ISSN 0002-306X. Изв. НАН РА и ГИУА. Сер. ТН. 2006. Т. LIX, № 1.

UDC 62-50

AUTOMATION &
CONTROL SYSTEMS

R. PAICHUK

MODELLING SYSTEM RELIABILITY OF FAULT-TOLERANT SYSTEMS WITH THE SEMI-MARKOV STATE SPACE APPROACH

Fault-tolerant systems can be analyzed by Markov state space approach but for more sophisticated and large systems, there should be some other means to estimate the system parameters. Here we extend the Bounding Theorem, we use it in software developements of ultrareliable computer systems to Fire & Gas systems which is a new approach in their safety parameter calculations.

Keywords: state-space, fault-tolerant, reliability, mean, variance.

Introduction. Traditionally, the reliability analysis of a complex system has been accomplished with combinatorial mathematics. The standard fault-tree method of reliability analysis is based on such mathematics. Unfortunately, the fault-tree approach is incapable of analyzing systems in which reconfiguration is possible. Basically, a fault tree can be used to model a system with :

1. Only permanent faults (no transient or intermittent).
2. No reconfiguration.
3. No time or sequence failure dependencies.
4. No state-dependent behavior.

Because fault trees are easier to solve than Markov models, fault trees should be used wherever these fundamental assumptions are not violated.

In reconfigurable systems the critical factor often becomes the effectiveness of the dynamic reconfiguration process. It is necessary to model such systems by using more powerful Markov modelling technique. A Markov process is a stochastic process whose behavior depends only upon the current state of the system. Markov state-space models have four main categories:

1. Discrete space and discrete time.
2. Discrete space and continuous time.
3. Continuous space and discrete time.
4. Continous space and continuous time.

The second category is the one most useful for modelling fault-tolerant systems. Only models that contain a finite number of states will be used. However, the transition time between the states is not discrete and can take on any real value.

Reliability Modelling. The first step in modelling a system with a discrete space and continuous-time Markov model is to represent the state of the system with a vector of attributes that change over time. These attributes are typically system characteristics such as the number of working processors, the number of spare units or the number of faulty units that have not been removed. The more attributes in the model, the more complex the model, thus, the smallest set of

attributes that can accurately describe the fault-tolerant behavior of the system is typically chosen. The next step in the modelling process is to characterize the transition time from one state to another. Because this transition time is rarely deterministic, they are described by a probability distribution.

Typically, the transitions of a fault-tolerant system model fall into two categories; slow failure and fast recovery transitions. We will start modelling with two major types of systems; no reconfigurable and configurable systems.

Let *T* be a random variable representing the time to failure of the system. Next, we have to define a distribution for *T*, say *F(t)*. typically electronic component and consequently systems are assumed to fail according to exponential distribution [1]:

$$F(t) = \text{Prob}[\,T < t\,] = 1 - e^{-\lambda t}\,.$$

Then the important concept in reliability modelling the hazard rate, *h(t*) is defined as:

$$h(t) = F'(t)/[1 - F(t)] = \lambda\,,$$

which is the failure rate itself. The exponential distribution is the only distribution with a constant hazard rate. The Markov model representing this system is as follows.

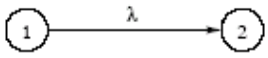

Fig. 1. Model of simplex system

In this Markov model, state 1 represents the operational state in which our system works, state 2 represents the system failure state in which the simplex system has failed, and the transition from state 1 to state 2 represents the occurrence of the failure.

For reliability modelling purposes, electronic components are generally assumed to fail according to the exponential distribution . Some handbooks offer a more complete discussion on the problem of estimating the reliability of electronic components. Once the reliability of each component in a system is known, the failure rate of the system is simply the sum of the failure rates of the individual components.

