ACCELERATED SIMULATION METHOD FOR ESTIMATING THE PROBABILITY OF FUNCTIONAL FAILURE IN HIGH-RELIABILITY SYSTEMS

N. Yu. Kuznetsov

UDC 519.248

We consider a class of systems whose required performance is described by a stochastic process $\eta(t)$, $t \geq 0$. An accelerated simulation method is proposed for estimating the probability that at some time instant $t \in [0, T]$ the required performance exceeds the available performance. A numerical example is considered.

Structure optimization subject to reliability requirements is one of the main problems in the design of technical systems for critical uses. At the same time, the development of high-reliability systems of optimal structure requires quantitative methods for calculating their basic reliability characteristics. Only high-accuracy, universal methods can provide an objective justification of a particular design solution, detect the weak spots in the system, and suggest ways for increasing its reliability.

The existing methods for reliability calculations can be divided into three groups: 1) analytical and, in particular, asymptotic methods; 2) direct simulation methods (statistical methods); 3) accelerated simulation methods. In recent years, increasing attention is being focused on accelerated simulation methods, which have a number of advantages compared to both analytical and statistical methods: while highly accurate, they at the same time allow for the specific operating features of real technical systems. An important subclass of accelerated simulation methods are so-called analytical-statistical methods, which combine direct simulation (greatly broadening the applications of analytical methods) with analytical formulas for low probabilities (greatly increasing the computational accuracy of statistical methods). The idea of combining analytical and statistical methods was advanced by Kovalenko [1-4]. It has produced a whole class of methods, known as analytical-statistical methods. The state of the art in this area is described in [2-12].

The previous studies have dealt with systems that were required to maintain the same performance at each time instant. In practice, however, it is relevant to study the reliability of systems with variable operating conditions, i.e., systems in which the performance $Z(t)$, $t \geq 0$, at each time instant should not be less than a given level defined by the stochastic process $\eta(t)$, $t \geq 0$ (see [13-15]). If at some time t the required performance $\eta(t)$ exceeds the available performance $Z(t)$ (i.e., the performance adjusted for the failed elements in the system), then this situation is characterized as functional failure of the system. In this paper, we introduce a mathematical model based on the analysis of a certain class of real systems and propose an accelerated simulation method for estimating the probability of functional failure with high accuracy. The application of the method is demonstrated with a particular example.

STATEMENT OF THE PROBLEM

A complex technical system of network structure consisting of m elements is given. The normal operation time of element i ($1 \leq i \leq m$) is distributed as $F_i(x)$. For each $i = 1,\ldots,m$, we know the probability p_i that the failed element i can be repaired. Then $1 - p_i$ is the probability that element i is not reparable and remains failed during the remaining operating time of the system. If the failed element i is reparable, then it immediately begins to be repaired with repair time distributed according to $G_i(x)$ (the assumption of no repair queue is made in order to simplify the presentation).

Translated from Kibernetika i Sistemnyi Analiz, No. 4, pp. 30-41, July-August, 1991. Original article submitted April 6, 1989.

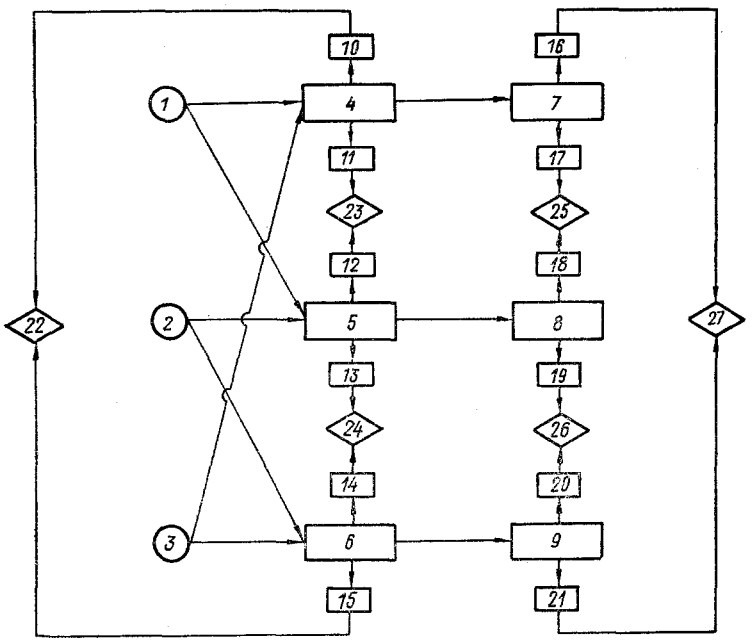

Fig. 1

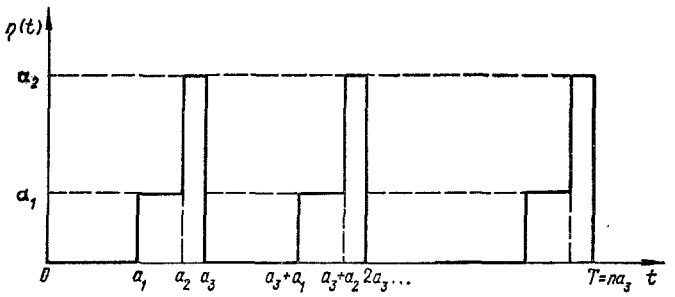

Fig. 2

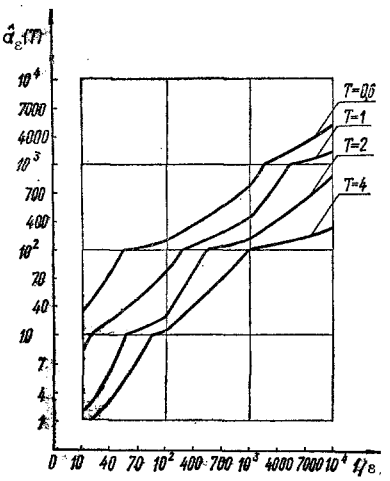

Fig. 3

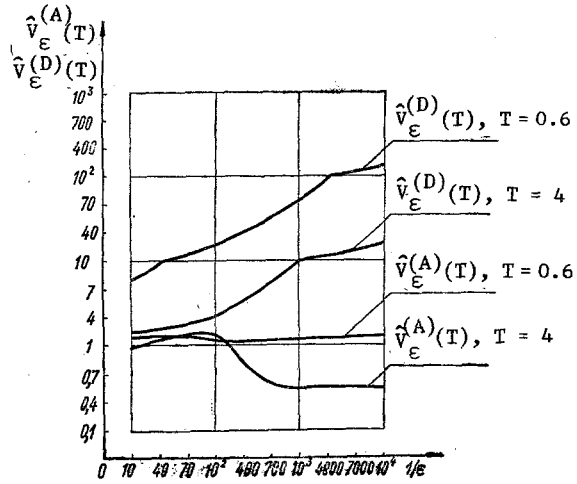

Fig. 4

Denote

$$\nu_j = \begin{cases} 1 \text{ if element j is nonfaulty,} \\ 0 \text{ if element j is faulty, } 1 \le j \le m. \end{cases}$$

