UDC 004.05

MORAVEJ SEYED MILAD, A.P. FECENIUK, V.A. ROMANKEVICH

National Technical University of Ukraine «KPI», Ukraine

THE PROBABILITY OF MULTIPROCESSOR SYSTEM FALLING INTO DANGEROUS STATE ESTIMATION

In this paper the problem of determining the probability of multiprocessing control system falling into one of states marked as dangerous, were formalized. Statistical estimates of the probability that a system is in a dangerous state were obtained. This estimates, may help in providing safety for multiprocessor systems. There were proposed equations to change the estimation for probability of system falling into a dangerous state during operation for multi-processor systems with embedded self test feature.

Key words: *control system, dangerous state, failure.*

Introduction

Multiprocessor control systems are applied in the most critical fields of human activity, such as aviation and space systems, nuclear power plant control systems, large-scale production systems. Such systems shall satisfy the highest standard of functional safety, because the cost of their failure is significant financial loss or even human life. Modern multi-processor control systems may be builton any variety of processors, may be equipped with built-in failure detection and trouble-shooting system, may have a multi-level hierarchical structure. Safety analysis of the above control systems is relevant and highly complex scientific task.

Note that the security is the compound concept [1]. In this paper we paid attention to one probabilistic safety indicator that is the probability of a multiprocessor control system falling into a dangerous state.

1. Definitions and naming

Let us consider the behave or of multiprocessor control system in the interval of working time $[0;t]$. Let the number of processor sin the system be n. Let $x_1, x_2, ..., x_n$, be binary variables reflecting the state of processors: $x_i = 0$ if failure occurs during the interval of working time $[0;t]$ and $x_i = 1$ otherwise/

Let's denote p_i as probability of failure-free functioning over a period $[0;t]$, then $q_i = 1 - p_i$ would be the probability of fault of the i-th processor in this time period. We should note that the probability of failure-free functioning of the i-th processor in the interval $[0;t]$ is determined according to well-known relation $p_i = e^{-\lambda_i t}$, where λ_i - the failure rate of i-th processor. λ_i values are tabulated.

Also let's denominate binary vector $\mathbf{X} = (x_1, x_2, ..., x_n)$, whose components are the states of processors, as the state vector of the system. Within this paper, we assume that the system state is defined by a set of states of all its components, and thus the concept of "system state" and "state vector" are used interchangeably.

The set of all possible system states is denoted $B(n)$, it is obvious that the number of different states of the system equals 2^n. Among the set of functions performed by the control system, there are those even a single failure of which leads to a dangerous state of the complex "object of control - the control system." Let us term this state of a multiprocessor system as dangerous.

Let the set of dangerous states of the system be denoted $D(n)$. Also, let's introduce the term – the function that indicates dangerous states of the system, $\varphi(\mathbf{X})$:

$$\varphi(\mathbf{X}) = \begin{cases} 0, & \mathbf{X} \notin D(n), \\ 1, & \mathbf{X} \in D(n). \end{cases}$$

2. The probability of system falling into a dangerous state assessment

The probability $P(D(n))$ system is falling into a dangerous state is:

$$P(D(n)) = \sum_{\mathbf{X} \in B(n)} \varphi(\mathbf{X}) P(\mathbf{X}), \qquad (1)$$

here $\mathbf{X} \in B(n)$ denotes that the sum is performed for all binary vectors of length n, $P(\mathbf{X})$ - stands for the probability of the processors for which $x_i = 0$ failed in $[0;t]$ period, and processors for which $x_i = 1$ were functioning properly.

The probability of the state vector of the system $P(\mathbf{X})$ used in equation (1) is:

$$P(\mathbf{X}) = \prod_{i=1}^{n} \tilde{p}_i ,$$

where $\tilde{p}_i$ is the probability that the i-th processor is in a state designed by x_i, i.e.,

$$\tilde{p}_i = x_i \cdot p_i + (1 - x_i) \cdot q_i . \qquad (2)$$

Note that in (2) binary variables x_i are used as integers that posses values 0 or 1, which allows us to write conditional statements in short form. It is obvious that for large enough values of n calculations in (1) are impossible to perform in approachable time. In this case, the value of the probability of system falling into a dangerous state can be evaluated using statistical tests.

Specialized generator produces random or pseudo-random test affections that are applied to the model of the object and that is the way statistical tests are running. Statistics accumulates and statistical estimates of studied amounts can be formed according to the list of results of such tests. The general scheme of the statistical tests described in detail in [2].

