



## Original Article

## Design of safety critical and control systems of Nuclear Power Plants using Petri nets

Pooja Singh <sup>a,\*</sup>, Lalit Kumar Singh <sup>b</sup><sup>a</sup> Dept of Mathematical Sciences, IIT (BHU), Varanasi, India<sup>b</sup> Dept of Computer Sc. & Engg IIT (BHU), IIT (BHU), Varanasi, India

## ARTICLE INFO

## Article history:

Received 14 December 2018

Received in revised form

11 February 2019

Accepted 22 February 2019

Available online 2 March 2019

## Keywords:

Safety-critical systems

Performance analysis

Petri nets

Markov chain

## ABSTRACT

Non-functional requirements plays a critical role in designing variety of applications domain ranges from safety-critical systems to simple gaming applications. Performance is one of the crucial non-functional requirement, especially in control and safety systems, that validates the design. System risk can be quantified as a product of probability of system failure and severity of its impact. In this paper, we devise a technique to do the performance analysis of safety critical and control systems and to estimate performance based risk factor. The technique elaborates Petri nets to estimate performability to ensure system dependability requirements. We illustrate the technique on a case study of Nuclear Power Plant system. The technique has been validated on 17 safety critical and control systems of Nuclear Power Plant.

© 2019 Korean Nuclear Society, Published by Elsevier Korea LLC. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

## 1. Introduction

Validation of non functional requirement still poses a challenge in practice [1]. Relatively, a very less effort is devoted to address these requirements, considering an impractical approach of “Fix-it-Later”. Unfortunately, such practices must never be acceptable to safety critical and control systems. Today’s such systems are complex in nature, being composed of heterogeneous hardware, firmware and software components. These systems measure a big set of process parameters to ensure the healthiness of the system, and data routes through such complex architectural environment to fulfill the intended requirements [1–3].

System designers have started taking benefits of recent advancements of high speed microprocessors, their performance, large memory and low cost to design distributed systems. Such systems use more number of microprocessors and heterogeneous components to meet the performance requirements of the system. However the reliability of such system actually depends on the effectiveness of the synchronization among such different and heterogeneous components.

Not meeting performance requirements, a safety system is

declared as fail. Failure of any safety system can lead to catastrophic disasters and hence there is an utmost requirement to deal with. For this reason, researchers are continuously putting their tireless efforts to deal with performability [2] of safety-systems.

The objective of this paper is to introduce the concept of performance-based risk in case of safety critical systems. In order to explain our technique, we first explain the risk that can be involved in safety critical and control system. Then we consider a safety critical distributed system as a set of loosely or tightly coupled components working in synchronized fashion to meet the intended requirements. The performance analysis can be done by using deterministic or stochastic models. However, deterministic models do have several unpractical assumptions like task execution times, task arrival times, and level of synchronization. However, if these parameters are known, a very accurate estimate of performance can be predicted, which will be very useful for safety critical and control systems as generally such systems are real time in nature.

In case stochastic models for performance evaluation, task execution times, task arrival times, etc are usually determined by probability distribution functions. Moreover in case of safety critical and control systems, the synchronization among the tasks can also be modeled because such systems are very small in size and hence there state space is very small. The benefit of using stochastic models is prediction of performance at the early stages of system development life cycle when all the system characteristics are not known and well understood. This predicted value saves a

\* Corresponding author.

E-mail addresses: [poojasingh1615@gmail.com](mailto:poojasingh1615@gmail.com) (P. Singh), [lalit.rs.cse@iitbhu.ac.in](mailto:lalit.rs.cse@iitbhu.ac.in) (L.K. Singh).

significant effort and avoid delay in system development.

In this work, we use Petri nets (PN) to perform the performance analysis to validate the design of safety-critical systems of Nuclear Power Plant (NPP). For this we have taken a real case study of NPP, known as Shutdown System.

In section 2, the related work along with their shortcomings is brought out. Section 3 provides an overview of basic terminologies. Section 4 discusses Bayesian Updating mechanism, on which the proposed technique based on. Section 5 discusses Shutdown System-2 (SDS-2), as a case study, in detail. Our approach for critical component identification of SDS2 is shown in section 6. In section 7, we apply our technique on the case study and show the experimental results along with its validation. Section 8 concludes this paper.