For example, suppose $\lambda_1, \lambda_2, \ldots, \lambda_n$ represent the failure rates of the components, letting *T* be a random variable representing the time of failure of the system and T_i, i=1,2,...,n, representing the time of the *i* th component of failure, the distribution of failure for the system $F_c(t)$ is determined as follows [2] :

$$\begin{aligned} F_c(t) &= \text{Prob}\,\left[\,T < t\,\right] = \\ &= \text{Prob}\left[\,\min\{T_1, T_2, \ldots, T_n\} < t\,\right] = \\ &= 1 - \text{Prob}\,[\,T_1 > t,\, T_2 > t, \ldots, T_n > t\,]. \end{aligned}$$

And if we assume that the components fail independently, then :

$$F_c(t) = 1 - \prod_{i=1}^{n} \text{Prob}\,[T_i > t\,] =$$

$$= 1 - \prod_{i=1}^{n} \exp(-\lambda_i\, t) =$$

$$= 1 - \exp + \left(- \sum_{i=1}^{n} \lambda_i\, t \right),$$

which is an exponential distribution with failure rate :

$$\lambda = \sum_{i=1}^{n} \lambda_i$$

Modelling Static Redundant Systems. The triple modular redundant (TMR) is one of the simplest fault tolerant architectures and the more sophisticated model of this kind which can be called NMR (N modular redundant). The computers are assumed to be physically isolated, so that a failed computer cannot affect another working computer. This means that they are assumed to fail independently.

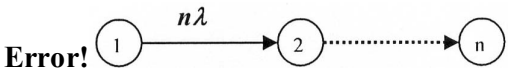

Fig. 2. Model of NMR System

The solution of the Markov model is conceptually simple, although the details can be cumbersome. The *n*-state Markov model leads to a system of *n*-coupled differential equations. These equations may simply be represented with the vector notation. Let ***P(t)*** be a vector that gives the probability of being in each state at time *t*. The n-state Markov model in Figure 2 [3] is

$$\boldsymbol{P}(t) = \left[\boldsymbol{P}_1(t), \boldsymbol{P}_2(t), \ldots, \boldsymbol{P}_n(t)\right].$$

The system of differential equations is given by :

$$\boldsymbol{P}'(t) = \boldsymbol{P}(t)\boldsymbol{A}\ ,$$

where

$$\boldsymbol{A} = \begin{bmatrix} -n\lambda & n\lambda & \cdots & \cdots & 0 \\ 0 & -(n-1)\lambda & (n-1)\lambda & \cdots & 0 \\ 0 & & -(n-2)\lambda & & \\ \vdots & & & \ddots & (n-1)\lambda \\ 0 & & & & 0 \end{bmatrix}.$$

The matrix $\boldsymbol{A}$ is easily constructed by thinking of the Markov model in terms of flow in and flow out. You can begin with the off-diagonal components. As there is a transition from state 1 to state 2 the entry at a_{12} is nonzero, and the value of a_{12} is the transition rate $n\lambda$. The diagonal entries are obtained by summing all non-diagonal entries on the same row and negating it. The solution will be :

$$P(t) = P(0)e^{At},$$

where

$$P(0) = [1,0,0]$$

is the initial state probability and the system begins in a fault free state. If the model is changed in Figure 3, then the matrix $\boldsymbol{A}$ becomes:

$$\boldsymbol{A} = \begin{bmatrix} -n\lambda & n\lambda & \cdots & \cdots & 0 \\ \alpha & -(n-1)\lambda - \alpha & (n-1)\lambda & \cdots & 0 \\ 0 & & -(n-2)\lambda & & \\ \vdots & & & \ddots & \\ 0 & & & & 0 \end{bmatrix}.$$

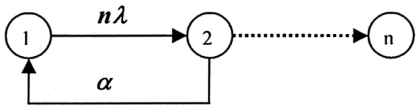

Fig. 3. Altered model

The probability of NMR system failure as a function of mission time and also as a function of *N* is given in Figures 4 and 5.