In this paper $P(D(n))$ the probability of the system falling into a dangerous state is discussed. Pseudo-random probations series are represented by state vector $\mathbf{X}$. Model must determine whether a state is dangerous. It is specified as function $\varphi(\mathbf{X})$. For these purposes GL-model [3] with minor modifications can be used.

Note that for the same amount during statistical tests estimates may differ. Here are four statistical estimates of $P(D(n))$ which are denoted as $\overline{P_1(D(n))}$, $\overline{P_2(D(n))}$, $\overline{P_3(D(n))}$ and $\overline{P_4(D(n))}$. Parameters $p_{gen}^{(1)}(x_i = 1)$, $p_{gen}^{(2)}(x_i = 1)$, $P_{gen}^{(3)}(\mathbf{X})$, $P_{gen}^{(4)}(\mathbf{X})$ are pseudorandom generators for vectors of the system. Properties of un bias edness and consistency can be proven for all these statistical estimates, taking into account generation parameters shown above.

According to the classical approach of the probability parameters of computer systems evaluation by statistical tests, probability of a dangerous state is [4]:

$$\overline{P_1(D(n))} = \frac{1}{L_1} \sum_{\mathbf{X} \in \Omega_1(n)} \varphi(\mathbf{X}) , \qquad (3)$$

where $\Omega_1(n)$ is the set of a pseudo-random binary vectors of length n. It is formed with a specialized generator, for which probability of 1-value occurrence for i-th position in each test run is

$$p_{gen}^{(1)}(x_i = 1) = p_i ,$$

$L_1 = |\Omega_1(n)|$ is number of statistical tests. Note that this approach is rarely used in practice since it requires a large number of experiments to achieve an acceptable accuracy of the estimate.

Statistical estimates of the dangerous state's probability may be obtained using so-called "quickening of statistical tests" [4] method:

$$\overline{P_2(D(n))} = \frac{\sum_{\mathbf{X} \in \Omega_2(n)} \varphi(\mathbf{X}) \cdot \gamma^{-(n - w(\mathbf{X}))}}{L_2 \cdot K} , \qquad (4)$$

where γ is the coefficient determining the degree of speeding up, $\Omega_2(n)$ is the set of binary vectors of length n, formed with a specialized generator for which probability of 1-value occurencef or i-th position in each test run is

$$p_{gen}^{(2)}(x_i = 1) = \frac{p_i}{p_i + \gamma \cdot q_i} ,$$

$L_2 = |\Omega_2(n)|$ is the number of statistical tests performed, $w(\mathbf{X})$ stands for weight (number of 1-value components) of binary vector $\mathbf{X}$, K is a constant for a given system, which is defined as follows:

$$K = \prod_{i=1}^{n} \frac{1}{p_i + \gamma \cdot q_i} .$$

In papers [5, 6] the grouping of state vectors $\mathbf{X}$ according to their weights (the number of 1-valued components) are used in order to reduce the statistical error.

Using the technique of the statistical test proposed in [5], we can obtain statistical estimate

$$\overline{P_3(D(n))} = \sum_{m=0}^{n} \left(\frac{S(n,m)}{L_3(m)} \cdot \sum_{\mathbf{X} \in \Omega_3(n,m)} \varphi(\mathbf{X}) \right), \qquad (5)$$

where $\Omega_3(n,m)$ is the set of pseudo-random binary vectors of length n and weight m, formed with a specialized generator for which the probability of vector $\mathbf{X}$ occurrence in each test is

$$P_{gen}^{(3)}(\mathbf{X}) = \frac{P(\mathbf{X})}{S(n,m)} ;$$

$L_3(m) = |\Omega_3(n,m)|$ is the number of statistical tests (for each m);

$S(n,m)$ – the sum of the probabilities of the state vector with weight m and length n, ie

$$S(n,m) = \sum_{\mathbf{X} \in W(n,m)} P(\mathbf{X}) ,$$

where $\mathbf{X} \in W(n,m)$ notation means that the sum is performed for all binary vectors of length n with the weight m, $W(n,m)$ - the set of all binary vectors of length n, who has weight m.

Values $S(n,m)$ can be computed using the Rushdie algorithm [7]:

$$S(i,j) = p_i \cdot S(i-1,j-1) + q_i \cdot S(i-1,j),$$

where $i,j \le n$; $S(0,0) = 1$; $S(i,j) = 0$ if $i < 0$.