The structure of the system and its performance in state $\nu = (\nu_1,\ldots,\nu_m)$ are characterized by the function $\Phi(\nu_1,\ldots,\nu_m)$, $\Phi(1,\ldots,1) = 1$, $\Phi(\nu_1,\ldots,\nu_m) \ge 0$ for all ν. We assume that the system has monotone structure, i.e., $\Phi(\nu_1,\ldots,\nu_m) \ge \Phi(\nu_1',\ldots,\nu_m')$ for $\nu_j \ge \nu_j'$, $1 \le j \le m$. In other words, the performance of the system does not increase when one of its elements fails. The stochastic process $Z(t) = \Phi(\nu_1(t),\ldots,\nu_m(t))$ is called the available performance. Here $\nu_j(t)$ is the state of element j at time t.

At different time instants different performance is required. The required performance at time t is defined by a right-continuous stochastic process $\eta(t)$. Without loss of generality, we take $\eta(t) \in [0, 1]$ for all t. The problem is to estimate the probability Q(T) of functional failure of the system in a given time interval [0, T], i.e., the probability that for some instant $t \in [0, T]$ the available performance is less than the required performance, $Z(t) < \eta(t)$.

ANALYTICAL-STATISTICAL METHOD

We use the general idea of accelerated simulation from [9, 12]. Suppose that a sampling trajectory of the process $\eta(t)$, $t \ge 0$, has been constructed. In what follows, this trajectory s(t), $t \ge 0$, is assumed known and fixed. We introduce a right-continuous Markov process $\xi(t)$, $t \ge 0$, describing the behavior of the system. This process includes a number of additional components which are required by the analytical-statistical method described below. Let

$$\xi(t) = (\mu_1(t), \ldots, \mu_m(t);\ \alpha_1(t), \ldots, \alpha_m(t);\ \gamma_1(t), \ldots, \gamma_m(t);\ v_1(t), \ldots, v_m(t)),\ t \ge 0.$$

Here

$$\mu_i(t) = \begin{cases} 1 \text{ if element i is nonfaulty at time t,} \\ 0 \text{ if element i is faulty and is being repaired,} \\ -1 \text{ if element i is faulty and irreparable;} \end{cases}$$

$$\alpha_i(t) = \begin{cases} 1 \text{ if } \mu_i(t) = 0 \text{ and the remaining repair time of the element is known,} \\ 0 \text{ if } \mu_i(t) \ne 0 \text{ or } \mu_i(t) = 0 \text{ and the elapsed time since the element i was begun to be repaired is known;} \end{cases}$$

$$\gamma_i(t) = \begin{cases} 0 \text{ if } \mu_i(t) = -1 \text{ or } \mu_i(t) = 0,\ \alpha_i(t) = 1, \\ \sup\{u\text{: for any } v \in (t-u, t),\ \mu_i(v) = \mu_i(t)\} \text{ if } \mu_i(t) = 1 \text{ or } \mu_i(t) = 0,\ \alpha_i(t) = 0. \end{cases}$$

If $\alpha_i(t) = 1$, then $v_i(t)$ is the remaining time until the element i is repaired; if $\alpha_i(t) = 0$, then $v_i(t) = 0$.

The state change algorithm of the process $\xi(t)$, $t \geq 0$, will be described below in connection with the analytical-statistical method of computing the probability Q(T) of functional failure.

Suppose that at some time t the process $\xi(u)$, $u \geq 0$, is in state

$$x = \xi(t) = (\mu_1, \ldots, \mu_m;\ \alpha_1, \ldots, \alpha_m;\ \gamma_1, \ldots, \gamma_m;\ v_1, \ldots, v_m)$$

such that the performance $W(x) = \Phi(\nu_1, \ldots, \nu_m) \geq s(t)$, where

$$\nu_i = \begin{cases} 1, & \text{if} \quad \mu_i = 1, \\ 0 & \text{otherwise} \quad 1 \leqslant i \leqslant m. \end{cases}$$

Denote by $z_i(x)$, i: $\mu_i = 1$ the performance of the system if element i fails in state x. Moreover, let

$$\varkappa(t; x) = \begin{cases} \inf\{u \in [t, T] : s(u) > W(x)\}, & \text{if there exists } u \in [t, T] \\ \text{such that } s(u) > W(x), \\ T + 1 \text{ otherwise.} \end{cases}$$

For a fixed $x = \xi(t)$ introduce the events $C_i(t; x)$, i = 1, 2, 3, such that any of them leads to functional failure directly from state x. These events are needed in what follows. Thus:

if $\kappa(t; x) \leq T$, then

$C_1(t; x)$ = {the system does not change its state until the instant $\kappa(t; x)$, i.e., in the interval $(t, \kappa(t; x))$ none of the elements finishes being repaired and none of the elements fails},

if $\kappa(t; x) > T$, then $C_1(t; x) = \varnothing$;

$C_2(t; x)$ = {at some instant $u < \min(T, \kappa(t; x))$ the element j failed so that a) the failed element is irreparable, b) there exists $y \in [u, \min(T, \kappa(t; x))]$ such that $z_j(x) < s(y)$, c) none of the elements that were faulty at time t finished being repaired in the interval (t, y), d) no other elements failed in the interval (t, u)};

