We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

185,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Chapter

Reliability Analysis of Instrumentation and Control System: A Case Study of Nuclear Power Plant

Mohan Rao Mamdikar, Vinay Kumar and Pooja Singh

Abstract

Instrumentation and control system (I&Cs) plays a key role in nuclear power plants (NPP) whose failure may cause the major issue in a form of accidents, hazardous radiations, and environmental loss. That is why importantly ensure the reliability of such system in NPP. In this proposed method, we effectively analyze the reliability of the instrumentation and control system. An isolation condenser system of nuclear power plant is taken as a case study to show the analysis. The methodology includes the dynamic behavior of the system using Petri net. The proposed method is validated on operation data of NPP.

Keywords: reliability, control system, nuclear power plant, isolation condenser system

1. Introduction

Instrumentation and control system (I&C) plays a vital role in the field of the nuclear industry. Nowadays I&C systems are embedded into the nuclear power plant (NPP) operation and reliability. Each component of NPP, such as transformers, valves, circuit breakers, heat exchangers. is equipped with digital I&C system whose reliability plays a vital role to avoid any accidents. Because these components are safety-critical systems (SCS) whose failure may cause huge losses in the form of economic loss, human resource damage, and environmental loss. As instrumentation and control systems are the important and first layer of safety, reliability, and stability in the NPP [1] that is the reason, it is essential to ensure the reliability of such a safety system. With, the introduction of digital control systems in the last few decades where the reliability of digital I&C must not be degraded. Therefore, researchers are rigorously working to address the dependability of the system. The dependability includes reliability, safety analysis, performance, and availability attributes that are ultimately related to security. The model checking may be used to various issues, which can lead to spurious actuation of the I&C system [2]. The transformation from analog to digital I&C safety systems added new challenges for researchers as well as software developers to deliver correct software reliability [3]. Based on this software experts could take essential steps early in the design phase of software by avoiding failures in I&C of NPP. The cyberattack occurred in the I&C system in the Iranian Bushehr nuclear power plant,

where configure was destroyed by malicious code [4]. Therefore, it is essential to I&C systems required having secure and reliable to avoid any kind of attacks causing major accidents. Many researchers have put efforts to address the reliability analysis on such systems using various techniques, such as fault tree analysis (FTA), reliability block diagram (RBD), Bayesian network, etc.

This work proposes the reliability analysis of instrumentation and control system (I&C) of NPP using stochastic Petri net (SPN).

The organization of this paper is as follows. In Section 2, our focus is on the related work of the proposed work. In Section 3, we discuss the background and mathematical fundamentals. In Section 4, proposes the framework of the proposed method. In Section 5, the case study of the proposed work. In Section 6, reliability analysis of the proposed work. In Section 7, the validation part is covered. In Section 8, the conclusion is made with future work.

2. Related work

Zeller et al. [5] proposed a combined approach of Markov chain and component fault tree to analyze the complex software-controlled system in the automotive domain. The authors have addressed safety and reliability in modular form. However, authors have missed to validate the result and failed to express reliability accuracy in percentage.

Nidhin et al. [6] presented a survey for understanding radiation effects in SRAM-based FPGAs for implementing I&C of NPP. Authors have found that for implementing NPP with I&C in SRAM-based FPGAs, the effect of radiation issue is a major concern. To reduce radiation-related issues some components, which have SRAM-based FPGAs, must keep outside of reactor containment building (RCB). However, the authors have failed to discuss the case study.

Jia et al. [7] proposed an approach for the identification of vulnerabilities present in elements that affect the reliability of digital instrumentation and control system (DI&C) software life cycle using Bayesian network. A reliability demonstration of safety-critical software (RDSS) integrates the claim-argument-evidence (CAE) and sensitivity to estimate the reliability of the system. However, there is a limitation with BN that has no time constraints and dynamic property. Authors have missed addressing the reliability with validation from the real-time dataset.

Rejzek and Hilbes [8] proposed system-theoretic process analysis (STPA) for design verification and risk analysis of digital I&C of NPP. This method is considered as a prominent approach for analysis of the I&C system theoretically as the authors claim. However, the authors are not very much sure, that method correct result.

Torkey et al. [9] proposed a reliability improvement framework of the digital reactor protection system by transforming reliability block diagram to Bayesian belief network (BBN). The proposed method gives the highest availability as a result and found some modules are riskier than others of I&C. However, authors claim that it gives the highest availability but missed to validate the result with real-time data.

Kumar et al. [3] proposed a framework for predicting the reliability of the safety-critical and control system using the Bayesian update methodology. The authors have validated the result with real-time data of 12 safety-critical control systems of NPP. However, the result obtained is purely based on the failure data, if failure data is unavailable then it is difficult to predict the reliability.

Mamdikar et al. [10] devise a framework for reliability analysis, performance analysis that maps unified modified language (UML) to Petri net. The proposed framework is validated with 32 safety-critical systems of NPP. However, Petri net has a state space explosion problem as a system grows gradually, so it is not a generalized approach.

Nayak et al. [11] proposed a methodology called assessment of passive system reliability (APSRA) is used to estimate the reliability of the passive isolation condenser system of the Indian advanced heavy water reactor (AHWR). In this methodology, reliability is estimated through PSA treatment using generic data of the component. A classical fault tree analysis is used to find the root cause of the critical parameter, which leads to failure. However, the authors have failed to validate the result.

