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 [2] are complex systems that require high levels of safety and reliability. One of the critical components of a nuclear power plant is the rod control system, which regulates the position of the control rods in the reactor core. The control rods are used to adjust the rate of the nuclear fission reaction and to shut down the reactor in case of an emergency. A failure of the rod control system can lead to severe consequences, such as a meltdown or a radiation leak. To analyze the reliability and availability of the rod control system, we have used Petri nets, a graphical and mathematical tool that can model the dynamic behavior and interactions of concurrent and distributed systems. Petri nets can capture both the structural and functional aspects of a system[5], as well as the stochastic properties of its components. Petri nets can also be used to derive other reliability models, such as fault trees and reliability block diagrams, which can provide quantitative measures of system performance.

In this project, we have designed a Petri net model [1] of the rod control system of a nuclear power plant, based on a reference paper that had a fault tree with data taken from relevant sources. We have also constructed an equivalent reliability block diagram for the same system. We have simulated both models on SHARPE tool, a software package that can perform various reliability analyses. We have compared the results obtained from both models and discussed their similarities and differences. We have also evaluated the sensitivity of the system reliability to various parameters, such as failure rates, repair rates, and operational modes. Nuclear power plants (NPPs) are complex systems that generate electricity by using nuclear fission reactions in reactor cores. NPPs require various safety systems to ensure the safe and reliable operation of the reactors and to prevent or mitigate severe accidents and core damage. One of the safety systems is the poison injector, which is a device that injects a neutron-absorbing material (such as boron) into the reactor core to shut down the fission reaction in case of an emergency. Poison injector is usually activated by a signal from the reactor protection system (RPS), which monitors the reactor parameters and initiates the shutdown sequence when certain conditions are met. The design and performance of poison injector are critical for the safety of NPPs, as it can affect the speed, completeness, and stability of the reactor shutdown. Therefore, it is important to model and analyze the behavior of poison injector under various scenarios and to verify its correctness and effectiveness. However, conventional modeling tools such as differential equations or state machines may not be suitable for capturing the dynamic and concurrent nature of poison injector, as they may not be able to represent the interactions, conflicts, or synchronization among different components or events.

II. RELATED WORK

A. Overall Working of system

1) Rod control: The rod control system (RCS) is a system that controls the movement of control rods in a nuclear reactor.

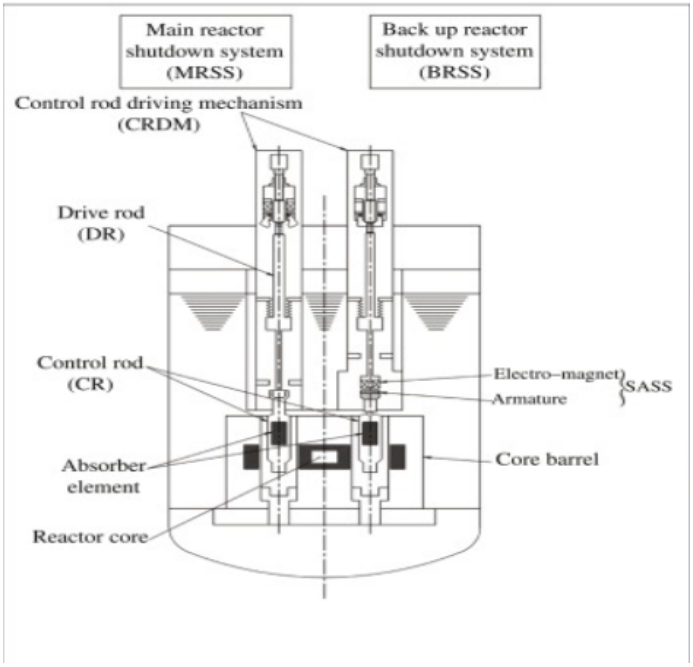

Fig. 1. Working of Rod control System

Control rods are devices that can absorb neutrons and regulate the rate of fission in the nuclear fuel. By adjusting the position of control rods, the RCS can change the reactivity of the reactor and maintain it at a desired level.