Based on the results published in [6], statistical evaluation of the probability that a system in a dangerous state is:

$$\overline{P_4(D(n))} = \sum_{m=0}^{n} \left(\frac{C_n^m}{L_4(m)} \sum_{\mathbf{X} \in \Omega_4(n,m)} \varphi(\mathbf{X}) P(\mathbf{X}) \right), \quad (6)$$

where $\Omega_6(n,m)$ is the set of pseudo-random binary vectors of length n and weight m, formed with a specialized generator for which the probability of occurrence of vector $\mathbf{X}$ in each test is

$$P_{gen}^{(4)}(\mathbf{X}) = \frac{1}{C_n^m};$$

$L_4(m) = |\Omega_4(n,m)|$ is the number of statistical tests (for each m).

3. The probability of multiprocessor system entering dangerous state after the failure of processor subset

Modern multi-processor systems are designed with embedded self testing features, that can detect faults during system's operating. This section proposes the mathematical tool for revaluating the probability of hitting the system in a dangerous state after subset of its processors failure.

We denote I as the set of indices of failed processors, let J be the set of indexes of processors that are up at the time of control, it is obvious that $I \cup J = \{1,2,...,n\}$. Let $\mathbf{X}(I) = (x_i | i \in I)$ be the part of the state vector of the system $\mathbf{X}$, containing only the binary variables x_i with indices from the set I, and $\mathbf{X}(J) = (x_i | i \in J)$ be the part of the state vector of the system $\mathbf{X}$, containing only the binary variables x_i with indices from the set J. $\mathbf{X}(I) \equiv 0$ means that in positions of vector $\mathbf{X}$ from the set of I only zero values were found, and the binary variables from $\mathbf{X}(J)$ can be set arbitrarily. Let $k = |J|$ be the cardinality of the set J, it is obvious that $|I| = n - k$.

Due to this, the probability of system falling into dangerous state after a subset of processors failure is:

$$P(D(n) | \mathbf{X}(I) \equiv 0) = \sum_{\mathbf{X}(J) \in B(k)} \varphi(\mathbf{X}) \cdot P(\mathbf{X}).$$

During calculating $P(\mathbf{X})$ we may consider that x_i with indices from the I set are equal to zero, so that

$$P(D(n) | \mathbf{X}(I) \equiv 0) = \left(\prod_{i \in I} q_i \right) \times \times \left(\sum_{\mathbf{X}(J) \in B(k)} \varphi(\mathbf{X}) \cdot P(\mathbf{X}(J)) \right).$$

When fixing zero-values on $(n-k)$ positions, the indicator function of the dangerous state of the system degenerates into a function of k boolean variables, which we denote as ψ:

$$\varphi(\mathbf{X})|_{\mathbf{X}(I) \equiv 0} = \psi(\mathbf{X}(J)).$$

Thus,

$$P(D(n) | \mathbf{X}(I) \equiv 0) = \left(\prod_{i \in I} q_i \right) \times \times \left(\sum_{\mathbf{X}(J) \in B(k)} \psi(\mathbf{X}(J)) \cdot P(\mathbf{X}(J)) \right). \quad (7)$$

Denote the sum in (7) through $P(D(k))$:

$$P(D(k)) = \sum_{\mathbf{X}(J) \in B(k)} \psi(\mathbf{X}(J)) \cdot P(\mathbf{X}(J)).$$

Then

$$P(D(n) | \mathbf{X}(I) \equiv 0) = \left(\prod_{i \in I} q_i \right) \cdot P(D(k)). \quad (8)$$

If the number of failed processors is small, and the k quantity is large enough for direct computation in (7), then, to determine $P(D(k))$ without any significant changes statistical evaluation (3), (4), (5) or (6) may be used:

$$\overline{P_1(D(k))} = \frac{1}{L_1} \sum_{\mathbf{X}(J) \in \Omega_1(k)} \psi(\mathbf{X}(J));$$

$$\overline{P_2(D(k))} = \frac{\sum_{\mathbf{X}(J) \in \Omega_2(k)} \psi(\mathbf{X}(J)) \cdot \gamma^{-(n - w(\mathbf{X}(J)))}}{L_2 \cdot K};$$

$$\overline{P_3(D(k))} = \sum_{m=0}^{k} \left(\frac{S(k,m)}{L_3(m)} \cdot \sum_{\mathbf{X}(J) \in \Omega_3(k,m)} \psi(\mathbf{X}(J)) \right);$$

$$\overline{P_4(D(k))} = \sum_{m=0}^{k} \left(\frac{C_k^m}{L_4(m)} \sum_{\mathbf{X}(J) \in \Omega_4(k,m)} \psi(\mathbf{X}(J)) P(\mathbf{X}(J)) \right).$$

Note that the latest statistical estimate $\overline{P_4(D(k))}$ has the smallest error [5].