Kumar et al. [12] proposed a safety analysis framework that maps UML into the state-space model as Petri net of the safety-critical system of NPP. In this methodology, the result is validated on 29 different safety-critical systems of NPP. However, the authors have used Petri net that has a state space explosion problem.

Tripathi et al. [13] proposed a noble methodology dynamic reliability analysis of the passive decay heat removal system of NPP using Petri net. The authors have validated the estimated reliability based on the data available using fault tree analysis. Most of the system does not have such type data, and then it is difficult to validate the result with missing failure data. Therefore, this methodology may not applicable for every safety-critical system of NPP.

Buzhinsky and Pakonen [14] proposed an automated symmetry breaking approach for checking failure tolerance of I&C system. With this method a fewer failure combination has to be checked. The complex structure paired with various specifications has to be checked under failure assumptions, which is the limitation of this work.

Singh et al. [15] proposed a system modeling strategy for design verification of I&C of nuclear power plant using Petri net and converting PN into Markov chain. In this approach, verification is validated on real-time data. However, Petri net has a state-space explosion problem, in such circumstances, it is difficult to handle complex systems, which is the limitation of the work.

Xi et al. [16] proposed a test strategy based on the random selection of logic path by which provides reliability estimation and is used for control system testing in digital control software systems in the NPP. However, the authors have not been addressed and validated the reliability evaluation.

Bao et al. [17] proposed hazard analysis for identifying common cause failure of digital I&C using redundancy guided system in NPP. To conduct using redundancy guided systems, theoretic hazard analysis a modularized approach was applied. This method is helpful to remove casual effects of potential single points of failure that exist in I&C. However, authors have missed addressing the reliability analysis using this methodology in NPP.

Gupta et al. [1] proposed a method for stability analysis and steady-state analysis of the safety system of NPP using Petri net. The stability and steady-state were estimated and validated, however, authors have missed estimating reliability. The authors have to correlate stability with reliability. Further, this methodology is applicable only for discrete-time systems.

3. Background and mathematical fundamentals

This section consists of background and mathematical fundamentals to carry out reliability analysis of instrumentation and control system: a case study of nuclear power plant.

3.1 Petri net

A Petri net (PN) is mathematically defined 5-tuple $\boldsymbol{PN} = (\boldsymbol{P}, \boldsymbol{T}, \boldsymbol{F}, \boldsymbol{W}, \boldsymbol{M_0})$ where $\boldsymbol{P}$ the finite is set places, $\boldsymbol{T}$ is a finite set of transitions, $\boldsymbol{F}$ is a finite set of arcs also referred to as flow relation, i.e., $\boldsymbol{F}$ $(\boldsymbol{P} \times \boldsymbol{T})$ $(\boldsymbol{T} \times \boldsymbol{P})$, $\boldsymbol{W} : \boldsymbol{F}$ $\{\boldsymbol{1}, \boldsymbol{2}, \boldsymbol{3}, \ldots .\}$ is the

weight function, and M_0 is the initial marking $M_0 : P \{0, 1, 2, 3, \ldots .\}$. $P\ T =$ and $P\ T \neq$. If the Petri net does not have an initial marking, it is denoted as $N = (P, T, F, W)$ with an initial marking denoted by (N, M_0). A simple example of the PN is shown in **Figure 1**.

The marking changes in the Petri net as per the transition firing are as follows:

i. A transition in the enable mode when each input place of p of t is marked with at least $w(p, t)$ tokens.

ii. An enabled transition is not necessarily fired.

iii. A firing of enabled transition removes tokens from the input place and deposited in the output place.

3.2 Stochastic Petri net

A stochastic Petri net (SPN) is the extension of Petri net. In SPN, each transition is associated with a time delay that is an exponentially distributed random variable that expresses delay denoted by $SPN = (P, T, F, W, M_0)$.

3.3 Reachability

Reachability is the fundamental study of the dynamic property of the system. A marking M_n is said to be reachable from another marking M_1 if there exists a firing sequence that transforms M_n to M_1 such that$\partial = \{M_1 t_0 M_2 t_1 M_3 \ldots . t_n M_n\}$.

3.4 Reachability graph and Markov chain (MC)

A marking M is reachable from the initial marking M_0 if there exists a firing ∂ that brings back from the initial state of PN to a state that corresponds to M_0.

The Markov chain (MC) is the Markov process with discrete state space. The MC is obtained from the reachability graph of the SPN. Let SPN be the reversible, i.e., $M_0 \in R(M_i)$ for every M_i in $R(M_0)$, then the SPN generates an ergodic continuous time Markov chain (CTMC) and it is possible to compute the steady-state probability distribution $\prod$ by solving the following (Eq. (1)) and (Eq. (2)).