$C_3(t; x)$ = {at some instant $u < \min(T, \kappa(t; x))$ the element j failed so that a) the failed element can be repaired in time w; b) there exists $y \in [u, \min(T, u + w, \kappa(t; x))]$ such that $z_j(x) < s(y)$, c) none of the elements that were faulty at time t finished being repaired in the interval (t, y), d) no other elements failed in the interval (t, u)};

$$B(t; x) = C_1(t; x) \cup C_2(t; x) \cup C_3(t; x);$$

$$p(t; x) = \mathrm{P}\{B(t; x)\} = \sum_{i=1}^{3} \mathrm{P}\{C_i(t; x)\}. \tag{1}$$

The event $C_1(t, x)$ implies that the system failed at the instant when the required performance level, described by the function $s(\cdot)$, exceeded the available level W(x). This occurred at time $\kappa(t; x)$, and prior to that time the state of the system did not change. The event $C_2(t; x)$ implies that the system failed at the instant when the first, after t, irreparable failure of an element occurred. As a result of this failure, the performance of the system declined to the level $z_j(x)$ (j is the index of the failed element) and system failure occurred at time $y < \kappa(t; x)$, i.e., $z_j(x) < s(y)$. None of the elements finished being repaired in the interval (t, y). The event $C_3(t; x)$ differs from $C_2(t; x)$ only in that the failed element is repairable. In this case, system failure occurs while the element is being repaired.

The idea of the general method of [9, 12] in application to this system is the following. Assume that for any t and x a method exists for computing the probability p(t; x) (one of such methods – the accelerated simulation method – is described in the next section). To avoid functional failure in [0, T], it is necessary and sufficient that the event B(t; x) does not occur in each state change of the system. In other words, given the current state x_i at time t_i, we compute the probability $1 - p(t_i; x_i)$ and construct the next state x_{i+1} and the transition time t_{i+1} to this state so that the event $B(t_i; x_i)$ does not occur. The one-realization estimate of the probability that functional failure does not occur is taken in the form

$$\prod_{i=1}^{n} [1 - p(t_i; x_i)],$$

where n is the total number of state changes of the system in [0, T].

The algorithm to construct the one-realization estimate $\hat{q}_1(T)$ for the probability Q(T) of functional failure is described as follows.

1. Set $t_1 = 0$ and define the initial state x_1 of the process $\xi(t)$, $t \geq 0$:

$$x_1 = (1, \ldots, 1; 0, \ldots, 0; 0, \ldots, 0; 0, \ldots, 0).$$

2. Compute the probability $p(t_1; x_1)$.

3. Assume that $t_1, x_1, \ldots, t_n, x_n$ have been constructed for some $n \geq 1$ and the probabilities $p(t_i; x_i)$, $i = 1, \ldots, n$, have been computed. If the event $B(t_n; x_n)$ has not occurred, then construct the next state x_{n+1} of the process $\xi(t)$ and the transition time t_{n+1} to this state. Let

$$x_n = (\mu_1, \ldots, \mu_m; \alpha_1, \ldots, \alpha_m; \gamma_1, \ldots, \gamma_m; v_1, \ldots, v_m),$$
$$x_{n+1} = (\mu_1', \ldots, \mu_m'; \alpha_1', \ldots, \alpha_m'; \gamma_1', \ldots, \gamma_m'; v_1', \ldots, v_m').$$

To construct t_{n+1} and x_{n+1}, find

$$\theta^{(0)} = \min_{i:\mu_i=1} \sigma_i^{(0)}, \quad \theta^{(b)} = \min \Big(\min_{\substack{i:\mu_i=0, \\ \alpha_i=0}} \sigma_i^{(b)}, \min_{\substack{i:\mu_i=0, \\ \alpha_i=1}} v_i \Big),$$

where

$$\mathbf{P}\{\sigma_i^{(0)} < y\} = [F_i(\gamma_i + y) - F_i(\gamma_i)]/[1 - F_i(\gamma_i)], \quad y \geqslant 0, \ i: \mu_i = 1,$$
$$\mathbf{P}\{\sigma_i^{(b)} < y\} = [G_i(\gamma_i + y) - G_i(\gamma_i)]/[1 - G_i(\gamma_i)], \quad y \geqslant 0, \ i: \mu_i = 0, \ \alpha_i = 0.$$

Take $\theta = \min(\theta^{(0)}, \theta^{(b)})$. Let $t_n + \theta > \kappa(t_n; x_n)$. If $\kappa(t_n; x_n) > T$, then end the realization; the estimate is given in the form

$$\hat{q}_1(T) = 1 - \prod_{i=1}^{n} [1 - p(t_i; x_i)]. \tag{2}$$

If $\kappa(t_n; x_n) \leq T$, this means that the event $C_1(t_1; x_1)$ has occurred. Since the trajectory $\xi(t)$, $t \geq t_n$, is constructed given that none of the events $C_i(t_n; x_n)$, $i = 1, 2, 3$, has occurred, go back to step 3 of the algorithm and construct new values of $\theta^{(0)}$ and $\theta^{(b)}$.

Let $t_n + \theta < \kappa(t_n; x_n)$. If $t_n + \theta > T$, then the estimate has been constructed in the form (2). Let $t_n + \theta < \min(T, \kappa(t_n; x_n))$. Consider two cases.

A. $\theta^{(b)} < \theta^{(0)}$. Then set

$$t_{n+1} = t_n + \theta^{(b)}, \quad \mu_i' = \mu_i, \ i \neq j_0, \ \mu_{j_0}' = 1,$$
$$j_0 = \arg\min \Big(\min_{\substack{i:\mu_i=0, \\ \alpha_i=0}} \sigma_i^{(b)}, \min_{\substack{i:\mu_i=0, \\ \alpha_i=1}} v_i \Big),$$

$$\alpha_i' = \alpha_i, \quad i \neq j_0, \quad \alpha_{j_0}' = 0,$$

$$\gamma_i' = \begin{cases} \gamma_i + \theta^{(b)}, & \text{if} \quad \mu_i = 1 \quad \text{or} \quad \mu_i = 0, \ \alpha_i = 0, \ i \neq j_0, \\ 0, & \text{if} \quad i = j_0 \quad \text{or} \quad \mu_i = -1, \quad \text{or} \quad \mu_i = 0, \ \alpha_i = 1, \end{cases}$$

$$1 \leqslant i \leqslant m,$$

$$v_i' = v_i, \quad i \neq j_0, \quad v_{j_0}' = 0.$$

Then go to step 3 of the algorithm changing n to n + 1.