The RCS consists of several sub components, such as:

Control rod drive mechanism (CRDM): This is the device that physically moves the control rods in and out of the reactor core. It can be either electric, hydraulic, or pneumatic. The CRDM receives signals from the RCS controller and converts them into mechanical motion. The CRDM also provides feedback on the actual position of the control rods to the RCS controller. RCS controller: This is the device that monitors the reactor parameters, such as neutron flux, power level, temperature, pressure, etc., and calculates the optimal position of the control rods to achieve the desired reactivity. The RCS controller sends signals to the CRDM to move the control rods accordingly. The RCS controller also receives feedback from the CRDM and adjusts the signals if necessary. The RCS controller can operate in different modes, such as manual, automatic, or emergency. RCS power supply: This is the device that provides the electrical power to the RCS controller and the CRDM. It can be either AC or DC, depending on the type of CRDM. The RCS power supply must be reliable and redundant to ensure the safety of the RCS operation. RCS instrumentation: This is the device that measures and displays the reactor parameters and the control rod positions. It can include sensors, detectors, indicators, alarms, etc. The RCS instrumentation provides the information to the RCS controller and the reactor operators. The RCS instrumentation must be accurate and calibrated to ensure the validity of the RCS operation. The RCS is an important system for the safe and efficient operation of a nuclear power plant. It can perform various functions, such as:

Reactor startup: The RCS can withdraw the control rods gradually from the reactor core to initiate the fission chain reaction and increase the reactor power to the desired level. Power maneuvering: The RCS can adjust the position of the control rods to change the reactor power according to the grid demand or the operational requirements. The RCS can also compensate for the changes in the fuel burnup and the xenon poisoning effects. Axial offset control: The RCS can control the axial power distribution in the reactor core by inserting or withdrawing the control rods in different groups or banks. This can optimize the thermal efficiency and the fuel utilization of the reactor. Reactor shutdown: The RCS can insert the control rods fully into the reactor core to stop the fission chain reaction and decrease the reactor power to zero. Emergency shutdown (SCRAM): The RCS can rapidly insert the control rods into the reactor core in case of an abnormal or hazardous situation, such as a loss of coolant, a loss of power, a reactor trip, etc. This can prevent the reactor from reaching a critical or supercritical state and avoid a potential meltdown or explosion.

2) Poison Injector System : The poison injector system (PIS) is a system that injects a liquid containing a neutron-absorbing substance, such as boric acid or gadolinium nitrate, into the reactor core to quickly stop the nuclear chain reaction in case of an emergency. The PIS is one of the two independent and equally effective shutdown systems that all nuclear power reactors in Canada have. The other system is the control rod system, which uses rods that drop into the core to absorb neutrons1

The PIS consists of several sub components, such as:

Poison tanks: These are the tanks that store the liquid poison, which is usually diluted with water to a certain concentration. The poison tanks are located outside the reactor building and are connected to the injection tubes by pipes and valves. The poison tanks have heaters to prevent the liquid from freezing and sensors to monitor the temperature, pressure and level of the poison23 Injection tubes: These are the tubes that deliver the liquid poison from the poison tanks to the reactor core. The injection tubes are made of stainless steel and have holes along their length to distribute the poison evenly in the core. The injection tubes are located inside the reactor vessel or the calandria, depending on the type of reactor. The injection tubes are also connected to the actuation system and the instrumentation system23 Actuation system: This is the system that triggers the injection of the poison into the core when a signal from the reactor protection system is received. The actuation system can be either pneumatic, hydraulic or electric. The actuation system opens the valves that allow the poison to flow from the tanks to the tubes and closes the valves that isolate the tubes from the reactor coolant system. The actuation system also provides backup power to the PIS in case of a loss of power23 Instrumentation system: This is the system that measures and displays the parameters of the PIS, such as the poison flow rate, pressure, temperature and concentration. The instrumentation system also provides

feedback to the reactor protection system and the reactor operators. The instrumentation system can include sensors, detectors, indicators, alarms, etc. The instrumentation system must be accurate and reliable to ensure the effectiveness of the PIS23 The PIS is an important system for the safety of a nuclear power plant. It can perform the following functions:

Emergency shutdown (SCRAM): The PIS can rapidly inject the poison into the core in case of an abnormal or hazardous situation, such as a loss of coolant, a loss of power, a reactor trip, etc. This can prevent the reactor from reaching a critical or supercritical state and avoid a potential meltdown or explosion. The PIS can operate without power or operator intervention, but it can also be manually activated. The PIS is regularly and safely tested12 Power maneuvering: The PIS can also adjust the position of the poison in the core to change the reactor power according to the grid demand or the operational requirements. The PIS can also compensate for the changes in the fuel burnup and the xenon poisoning effects. The PIS can operate in manual or automatic mode, depending on the type of reactor

B. Background

The research started with understanding the working of the rod control system and the poison injector system the details are as follows.

