Reliability Engineering and System Safety 150 (2016) 44–57

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Study on the systematic approach of Markov modeling for dependability analysis of complex fault-tolerant features with voting logics

Kwang Seop Son [a,b,*], Dong Hoon Kim [a], Chang Hwoi Kim [a], Hyun Gook Kang [b]

[a] I&C/Human Factors Research Division, Korea Atomic Energy Research Institute, Republic of Korea
[b] Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, Republic of Korea

ARTICLE INFO

Article history:
Received 1 June 2015
Received in revised form
11 January 2016
Accepted 24 January 2016
Available online 1 February 2016

Keywords:
Systematic approach
Markov modeling
System failure rate
System unavailability rate
Reactor protection system

ABSTRACT

The Markov analysis is a technique for modeling system state transitions and calculating the probability of reaching various system states. While it is a proper tool for modeling complex system designs involving timing, sequencing, repair, redundancy, and fault tolerance, as the complexity or size of the system increases, so does the number of states of interest, leading to difficulty in constructing and solving the Markov model. This paper introduces a systematic approach of Markov modeling to analyze the dependability of a complex fault-tolerant system. This method is based on the decomposition of the system into independent subsystem sets, and the system-level failure rate and the unavailability rate for the decomposed subsystems. A Markov model for the target system is easily constructed using the system-level failure and unavailability rates for the subsystems, which can be treated separately. This approach can decrease the number of states to consider simultaneously in the target system by building Markov models of the independent subsystems stage by stage, and results in an exact solution for the Markov model of the whole target system. To apply this method we construct a Markov model for the reactor protection system found in nuclear power plants, a system configured with four identical channels and various fault-tolerant architectures. The results show that the proposed method in this study treats the complex architecture of the system in an efficient manner using the merits of the Markov model, such as a time dependent analysis and a sequential process analysis.

1. Introduction

The Markov model is a mathematical model in which the future state of a system depends only on its current state and not on its past history. This model is accomplished by drawing system state transition diagrams and examining theses diagrams to understand how certain undesirable (failed) states are reached and their relative probability. The Markov model is a proper tool for modeling complex systems involving timing, sequencing, repair, redundancy, and fault tolerance [1]. Therefore, it is widely used to quantify system dependability in areas such as performance, availability, reliability, and safety [2–10], and different solution techniques for various Markov models have been studied [11]. However, the Markov model rapidly becomes large and unwieldy as the system size increases and thus it is difficult to construct and solve Markov models for large systems [12–14]. To cope with this drawback, the dynamic fault tree analysis (DFTA) which includes dynamic behavior gates such as functional dependency gates, spare gates, and priority-AND gates has been proposed [15–17], but in general a repair process could not be applied to DFTA. Simplifying the Markov model is necessary to handle complex systems with ease. Some mathematical simplification approaches have been studied, such as a size reduction of the transient probability matrix [18,19], and state merging [20,21]. However these methods have some limitations, such as that the transient matrix should have lumpability of states, as well as identical transition rates to common states. Further, to obtain a simplified Markov model, the original Markov model for the complex system is still necessary in these cases.

Various other works on Markov model simplification have been done. Ranjbar et al. analyzed system states using a performance matric and simplified the Markov model by eliminating the states

Abbreviations: BLM, Bistable logic module; CLM, Coincidence logic module; CTMC, Continuous time Markov chain; DFTA, Dynamic FTA; DMR, Dual modular redundant; DTMC, Discrete time Markov chain; FCF, Fault coverage factor; FTA, Fault tree analysis; IEC, International Electrotechnical Commission; MA, Markov model for availability analysis; MTTF, Mean time to failure; MTTR, Mean time to repair; NPP, Nuclear power plant; PFD, Probability failure on demand; PLC, Programmable logic controller; RBD, Reliability block diagram; RPS, Reactor protection system; TMR, Triple modular redundant

* Corresponding author.
E-mail address: ksson78@kaeri.re.kr (K.S. Son).

http://dx.doi.org/10.1016/j.ress.2016.01.014
0951-8320/

that result from failed states and will never happen in the system [22], a method that can only be applied to specific systems because the performance metric should be defined considering the target system's performance requirements. In some literature, simplification methods for the Markov model in DFTA were proposed [23–27]. In these works, elimination of irrelevant states and their aggregation were proposed to simplify the Markov model in a similar way shown in [18–21] and state truncation was used to approximate the Markov model, being valid for small probabilities. A repair process was not considered in these cases though, so Yevkin proposed an approximation of the Markov model for a repairable system in DFTA [28] using state truncation. According to this work, approximation quality depends on the truncation order; the greater the order of truncation, the more dynamic the model. Therefore, in order to obtain accurate results, the order of truncation should be large, which means that Markov model generation for the target system must have already been completed.