$$\sum \prod Q = 1 \tag{1}$$

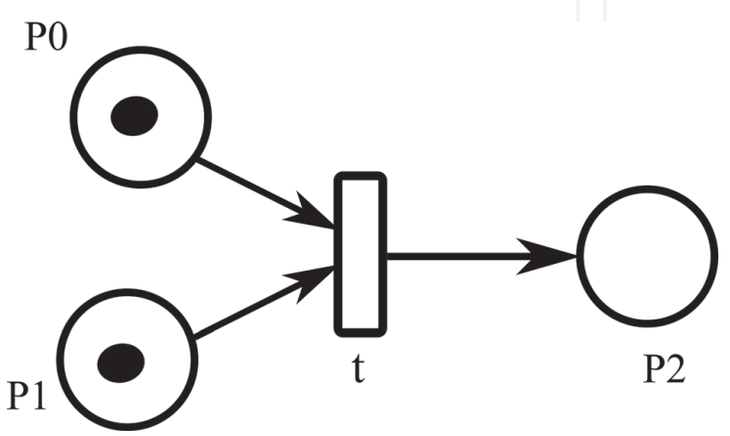


Figure 1.
Simple Petri net.

$$\sum_{i=1}^{s} \pi_i = 1 \tag{2}$$

Where, π_i is the probability being in the state M_i and $\prod = (\pi_1, \pi_2, \ldots \pi_s)$.

4. Framework of the proposed method

The proposed framework has six steps shown in **Figure 2**. Step 1—based on the system requirement we model the stochastic Petri net.

In step 2—by executing the PN model, we generate possible tangible states. Based on the tangible states, we construct the reachability graph in step 3. In step 4—obtained Markov chain form reachability, the graph of SPN. In step 5, we estimate the reliability of the ISO system. In step 6, we validate the result with real-time operation data of NPP.

5. Case study: Isolation condenser system (ISO)

The isolation condenser system simply referred to as ISO is a standby high-pressure system that removes residual and decay heat from the reactor vessel in the event of a scram signal in which the reactor becomes isolated from the main condenser, or if any other high-pressure condition exists. The schematic diagram is shown in **Figure 3**. The ISO system transfers residual and decays heat from the reactor coolant to the water in the shell side of the isolation condenser resulting in steam generation (SG). The steam generated in the shell side of the isolation condenser is then vented to the outside atmosphere. During the normal operation, the ISO system is in standby mode. During the standby mode, the steam isolation valves (VS1 and VS2) are open because the condenser tube bundles are at the reactor

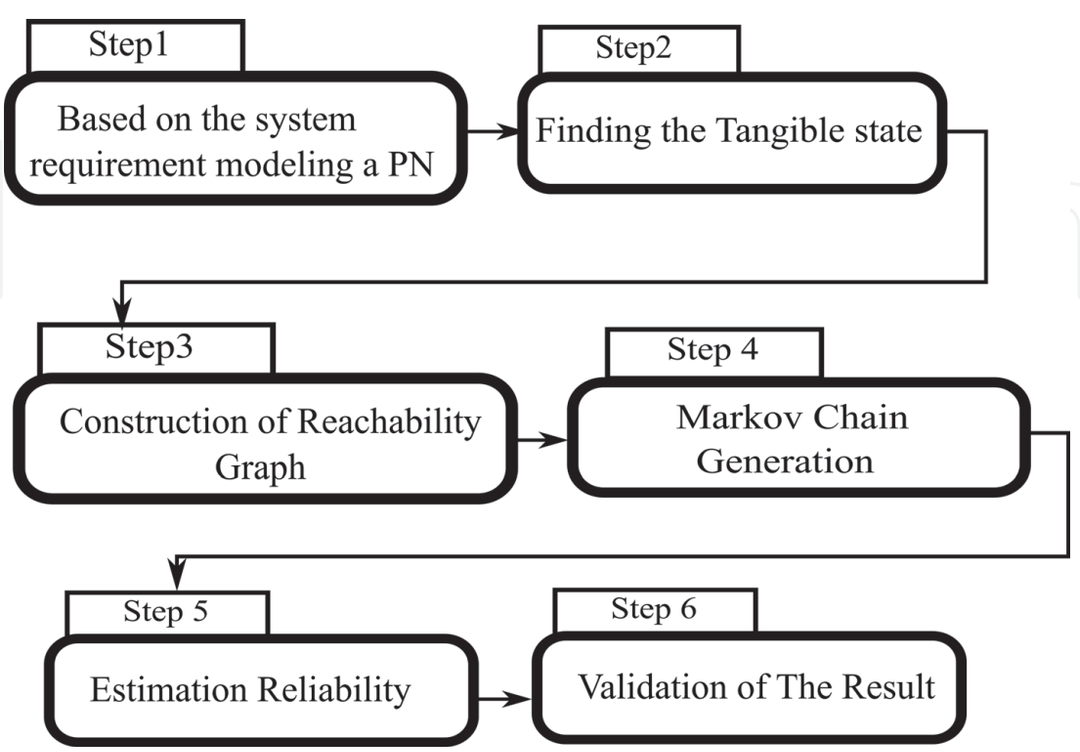


Figure 2.
Proposed framework of the system.

pressure. The condensate is built in the condenser and condensate by returning pipe. The condensate is stopped from a return back to the reactor by closing the condensate return valve (V_{C2}). The condensate valve (V_{C1}) is open at the stand-by condition and vent valves (VV) at main steam lines normally open to vent noncondensable gases from ISO. The makeup water must be provided to prevent uncovering the condenser tubes that are the combination of firewater and condensate using makeup water valve (V_W) normally closed at standby mode. The water inventory on the shell side of the condenser will provide heat removal for between 20 and 90 minutes depending on the plant design, at which time makeup water must be provided to prevent uncovering the condenser tubes. On the shell side of the condenser, the water inventory will be provided for the heat removal between 20 to 90 minutes. At which time water makeup has to be provided to prevent uncovering the condenser system tubes (**Figure 3**).