B. $\theta^{(b)} > \theta^{(0)}$. This means that at time $t_n + \theta^{(0)}$ the element i_0 failed, where

$$i_0 = \arg \min_{i:\mu_i=1} \sigma_i^{(0)}.$$

Realize the random variable φ, which equals 1 with probability p_{i_0} and 0 with probability $1 - p_{i_0}$. If $\varphi = 1$, then the failed element is reparable; if $\varphi = 0$, then it is irreparable. Let us consider both these cases separately.

Let $\varphi = 0$. If there exists $y \in [t_n + \theta^{(0)}, \min(T, \kappa(t_n; x_n))]$ such that $z_{i_0}(x_n) < s(y)$, then this means that the event $C_2(t_n; x_n)$ has occurred. Since the trajectory of the process $\xi(t)$, $t \geq t_n$, is constructed given that none of the events $C_i(t_n; x_n)$, $i = 1, 2, 3$, occurs, we return to step 3 of the algorithm and construct new values $\theta^{(0)}$ and $\theta^{(b)}$. If this y does not exist, then set

$$t_{n+1} = t_n + \theta^{(0)}, \quad \mu_{i_0}' = -1, \quad \alpha_{i_0}' = 0, \quad \gamma_{i_0}' = 0, \quad v_{i_0}' = 0.$$

Let $\varphi = 1$. In this case, realize the random variable β_{i_0} with the distribution function $G_{i_0}(u)$. If there exists $y \in [t_n + \theta^{(0)}, \min(T, t_n + \theta^{(0)} + \beta_{i_0}, \kappa(t_n; x_n))]$ such that $z_{i_0}(x_n) < s(y)$, this means that the event $C_3(t_n; x_n)$ has occurred. Then return to step 3 of the algorithm and construct new values of $\theta^{(0)}$ and $\theta^{(b)}$. If this y does not exist, then set

$$t_{n+1} = t_n + \theta^{(0)}, \quad \mu_{i_0}' = 0, \quad \alpha_{i_0}' = 1, \quad \gamma_{i_0}' = 0, \quad v_{i_0}' = \beta_{i_0}.$$

Moreover, regardless of the value of φ, let

$$\mu_i' = \mu_i, \quad \alpha_i' = \alpha_i, \quad v_i' = v_i,$$

$$\gamma_i' = \begin{cases} \gamma_i + \theta^{(0)}, & \text{if} \quad \mu_i = 1 \quad \text{or} \quad \mu_i = 0, \ \alpha_i = 0, \\ 0 \quad \text{otherwise}, & i \neq i_0. \end{cases}$$

Then go to step 3 of the algorithm replacing n with n + 1.

The proposed algorithm completely describes the sequence of nodal instants $\{t_i\}$ and the states $\{x_i\}$ of the process $\xi(t)$, $t \geq 0$, at these instants. This algorithm is the statistical part of the analytical-statistical method. The analytical part of this method consists of formula (2), which generates unbiased estimators of the probability of functional failure given the trajectory $\{(x_i, t_i)\}$. In the next section we describe the method of accelerated simulation of the probability p(t; x). The combination of this method with formula (2) substantially increases the estimation accuracy compared with the traditional direct simulation methods (and thus substantially reduces machine costs – see the example given below).

ACCELERATED SIMULATION OF THE PROBABILITY p(t; x)

To apply formula (2), we need a method for constructing estimators of the probability p(t; x) for any t and x. If $\hat{p}_1(t_i, x_i)$, $1 \leq i \leq n$, are the one-realization unbiased estimators of p(t; x) for various $\{(t_i, x_i)\}$, then the one-realization unbiased estimator for Q(T) has the form

$$\hat{q}_1(T) = 1 - \prod_{i=1}^{n} [1 - \hat{p}_1(t_i; x_i)]. \tag{3}$$

In other words, the algorithm that constructs the estimator $\hat{q}_1(T)$ consists of two parts: first we apply the previously described method to construct the random sequence $(n; t_1, x_1, \ldots, t_n, x_n)$ and then for all $i = 1, \ldots, n$ we construct the estimators $\{\hat{p}_1(t_i; x_i)\}$ and find $\hat{q}_1(T)$ from formula (3).

In this section, we propose the accelerated simulation method for estimating p(t; x). Let

$$\xi(t) = x = (\mu_1, \ldots, \mu_m;\ \alpha_1, \ldots, \alpha_m;\ \gamma_1, \ldots, \gamma_m;\ v_1, \ldots v_m),\ 0 \leqslant t < T,$$

and W(x), $z_i(x)$, i: $\mu_i = 1$, $\kappa(t; x)$ have the same meaning as previously. By (1), it suffices to estimate each term in the right-hand side of (1). The probability $\mathbf{P}\{C_1(t; x)\}$ is computed in explicit form:

$$\mathbf{P}\{C_1(t;\ x)\} = \prod_{i:\mu_i=1} \frac{1 - F_i(\gamma_i + \varkappa(t;\ x) - t)}{1 - F_i(\gamma_i)} \times \times \prod_{\substack{i:\mu_i=0,\\ \alpha_i=0}} \frac{1 - G_i(\gamma_i + \varkappa(t;\ x) - t)}{1 - G_i(\gamma_i)}, \tag{4}$$

if $\kappa(t; x) \leq T$ and there is no i such that $\mu_i = 0$, $\alpha_i = 1$, $v_i < \kappa(t; x) - t$. Otherwise, $\mathbf{P}\{C_1(t; x)\} = 0$.

It is easy to see that the probabilities $\mathbf{P}\{C_2(t; x)\}$ and $\mathbf{P}\{C_3(t; x)\}$ cannot be computed in explicit form. We will develop special accelerated simulation algorithms for estimation of these probabilities.

First consider $\mathbf{P}\{C_2(t; x)\}$. Let

$D(t; x) = \{j$: there exists u such that $z_j(x) < s(u)$ and $u < \kappa(t; x)\}$;

$$r_j(t; x) = \sup\{u: z_j(x) < s(u)\} - t,\ j \in D(t; x);$$

ξ_j, j: $\mu_j = 1$, are random variables with distribution functions

$$A_j(y) = \frac{F_j(\gamma_j + y) - F_j(\gamma_j)}{1 - F_j(\gamma_j)},\ y \geqslant 0;$$

β_j, j: $\mu_j = 0$, $\alpha_j = 0$, are random variables with distribution functions

$$B_j(y) = \frac{G_j(\gamma_j + y) - G_j(\gamma_j)}{1 - G_j(\gamma_j)},\ y \geqslant 0;$$

H_j, j: $\mu_j = 1$, are events which imply that faulty element j is reparable, $\mathbf{P}\{H_j\} = p_j$;

$\bar{H}_j$, j: $\mu_j = 1$, are events complementary to H_j, $\mathbf{P}\{\bar{H}_j\} = 1 - p_j$.