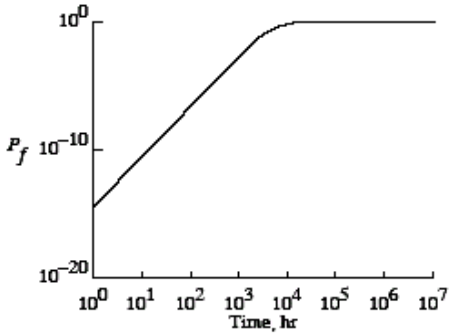

Fig. 4. As a function of mission time

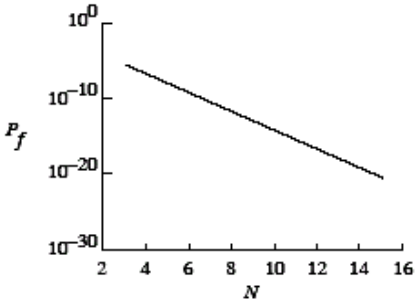

Fig. 5. As a function of N

Modelling Reconfigurable Systems. Fault tolerant systems are often designed by using a strategy of reconfiguration. Reconfiguration strategies come in many varieties, but always involve the logical or physical removal of a faulty component. Two basic reconfiguration strategies occur–degradation and replacements with spares. The degradation method involves the permanent removal of a faulty component without replacement. The reconfigured system continues with reduced set of components. The replacement with spares method involves both the removal of faulty components and their replacement with a spare.

Reliability Analysis Programs. Some reliability analysis programs have been developed for ultra reliable computer/electronic system architectures. These methods provide an efficient means for computing accurate upper and lower bounds for the state probabilities of a large class of semi-Markov models. These programs distinguish between fast and slow transitions. If the mean transition time μ is small with respect to the mission time T, that is $\mu<T$, then the transition is fast, otherwise it is slow. The mathematics on which these reliability analysis programs are based is called "Bounding Theorem".

Path-Step Classification & Notation. The theorem provides bound on the death state probabilities at a specified time. It is assumed that the system is initially in a single state that is P(o) = 1. The programs find every path from the start state to a death state. The contribution of each path to system failure is calculated separately by using the semi-Markov bounding theorem of white.

Each state along the path can be classified into one of there classes that are distinguished by the type of transitions leaving the state. A state and all transitions leaving it will be referred to as a "path step". The transition on the path that is currently being analyzed will be referred to as a "path step". The transition on the path that is currently being analyzed will be referred to as the "on-path transition".

The remaining transitions will be referred to as the "off-path transitions". The classification is made on the basis of whether on-path and off-path transitions are slow or fast [4].

Class I path step ; Slow on path, slow off path . If all transitions leaving the state are slow, then the path step is class 1. The rate of on-path exponential transition is λ_i.
(see fig 6).

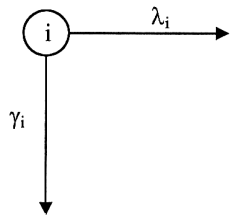

Fig. 6. Class I path step

An arbitrary number of slow off-path transitions can occur and the sum of their exponential transition rates is λ_i .

Class 2 path step ; Fast on path, arbitrary off path . If the on-path transition is fast, the path step is class 2. An arbitrary number of slow or fast off-path transitions may exist. As before, the slow off-path, exponential transitions can be represented as a single transition with a rate equal to the sum of all the slow off-path transitional rates. The distribution of the fast on-path transition is $F_{i,1}$.
The distributions of time for the *k*th fast transition from state *i* is referred to as $F_{i,k}$ (the probability that the next transition out of state *i* goes into state *k* and occurs within time *t* is $F_{i,k}$) . Three measurable parameters must be specified for each fast transition. The transition probability $\rho(F^*_{i,k})$, the conditional mean $\mu(F^*_{i,k})$, and the variance σ^2 ($F^*_{i,k}$), given that this transition occurs. The asterisk is used to note that the parameters are defined in terms of the conditional distributions combined with definition.