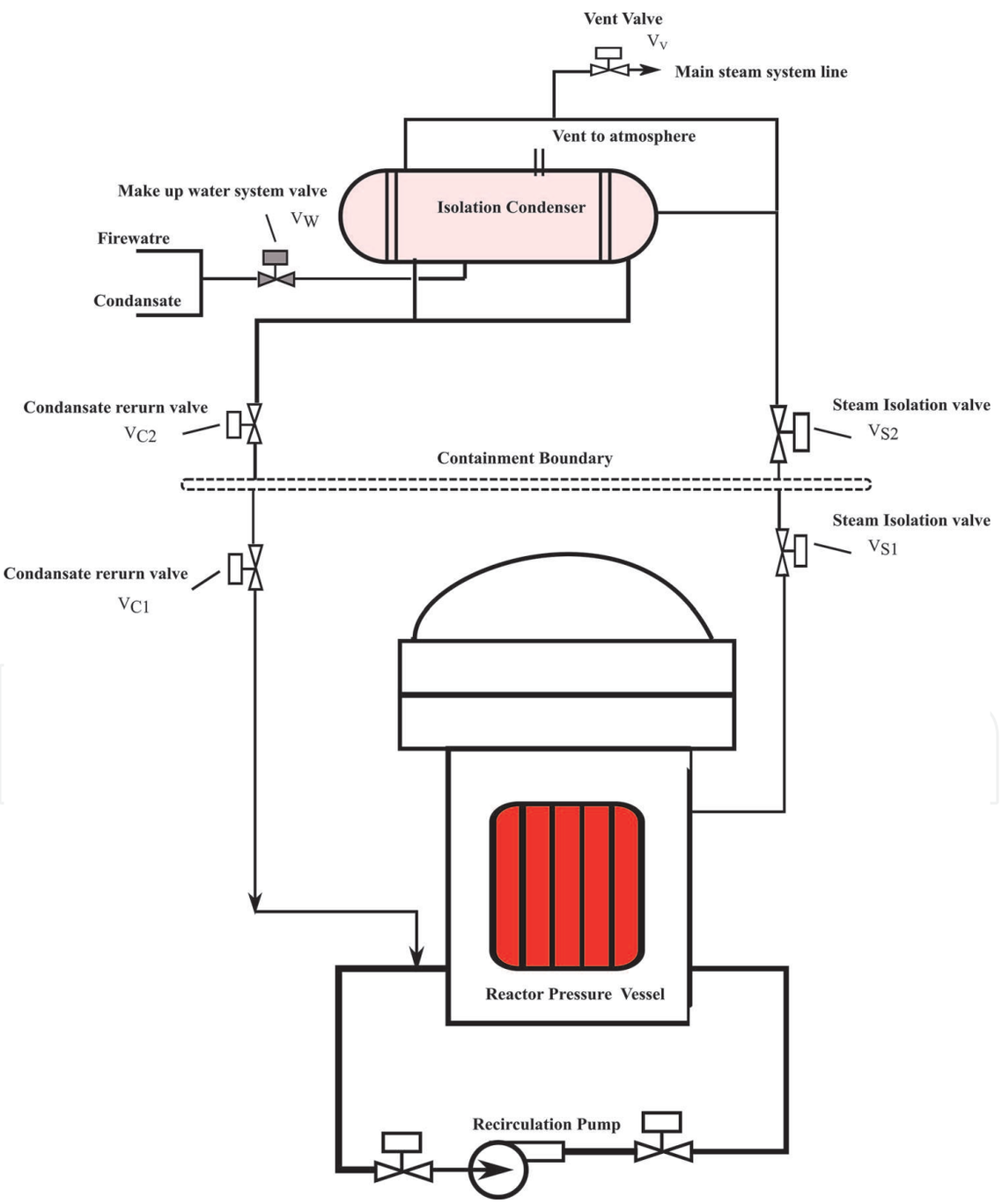


Figure 3.
Schematic diagram of isolation condenser system.

The ISO system may be initiated manually, or automatically initiated on high reactor pressure or low reactor pressure. On the initiation of ISO, one of the condensate return valves (V_{C2}) opens and the vent valve (V_V) gets closed. The steam flows from the reactor vessel to steam isolation valves (V_{S1} and V_{S2}). The steam gets condensed in condenser tube bundles and condensed steam returns to the reactor vessel (V_{C2} and V_{C2}) with help of a recirculation pump. The boiled-off water is replaced by the condensate transfer system or the firewater system. The ISO system is designed in such a way that, the system automatically gets isolated from the reactor pressure vessel in the event of a system pipe break. All the valves are closed automatically (V_{S1}, V_{S2}, V_{C2}, V_{C2}, and V_V) in the event of low differential pressure exceeds three times the normal flow value. This isolation will mitigate the loss of water inventory. The ISO system instrumentation and control consists of initiation and containment isolation circuitry [18]. These circuits provide different functions, both of which are important to system reliability. The entire system is operating in a closed-loop manner.

