ISSN 0005-1179, Automation and Remote Control, 2008, Vol. 69, No. 10, pp. 1765–1777. © Pleiades Publishing, Ltd., 2008.
Original Russian Text © R. Goot, I. Levin, 2008, published in Avtomatika i Telemekhanika, 2008, No. 10, pp. 128–141.

TECHNICAL DIAGNOSTICS

Estimating the Latent Time of Fault Detection in Finite Automaton Tested in Real Time

R. Goot* **and I. Levin****

*Haifa Institute of Technology, Haifa, Israel
**Tel Aviv University, Tel Aviv, Israel

Received October 10, 2006

Abstract—The notions of potential and real latent times of fault detection in finite automata were introduced. The potential latent time is the minimal theoretical time of automaton fault detection, the real time is defined as the time of fault manifestation at a certain point. A method for determination of the statistical characteristics of both times for the automaton tested in the course of its real operation was proposed. It is based on selection of the trajectories of the Markov chain describing behavior of the operable and faulty automata. Additionally, a method for determination of the upper bound of the mean latent time in the case of limited information about the automaton characteristics was proposed.

PACS number: 89.20.Ff

DOI: 10.1134/S000511790810010X

1. INTRODUCTION

Digital system controllers usually are the most critical units in terms of checking and testing. Design of self-testing controllers and analysis of their efficiency is a challenge due, on the one hand, to their complexity and, on the other hand, to the key role they play in the system [1]. The present paper considers the statistical characteristics of the latent time of fault detection for finite automata-controllers tested in real time.

A method for calculation of the length of testing sequence required for fault detection with the given probability in the mode of autonomous checking where the automaton is driven in a special mode of testing was described in [2]. It relies on constructing a special $R+1$-state Markov chain, where R is the number of states of the checked automaton. The additional $(R+1)$st state is defined as the absorbing state, and the matrix of transition probability is constructed so that the process gets into the additional state in the case of fault detection, In principle, this method can be used also for analysis of the automaton tested in real time, but it would require too bulky and lengthy calculations. In contrast to [2], we pose the problem as applied to the real time and propose a method for its solution which is much easier in terms of calculation. At the same time, this method, as well as that of [2], needs a sufficiently large amount of preliminary information about the structure and characteristics of the checked automaton which is not necessarily available, especially at the initial stages of design [3]. Therefore, we present a method for determination of the mean time of fault detection operating with a rather limited information about the automaton structure. On this basis, given is the upper boundary of the mean latent time which uses only the main parameters of the automaton such as the numbers of states, inputs, outputs, and so on. For that, constructed is the "worst" automaton with the same parameters and the maximum latent time which is then used to determine the desired estimates.

Section 2 of this paper presents the definitions and assumptions. The distribution functions of the latent time of fault detection of the checked automaton itself and the checker are established in Section 3. Section 4 determines the aforementioned estimates. The experimental results are described in Section 5. The paper is concluded by Section 6.

2. FORMULATION OF THE PROBLEM. BASIC CONDITIONS AND DEFINITIONS

We make use of the Mealy model to describe the finite automaton.

Let:

$\mathbf{Q}, \mathbf{I}, \mathbf{O}$ be the sets of states, input vectors, and output vectors, respectively, and N_Q, N_I, and N_O, the numbers of their elements,

a_1 be the initial state,

δ be the transition function: δ: $Q \times I \rightarrow Q$,

λ be the output function: λ: $Q \times I \rightarrow O$.

We use the following notation:

$X = \{x_1, \ldots, x_{Nx}\}$ is the set of input variables;

$Y = \{y_1, \ldots, y_{Ny}\}$ is the set of state variables;

$Z = \{z_1, \ldots, z_{Nz}\}$ is the set of output variables,

all variables being regarded as binary.

A definition of the finite automaton that is somewhat distinct from the generally accepted definition will be useful here. Namely, we say that the automaton S with random input vectors of the values of variables is $\mathbf{S} = \langle Q, \{I, \mathbf{\Omega}, p\}, O, \delta, \lambda \rangle$, where $\{I, \mathbf{\Omega}, p\}$ is the ordinary probabilistic space with the set of elementary events I, σ algebra $\mathbf{\Omega}$, and the probabilistic measure p [4]. In this manner, the probabilistic model of action on the deterministic automaton is postulated. Behavior of such automaton is adequately described by the Markov chain [5]. We use the uniform Markov chain defined by the matrix of transition probabilities (p_{ms}), where p_{ms} is the probability of transition from the state m to the state s. As it is generally accepted, we also assume that the fault is single and bit-stuck, that is, during the entire time of analysis from the instant of fault occurrence to that of its detection the fault does not disappear and the probability of occurrence of another fault is negligible.