Then

$$\mathbf{P}\{C_2(t;\ x)\} = \mathbf{P}\Big\{ \bigcup_{j \in D(t;x)} \Big(\bar{H}_j \cap \{\xi_j < r_j(t;\ x)\} \cap \bigcap_{\substack{i:\mu_i=1\\ i\neq j}} \{\xi_i > \xi_j\} \cap \cap \bigcap_{\substack{i:\mu_i=0,\\ \alpha_i=0}} \{\beta_i > \xi_j\} \cap \bigcap_{\substack{i:\mu_i=0,\\ \alpha_i=1}} \{v_i > \xi_j\}\Big)\Big\}.$$

Denoting

$$\varphi(t;\ x) = \min\Big(T - t,\ \min_{\substack{i:\mu_i=0,\\ \alpha_i=0}} \beta_i,\ \min_{\substack{i:\mu_i=0,\\ \alpha_i=1}} v_i\Big), \tag{5}$$

we obtain

$$\mathbf{P}\{C_2(t;\ x)\} = \int_0^\infty \mathbf{P}\Big\{ \bigcup_{j \in D(t;x)} \Big(\bar{H}_j \cap \{\xi_j < \min(y,\ r_j(t;\ x))\} \cap \cap \bigcap_{\substack{i:\mu_i=1\\ i\neq j}} \{\xi_i > \xi_j\}\Big)\Big\}\, d\mathbf{P}\{\varphi(t;\ x) < y\}. \tag{6}$$

Denote by $a(t, x, y)$ the integrand in the right-hand side of the last relationship. The next theorem suggests a technique for simulating $a(t, x, y)$ and thus also $\mathbf{P}\{C_2(t; x)\}$. To simplify the notation, we write

$$h_j = \min(y, r_j(t; x)).$$

THEOREM 1.

$$a(t, x, y) = \left[1 - \prod_{j=1}^{m} (1 - d_j)\right] \mathbf{M} \prod_{\substack{j:\pi_j=1, \\ j\in D(t;x)}} \left[p_j \frac{1 - F_j(\gamma_j + \psi)}{1 - F_j(\gamma_j)} + \right.$$

$$\left. + (1 - p_j) \frac{1 - F_j(\gamma_j + \max(\psi, h_j))}{1 - F_j(\gamma_j)}\right] / (1 - d_j) \times \tag{7}$$

$$\times \prod_{\substack{j\bar{\in}D(t;x), \\ j:\mu_j=1}} \frac{1 - E_j(\gamma_i + \psi)}{1 - F_j(\gamma_j)}\Bigg\},$$

where

$$d_j = \begin{cases} (1 - p_j) \dfrac{F_j(\gamma_j + h_j) - F_j(\gamma_j)}{1 - F_j(\gamma_j)}, & \text{if} \quad j \in D(t; x), \\ 0, & \text{if} \quad j \bar{\in} D(t; x), \end{cases}$$

and the random variables ψ and $\{\pi_j\}$ are constructed as follows:

$$\pi_j = 1, \quad \text{if} \quad j < \sigma, \ j \in D(t; x), \ \pi_\sigma = 0,$$

$$\pi_j = \begin{cases} 0 \text{ with probability } d_j, \\ 1 \text{ with probability } 1 - d_j, \ j > \sigma, \ j = D(t; x), \end{cases}$$

$$g_j = d_j \prod_{i=1}^{j-1} (1 - d_i), \ j = 1, \ldots, m,$$

$$\sigma = k \text{ with probability } g_k / \sum_{j=1}^{m} g_j = g_k / \left[1 - \prod_{j=1}^{m} (1 - d_j)\right],$$

$$\psi = \min_{i:\pi_i=0} \zeta_i^*,$$

$$\mathbf{P}\{\zeta_i^* < u\} = \mathbf{P}\{\zeta_i < u \mid \zeta_i < h_i\} = \frac{F_i(\gamma_i + u) - F_i(\gamma_i)}{F_i(\gamma_i + h_i) - F_i(\gamma_i)}.$$

Proof. Denote by $b(t, x, y)$ the right-hand side of (7). We have to show that $b(t, x, y) = a(t, x, y)$. Using the notation introduced in Theorem 1, we obtain

$$b(t, x, y) = \left[1 - \prod_{j=1}^{m} (1 - d_j)\right] \cdot \mathbf{M}\left\{ \prod_{\substack{j:\pi_j=1, \\ j\in D(t;x)}} [p_j \mathbf{P}\{\zeta_j > \psi\} + \right.$$

$$\left. + (1 - p_j) \mathbf{P}\{\zeta_j > \max(\psi, h_j)\}] / (1 - d_j) \cdot \prod_{\substack{j\bar{\in}D(t;x), \\ j:\mu_j=1}} \mathbf{P}\{\zeta_j > \psi\}\right\} =$$

$$= \sum_{k=1}^{m} g_k \sum_{k=j}^{m-k+1} \sum_{\substack{k=j_1<j_2<\ldots<j_l\leqslant m, \\ j_i\in D(t;x), i=1,\ldots,l}} \prod_{i=2}^{l} d_{j_i} \prod_{\substack{i>k,, \\ i\in D(t;x), \\ i\neq j_1,\ldots,i\neq j_l}} (1 - d_i) \times$$

$$\times \prod_{\substack{i\in D(t;x), \\ j\neq j_1,\ldots,i\neq j_l}} [p_i \mathbf{P}\{\zeta_i > \min(\zeta_{j_1}^*, \ldots, \zeta_{j_l}^*)\} + (1 - p_i) \mathbf{P}\{\zeta_i > \max(h_i, \min(\zeta_{j_1}^*, \ldots$$

$$\ldots, \zeta^*_{j_l})\}]/(1-d_i)\cdot \prod_{\substack{j\in D(t;x),\\ j:\mu_j=1}} \mathbf{P}\{\zeta_j > \min(\zeta^*_{j_1}, \ldots, \zeta^*_{j_l})\} =$$