6. Proposed framework of approach

To estimate the reliability by our approach of the ISO which consist of six steps as shown in **Figure 2** as described step by step as follows:

6.1 PN model generation

In this phase, we construct the PN model of ISO system based on system requirements and specifications. As several researchers have proposed methods [19], based on that we generated a PN model. Based on functional requirements, the activity involves the PN generation to identify the places and transitions of the case study: ISO system. The identified places and transitions as illustrated in **Table 1**.

Thereafter, we use the TimeNet4.5 [20] tool for SPN creation. Then we assign the transition delay to the transition based on the system requirement. To get

Places	Description	Transitions	Description
P0	Sensors detect trip	T0	Sensors detects initial condition
P1	Initial signal generated	T1	Triggers V_V valve close and V_V valve close
P2	Initial condition holds	T2	IC loop triggers
P3	Initial condition forwards	T3	Triggers V_V valve open and V_V valve close
P4	IC loop activated	T4	Triggers V_{s1} valve and V_{s2} valve open
P5	V_{c2} valve close	T5	Send signal to V_w valve open
P6	V_{c1} valve open	T6	Triggers V_w valve open
P7	V_V valve close	T7	Reset
P8	V_{s1} valve open	T8	Reset of AC loss
P9	V_{s2} valve open	T9	Reset of restoration
P10	Level measure makeup		
P11	V_w valve open		
P12	Reset		

Table 1.
ISO places and transitions based on function specification.

throughput values of transition stationary analysis was performed in the TimeNet tool as shown in **Table 2**.

The PN model was generated using TimeNet tools shown in **Figure 4**.

6.2 Tangible states and reachability graph creation

Tangible states are those for timed transitions [21], since we used SPN so there are e tangible states with markings as shown in **Table 3**.

Based on the tangible states of the PN a reachability graph of the PN (**Figure 4**) can be obtained as shown in **Figure 5**.

Transition	Rate	Symbol	Throughput value
T0	1 ms	λ0	0.26966908
T1	1 ms	λ1	0.10385724
T2	1 ms	λ2	0.28610826
T3	1 ms	λ3	0.1771261
T4	1 ms	λ4	0.08883328
T5	1 ms	λ5	0.09000000
T6	1 ms	λ6	0.03244971
T7	1 ms	λ7	0.06681974
T8	1 ms	λ8	0.03152016
T9	1 ms	λ9	0.03244971

Table 2.
ISO throughput values.

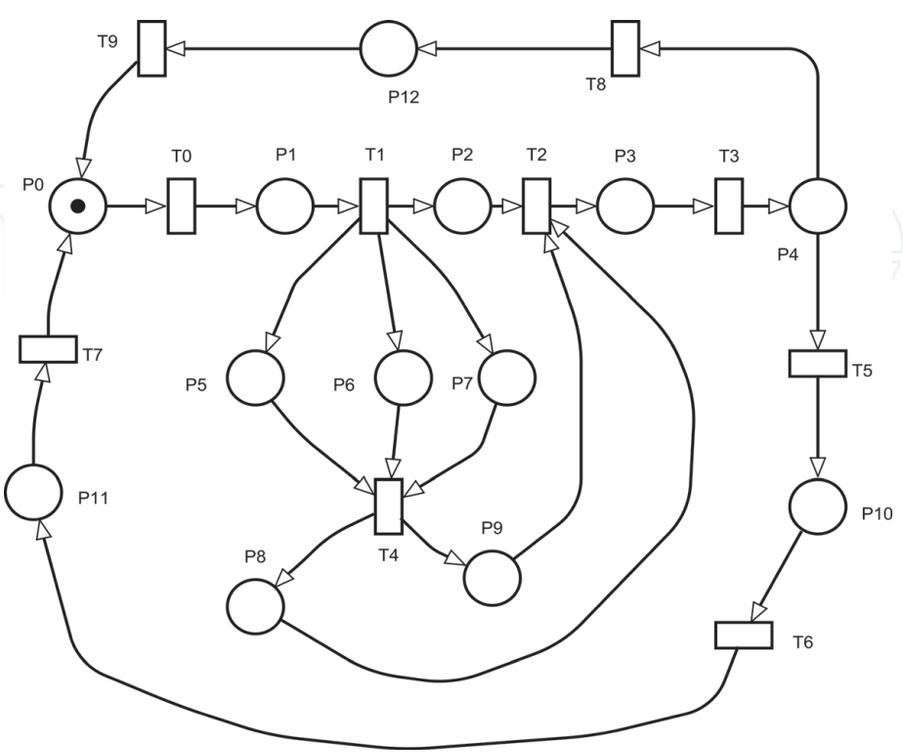


Figure 4.
PN model of ISO.

States	Marking	Tangible
M_0	1,000,000,000,000	Yes
M_1	0100000000000	Yes
M_2	0000010011100	Yes
M_3	0000010000011	Yes
M_4	0000001000000	Yes
M_5	0000000100000	Yes
M_6	0000100000000	Yes
M_7	0010000000000	Yes
M_8	0001000000000	Yes

Table 3.
ISO tangible states with markings of PN.