Conclusion

In this paper the problem of determining the probability of multiprocessing control system falling into one of states marked as dangerous, were formalized. Statistical estimates of the probability that a system is in a dangerous state were obtained.

This estimates, may help in providing safety for multiprocessor systems.

There were proposed equations to change the estimation for probability of system falling into a dangerous state during operation for multiprocessor systems with embedded self test feature.

Literature

1. Харченко, В.С. Гарантоспособность и гарантоспособные системы: элементы методологии [Текст] / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2006. – № 5.–С. 7 – 18.

2. Бусленко, Н.П. Метод статистических испытаний (Монте-Карло) и его реализация на цифровых вычислительных машинах [Текст] / Н.П. Бусленко, Ю.А. Шрейдер.– М.: Физматгиз, 1961. – 227 с.

3. Романкевич, А.М. Графо-логические модели для анализа сложных отказоустойчивых вычислительных систем [Текст] / А.М. Романкевич, Л.Ф. Карачун, В.А. Романкевич // Электронное моделирование. – 2001. – Т. 23, № 1. – С. 102 – 111.

4. Надежность технических систем: справочник [Текст] / Ю.К. Беляев, В.А. Богатырев, В.В. Болотин и др.; под ред. И.А.Ушакова. – М.: Радио и связь, 1985. – 608 с.

5. Романкевич, А.М. Об одном методе расчета показателей надежности отказоустойчивых многопроцессорных систем [Текст] / А.М. Романкевич, В.А. Романкевич, А.П. Фесенюк // УСиМ. – 2011. – № 6. – С. 14–18, 37.

6. Генерування рівноважних векторів для проведення статистичних експериментів з GL-моделями [Текст] / В.О. Романкевич, І.В. Майданюк, А.П. Фесенюк, Д.С. Шкира // Науковий вісник Чернівецького національного університету. Серія: Комп'ютерні системи та компоненти. – 2010. – Т. 1, вип. 2. – С. 28 – 30.

7. Rushdi, A.M. Utilization of symmetric switching functions in the computation of k-out-of-n system reliability [Text] / A.M. Rushdi // Microelectronics and Reliability. –1986. – R 26(5). – P. 973 – 987.

Поступила в редакцию 12.02.2012

Рецензент: д-р техн. наук, проф. И.А. Фурман, Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Харьков, Украина.

ОЦІНКА ЙМОВІРНОСТІ ПОПАДАННЯ БАГАТОПРОЦЕСОРНОЇ СИСТЕМИ КЕРУВАННЯ В НЕБЕЗПЕЧНИЙ СТАН

Мораведж Сейед Мілад, А.П. Фесенюк, В.О. Романкевич

У даній статті проведена оцінка вірогідності попадання багатопроцесорної системи управління в небезпечний стан. Формалізований стан багатопроцесорної системи, яке кваліфікується як небезпечне. У роботі отримані статистичні оцінки ймовірності попадання багатопроцесорної системи керування в один зі станів, визначених як небезпечні. Отримано співвідношення для визначення ймовірності попадання багатопроцесорної системи керування в небезпечний стан після відмови деякої підмножини процесорів системи.

Ключові слова:системи керування, небезпечний стан, відмова.

ОЦЕНКА ВЕРОЯТНОСТИ ПОПАДАНИЯ МНОГОПРОЦЕССОРНОЙ СИСТЕМЫ УПРАВЛЕНИЯ В ОПАСНОЕ СОСТОЯНИЕ

Мораведж Сейед Милад, А.П. Фесенюк, В.А. Романкевич

В данной статье проведена оценка вероятности попадания многопроцессорной системы управления в опасное состояние. Формализовано состояние многопроцессорной системы, квалифицируемое как опасное. В работе получены статистические оценки вероятности попадания многопроцессорной системы управления в одно из состояний, определенных как опасные. Получены соотношения для определения вероятности попадания многопроцессорной системы управления в опасное состояние после отказа некоторого подмножества процессоров системы.

Ключевые слова: системы управления, опасное состояние, отказ.

Милад Мораведж Сейед – аспирант Национального технического университета Украины «КПИ», Киев, Украина, e-mail: romankev@scs.ntu-kpi.kiev.ua.

Фесенюк Андрей Петрович – соискатель Национального технического университета Украины «КПИ», Киев, Украина, e-mail: andrew_fesenyuk@ukr.net.

Романкевич Виталий Алексеевич – канд. техн. наук, доцент Национального технического университета Украины «КПИ», Киев, Украина, e-mail: romankev@scs.ntu-kpi.kiev.ua.