In related research, Markov model simplification has been studied to obtain the probability failure on demand (PFD) for quantitative safety assessments to determine safety integrity levels as defined by the IEC 61508 standard. The combination of a Markov model with a reliability block diagram (RBD) has been suggested [29,30], where an RBD of the target system is first constructed, then simplified by removing the blocks with a rare probability, with Markov models built for each simplified RBD. In a similar way, Verlinden et al. proposed a hybrid method combining the RBD and Markov model [31], where the RBD can describe a series and parallel connections; this model however cannot express the sequencing and repairing process between blocks. Bowles et al. suggested an approximation method to obtain the mean time to failure (MTTF) of the target system [32]. They noted that the target system is composed of a series of k-out-of-n subsystems, so they substituted the failure rate of the subsystems with 1/MTTF (which they called effective failure rate) from the subsystem Markov models, and then obtained the system MTTF through the summation of the effective failure rates of each subsystem (as the target system is formed as a series of connected subsystems). This approximation approach is similar to those of [29–31] and is valid for MTTF larger than mean time to repair (MTTR), but the approximation error will be larger when there is no repair process in the subsystem. Guo et al. developed an automatic Markov model creation technique using a computer program [33], although the large size of the model caused by the large number of states makes it difficult to read and revise manually whenever necessary.

Generally, these studies have shown that the Markov model can be simplified by state merging and aggregation, with these methods resulting in an exact solution. However, there are limitations for practical applications and thus some approximation approaches have been studied using the elimination of rare probability states, truncation of states, and hybrid methods.

In the current study, we present a systematic approach to simplify the Markov model using system failure rate and system unavailability rate in order to analyze the dependability of complex fault-tolerant systems. This approach results in an exact solution for the continuous-time Markov chain (CTMC) in contrast with those studies that result in an approximation solution for the discrete-time Markov chain (DTMC). We decompose the target system into several failure-independent subsystems based on the function block diagram of the target system, and then obtain the system failure rate and system unavailability rate from the Markov models of the subsystems. These rates allow us to easily make the Markov model for the target system and obtain its reliability and availability.

The paper is mainly composed of two sections. In Section 2, we describe the system decomposition method based on the function block diagram of the target system, and define the system failure rate and system unavailability rate. A simple example demonstrates how the systematic approach for the Markov model analyzes reliability and availability. In Section 3, this approach is applied to the reactor protection system (RPS) in nuclear power plants (NPP). These systems usually contain four identical channels with various fault-tolerant architectures applied in each channel, making an RPS typically very difficult to model without a systematic approach.

2. Systematic approach to build a Markov model

For a given system, the Markov model consists of a list of possible states, the possible transition paths between these states, and the rate parameters (failure rate and repair rate) of these transitions. When representing the Markov model graphically, each state is usually depicted as a circle with arrows denoting the transition path between states, as depicted in Fig. 1.

In Fig. 1, λ (the failure rate) denotes the rate parameter of the transition from state 0 to state 1, and μ (the repair rate) denotes the rate parameter of the transition from state 1 to state 0 (this paper assumes that all components' failure and repair rates are constant). $P_j(t)$ denotes the probability of the system being in state j at time t. Typically it is assumed that the device is in a normal state at the initial time $t=0$, and therefore the initial probabilities of the two states are $P_0(0)=1$ and $P_1(0)=0$. Thereafter, the probability of state 0 decreases at the constant rate λ, which means that if the system is in state 0 at any given time, the probability of making the transition to state 1 during the next increment of time dt is λdt . In a similar way, if the system is in state 1, the probability of making the transition to state 0 during the next increment of time dt is μdt. Therefore, the incremental change dP_0 is expressed by the sum of the product of dP_0 and λdt with the product of dP_1 and μdt as:

$$dP_0(t) = -P_0(t)\lambda dt + P_1(t)\mu dt \tag{1}$$

The state equation for state 1 can be obtained in a similar way. For the system, equations can be expressed in a matrix form:

$$\begin{bmatrix} \frac{dP_0(t)}{dt} \\ \frac{dP_1(t)}{dt} \end{bmatrix} = \begin{bmatrix} P_0(t)' \\ P_1(t)' \end{bmatrix} = \begin{bmatrix} -\lambda & \mu \\ \lambda & -\mu \end{bmatrix} \begin{bmatrix} P_0(t) \\ P_1(t) \end{bmatrix}, \begin{bmatrix} P_0(0) \\ P_1(0) \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} (\text{initialcondition}) \tag{2}$$

Eq. (2) can be also expressed as a vector notation (see Appendix):

$$\boldsymbol{P}' = \boldsymbol{AP}, \boldsymbol{P}(0) = \boldsymbol{K} \tag{3}$$

The eigen value $\boldsymbol{\lambda}$ and eigen vector $\boldsymbol{\Phi}$, of $\boldsymbol{A}$ are:

$$\boldsymbol{\lambda} = \begin{bmatrix} 0 \\ -\lambda-\mu \end{bmatrix}, \boldsymbol{\Phi} = \begin{bmatrix} \frac{\mu}{\lambda} & -1 \\ 1 & 1 \end{bmatrix} \tag{4}$$

The solution of Eq. (4) can be obtained through

$$\boldsymbol{P} = \begin{bmatrix} P_0(t) \\ P_1(t) \end{bmatrix} = \boldsymbol{\Phi C_N} e^{-\lambda t} = \begin{bmatrix} \frac{\mu}{\lambda} & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & -\lambda-\mu \end{bmatrix} \begin{bmatrix} 1 \\ e^{-(\lambda+\mu)t} \end{bmatrix}$$

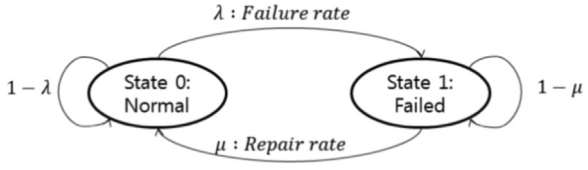

Fig. 1. Simple Markov model.