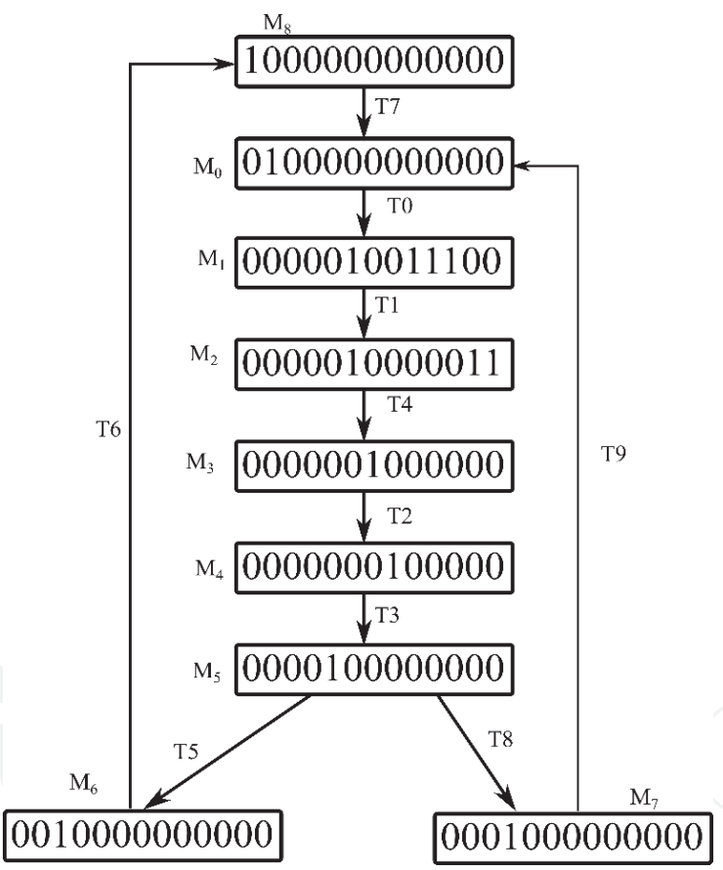


Figure 5.
Reachability graph.

6.3 Markov chain model creation

The MC model shown in **Figure 6** is obtained from the reachability graph of the PN shown in **Figure 4**.

With the help of Q which is transition probability matrix, the transition probability P_{ij} of MC can be computed from SPN. For the transition matrix Q, transitionrate q_{ij} is the transition of one state to another states unit/per time, therefore we take the ratio of the transition q_{ij} and the transition rate of the states sum must be zero. The diagonal elements can be defined as:

$$q_{ii} = -\sum_{j \neq i} qij \tag{3}$$

It is clear that the system is no ergodic, therefore, P_{ij} will be zero and defined as:

$$P_{ij} = \begin{cases} \dfrac{q_{ij}}{\sum_{k \neq i} q_{ik}}, if\ k \neq i \\ \\ 0,\ otherwise \end{cases} \tag{4}$$

$P = I - d_Q^{-1}Q$, where $d_Q = dia(Q)$ *diagonal matrix of* Q.
The transition matrix is given in Eq. (5) as follows:

$$\begin{bmatrix} & M_0 & M_1 & M_2 & M_3 & M_4 & M_5 & M_6 & M_7 & M_8 \\ M_0 & -\lambda 0 & \lambda 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ M_1 & 0 & -\lambda 1 & \lambda 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ M_2 & 0 & 0 & -\lambda 4 & \lambda 4 & 0 & 0 & 0 & 0 & 0 \\ M_3 & 0 & 0 & 0 & -\lambda 2 & \lambda 2 & 0 & 0 & 0 & 0 \\ M_4 & 0 & 0 & 0 & 0 & -\lambda 3 & \lambda 3 & 0 & 0 & 0 \\ M_5 & 0 & 0 & 0 & 0 & 0 & -(\lambda 5 + \lambda 8) & \lambda 8 & \lambda 5 & 0 \\ M_6 & \lambda 9 & 0 & 0 & 0 & 0 & 0 & -\lambda 9 & 0 & 0 \\ M_7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda 6 & \lambda 6 \\ M_8 & \lambda 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda 7 \end{bmatrix}$$

$$= \begin{bmatrix} & M_0 & M_1 & M_2 & M_3 & M_4 & M_5 & M_6 & M_7 & M_8 \\ M_0 & -0.26966 & 0.26966 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ M_1 & 0 & -0.1038 & 0.1038 & 0 & 0 & 0 & 0 & 0 & 0 \\ M_2 & 0 & 0 & -0.0888 & 0.0888 & 0 & 0 & 0 & 0 & 0 \\ M_3 & 0 & 0 & 0 & -0.2861 & 0.2861 & 0 & 0 & 0 & 0 \\ M_4 & 0 & 0 & 0 & 0 & -0.1771 & 0.1771 & 0 & 0 & 0 \\ M_5 & 0 & 0 & 0 & 0 & 0 & -0.0630 & 0.0315 & 0.090 & 0 \\ M_6 & 0.0324 & 0 & 0 & 0 & 0 & 0 & -0.0324 & 0 & 0 \\ M_7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -0.0324 & 0.0324 \\ M_8 & 0.0668 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -0.0668 \end{bmatrix} \tag{5}$$