## 2. Related work

Lalit Kumar Singh et al. [1] proposed a methodology for verifying the design of Instrumentation & Control (I&C) systems, for which authors have address the reliability attribute. The proposed methodology is based on Petri nets and demonstrated step-by-step to ease its usage to theoreticians, researchers and practitioners. However, reliability is only one important attribute of dependability. There is a need to address more dependability attributes like safety, security, and performability.

Lalit Kumar Singh and Hitesh Rajput [3] proposed Petri nets based model for dependability analysis, in which reliability and safety attributes are considered. Some of the system properties are also verified like deadlocks, liveness, and boundedness. The proposed method is verified on several safety critical and control systems of NPP. However, being such systems real time in nature, there is a need to perform the performance analysis.

Singh, L. et al. [4] uses Petri net modelling technique to quantify the reliability of safety critical and control systems. The proposed technique transforms Petri net into Markov chain, where evaluation of transition probabilities among states is a challenge. Authors demonstrate a technique to compute transition probabilities on a safety critical system of NPP. However, nothing has been discussed on performance attribute.

Lalit et al. [2] proposed techniques to quantify performance of a test facility system of NPP. Authors have well described the case study of NPP along with system architecture, control flow, etc. The considered system is distributed in nature, where an embedded processing node is exchanging the data with display unit. Although the system is not safety critical in nature but embedded unit is real time in nature. However, token transferred execution time is not accurately modeled, and evaluated only on the assigned delay associated with timed transitions.

Lalit Singh and Hitesh Rajput [5] proposed an effective technique to perform safety analysis during the design phase of safety critical computer based system of NPP. Shutdown system 2 is taken as case study to demonstrate the technique, step by step. However, there are two issues in this method. It very well perform safety analysis qualitatively and also propose technique to address the shortcomings, in case safety analysis results any sort of threat. However, it would prove more beneficial, if a quantitative figure of safety could be derived to gain a significant amount on the system with respect to safety. Also, performance has not been considered in this paper.

V. Kumar et al. [6] proposed a technique for parameter estimation for quantitative dependability analysis of safety critical and control systems. Authors identified an important issue of assumed state transition probabilities, in state-space models that were used for quantification for several attributes of dependability. In this paper, the system requirements are captured using UML approach,

which is transformed into Petri nets. Possible failures are identified in concurrence with system designer. Thereafter, quantitative safety assessment of the system was derived. The technique is demonstrated on Digital Feed Water Control System of NPP. However, performance analysis subject was remain silent, which needs to be addressed.

Vinay et al. [7] proposed a technique for transformation of deterministic models into state space models to perform safety analysis of safety critical systems. The method is validated on many safety critical systems of NPP and demonstrated on Reactor Core Isolation Cooling System. In this method, the probabilities of all the possible hazardous states are computed. However, nothing is dealt as far as performance of the system is concerned.

Raj et al. [8] have taken another interesting dependability attribute – security. This attribute is very important in two situations: (i) when the system is distributed in nature and (ii) when the system is connected with external network. Authors propose threat-driven framework to perform security analysis of safety critical systems. The proposed methodology is demonstrated step-by-step on Digital Feed Water Control System of NPP, in which Petri nets are used to model the system. Security threat may effect performance of the system, which have not been discussed in this paper.

Kumar P et al. [9] proposed an effective and optimized technique to predict the reliability of safety critical systems using Markov chain. In this technique, state explosion problem is attempted to be addressed by minimizing the number of possible states, devising some rules. The technique is validated on shut sown system of NPP. However, there are some limitations of Markov chain like transition rates among states follows exponential distribution, concurrent tasks cannot be modeled, etc. Further, performability issue is not addressed.

## 3. Background of Petri nets

A Petri net is a mathematical and visualization tool, which can model flow of information and control of any kind of system [10]. Mathematically, it is a 5-tuple  $PN = (P, T, F, W, M_0)$  where P is a finite set of places, T is a finite set of transitions, F is a set of arcs such that  $F \subseteq (P \times T) \cup (T \times P)$ , W is a weight function that ranges from 1 to infinity,  $M_0$  is the initial marking that ranges from 0 to infinity. Also,  $P \cap T = \emptyset$  and  $T \cap P = \emptyset$ .

A place, denoted by circle, represents conditions and a transition, denoted by rectangular bar, represents events. A black solid circle, embeds in a place, is known as token and represents the holding of the condition of the place. The number of tokens in each place of PN at a given time represents state of the system and is called marking.