The rod control system (RCS) is a system that controls the movement of control rods in a nuclear reactor. Control rods are devices that can absorb neutrons and regulate the rate of fission in the nuclear fuel. By adjusting the position of control rods, the RCS can change the reactivity of the reactor and maintain it at a desired level. The RCS consists of several sub components, such as:

Control rod drive mechanism (CRDM): This is the device that physically moves the control rods in and out of the reactor core. It can be either electric, hydraulic, or pneumatic. The CRDM receives signals from the RCS controller and converts them into mechanical motion. The CRDM also provides feedback on the actual position of the control rods to the RCS controller. RCS controller: This is the device that monitors the reactor parameters, such as neutron flux, power level, temperature, pressure, etc., and calculates the optimal position of the control rods to achieve the desired reactivity. The RCS controller sends signals to the CRDM to move the control rods accordingly. The RCS controller also receives feedback from the CRDM and adjusts the signals if necessary. The RCS controller can operate in different modes, such as manual, automatic, or emergency. RCS power supply: This is the device that provides the electrical power to the RCS controller and the CRDM. It can be either AC or DC, depending on the type of CRDM. The RCS power supply must be reliable and redundant to ensure the safety of the RCS operation. RCS instrumentation: This is the device that measures and displays the reactor parameters and the control rod positions. It can include sensors, detectors, indicators, alarms, etc. The RCS instrumentation provides the information to the RCS controller and the reactor operators. The RCS instrumentation must be accurate and calibrated to ensure the validity of the RCS operation. The RCS is an important system for the safe and efficient operation of a nuclear power plant. It can perform various functions, such as: Reactor startup: The RCS can withdraw the control rods gradually from the reactor core to initiate the fission chain reaction and increase the reactor power to the desired level. Power maneuvering: The RCS can adjust the position of the control rods to change the reactor power according to the grid demand or the operational requirements. The RCS can also compensate for the changes in the fuel burnup and the xenon poisoning effects. Axial offset control: The RCS can control the axial power distribution in the reactor core by inserting or withdrawing the control rods in different groups or banks. This can optimize the thermal efficiency and the fuel utilization of the reactor. Reactor shutdown: The RCS can insert the control rods fully into the reactor core to stop the fission chain reaction and decrease the reactor power to zero. Emergency shutdown (SCRAM): The RCS can rapidly insert the control rods into the reactor core in case of an abnormal or hazardous situation, such as a loss of coolant, a loss of power, a reactor trip, etc. This can prevent the reactor from reaching a critical or supercritical state and avoid a potential meltdown or explosion.

The poison injector system (PIS) is a system that injects a liquid containing a neutron-absorbing substance, such as boric acid or gadolinium nitrate, into the reactor core to quickly stop the nuclear chain reaction in case of an emergency. The PIS is one of the two independent and equally effective shutdown systems that all nuclear power reactors in Canada have. The other system is the control rod system, which uses rods that drop into the core to absorb neutrons1.The PIS consists of several sub components, such as:

Poison tanks: These are the tanks that store the liquid poison, which is usually diluted with water to a certain concentration. The poison tanks are located outside the reactor building and are connected to the injection tubes by pipes and valves. The poison tanks have heaters to prevent the liquid from freezing and sensors to monitor the temperature, pressure and level of the poison23 Injection tubes: These are the tubes that deliver the liquid poison from the poison tanks to the reactor core. The injection tubes are made of stainless steel and have holes along their length to distribute the poison evenly in the core. The injection tubes are located inside the reactor vessel or the calandria, depending on the type of reactor. The injection tubes are also connected to the actuation system and the instrumentation system23 Actuation system: This is the system that triggers the injection of the poison into the core when a signal from the reactor protection system is received. The actuation system can be either pneumatic, hydraulic or electric. The actuation system opens the valves that allow the poison to flow from the tanks to the tubes and closes the valves that isolate the tubes from the reactor coolant system. The actuation system also provides backup power to the PIS in case of a loss of power23 Instrumentation system: This is the system that measures and displays the parameters of the PIS, such as the poison flow rate, pressure, temperature