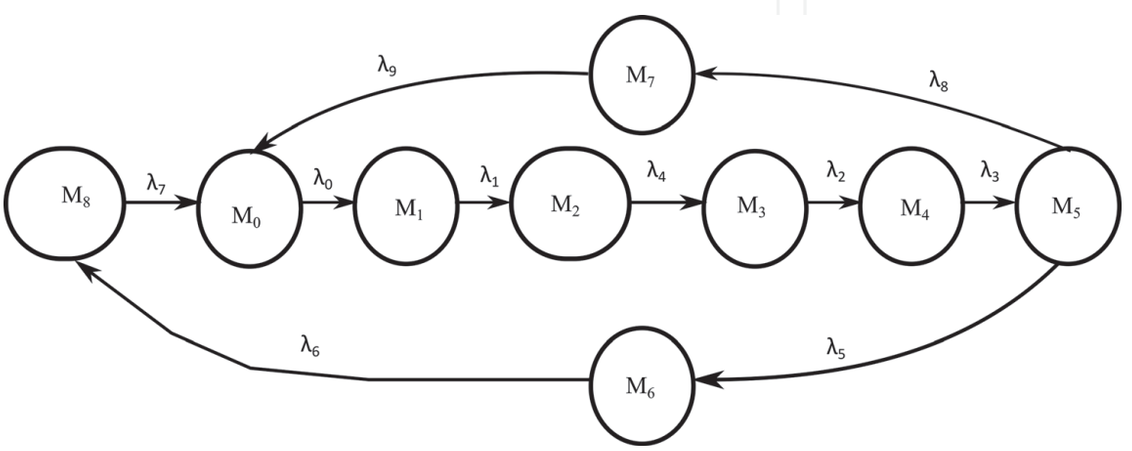


Figure 6.
Markov chain.

Now we solve Eq. (5) to get the design metrics and it seriousness of the NPP as defined in Eq. (6). We solve the Eq. (6) then we get the following linear equations.

$$\begin{bmatrix} & M_0 & M_1 & M_2 & M_3 & M_4 & M_5 & M_6 & M_7 & M_8 \\ M_0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ M_1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ M_2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ M_3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ M_4 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ M_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.7 & 0 \\ M_6 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ M_7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ M_8 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{6}$$

$$M_0 = M_1 \tag{7}$$

$$M_2 = M_1 \tag{8}$$

$$M_2 = M_3 \tag{9}$$

$$M_3 = M_4 \tag{10}$$

$$M_4 = M_5 \tag{11}$$

$$M_5 = 0.2M_6 \tag{12}$$

$$M_5 = 0.7M_7 \tag{13}$$

$$M_6 = M_0 \tag{14}$$

$$M_7 = M_8 \tag{15}$$

$$M_8 = M_0 \tag{16}$$

$$\sum_{i=0}^{8} M_i = 1 \tag{17}$$

6.4 Reliability analysis of proposed framework

Let $p_i(t)$ be the probability which component in state at time t is i. When components execute for $t \to \infty$ then probability leads to the stationary distribution. Then probability is defined as:

$$\vec{p}[p(M_0), p(M_1), p(M_2), p(M_3), p(M_4), p(M_5), p(M_6), p(M_7), p(M_8),] \tag{18}$$

$$\sum_{i \epsilon M} p(i) = 1 \tag{19}$$

$$Reli_{ISO}^{est} = 1 - \sum_{i \epsilon 6} M_i \tag{20}$$

There is only one failure state M_6 in MC. Now we solve the linear equation Eqs. (7)-(16) and Eq. (17) using the standard method, we get steady-state probability of each state as follows:

$M_0 = 0.1282051$, $M_1 = 0.1282051$, $M_2 = 0.1282051$, $M_3 = 0.1282051$, $M_4 = 0.1282051$, $M_5 = 0.1282051$, $M_6 = 0.025641$, $M_7 = 0.1025641$, and $M_8 = 0.1025641$

Hence the reliability of ISO is:

$$\text{Reliability} = 1 - 0.025641 = 0.974359. \tag{21}$$

7. Validation of proposed framework

In section, we compute the rate of failure to ensure the result experimentally of the proposed framework and follow the six steps for reliability estimation [10, 22]. We divide the entire input class into several subclass and for estimating reliability following equation required as:

$$R(t) = \sum_{i=1}^{6} \frac{h_i}{n_i} P(e_i) \tag{22}$$

$P(e_i)$ is the probability specified from input operation data. n_i is the number of trials from each comparable class. h_i is a number of trial cases that are failed.

To estimate the actual reliability **Table 4** data will be used.

Now using Eq. (22) we estimate actual reliability as:

$$Rel_{actual} = 1 - \sum_{i=1}^{6} \frac{h_i}{n_i} P(e_i) = 0.989999$$

Now we compare estimated (predicted) and actual reliability as:

$$\begin{aligned} Reli(diff) &= Rel_{actual} - Reli_{estimated} \\ &= 0.989999 - 0.974359 \\ &= 0.01564 \end{aligned}$$

Hence, the error percentages can be computed as:

$$Error\% = \frac{Rel(diff)}{Rel_{actual}} X100 = \frac{0.01564}{0.989999} X100 = 1.57981\%$$

Hence, the accuracy of proposed reliability computed of proposed framework is $(100 - error\%) = 98.4201\%$ that indicates the validation of our work.