Mathematically, these parameters are defined as follows:

$$\rho\ (F^*_{i,k}) = \int_0^\infty \prod_{j \neq k} \left[1 - F_{i,j}(t)\right] dF_{i,k}(t),$$

$$\mu\ (F^*_{i,k}) = \frac{1}{\rho\ (F^*_{i,k})} \int_0^\infty t \prod_{j \neq k} \left[1 - F_{i,j}(t)\right] dF_{i,k}(t),$$

$$\sigma^2\ (F^*_{i,k}) = \frac{1}{\rho\ (F^*_{i,k})} \int_0^\infty t^2 \prod_{j \neq k} \left[1 - F_{i,j}(t)\right] dF_{i,k}(t) - \mu^2(F_{i,k}).$$

Experimentally, these parameters correspond to the fraction of times that a fast transition is successful and the mean and the variance of the conditional distribution given that the transition occurs.

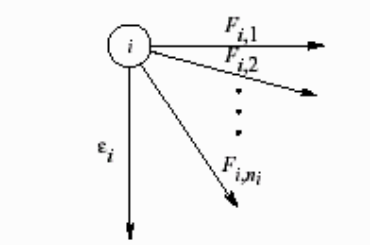

Fig. 7. Class 2 path step . Fast on path, arbitrary off path

Note, in any experiment where competing processes in a system are studied, the observed empirical distributions will be conditional. The time it takes a system to transition to the next state will only be observed when that transition occurs. These expressions are defined independently of the exponential transitions ε_j.

Consequently, the sum of the fast transition probabilities $\Sigma\rho(F^*_{i,k})$ must be 1. In particular, if only one fast transition occurs, its probability is I and the conditional mean is equivalent to the unconditional mean. (The user does not have to deal explicitly with the unconditional distributions $F_{i,k}$. However, to develop the mathematical theory, the distribution must be used)

Class 3 path step : slow on path, fast off path. The on-path transition must be slow for a path step to be categorized as class 3. Both slow and fast off-path transitions can exist; however, at least one off-path transition must be fast (see Fig.7). The path step 2 3 in the model of the triad plus one spare shown in Figure 8 are in this class. The slow on-path transition rate is α_j. The sum of the slow off-path transition rates in β_j . As in class2, the transition probability $\rho(G^*_{j,k})$, the conditional mean $\mu(G^*_{j,k})$, and the conditional variance $\sigma^2(G^*_{j,k})$ must be given for each fast off-path transition with distribution $G_{j,k}$. Two letters are used to help track whether the transition is a class 2 (labeled *F*) or class 3 (labelled *G*) in the current path.

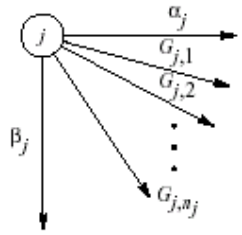

Fig. 8. Class 3 path step. Slow on path, fast off path

In either case, the analyst supplies the conditional mean, the conditional standard deviation, and the transition probability. Although, the parameters described above suffice to specify a class 3 path step, the mathematical theory is more easily expressed in terms of the holding time in a state. It is the time the system remains in the state before it transitions to some other state. The bounding theorem is expressed by using a slightly different holding time, which will be referred to as "recovery holding time" to prevent confusion. The recovery holding time is the holding time in the state with the slow exponential distributions removed. Because the slow exponential transitions occur at a rate many orders of magnitude less than the fast transitions, the recovery holding time is approximately equal to the traditional holding time. Let H_j represent the distribution of the recovery holding time in state *j*:

$$H_j(t) = 1 - \prod_{k=1}^{n_j} \left[1 - G_{j,k}(t) \right] .$$

Then the following parameters are used in the theorem :

$$\mu(H_j) = \int_0^{\infty} \prod_{k=1}^{n_f} \left[1 - G_{j,k}(t)\right] dt,$$

$$\sigma^2(H_j) = 2\int_0^{\infty} t \prod_{k=1}^{n_j} \left[1 - G_{j,k}(t)\right] dt - \mu^2(H_j).$$