$$= \sum_{k=1}^{m}\sum_{l=1}^{m-k+1} \sum_{\substack{k=j_1<j_2<\ldots<j_l\leqslant m,\\ j_i\in D(t;x),\ i=1,\ldots,l}} \prod_{i=1}^{l} d_{j_i} \int_0^{h_{j_1}} \ldots \int_0^{h_{j_l}} \prod_{\substack{i\in D(t;x),\\ i\neq j_1,\ldots,i=j_l}} [p_i \mathbf{P}\{\zeta_i > \min(u_1, \ldots$$

$$\ldots, u_l)\} + (1-p_i)\,\mathbf{P}\{\zeta_i > \max(h_i, \min(u_1, \ldots, u_l))\}] \times$$

$$\times \prod_{\substack{j\in D(t;x),\\ j:\mu_j=1}} \mathbf{P}\{\zeta_j > \min(u_1, \ldots, u_l)\} \frac{1-p_{j_1}}{d_{j_1}} dF_{j_1}(u_1) \ldots \frac{1-p_{j_l}}{d_{j_l}} dF_{j_l}(u_l) =$$

$$= \sum_{l=1}^{m} \sum_{\substack{1\leqslant j_1<j_2<\ldots<j_l\leqslant m,\\ j_i\in D(t;x), i=1,\ldots,l}} \int_0^{h_{j_1}} \ldots \int_0^{h_{j_l}} \prod_{\substack{i\in D(t;x),\\ i\neq j_1,\ldots,i\neq j_l}} [p_i \mathbf{P}\{\zeta_i > \min(u_1, \ldots, u_l)\} +$$

$$+ (1-p_i)\,\mathbf{P}\{\zeta_i > \max(h_i, \min(u_1, \ldots, u_l))\}] \times$$

$$\times \prod_{\substack{j\in D(t;x),\\ j:\mu_j=1}} \mathbf{P}\{\zeta_j > \min(u_1, \ldots, u_l)\}(1-p_{j_1})\,dF_{j_1}(u_1) \ldots (1-p_{j_l})\,dF_{j_l}(u_l).$$

It is easy to show that the last expression is indeed $a(t, x, y)$, i.e., the integrand in the right-hand side of (6). Q.E.D.

Remark. Despite its apparent complexity, the simulation algorithm has proved highly accurate in computation of $a(t, x, y)$ both for systems with moderately reliable elements and for systems with highly reliable elements. Simpler algorithms exists for simulation of $a(t, x, y)$. However, of all the algorithms known to the author, the algorithm of Theorem 1 produces the most accurate estimates of $a(t, x, y)$.

Let us now consider an accelerated simulation algorithm for the probability $\mathbf{P}\{C_3(t; x)\}$. We have an analog of (6):

$$\mathbf{P}\{C_3(t; x)\} = \int_0^{\infty}\int_0^{\infty}\ldots\int_0^{\infty} \mathbf{P}\Big\{\bigcup_{j\in D(t;x)} (H_j \cap \Big\{\zeta_j \in \bigcup_{k=1}^{m_j} \Delta_{jk}\Big\} \cap$$
$$\cap \bigcap_{\substack{i:\mu_i=1,\\ i\neq j}} \{\zeta_i > \zeta_j\}\Big\} \prod_{i\in D(t;x)} dB_i(w_i)\,\mathbf{P}\{\varphi(t; x) < y\}, \tag{8}$$

where $|D(t; x)|$ is the number of elements in the set $D(t; x)$, $\varphi(t; x)$ is the random variable defined by (3), and

$$\Delta_{jk} = \Delta_{jk}(y;\ w_i,\ i\in D(t;\ x)) = (a_{jk},\ b_{jk}),\ j\in D(t;\ x),\ k = 1, \ldots, m_j,$$

are time intervals such that $b_{jm_j} \leq y$ and if element j fails at time $u \in (a_{jk}, b_{jk})$, then there exists $v \in (u, u + w_j) \cap (a_{jk}, b_{jk})$ for which $s(v) > z_j(x)$ (in other words, a functional failure occurred in (a_{jk}, b_{jk}) while the element j was being repaired).

Denote by $f(t, x, y, w_i, i \in D(t; x))$ the integrand in the right-hand side of (8). It is easy to note that this expression differs from $a(t, x, y)$ only in that $\{H_i\}$ have been replaced with $\{H_i\}$ and the intervals $\{(0, \min(y, r_j(t; x)))\}$ have been replaced with the unions $\Big\{\bigcup_{k=1}^{m_j} \Delta_{jk}\Big\}$.

THEOREM 2.

$$f(t, x, y, w_i, i\in D(t; x)) = \Big[1 - \prod_{j\in D(t;x)} (1-d_j)\Big] \cdot \mathbf{M}\Big\{\prod_{\substack{j:\pi_j=1,\\ j\in D(t;x)}} \Big[(1-p_j)\times$$
$$\times \frac{1-F_j(\gamma_j+\psi)}{1-F_j(\gamma_j)} + p_j U_j(\psi)\Big]/(1-d_j) \cdot \prod_{\substack{j\in D(t;x),\\ j:\mu_j=1}} \frac{1-F_j(\gamma_j+\psi)}{1-F_j(\gamma_j)}\Big\}, \tag{9}$$

where

$$d_j = p_j \sum_{k=1}^{m_j} \frac{F_j(\gamma_j + b_{jk}) - F_j(\gamma_j + a_{jk})}{1 - F_j(\gamma_j)}, \quad j \in D(t;\ x),$$

$$U_j(\psi) = \sum_{\substack{k=1 \\ k:a_{jk}>\psi}}^{m_j} \frac{F_j(\gamma_j + a_{jk}) - F_j(\gamma_j + \max(\psi,\ b_{jk-1}))}{1 - F_j(\gamma_j)} + \frac{1 - F_j(\max(\psi,\ b_{jm_j}))}{1 - F_j(\gamma_j)}, \quad b_{j0} = 0,$$

and the random variables ψ and $\{\pi_j\}$ are constructed as follows:

$$\pi_j = 1, \text{ if } \quad j < \sigma,\ j \in D(t;\ x),\ \pi_\sigma = 0,$$

$$\pi_j = \begin{cases} 0 \text{ with probability } d_j, \\ 1 \text{ with probability } 1 - d_j, \end{cases} \quad j > \sigma,\ j \in D(t;\ x),$$

$$g_j = d_j \prod_{\substack{i=1 \\ i \in D(t;x)}}^{j-1i} (1 - d_i),\ j \in D(t;\ x),\ \sigma = k \text{ with probability } \quad g_k / \sum_{j \in D(t;x)} g_j,$$

$$\psi = \min_{i:\pi_i=0} \zeta_i^*,\ \mathbf{P}\{\zeta_i^* < u\} = \mathbf{P}\left\{\zeta_i < u / \zeta_i \in \bigcup_{k=1}^{m_i} \Delta_{ik}\right\}.$$

The proof of Theorem 2 is similar to the proof of Theorem 1 and is therefore omitted.