Class	$P(e_i)$	h_i	n_i	$\frac{h_i}{n_i} P(e_i)$
Triggers V_V valve close and V_V valve close	0:028	2	170	0.00039
IC loop triggers	0.023	1	200	0.000115
Triggers V_V valve open and V_V valve close	0.0304	4	200	0.000608
Triggers V_{s1} valve and V_{s2} valve open	0.0987	2	40	0.004935
Send signal to V_w valve open	0.0342	3	30	0.00342
Triggers V_w valve open	0.0032	5	30	0.000533

Table 4.
Reliability estimation using [22].

8. Conclusion

The proposed method is centered technique for computing reliability of instrumentation and control system of the safety-critical system of NPP. We have validated the result with operational and found accuracy with 98.4201%. With this method, software designers take necessary preventive measures early design phase to avoid any kind of failure.

IntechOpen

IntechOpen

Author details

Mohan Rao Mamdikar[1], Vinay Kumar[1*] and Pooja Singh[2]

1 National Institute of Technology, Jamshedpur, India

2 VJIT, Mumbai, India

*Address all correspondence to: vkumar.cse@nitjsr.ac.in

IntechOpen

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Gupta B, Singh P, Singh L. Stability and steady state analysis of control and safety systems of nuclear power plants. Annals of Nuclear Energy. 2020;**147**:107676

[2] Pakonen A, Buzhinsky I, Björkman K. Model checking reveals design issues leading to spurious actuation of nuclear instrumentation and control systems. Reliability Engineering and System Safety. 2021; **205**:107237

[3] Kumar P, Singh LK, Kumar C. Software reliability analysis for safety-critical and control systems. Quality and Reliability Engineering International. 2020;**36**(1):340-353

[4] Chung M, Ahn W, Min B, Seo J, Moon J. An analytical method for developing appropriate protection profiles of instrumentation & control system for nuclear power plants. The Journal of Supercomputing. 2018;**74**(5): 1-16

[5] Zeller M, Montrone F. Combination of component fault trees and Markov chains to analyze complex, software-controlled systems. In: 2018 3rd International Conference on System Reliability and Safety (ICSRS). 23-25 November 2018; 2019. pp. 13-20

[6] Nidhin TS, Bhattacharyya A, Behera RP, Jayanthi T, Velusamy K. Understanding radiation effects in SRAM-based FPGAs for implementing instrumentation and control systems of nuclear power plants. Nuclear Engineering and Technology. 2017;**49**: 1589-1599

[7] Jia G, Ming Y, Bowen Z, Yuxin Z, Jun Y, Xinyu D. Annals of nuclear energy nuclear safety-critical digital instrumentation and control system software: Reliability demonstration. Annals of Nuclear Energy. 2018;**120**: 516-527

[8] Rejzek M, Hilbes C. Use of STPA as a diverse analysis method for optimization and design verification of digital instrumentation and control systems in nuclear power plants. Nuclear Engineering and Design. 2018;**331**:125-135

[9] Torkey H, Saber AS, Shaat MK, El-Sayed A, Shouman MA. Bayesian belief-based model for reliability improvement of the digital reactor protection system. Nuclear Science and Techniques. 2020; **31**(10):1-19

[10] Mamdikar MR, Kumar V, Singh P, Singh L. Reliability and performance analysis of safety-critical system using transformation of UML into state space models. Annals of Nuclear Energy. 2020;**146**:107628

[11] Nayak AK et al. Reliability assessment of passive isolation condenser system of AHWR using APSRA methodology. Reliability Engineering & System Safety. 2009;**94**: 1064-1075

[12] Kumar V, Singh LK, Singh P, Singh KV, Maurya AK, Tripathi AK. Parameter estimation for quantitative dependability analysis of safety-critical and control systems of NPP. IEEE Transactions on Nuclear Science. 2018; **65**(5):1080-1090

[13] Tripathi AM, Singh BLK, Singh CS. Dynamic reliability analysis framework for passive safety systems of nuclear power plant. Annals of Nuclear Energy. 2020;**140**:107139

[14] Buzhinsky I, Pakonen A. Symmetry breaking in model checking of fault-tolerant nuclear instrumentation and control systems. IEEE Access. 2020;**8**: 197684-197694

[15] Singh LK, Vinod G, Tripathi AK. Design verification of instrumentation and control systems of nuclear power

plants. IEEE Transactions on Nuclear Science. 2014;**61**(2):921-930

[16] Xi W, Liu W, Bai T, Ye W, Shi J. An automation test strategy based on real platform for digital control system software in nuclear power plant. Energy Reports. 2020;**6**:580-587

[17] Bao H, Shorthill T, Zhang H. Hazard analysis for identifying common cause failures of digital safety systems using a redundancy-guided systems-theoretic approach. Annals of Nuclear Energy. 2020;**148**:107686

[18] Kvarfordt KJ, Schroeder JA, Wierman TE. System study: Isolation condenser 1998–2018. December 2019

[19] Murata T. Petri nets: Properties, analysis and applications. Proceedings of the IEEE. 2015;**77**(4):541-580

[20] Zimmermann A, German R. Petri Net Modelling and Performability Evaluation with TimeNET 3.0. 2000. pp. 188-202

[21] Akharware N, Miee M, editors. PIPE2: Platform Independent Petri Net Editor. 2005

[22] Brown JR, Lipow M. Testing for software reliability. ACM SIGPLAN Notices. 1975;**10**(6):518-527