and concentration. The instrumentation system also provides feedback to the reactor protection system and the reactor operators. The instrumentation system can include sensors, detectors, indicators, alarms, etc. The instrumentation system must be accurate and reliable to ensure the effectiveness of the PIS23 The PIS is an important system for the safety of a nuclear power plant. It can perform the following functions: Emergency shutdown (SCRAM): The PIS can rapidly inject the poison into the core in case of an abnormal or hazardous situation, such as a loss of coolant, a loss of power, a reactor trip, etc. This can prevent the reactor from reaching a critical or supercritical state and avoid a potential meltdown or explosion. The PIS can operate without power or operator intervention, but it can also be manually activated. The PIS is regularly and safely tested12 Power maneuvering: The PIS can also adjust the position of the poison in the core to change the reactor power according to the grid demand or the operational requirements. The PIS can also compensate for the changes in the fuel burnup and the xenon poisoning effects. The PIS can operate in manual or automatic mode, depending on the type of reactor.

C. Literature Survey

The design and verification of the shutdown system of a nuclear power plant (NPP) [2] is a critical task that ensures the safety and reliability of the reactor operation. The 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 into the reactor core, respectively, to stop the fission chain reaction[3]. The shutdown system can be activated under normal or abnormal conditions, such as scheduled maintenance, emergency situations, or seismic events. Therefore, it is important to analyze the dynamic behavior and performance of the shutdown system under various scenarios and evaluate its effectiveness and robustness. One of the methods that can be used to model and analyze the shutdown system is Petri nets, which are a graphical and mathematical tool for describing and studying systems that are concurrent, asynchronous, distributed, parallel, nondeterministic, and/or stochastic. Petri nets have been widely used in various domains, such as computer science, engineering, biology, and social sciences. Petri nets have several advantages over other modeling techniques, such as their simplicity, expressiveness, formality, and graphical representation[6]. Petri nets[1] can also be extended with different features, such as time, color, hierarchy, stochasticity, and hybridity, to capture more complex and realistic systems.

One of the papers that uses Petri nets to analyze the shutdown system of a NPP is [1], which models the rod control system and the poison injection system using Petri nets and simulates their operation under normal and abnormal conditions. The paper also evaluates the performance and safety of the shutdown system using Petri net analysis methods, such as reachability graph, invariant analysis, deadlock detection, and liveness analysis. The paper shows that Petri nets can effectively capture the dynamic behavior of the shutdown system and provide useful insights for its design and verification.

Another paper that uses Petri nets for the design verification of the instrumentation and control (I&C) systems of NPPs is [4], which presents a design verification methodology for I&C systems using Petri nets. The paper shows how to model the I&C systems using Petri nets, convert them into Markov chains, and solve the linear system mathematically to verify the system functionality and reliability. The paper also demonstrates the applicability of the methodology to a case study of a pressurized water reactor (PWR) I&C system.

Besides Petri nets, there are other methods and tools that can be used for the design and verification of the shutdown system and other related systems of NPPs. For example, [3] provides guidance on the design of control room systems for NPPs, including the human factors, ergonomic, and operational aspects. The paper also discusses the design process, methods, tools, standards, and evaluation techniques for control room systems. Another example is [4], which presents the design and testing of seismic isolation systems for NPPs, which can reduce the seismic response of the structures and equipment. The paper also describes the application of seismic isolation to a NPP in Italy, which uses high damping rubber bearings as isolators. This shows that there is a rich body of research on the design and verification of the shutdown system and other related systems of NPPs using various methods and tools. However, there are also some limitations and gaps in the existing literature that need to be addressed. For instance,

Most of the papers focus on specific subsystems or components of NPPs, such as rod control system or poison injection system, but do not consider their interactions or dependencies with other subsystems or components. Therefore, there is a need for a more holistic and integrated approach that can model and analyze the whole shutdown system or even the whole NPP as a single entity.Some of the papers use simplified or idealized assumptions or parameters for their models or simulations, such as neglecting noise, disturbances, uncertainties, or failures. Therefore, there is a need for more realistic and robust models or simulations that can account for these factors and evaluate their impacts on the system behavior and performance.Some of the papers use qualitative or descriptive methods or tools for their analysis or evaluation, such as reachability graph or invariant analysis. Therefore, there is a need for more quantitative or numerical methods or tools that can provide more precise and objective measures or indicators for the system behavior and performance. A Global Review of PWR Nuclear Power Plants[2]: This paper provides a comprehensive overview of the technical evolution, implementation level, and life extension scenario of PWR nuclear power plants in the world. The paper also discusses the main challenges and opportunities for PWR technology, such as safety, economics, waste management, and public acceptance. This paper considers the benefits of nuclear power compared with generating energy from fossil fuel sources and discusses the reasons why nuclear power may be the better option, taking into account costs, safety, and environmental