These parameters are the mean and the variance of the holding time in state *j* without consideration for slow exponential transitions (i.e., with the slow exponential transition removed) . These parameters do not have to be supplied to the programs. The program derives these parameters from the other available inputs, such as $\rho(G^*_{j,k})$, $\mu(G^*_{j,k})$, and $\sigma^2(G^*_{j,k})$ $\sigma^2(G^*_{j,k})$, as follows [4]:

$$\mu(H_j) = \sum_{k=1}^{n_j} \rho(G^*_{j,k}) \mu(G^*_{j,k}),$$

$$\sigma^2(H_j) = \left\{ \sum_{k=1}^{n_j} \rho(G^*_{j,k}) \left[\sigma^2(G^*_{j,k}) + (\mu^2 G^*_{j,k})\right] \right\} - \mu^2(H_j).$$

The parameters $\rho(G^*_{j,k})$, $\mu(G^*_{j,k})$, and $\sigma^2(G^*_{j,k})$ are defined exactly as the class 2 path step parameters.

Although the fast distributions are specified without consideration of the competing slow exponential transitions, the theorem gives bounds that are correct in the presence of such exponential transitions . The parameters were defined in this manner to simplify the process of specifying a model . throughout the paper, the holding time in a state in which the slow transitions have been removed will be referred to as "recovery holding time." For convenience, when referring to a specific path in the model, the distribution of a fast on-path transition will be indicated by a single subscript that specified the source stat. For example, if the transition with distribution $F_{j,k}$ is the on-path transition from state *j* , then it can be referred to as F_j, where $F_{j,k}$ is the *k*th fast transition from state *j* and F_j is the on-path fast transition from state *j*.

Let us formulate the result. Let *D(T)* be the probability of entering a particular death state within the mission time *T,* following a path with *k* class1, *m* class 2 and *n* class 3 path steps.

$$LB < D(T) < UB,$$

where

$$UB = Q(T) \prod_{i=1}^{m} \rho(F_i^*) \prod_{j=1}^{n} \alpha_j \mu(H_j),$$

$$LB = Q(T - \Delta) \prod_{i=1}^{m} \rho(F_i^*) \left[1 - \varepsilon_i \mu(F_i^*) - \frac{\mu^2(F_i^*) + \sigma^2(F_i^*)}{r_i^2} \right] \times$$

$$\times \prod_{j=1}^{n} a_j \left\{ \mu(H_j) - \frac{(a_j + \beta_j)\left[\mu^2(H_j) + \sigma^2(H_j)\right]}{2} - \frac{\mu^2(H_j) + \sigma^2(Hj)}{s_j} \right\}$$

for all r_j , $s_j > 0$ with $\Delta = r_1 + r_2 \ldots + r_n + s_1 + s_2 \ldots + s_n$ and $Q(T)$ = the probability of traversing a path consisting of only the class 1 path steps within time T.

The theorem is true of any $r_j>0$ and $s_j>0$ provided that $\Delta < T$. Different choices of these parameters will lead to different bounds. The SURE program uses the following values of r_j and s_j:

$$r_i = \left\{2T\left[\mu^2(F_i^*) + \sigma^2(F_i^*)\right]\right\}^{1/3},$$

$$s_j = \left\{T\left[\frac{\mu^2(H_j) + \sigma^2(H_j)}{\mu(H_j)}\right]\right\}^{1/2}.$$

These values have been found to give very close bounds in practice and are usually very near the optimal choice [1].