The state of the system depends on firing of transitions that depends on the marking. Firing of transitions causes movement of the tokens. The firings of transitions are governed by the following rules.

- A transition to be fired, needs to be in enable state, which is possible only when each of its input places contains sufficient number of tokens. The sufficiency of the tokens is equal to weight on its input arc.
- On firing of transitions, tokens are removed from each of its input places that depends on the weight of its input arc and tokens are deposited into each of its output arcs that also depends on the weight of its output arc.

The working of PN can be understood by Fig. 1. This scenario represents a reader writer process, where k tokens in place  $p_1$  represents k processes which can read or write in place,  $p_3$ , which







$$= \begin{cases} P(A_{i,t} = h_i - k_i + \eta_i), k_i > \eta_i, h_i \neq K \\ P(A_{i,t} = h_i), k_i \leq \eta_i, h_i \neq K \\ P(A_{i,t} \geq K - k_i + \eta_i), k_i > \eta_i, h_i = K \\ P(A_{i,t} \geq K), k_i \leq \eta_i, h_i = K \end{cases} \quad (5)$$

From Poisson assumptions,  $\eta_i = \frac{R_i \Delta T}{B}$ ,  $P(A_{i,t} = a) = \frac{(\lambda_i \Delta T)^a}{a!} e^{-\lambda_i \Delta T}$   
Also,  $p_{i,k_i}^{h_i}$  depends only on the server through which it is connected and queue states.

$$\therefore p_{(\vec{l}, \vec{k})}^{\vec{h}} = \prod_{i=1}^D p_{i,k_i}^{h_i} \quad (6)$$

**Theorem 1.**  $\forall \vec{Q}_t = \vec{k} \in S_{Q_t} \times \vec{S}_{\theta_t}^i$  and  $\forall \vec{Q}_{t+1} = \vec{h} \in S_{Q_t} \times \vec{S}_{\theta_t}^i$ , the values of  $p_{i,k_i}^{h_i}$  are identical and can be represented as  $p_{i,\theta_v,\theta_\omega}^{n_i}$ .

**Proof** - the proof of this Theorem is straightforward from equation (3). We can write

$$p_{(i,\theta_v,\theta_\omega)}^{n_i} = \frac{p_{(\theta_v,\theta_\omega)}^{(i,n_i)}}{p_{\theta_v}^i} \quad (7)$$

We can create finite state Markov model with respect to SNR for each link, which also considers the noise of Electromagnetic Interference. The transition in states of SNR based finite state Markov model can be because of variations of SNR elements in SNR vector  $\{\gamma_{ji}\}_{j \in \{i\} \cup \xi_i}$ . We make a practical assumption that state transition can occur only in adjacent states.

$$\therefore p_{(\theta_v,\theta_\omega)}^{(i,n_i)} = 0, \forall |n_i - l_i| > 1$$

Let  $LCR(X_{l_i})$  is rate of level crossing, defined as number of times per second SNR passes downward across  $X_{l_i}$  and  $LCR(X_{l_i})\Delta T$  is probability that SNR passes downward across  $X_{l_i}$  in a time slot interval  $\Delta T$ .

$$\therefore LCR(X_{l_i})\Delta T < 1$$

For  $\Delta t \rightarrow 0$ ,  $LCR(X_{l_i})\Delta t$  will represent the probability that SNR passes downward across  $X_{l_i}$  interval small interval of  $\Delta t$ .

Therefore,

$$p_{(\theta_v,\theta_\omega)}^{(l_i,l_i+1)} \approx LCR(X_{l_i})\Delta T, p_{(\theta_v,\theta_\omega)}^{(l_i,l_i-1)} \approx LCR(X_{l_i-1})\Delta T \quad (8)$$

Let  $E_j$  is defined as event that SNR passes downward/upward across a threshold, then we can write:

$$LCR(X_{l_i})\Delta t = \sum_{j \in D} P(E_j) \quad (9)$$

From equations (8) and (9), we get:

$$p_{(\theta_v,\theta_\omega)}^{(l_i,l_i+1)} \approx \sum_{j=1}^D \int \dots \int_0^\infty N_j(\Gamma_{j,l_i}) \Delta T \prod_{k \in \{i\} \cup \xi_i \setminus \{j\}} f(\gamma_{ki}) d\gamma_{ki}$$

and

$$p_{(\theta_v,\theta_\omega)}^{(l_i,l_i-1)} \approx \sum_{j=1}^D \int \dots \int_0^\infty N_j(\Gamma_{j,l_i-1}) \Delta T \prod_{k \in \{i\} \cup \xi_i \setminus \{j\}} f(\gamma_{ki}) d\gamma_{ki} \quad (10)$$

where  $N_j(\Gamma)$  is the level crossing rate of SNR.

