrical current supplied
t1	Logic cabinet worked
t2	Current control system worked
t3	Electrical current from current control and circuit supplied
t4	Electrical current supplied to system

The failure of the poison injection system can lead to a dangerous increase in power, causing the design parameters to go beyond their safe limits and potentially exposing the public to radiation. This injection system is composed of various components, such as sensors, logic elements, actuators, and a specific human-machine interface, all working together to achieve its intended function. Each quick-open valve line is equipped with two vent valves, both of which are normally open during regular conditions.

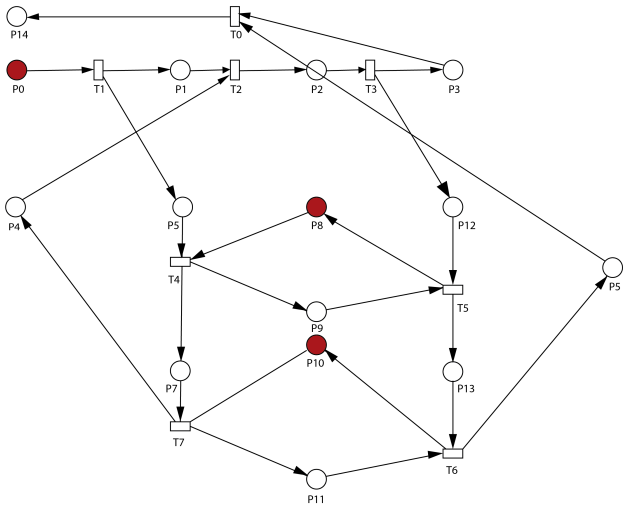

Fig. 9. Petri Net of Poison injection System

TABLE IV
DESCRIPTION OF PETRI-NETS PLACES OF PIS

Places	Description
P0	Trip parameters deviation
P1	Logical condition creation
P2	Logical condition on hold
P3	Logical condtion restored
P4	Priortize T6 over T2
P5	Reversibility properties
P6	Close vent values
P7	Vent values closed
P8	Redundant information of Quick open valve (closed state)
P9	Redundant information of Quick open valve (open state)
P10	Quick open valve (close)
P11	Quick open valve (open)
P12	De-energized open vent valve
P13	Open vent valve

TABLE V
DESCRIPTION OF PETRI-NETS TRANSITIONS OF PIS

Transitions	Description
T0	Resend signal to open Quick open valves if it fails to open
T1	Sends signal to LC to close the vent valves
T2	Hold LC at created state
T3	Restore LC and relay de-energizes
T4	Close the vent values
T5	Open all vent values
T6	Close all Quick open values
T7	Open all Quick open values

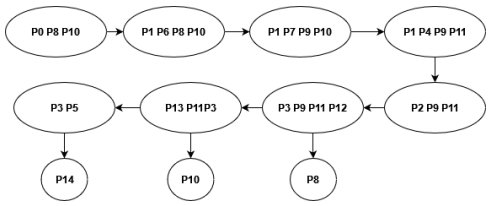

Fig. 10. Reachability graph of PIS

These vent valves relieve pressure in the line and prevent any accidental poison injection.

In this system, we use tokens to represent different aspects of its operation. Token "m1" stands for deviations from the design limits of trip parameters, while "P1" represents the creation of logic conditions, and "P2" indicates the holding state of these logic conditions. A relay is activated (token P6) to close the vent valves. Poison is injected into the moderator when the quick-open valve is opened (token P11). To enhance reliability, redundant sensor information about the quick-open valve state is monitored (token P9). We also have a mechanism in place (token P4) to prioritize one action (T7) over another (T2) in case of a race condition, ensuring that the quick-open valve opens if there's a security threat or false information about its closed state. To summarize, there are two sets of closed process networks. The first set includes P0, P1, P2, and P3. The second set is composed of P6, P7, P4, P2, P12, P8, P9, P13, P10, P11, P5, and P0. These two sets of closed process networks communicate with each other through an asynchronous MP mechanism.

VI. CONCLUSION AND FUTURE SCOPE

The research focused on safety in nuclear power plants, especially the Rod Control System and Poison Injection System. Using a detailed Petri Net framework, we mapped out how these critical systems work and interact. This approach helped us understand their day-to-day operations and emergency procedures. We also added strict safety checks and verification methods to make sure everything works as it should. The study's design and validation process, following research standards, greatly improved the reliability of shutdown mechanisms without compromising safety. The results highlight the effectiveness of current safety measures in nuclear power plant shutdown procedures. Looking forward, there are opportunities to enhance the project further. Using real-world data from nuclear plants can make our model more accurate. We're also thinking about expanding the Petri Net model to include more crucial parts like the reactor core and cooling systems. This isn't just about improving current safety plans; it's about learning how to keep nuclear plants even safer.

REFERENCES

[1] Li, Liang, Zi-Ping Huang, Peng-Bin Duan, Wei-Jie Huang, and Cong Cui. "A Kind of Monitoring System for RGL in Nuclear Power Plant." In International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant, pp. 247-253. Singapore: Springer Nature Singapore, 2021.

[2] Wu, Xiaojun, and Zhizhong Li. "A review of alarm system design for advanced control rooms of nuclear power plants." International Journal of Human–Computer Interaction 34, no. 6 (2018): 477-490.

[3] Herrmann, Jeffrey W., and Edward Lin. "Petri Nets: Tutorial and Applications." In The 32th Annual Symposium of the Washington Operations Research-Management Science Council, Washington, DC. 1997.

[4] Dusi, A. "Seismic isolation of nuclear power plants." In 15th World Conference on Earthquake Engineering. 2012.

[5] Tripathi, Manish, Lalit Kumar Singh, Suneet Singh, and Pooja Singh. "A comparative study on reliability analysis methods for safety critical systems using Petri-nets and dynamic flowgraph methodology: A case study of nuclear power plant." IEEE Transactions on Reliability 71, no. 2 (2021): 564-578.

[6] Jyotish, Nand Kumar, et al. "Reliability and Performance Measurement of Safety-Critical Systems Based on Petri Nets: A Case Study of Nuclear Power Plant." IEEE Transactions on Reliability (2023).

[7] U.S. Nuclear Regulatory Commission. (2023). U.S. Nuclear Regulatory Commission (US NRC) Report. U.S. Nuclear Regulatory Commission.

[8] Cheremisinoff, N. P. (2022). Nuclear Power Plant Safety and Mechanical Integrity: Design and Operability of Mechanical Systems, Equipment and Supporting Structures. CRC Press.

[9] Modarres, M.,and Kaminskiy, M. (2021). Reliability analysis of pressurized water reactor control rod system using Petri nets and reliability block diagrams. Reliability Engineering and System Safety, 208,107403.

[10] Bakhri, Syaiful. "Investigation of rod control system reliability of pwr reactors." KnE Energy (2016): 94-105.