pollution. The paper also addresses some of the common myths and misconceptions about nuclear power and provides some recommendations for future research and policy. This helps to understand the background and context of our project topic and to identify the existing knowledge and gaps in the field. We have learned that poison injector is one of the safety systems that are designed to prevent or mitigate severe accidents and core damage in NPPs. We have also learned that there are different types of poison injector systems, such as active or passive, high or low pressure, single or multiple stage, etc., depending on the reactor type and design. Moreover, we have learned that poison injector[7] systems are usually activated by a signal from the RPS, which monitors the reactor parameters and initiates the shutdown sequence when certain conditions are met.

The aim of this research project is to address some of these limitations and gaps by developing a novel method that can model and analyze the shutdown system of a NPP using hybrid Petri nets (HPNs), which are an extension of Petri nets that can incorporate both discrete and continuous dynamics. HPNs can capture both the discrete events (such as rod insertion or poison injection) and the continuous processes (such as reactor temperature or pressure) of the shutdown system, and can also handle noise, disturbances, uncertainties, and failures. HPNs can also be converted into hybrid automata, which are a mathematical framework for modeling and analyzing hybrid systems. Hybrid automata can be used to perform various analysis and verification tasks, such as reachability analysis, safety analysis, stability analysis, and optimal control. The research project will also use a case study of a PWR shutdown system to demonstrate the applicability and effectiveness of the proposed method. The research project will contribute to the advancement of the knowledge and practice of the design and verification of the shutdown system of NPPs using HPNs and hybrid automata.

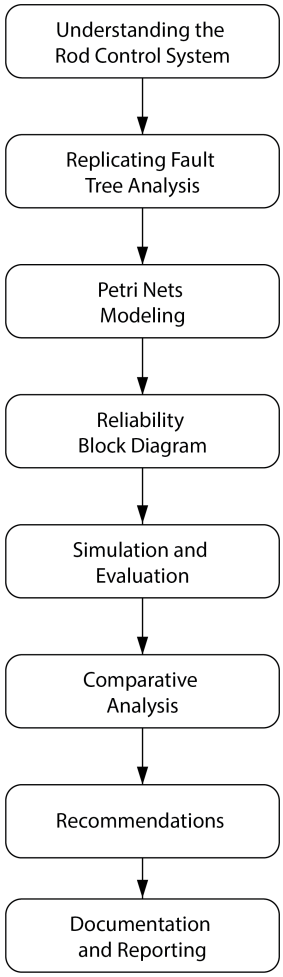

Fig. 2. Workflow of Rod control System

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)

Rod Control System In this workflow, the objective was to comprehensively analyze the reliability of the Rod Control System (RCS) in Advanced Pressurized Water Reactors (APWRs), building upon the reference paper's Fault Tree Analysis (FTA) by incorporating additional methodologies such as Petri nets and Reliability Block Diagrams (RBDs). The process involved the phases:

I. Understanding the Fault Tree Structure: In this phase, the structure and logic of the fault tree presented in the reference paper were thoroughly examined. The fault tree illustrated potential causes of RCS failure through the use of basic events, intermediate events, and logical gates, with symbols and definitions provided in the paper to aid in interpretation.

II. Converting the Fault Tree to a Petri Net Model: The second phase involved the transformation of the fault tree into a Petri net model, a graphical and mathematical tool for capturing dynamic system behavior. Elements of the fault tree were mapped to the Petri net, where places represented basic and intermediate events, transitions represented logic gates, arcs represented causal links, and tokens represented event occurrences. The use of colored Petri nets allowed the assignment of attributes and values to model elements, following insights from previous work using Petri nets for fault tree analysis.

III. Converting the Petri Net Model to a Reliability Block Diagram (RBD): The third phase of analysis involved converting the Petri net model into an RBD model, which is used to represent the reliability structure of a system. Blocks were employed to represent RCS components and subsystems, and connectors were used to depict their configuration and dependencies. Elements of the Petri net were mapped to the RBD, and dynamic RBDs were considered to capture time-dependent system behavior, with reference to prior research employing RBDs for modeling system reliability.