In conclusion of this section, note that formula (3) combined with (1), (4), (6)-(9) makes it possible to construct analytical-statistical estimators of the probability of functional failure of systems of this class. Taking a sufficient number of realizations, we can construct estimators with required accuracy and confidence. High estimation accuracy and substantial machine time savings (compared with the ordinary simulation method) are demonstrated by the following example.

EXAMPLE

Consider the electric power system shown in Fig. 1. The system consists of three power sources of identical outpug (elements 1, 2, 3), six main distribution panels (elements 4-9), twelve distribution panels (elements 10-21), and six users (elements 22-27). The problem is to ensure continuous supply of all users in a given time interval [0, T] so that at each instant $t \in [0, T]$ the available performance of the system exceeds the required performance as defined by the stochastic process $\eta(t)$ (Fig. 2). Let

$$a_1 = 0{,}1\,(2 - \varepsilon),\ a_2 = 0{,}2\,(1 - 0{,}1\varepsilon),\ a_3 = 0{,}2,\ T = na_3,$$

$$\alpha_1 = \frac{1}{3} - 0{,}1\,(1 - 2\omega_1),\ \alpha_2 = \frac{2}{3} - 0{,}1\,(1 - 2\omega_2),$$

where n is an integer, ω_1, ω_2 are [0, 1]-uniform random variables, and $\varepsilon > 0$ is a small parameter. Define the remaining system characteristics:

$$F_i(x) = 1 - e^{-0{,}1x},\ i = 1, 2, 3,\ F_i(x) = 1 - e^{-0{,}04x^2},\ i = 4, \ldots, 9,$$

$$F_i(x) = 1 - e^{-0{,}1x^2},\ i = 10, \ldots, 21,\ G_i(x) = 1 - e^{-\frac{5}{\varepsilon}x},\ i = 1, 2, 3,$$

$$G_i(x) = 1 - e^{-\frac{100}{\varepsilon}x^2},\ i = 4, \ldots, 9,\ G_i(x) = \begin{cases} 0, & x \leqslant 0, \\ \dfrac{10}{\varepsilon}x, & 0 < x \leqslant 0{,}1\varepsilon, \\ 1, & x > 0{,}1\,\varepsilon, \end{cases} \quad i = 10, \ldots, 21,$$

$$p_i = 1 - \varepsilon,\ i = 1, \ldots, 21.$$

The available performance Z(t), $t \geq 0$, is determined by the state of the power sources. If $k \in \{0, 1, 2, 3\}$ is the number of normally operating sources at time t, then Z(t) = k/3.

It is easy to see that the characteristics of the system and the process $\eta(t)$, $t \geq 0$, are chosen so that $Q(T) \to 0$ as $\varepsilon \to 0$ for any fixed T. The purpose of this example is to demonstrate the advantages of the proposed method compared with the direct simulation method for $\varepsilon \to 0$. We introduce the following notation:

$\hat{Q}_\varepsilon^{(D)}(T)$ and $\hat{Q}_\varepsilon^{(A)}(T)$ are the estimators of Q(T) constructed from s realizations by direct and accelerated simulation methods, respectively;

$\hat{D}_\varepsilon^{(A)}(T) = \frac{1}{s-1}\left\{\sum_{j=1}^{s}[\hat{q}_j^{(A)}]^2 - \frac{1}{s}\left[\sum_{j=1}^{s}\hat{q}_j^{(A)}\right]^2\right\}$ is the sample variance of the estimators obtained by the accelerated simulation method (here $\hat{q}_j^{(A)}$ is the estimator of Q(T) in realization j);

$\hat{V}_\varepsilon^{(A)}(T) = \sqrt{\hat{D}_\varepsilon^{(A)}(T)}/\hat{Q}_\varepsilon^{(A)}(T)$ is the estimated relative mean square error of the estimators obtained by the accelerated simulation method;

$\hat{D}_\varepsilon^{(D)}(T) = \hat{Q}_\varepsilon^{(A)}(T)[1 - \hat{Q}_\varepsilon^{(A)}(T)]$ is the estimated variance of the estimators obtained by direct simulation;

$\hat{V}_\varepsilon^{(D)}(T) = \sqrt{\hat{D}_\varepsilon^{(D)}(T)}/\hat{Q}_\varepsilon^{(A)}(T)$ is the estimated relative mean square error of the estimators obtained by direct simulation;

$\hat{W}_\varepsilon^{(D)}(T)$ and $\hat{W}_\varepsilon^{(A)}(T)$ are the estimated average machine time requirements to construct one-realization estimators by direct and accelerated simulation methods (in seconds);

$\hat{K}_\varepsilon^{(D)}(T) = \hat{W}_\varepsilon^{(D)}(T)\hat{D}_\varepsilon^{(D)}(T)$, $\hat{K}_\varepsilon^{(A)}(T) = \hat{W}_\varepsilon^{(A)}(T)\hat{D}_\varepsilon^{(A)}(T)$ are the estimated complexities of the two methods;

$\hat{\alpha}_\varepsilon(T) = \hat{K}_\varepsilon^{(D)}(T)/\hat{K}_\varepsilon^{(A)}(T)$ is the estimate gain in machine time due to the use of accelerated simulation.