We can decompose  $p_{(\theta_v,\theta_\omega)}^{(i,n_i)}$  as follows.

$$p_{(\theta_v,\theta_\omega)}^{(l_i,n_i)} = p_{(\theta_v,\theta_\omega)}^{(l_i,l_i+1)} \times \hat{p}_{(l_i+1,\theta_v,\theta_\omega)}^{n_i} + p_{(\theta_v,\theta_\omega)}^{(l_i,l_i-1)} \times \hat{p}_{(l_i-1,\theta_v,\theta_\omega)}^{n_i} + p_{(\theta_v,\theta_\omega)}^{(l_i,l_i)} \times \hat{p}_{(l_i,\theta_v,\theta_\omega)}^{n_i} \quad (11)$$

And we can have:

$$p_{(\vec{l}, \vec{k}, \vec{h})}^{\vec{n}} = \prod_{i=1}^D p_{(l_i, \vec{k}, \vec{h})}^{n_i} \quad (12)$$

**Theorem 2.** The stationary distribution of the Markov Chain  $(\vec{H}_t, \vec{Q}_t)$  exists;  $\pi$  is unique, and  $\pi > 0$ .

**Proof** - In order to prove the Theorem, we need to propose lemmas.

**Lemma 1.** The Markov chain  $(\vec{H}_t, \vec{Q}_t)$  is irreducible, if  $K < R_t \Delta T$ .

**Proof of Lemma 1:** Lemma 1 can be proved by proving that there exists a multi-transition path -  $(\vec{l}, \vec{k}) \rightarrow (\vec{n}, \vec{h})$  with probability greater than 0 for each transition from state  $(\vec{l}, \vec{k})$  to  $(\vec{n}, \vec{h})$ . The proof is as follows.

**a) Case 1:**  $(\vec{l}, \vec{k}) \rightarrow (\vec{l}^*, \vec{k}), \forall \vec{l}^* = \{\vec{l}_i \in \{1, \dots, L\} : \mathbf{R}_i \Delta T \geq \mathbf{k}_i\}_{i \in D}$

We start by proving  $p_{(\vec{l}, \vec{k}, \vec{k})}^{\{l_i+1\}_{i \in D}} > 0, p_{(\vec{l}, \vec{k}, \vec{k})}^{\{l_i-1\}_{i \in D}} > 0$  and  $p_{(\vec{l}, \vec{k}, \vec{k})}^{\vec{l}} > 0$ . From equation (12), there is a need to prove

$p_{(l_i, \vec{k}, \vec{k})}^{(l_i+1)} > 0, p_{(l_i, \vec{k}, \vec{k})}^{(l_i-1)} > 0$  and  $p_{(l_i, \vec{k}, \vec{k})}^{l_i} > 0$ , which is equivalent to

prove that  $p_{(l_i, \theta_v, \theta_\omega)}^{(l_i+1)} > 0, p_{(l_i, \theta_v, \theta_\omega)}^{(l_i-1)} > 0$  and  $p_{(l_i, \theta_v, \theta_\omega)}^{l_i} > 0$ , according to

**Theorem 1.** Here  $\vec{k} \in S_{Q_t} \times \vec{S}_{\theta_t}^i$ . This statement has strong validation from equation (7), as  $p_{\theta_v}^i > 0$ . Also from equation (10), we get  $p_{(\theta_v, \theta_\omega)}^{(l_i, l_i+1)} > 0, p_{(\theta_v, \theta_\omega)}^{(l_i, l_i-1)} > 0$  and  $p_{(\theta_v, \theta_\omega)}^{(l_i, l_i)} > 0$ .

Next, we need to prove that  $p_{(\vec{l}, \vec{k})}^{\vec{k}} > 0$ . Since  $A_{i,t} = k_i - \max[0, k_i - R_i \Delta T] \geq 0$ , from equations (5) and (5) we have  $p_{i,k_i}^{k_i} > 0$  and  $p_{(\vec{l}, \vec{k})}^{\vec{k}} > 0$ .