IV. Verification and Analysis of Models: The final phase centered on the verification and analysis of the models devel-

oped in the previous steps. Various tools and techniques were utilized to ensure model correctness and consistency, including reachability analysis, simulation, and formal methods. Metrics and measures such as failure rate, mean time to failure, and availability function were employed to evaluate the reliability and availability of the models. These results were then compared with those from the reference paper and other relevant sources.

V. Data Gathering: The datasets utilized in this study were obtained from various reliable sources, including the following: U.S. Nuclear Regulatory Commission (US NRC) Report: The US NRC is a prominent authority responsible for regulating nuclear power activities in the United States. The datasets from their report were chosen as a foundational data source due to the credibility and comprehensiveness of their data. The US NRC has extensive experience in the field of nuclear safety, making their data highly valuable for this analysis[9]. Norman P. Cheremisinoff's Book: Norman P. Cheremisinoff is a renowned author in the field of nuclear engineering and safety. His book provides a wealth of data and insights, making it a crucial resource for our study. The data from this source offers a diverse perspective on the RCS and contributes to the robustness of the analysis[10]. M. Modarres and M. Kaminskiy's Paper: The paper authored by M. Modarres and M. Kaminskiy is a scholarly work that contains valuable information on the RCS of a PWR. Academic sources, such as this, provide detailed research findings and methodologies that are instrumental in the construction of reliable models[11]. The data acquired from these sources serve as the basis for our reliability analysis, specifically for the RCS components and subsystems. This data allows us to assign realistic values to our Petri net and RBD models, enabling accurate simulations and calculations.The datasets selected are directly related to the RCS of a PWR. This relevance ensures that the data is suitable for assigning values to our models, leading to meaningful and accurate results.

VI. Novelty: This subsection provides an overview of the novel additions and advancements incorporated into our group project, focused on the reliability analysis of the Rod Control System (RCS) of a Pressurized Water Reactor (PWR). Building upon the existing research, we have introduced new methodologies and explored potential scenarios to enhance the project's depth and effectiveness. This collaborative effort was carried out using the SHARPE tool to simulate Petri nets and RBD models, ultimately improving the reliability and availability assessment. We harnessed the capabilities of the SHARPE tool, a sophisticated software package for reliability and availability analysis. This tool allowed us to simulate our Petri net and RBD models, providing numerical results and graphical representations. Furthermore, the SHARPE tool offered a range of analysis features, including sensitivity, importance, and optimization analysis, which bolstered our reliability assessment.We took a step beyond by comparing the reliability and fault rates of our Petri net and RBD models with those derived from the fault tree model. This comparative analysis provided insights into discrepancies and similarities, enabling a comprehensive evaluation of the models' effectiveness. We also delved into the advantages and disadvantages of employing different modeling tools, such as Petri nets, RBD, or fault trees, for RCS reliability analysis within a PWR reactor context. Our project extended into the realm of potential scenarios and variations. We considered modifications to the data set values, the addition or removal of specific components or subsystems, and the introduction of different types of failures or repairs. By exploring these alterations, we gained a deeper understanding of how changes affect the reliability and availability of our models, and we elucidated the underlying reasons behind these effects.By implementing these innovative approaches and conducting a comparative analysis, our project made valuable contributions to the existing body of knowledge and literature on the reliability of RCS in PWR reactors. These additions offer a fresh perspective on the subject and broaden the understanding of reliability analysis in 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. The literature

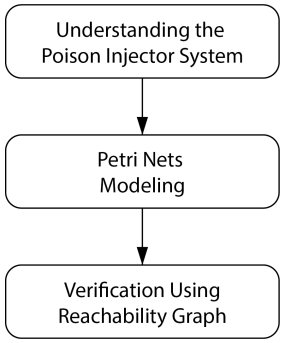

Fig. 3. Workflow of Posion Injection System

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: i. Reactor core: The part of the reactor where the fission reaction takes place and generates heat. ii. 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. iii. Poison valve: The valve that controls the flow of neutron poison from the poison tank to the reactor core. iv. 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: i. Normal operation: The event when the reactor operates normally under steady state conditions. ii.Shutdown signal: The event when the RPS sends a signal to activate the poison injector system. iii. Shutdown completion: The event when the reactor core reaches a subcritical state and stops the fission reaction. iv.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 PetriNets and RBD

I AND Gate:

i) FTA to RBD:

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

ii)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.