Let us investigate the variation of $\hat{\alpha}_\varepsilon(T)$ for various T (T = 0.6, 1, 2, 4). Figure 3 plots $\hat{\alpha}_\varepsilon(T)$ as a function of ε^{-1}. In view of very steep changes in machine time saving (as determined by the function $\hat{\alpha}_\varepsilon(T)$), different scales are used on different sections of the horizontal and vertical axes, although the same scale is preserved within each section. The use of different scales makes it possible to cover a very wide range of variation of the function $\hat{\alpha}_\varepsilon(T)$. All the estimators given above were constructed from s = 100 realizations.

The graphs in Fig. 3 clearly demonstrate the essential advantage of accelerated simulation: the gain in machine time increases with the increase of system reliability (i.e., as $\varepsilon \to 0$) and may reach very high levels.

The "accuracy" criterion of the statistical method in practice is the relative mean square error $V_\varepsilon(T)$. A method is regarded as efficient if $V_\varepsilon(T)$ remains bounded as the system reliability increases. Let us examine the variation of $\hat{V}_\varepsilon^{(D)}(T)$ and $\hat{V}_\varepsilon^{(A)}(T)$ as $\varepsilon \to 0$ for T = 0.6 and T = 4 (Fig. 4).

The graphs in Fig. 4 show that $\hat{V}_\varepsilon^{(A)}(T)$ does not exceed 2.4 for all ε. At the same time $\hat{V}_\varepsilon^{(D)}(T)$ is monotone increasing with the increase of ε^{-1}. This is another confirmation of the high efficiency of the proposed method.

LITERATURE CITED

1. I. N. Kovalenko, "Asymptotic method of reliability analysis of complex systems," in: Reliability of Complex Technical Systems [in Russian], Sovetskoe Radio, Moscow (1967), pp. 205-223.
2. I. N. Kovalenko, Studies in Reliability Analysis of Complex Systems [in Russian], Naukova Dumka, Kiev (1975).
3. I. N. Kovalenko, Analysis of Rare Events in Estimation of System Performance and Reliability [in Russian], Sovetskoe Radio, Moscow (1980).
4. I. N. Kovalenko, "Computing the characteristics of highly reliable systems by analytical-statistical method," Élektron. Model., 2, No. 4, 5-8 (1980).
5. V. D. Shpak, "Estimating the termination probability of a regeneration process during a fixed time by simulation method," Kibernetika, No. 1, 75-79 (1983).
6. L. A. Zavadskaya, "An approach to accelerated simulation of systems with redundancy," Élektron. Model., 6, No. 3, 57-60 (1984).
7. N. Yu. Kuznetsov, "A general approach to estimating the failfree probability of structurally complex systems by analytical-statistical method," Kibernetika, No. 3, 86-94 (1985).
8. A. N. Nakonechnyi, "On representation of failfree probability of a system as the average of the w-functional of a terminating Markov process," Kibernetika, No. 5, 91-94 (1985).
9. N. Yu. Kuznetsov, "Computing the on-line availability of a system with repair by analytical-statistical method," Kibernetika, No. 5, 95-101 (1985).
10. V. G. Krivutsa, "Determining the failfree probability of high-reliability systems by analytical-statistical method," in: Theory of Complex Systems and Methods of Their Modeling [in Russian], VNIISI, Moscow (1985), pp. 142-148.
11. O. T. Mar'yanovich, "Estimating the nonstationary availability of complex systems with reparable elements by analytical-statistical method," Kibernetika, No. 2, 87-91 (1987).

12. I. N. Kovalenko and N. Yu. Kuznetsov, Comptation Methods for High-Reliability Systems [in Russian], Radio i Svyaz', Moscow (1988).
13. A. I. Klemin, V. S. Emel'yanov, and V. B. Morozov, Computing the Reliability of Nuclear Power Plants. Markov Model [in Russian], Énergoizdat, Moscow (1982).
14. A. N. Nakonechnyi, "A class of systems with variable operation," in: Analysis of Reliability of Complex Systems by Analytical-Statistical Method [in Russian], Preprint Inst. Kiber., Akad. Nauk UkrSSR: 82-2, Kiev (1982), pp. 3-9.
15. N. Yu. Kuznetsov, "Reliability analysis of complex systems with variable operation," Issled. Operat. ASU, No. 24, 14-27 (1984).

ACTIVE FAULT PROTECTION IN COMPUTER SYSTEMS WHERE JOB PROCESSING TIME IS COMPARABLE WITH INTERARRIVAL TIME

I. B. Shubinskii and N. P. Vasil'ev

UDC 681.324

Principles of active fault protection in computer systems are presented. The probability of successful adaptation of the system to faulty modules is estimated as a function of information load, time reserve, number of modules, and regularity of the distribution of the relevant random variables in the system.

INTRODUCTION

Structural redundancy is a popular technique for fault tolerance in real-time computing systems. But inherent restrictions of fault checking facilities essentially reduce the effectiveness of redundancy. To achieve the required levels of fault tolerance in modular real-time computing systems, we have developed methods of active protection against faults [1-3].

1. During the active protection interval, a standby module performs parallel processing with all the main modules in prescribed order. This allows external checking of normal operation of all modules, including the standby module, classification of permanent and transient faults, elimination of errors, location of the faulty module, automatic replacement of the faulty module with the standby module, disconnection of the faulty standby module for the duration of its repair or for replacement with a normally operating unit, and finally restart of the computational process from the last check point.

2. The classification of permanent and transient faults and the location of the faulty module require no fewer than $m = 2$ main modules and one standby module. With simple organization of active fault protection, the standby module runs in parallel with the first main module in the first active protection interval, and then it runs in parallel with the second main module in the second protection interval (or after an interval). If the results produced by the pair of computing modules in the previous interval do not match, the computation is repeated, which eliminates the effect of a transient fault or establishes that one of the modules is faulty (if the results again do not match). The faulty module is located from the results of parallel processing of the standby module with the second main module. If the results match, then the decision is that the first main module is faulty; if the results do not match, then the decision is that the standby module is faulty.

3. The possibilities of active protection largely depend on the mean length of the protection interval τ. The value of τ should be chosen so that during the time $T_a^* = T_a - t_r$ the faulty module is located with a given degree of confidence and is replaced with the nonfaulty standby module. Here T_a is the admissible time during which processing may be interrupted. The time t_r is the recovery time of the computation process from the last check point with appropriately organized active

Translated from Kibernetika i Sistemnyi Analiz, No. 4, pp. 42-47, July-August, 1991. Original article submitted April 4, 1989.

1060-0396/91/2704-0508$12.50