Therefore from equation (4),

$$p_{(\vec{l}, \vec{k})}^{\{l_i+1\}_{i \in D}, \vec{k}} > 0, p_{(\vec{l}, \vec{k})}^{\{l_i-1\}_{i \in D}, \vec{k}} > 0,$$

$$p_{(\vec{l}, \vec{k})}^{\vec{l}} > 0$$

Also, there exists a multi-transition path from  $(\vec{l}, \vec{k})$  to  $(\vec{l}^*, \vec{k})$  as following two ways, with non zero probability of each transition.

$$(\vec{l}, \vec{k}) \rightarrow (\{l_i + 1\}_{i \in D}, \vec{k}) \rightarrow \dots \rightarrow (\{l_i^* - 1\}_{i \in D}, \vec{k}) \rightarrow (\vec{l}^*, \vec{k}) \quad (13)$$

$$(\vec{l}, \vec{k}) \rightarrow (\{l_i - 1\}_{i \in D}, \vec{k}) \rightarrow \dots \rightarrow (\{l_i^* + 1\}_{i \in D}, \vec{k}) \rightarrow (\vec{l}^*, \vec{k}) \quad (14)$$

**b) Case 2:**  $(\vec{l}^*, \vec{k}) \rightarrow (\vec{l}^*, \vec{h})$

In this case, we prove that  $p_{\vec{l}^*, \vec{k}}^{\vec{h}} > 0$ .

$\because A_{i,t} = h_i - \max[0, k_i - R_i \Delta T] \geq 0$ , given  $R_i \Delta T > k_i$

From equations (5) and (6),

$$p_{\vec{l}_i^*, k_i}^{h_i} > 0, p_{\left(\vec{l}^*, \vec{k}\right)}^{\vec{h}} > 0$$

Next we prove that  $p_{\vec{l}^*, \vec{k}}^{\vec{h}} > 0$ . It is clear from equation (12), we only need to prove that  $p_{\vec{l}_i^*, \vec{k}_i}^{\vec{h}_i} > 0$ . It is equivalent to prove that

$p_{\left(\vec{l}_i^*, \theta_v, \theta_\omega\right)}^{\vec{h}_i} > 0$ , where  $\vec{k} \in S_{Q_i} \times \vec{S}_{\theta_v}^i$  and  $\vec{h} \in S_{Q_i} \times \vec{S}_{\theta_\omega}^i$ . From equation (7), and  $\pi_{\vec{l}_i^* | \theta_v} > 0$ , we only have to prove that  $p_{\left(\theta_v, \theta_\omega\right)}^{\vec{l}_i^*, \vec{h}_i} > 0$ . We have already proved that  $p_{\left(\theta_v, \theta_\omega\right)}^{\left(\vec{l}_i^*, \vec{h}_i + 1\right)} > 0$ ,  $p_{\left(\theta_v, \theta_\omega\right)}^{\left(\vec{l}_i^*, \vec{h}_i - 1\right)} > 0$  and  $p_{\left(\theta_v, \theta_\omega\right)}^{\left(\vec{l}_i^*, \vec{h}_i\right)} > 0$ . Therefore we only need to prove:

$$\exists \hat{p}_{\left(\vec{l}_i^* + 1, \theta_v, \theta_\omega\right)}^{\vec{h}_i} \cup \hat{p}_{\left(\vec{l}_i^* - 1, \theta_v, \theta_\omega\right)}^{\vec{h}_i} \cup \hat{p}_{\left(\vec{l}_i^*, \theta_v, \theta_\omega\right)}^{\vec{h}_i} > 0$$

$\hat{p}_{\left(\vec{l}_i^*, \theta_v, \theta_\omega\right)}^{\vec{h}_i}$  is always greater than zero, irrespective of  $\theta_v$  and  $\theta_\omega$  relationship.

$$\therefore p_{\vec{l}^*, \vec{k}}^{\vec{h}} > 0$$

Therefore, from equation (4),

$$\left(\vec{l}^*, \vec{k}\right) \rightarrow \left(\vec{l}^*, \vec{h}\right) > 0 \tag{15}$$

**c) Case 3:**  $\left(\vec{l}^*, \vec{h}\right) \rightarrow \left(\vec{n}, \vec{h}\right)$

The proof is similar to case 1.