II OR Gate:

i) 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.

ii) 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

III AND Gate:

i) 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.

ii) 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.

IV OR Gate:

i) 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.

ii) 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.

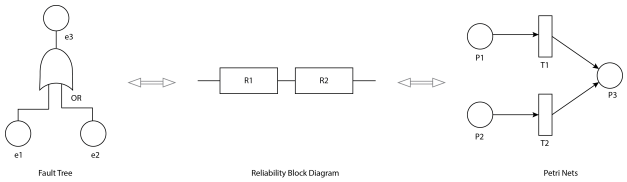

Fig. 4. Conversion Logic with OR gate

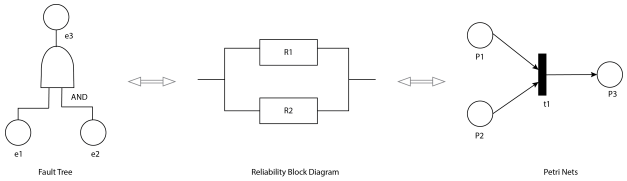

Fig. 5. Conversion Logic with AND gate

V. Results and Discussion

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.

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

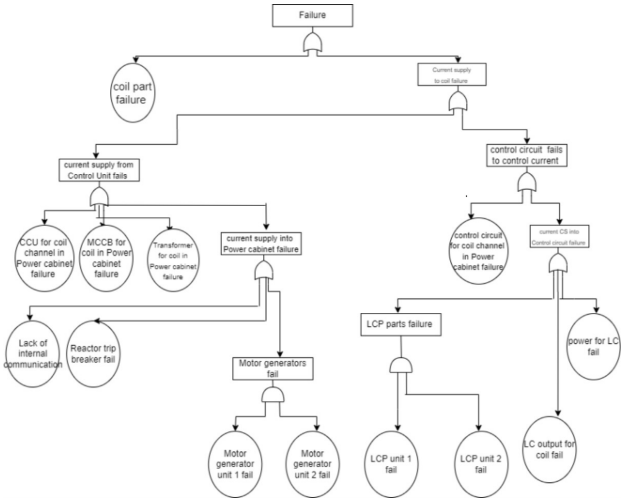

Fig. 6. FTA of Rod Control System [12]

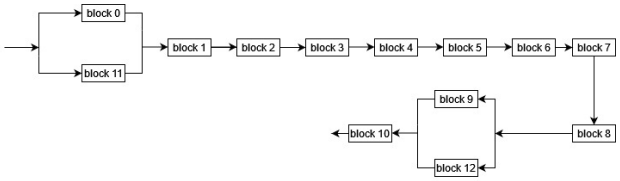

Fig. 7. RBD of Rod Control System

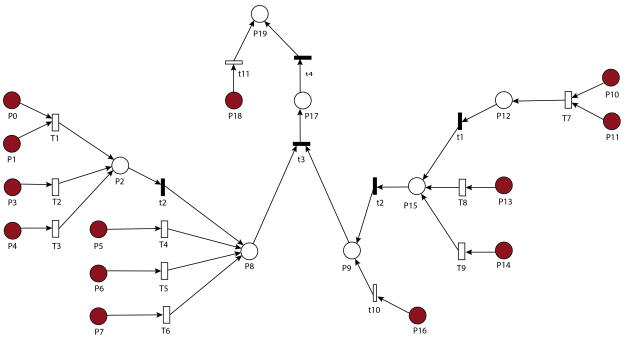

Fig. 8. Petri Net of Rod Control System

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

The research conducted provides a comprehensive analysis of the safety mechanisms within nuclear power plants, with a specific focus on the Rod Control System and Poison Injection System. By employing a detailed Petri Net framework, the study successfully mapped the complex interactions and dependencies within these critical systems. This

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

Fig. 9. Description of places petrinet 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

Fig. 10. Description of transitions petrinet 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**