Two simple algebraic approximations for $Q(T)$ were given. One approximation overestimates and one approximation underestimates, and are given respectively as

$$Q(T) < Q_u(T) = \frac{\lambda_1\lambda_2\lambda_3\ldots\lambda_k T^k}{kl}, \qquad Q(T) > Q_l(T) = Q_u(T)\left[1 - \frac{T}{k+1}\sum_{i=1}^{k}(\lambda_i + \gamma_i)\right].$$

Both $Q_u(T)$ and $Q_l(T)$ are close to $Q(T)$ as long as $\sum_{i=1}^{k}(\lambda_i + \gamma_i)T$ is small, that is, as long as the mission time is short compared with the average lifetime of the components. Some programs use the following slightly improved upper bound on $Q(T)$ [4]:

$$Q(T) < Q_u^*(T) = \frac{1}{|S|!}\prod_{i\in S}(\lambda_i T),$$

where

$$S = \{i \mid \lambda_i T < 1\}.$$

This bound is obtained by removing all the fast exponential transitions from the $Q(T)$ model. Because the path is short, the probability of reaching the death state is larger than that of the original $Q(T)$ model.

REFERENCES

1. **Beasley, Michael**. Reliability for Engineers. - McMillan, 1991.- 262 p.
2. “Reliability” Lecture 29, Engs 27-Discrete and Probabilistic Systems. Winter, 2003. – 42 p.
3. **Roush L. Marvin, Webb M.** Willie Applied Reliability Engineering. - Center for Reliability Engineering, The University of Maryland, 1998. – 535 p.
4. **Butler W. R., Johnson C. Sally.** Techniques for Modelling the Reliability of Fault-Tolerant Systems with the Markov State-Space Approach, 1995. – 125 p.

SEUA. The material is received on 15.02.2006.

Ր. ՓԱՅՉՈՒԿ

ԽԱՓԱՆՈՒՄՆԵՐԻ ՆԿԱՏՄԱՄԲ ԴԻՄԱՑԿՈՒՆ ՀԱՄԱԿԱՐԳԵՐԻ ՀՈՒՍԱԼԻՈՒԹՅԱՆ ՄՈԴԵԼԱՎՈՐՈՒՄԸ ԿԻՍԱՄԱՐԿՈՎՅԱՆ ՎԻՃԱԿՆԵՐԻ ՏԱՐԱԾՈՒԹՅԱՆ ՕԳՏԱԳՈՐԾՄԱՄԲ

Խափանումների նկատմամբ դիմացկուն համակարգերը կարող են վերլուծվել Մարկովյան վիճակների տարածության օգտագործմամբ, սակայն, երբ համակարգերը բավականաչափ բարդ են, անհրաժեշտ է օգտագործել այլ եղանակներ՝ վերջիններիս պարամետրերը հաշվարկելու նպատակով: Հավանականությունների տեսության կենտրոնական սահմանային թեորեմի հիման վրա մշակված մոտեցումը, որը [4] աշխատանքում օգտագործվել է գերբարձր հուսալիությամբ օժտված քոմփյութերային համակարգերի ծրագրային ապահովումների մշակման ժամանակ, ներկա աշխատանքում տարածվում է հակահրդեհային հուսալիության պարամետրերի գնահատման բնագավառի վրա:

Առանցքային բառեր. վիճակների տարածություն, խափանումանդիմացկուն, հուսալիություն, միջին արժեք, դիսպերսիա:

Р. ПАЙЧУК

МОДЕЛИРОВАНИЕ НАДЕЖНОСТИ ТОЛЕРАНТНЫХ ОТНОСИТЕЛЬНО ОТКАЗОВ СИСТЕМ С ПРИМЕНЕНИЕМ ПОЛУМАРКОВСКИХ ПРОСТРАНСТВ СОСТОЯНИЙ

Толерантные относительно отказов системы могут быть исследованы на основе применения полумарковских пространств состояний. Однако в случаях, когда системы достаточно сложны, необходимо воспользоваться другими методами с целью вычисления параметров таких систем. Подход, разработанный на основе центральной предельной теоремы теории вероятностей и примененный в [4] при разработке программного обеспечения компьютерных систем, в настоящей работе распространяется на область оценивания параметров надежности противопожарных систем.

Ключевые слова: пространство состояний, толерантный относительно отказов, надежность, среднее значение, дисперсия.