From equations (2)–(4), we can prove the following:

$$\exists \left(\vec{l}, \vec{k}\right) \rightarrow \left(\vec{l}^*, \vec{k}\right) \rightarrow \left(\vec{l}^*, \vec{h}\right) \rightarrow \left(\vec{n}, \vec{h}\right)$$

Where

$$R_i \Delta T \geq k_i$$

$\because K \leq R_i \Delta T$ ,  $\exists \vec{l}_i^*$  that satisfies this condition.

The stationary or steady state distribution of the ergodic process can be uniquely determined by the following balance equations.

$$\vec{\pi} = [\pi(M_0), \pi(M_1), \dots, \pi(M_{17})]$$

$$\vec{\pi} = \vec{\pi} P, \sum_{i \in M} \pi(i) = 1$$

Where  $\pi_i(t)$  be the probability that the system is in state  $i$  at time  $t$  and it is considered that system executes for a very long time  $t \rightarrow \infty$ . The steady state probabilities, for each marking is given in Table 2.

**5.4. Phase4: performance quantification**

In our case the reachability set of PN is finite. However, for

**Table 2**  
Steady state marking probabilities of SDS2 PN Places

$P[M_0] = 3.311 \times 10^{-3}$	$P[M_1] = 8.2 \times 10^{-4}$	$P[M_2] = 3.311 \times 10^{-3}$
$P[M_3] = 3.311 \times 10^{-3}$	$P[M_4] = 1.655 \times 10^{-3}$	$P[M_5] = 0.163$
$P[M_6] = 3.344 \times 10^{-5}$	$P[M_7] = 1.66 \times 10^{-5}$	$P[M_8] = 3.311 \times 10^{-3}$
$P[M_9] = 8.34 \times 10^{-10}$	$P[M_{10}] = 8.32 \times 10^{-6}$	$P[M_{11}] = 0.0815$
$P[M_{12}] = 0.0815$	$P[M_{13}] = 0.164$	$P[M_{14}] = 4.17 \times 10^{-10}$
$P[M_{15}] = 2.455 \times 10^{-3}$	$P[M_{16}] = 0.082$	$P[M_{17}] = 8.2 \times 10^{-4}$

several systems there may be infinite reachability set, for example in communication systems, acknowledgement may take longer time. Analysing such systems is complicated due to infinite reachability set. However, researchers have proposed many techniques to solve such cases empirically and analytically. For example, infinite reachability set can be truncated [9], ensuring integrity of system specification. The resultant reachability set will be finite which can give approximated results. Empirically, one could analyse the reachability set sincerely to eliminate practically possible states [3,5]. Also reachability set can be reduced by eliminating states which are not safe or by prioritising the transitions, which are in race condition. However, a care should be taken that such modifications destroys the Markovian property.

To quantify the performance, we consider two calculations.

**5.4.1. Communication channel to capture trip parameters values**

Token deposition in  $p_{pd}$ , on deviation of trip parameters process range. During communication CRC calculation is being done. The transitions reading value, sending, receive acknowledgement have exponentially distributed execution times. There is a fixed timeout time, in which the message needs to be send again. Therefore timeout transition does not follow exponential distribution. It is to be noted that random variable time that denotes timeout has Erlangian probability density function. The values communicate to system, represented by a token in  $p_{pd}$  at Poisson rate  $\lambda$ . Therefore, the throughput of the communication system is  $\lambda(1 - \rho)$ . In our case, the baud rate of communication network is 9600 with 5% of error probability and packet size is 128 bytes. Then performance measures for packet containing the values of trip parameters are: (i) for sending packet, the rate is 8.325 firings/second (ii) for lost packets (data packet of acknowledgement), the rate is 4.01 firings/second (iii) for CRC check, the rate is 80.23 firings/second (iv) for timeout condition, the rate is 1.00 firings/second.

**5.4.2. Poison injection process**

Once token gets deposited in  $p_{pd}$ , poison injection takes place as per Petri net model, shown in Fig. 5. We assume that the service times are independent and exponentially distributed with parameter  $\mu_i$ ,  $i = 0, \dots, 7$ . The objective function in this process is total throughput  $\sum_{i=0}^7 \lambda_0$ . The numerical results with 95% of confidence interval are presented in Table 3.