Fig. 11. Metric performances of RCS

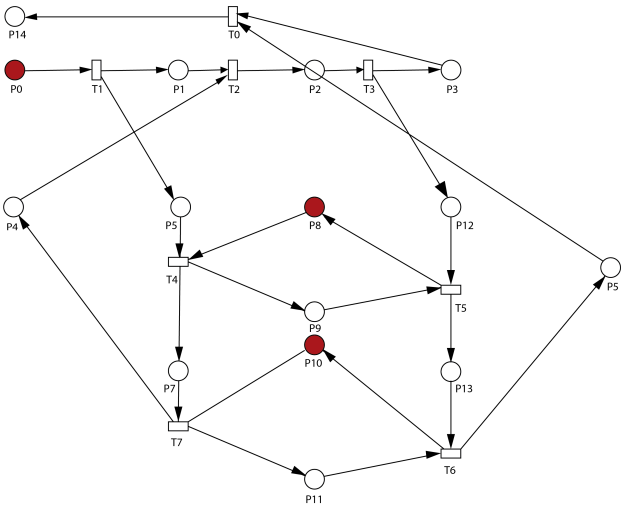

Fig. 12. Petri Net of Poison injection System

approach not only allowed for an in-depth understanding of operational intricacies and emergency protocols but also enabled the implementation of rigorous safety checks and formal verification methods. The iterative process of design and validation, aligned with established research benchmarks, has significantly enhanced the reliability and efficacy of the shutdown mechanisms. The results of this study underscore the effectiveness of current safety protocols and present an innovative perspective on nuclear power plant shutdown procedures, ensuring a higher level of operational security.

VII. Future Scope

Looking ahead, the project opens avenues for further refinement and expansion of the current model. Future work could focus on integrating more realistic, empirical data to enhance the model's accuracy and reliability. This could involve calibrating the model with real-world operational data from nuclear power plants, allowing for more precise simulation and analysis. Additionally, there is potential to extend the Petri Net model to encompass other vital components of the nuclear power plant, such as the reactor core and cooling systems, providing a more holistic view of the plant's safety mechanisms. This comprehensive approach would not only improve the existing model but also contribute valuable insights to the field of nuclear safety, supporting the development of more robust and effective safety protocols in nuclear power plant operations.

Places	Description
P0	Trip parameters deviation
P1	Logical condition creation
P2	Logical condition on hold
P3	Logical condition restored
P6	Close vent valves
P7	Vent valves closed
P4	Prioritize T6 over T2
P5	Reversibility properties
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

Fig. 13. Description of places petrinet of PIS

Transition	Description
T1	send signal to LC inorder to energize relays to close vent valves
T2	Hold LC at created state
T3	restore LC and relay de-energizes
T0	resend signal to open Quick open valves if it fails to open
T4	Close the vent valves
T7	open all Quick open valves
T5	open all vent valves
T6	close all Quick open valves

Fig. 14. Description of transitions petrinet of PIS

References

[1] 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.

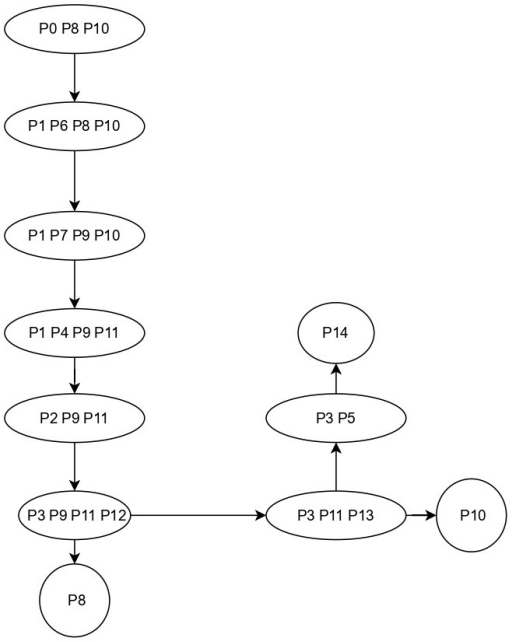

Fig. 15. Reachability graph of PIS

[2] 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.

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

[4] Singh, Lalit Kumar, Gopika Vinod, and A. K. Tripathi. "Design verification of instrumentation and control systems of nuclear power plants." IEEE Transactions on nuclear science 61, no. 2 (2014): 921-930.

[5] 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.

[6] 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.

[7] 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).

[8] Yan, Rundong, and Sarah Dunnett. "Resilience assessment for nuclear power plants using Petri nets." Annals of Nuclear Energy 176 (2022): 109282.

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

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

[11] 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.

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