The average delay may be computed when the system is busy or packet acknowledgement is lost or on-hold. In such case, delay can be computed using Little's result as  $N = \lambda T$ , where  $\lambda$  is throughput. For the values used above, the average delay in the entire process of injection of poison on trip parameter deviation is 0.2576 s.

The results have been validated on 17 systems of Nuclear Power Plants, out of which 9 systems are control systems, 6 systems are

**Table 3**  
Throughput (firings/sec) of SDS2 transitions.

$\lambda[t_{pd}] = 4.22$	$\lambda[t_{Ch}] = 5.21$	$\lambda[t_{Coff}] = 4.81$	$\lambda[t_{inc}] = 3.89$
$\lambda[t_{avo}] = 5.20$	$\lambda[t_{avo}] = 4.77$	$\lambda[t_{sta}] = 4.98$	$\lambda[t_{avc}] = 3.98$

safety critical systems and 2 systems are monitoring systems.

## 6. Conclusion

The work focuses on a technique for evaluating the performance of the system using Petri nets, to validate the design, especially of safety critical and control systems. The analysis was based on Petri nets, Markov chain and proposing new related theorems along with their proofs. The proposed technique has a potential to address the challenges and limitations of the existing techniques that are discussed in section 2. The technique is applied on 17 different safety critical, control and monitoring systems of NPP and is demonstrated on a SDS2. The case study is well described along with its functions, architecture and boundary conditions. Our experimental results strongly validate our approach.

## Appendix A. Supplementary data

Supplementary data to this article can be found online at <https://doi.org/10.1016/j.net.2019.02.014>.

## References

- [1] Lalit Kumar Singh, Gopika Vinod, A.K. Tripathi, Design verification of instrumentation and control systems of NPP, *IEEE Trans. Nucl. Sci.* 61 (April 2014) 921–930.
- [2] L.K. Singh, G. Vinod, A.K. Tripathi, Modeling and prediction of performability of safety critical computer based systems using Petri nets, in: 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops, Dallas, TX, 2012, pp. 85–94.
- [3] Lalit Kumar Singh, Hitesh Rajput, Dependability analysis of safety critical real-time systems by using Petri nets, *IEEE Trans. Control Syst. Technol.* (March 2017) 1–12.
- [4] L. Singh, H. Rajput, G. Vinod, A.K. Tripathi, Computing transition probability in Markov chain for early prediction of software reliability, *Qual. Reliab. Eng. Int.* (2015), <https://doi.org/10.1002/qre.1793>.
- [5] Lalit Singh, Hitesh Rajput, Ensuring safety in design of safety critical computer based systems, in: *Annals of Nuclear Energy*, vol. 92, Elsevier, June 2016, pp. 289–294.
- [6] V. Kumar, L.K. Singh, P. Singh, K.V. Singh, A.K. Maurya, A.K. Tripathi, Parameter estimation for quantitative dependability analysis of safety-critical and control systems of NPP, *IEEE Trans. Nucl. Sci.* 65 (5) (May 2018) 1080–1090.
- [7] Vinay Kumar, Lalit Singh, A.K. Tripathi, Transformation of deterministic models into state space models for safety analysis of safety critical systems: a case study of NPP, in: *Annals of Nuclear Energy*, vol. 105, Elsevier, July 2017, pp. 133–143.
- [8] Raj Kamal, Lalit Singh, Babita Pandey, Security analysis of safety critical and control systems: a case study of nuclear power plant system, *Nucl. Technol.* 197 (3) (2017) 296–307, <https://doi.org/10.1080/00295450.2016.1273702>.
- [9] P. Kumar, L.K. Singh, C. Kumar, An optimized technique for reliability analysis of safety-critical systems: a case study of nuclear power plant, *Qual. Reliab. Eng. Int.* (2018) 1–9. <https://doi.org/10.1002/qre.2340>.
- [10] T. Murata, Petri nets: properties analysis and applications, *Proc. IEEE* 77 (1989) 541–580.
- [11] C. Ramchandani, Analysis of Asynchronous Concurrent Systems by Petri Nets, M.I.T., Cambridge, MA, 1974. Project MAC, TR-120.
- [12] CANDU 6 Program Team, CANDU 6 Tech. Summary, May 2005.
- [13] Lalit Singh, Gopika Vinod, A.K. Tripathi, An approach for Parameter estimation in Markov model of software reliability for early prediction: a case study, *IET Softw.* 9 (3) (June 2015) 65–75.