It is generally accepted to define the latent time of fault detection as the time interval between the instants of its occurrence and manifestation [1]. By contrast, we consider the fault manifestation as any deviation of the automaton from the correct behavior that was caused by an impairment, regardless of occurrence of the output errors, and in this connection give the following definitions.

Definition 1. The potential latent time of fault manifestation is the time interval between the instant of fault occurrence and the instant of any its manifestation.

Definition 2. The real latent time of fault manifestation at some observed point(s) is the time between instant of occurrence of this fault and the instant of its manifestation there.

As may be seen from Definition 1, for the automaton tested in real time the potential latent time is the theoretically feasible minimal time of fault detection. As for the real latent time, it refers to a particular observation point(s), usually to that (those) to which the checker is connected. Therefore, the difference between the real and potential times is nonnegative, and its magnitude indicates to the basic possibility of improving the checkers. Additionally, the real latent time generally is different for various points of observation. This relation of times is illustrated by Fig. 1 and demonstrated by an example to be presented below.

According to the definition of self-testifiability which is the necessary condition for full self-testifiability (FST), for each fault there exists some input vector leading after some latent time

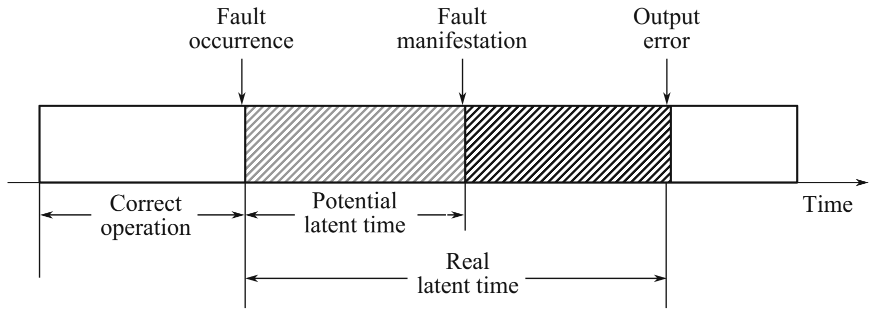

Fig. 1. Diagram of relations between the notions of real and potential latent time.

to the occurrence of an uncoded, that is, not belonging to the set O, output vector in the case of occurrence of this fault [6]. In the light of the aforementioned, detection of a fault does not necessarily give rise to an uncoded output vector, and, consequently, the automaton does not feature FST for this fault. At the same time, this fault is detectable in principle (see, for example, [7]).

We follow the generally accepted practice and consider only single faults, which implies that during the entire latent period the probability of occurrence of another fault is negligible. For the accepted definition of the automaton subjected to random actions, the duration of latent time also proves to be random, and out next purpose lies in determining the distribution function of the latent time.

3. DISTRIBUTION FUNCTION OF THE LATENT TIME OF FAULT MANIFESTATION

The gist of the proposed method lies in separating the set of possible trajectories (realizations, sample functions) of the random process describing behavior of the automaton into two subsets. The first subset which does not comprise the trajectories detecting the faults will be called the "nondetecting subset of trajectories." Its complement, the second subset, comprises only the states detecting the given fault. Then, the probability of fault detection at the tth step of operation of the automaton after the fault occurrence is the probability that until the tth step the process moves along the trajectories of the first subset and at the tth step gets into the second subset.

The method will be illustrated throughout the paper by the example of the automaton defined by the transition Table 1 where the rows correspond to the automaton transitions and columns from the left to the right correspond to the number of the row h; initial state a_m; transition state a_s; input $X(a_m, a_s)$—the Boolean function equal to one at the transition from a_m to a_s; the output

Table 1

h	a_m	a_s	$X(a_m, a_s)$	$Z(a_m, a_s)$
1	a_1	a_2	$x_1 x_2$	z_1, z_3
2	a_1	a_4	$x_1 \overline{x}_2 x_3$	z_4
3	a_1	a_1	$x_1 \overline{x}_2 \overline{x}_3$	$\sim$
4	a_1	a_3	$\overline{x}_1$	z_2
5	a_2	a_4	1	z_1, z_4
6	a_3	a_1	$x_4 x_1$	z_1, z_3
7	a_3	a_4	$x_4 \overline{x}_1$	z_1, z_4
8	a_3	a_4	$\overline{x}_4$	z_1, z_4
9	a_4	a_5	x_2	z_5, z_6
10	a_4	a_1	$\overline{x}_2$	$\sim$
11	a_5	a_1	1	z_1, z_3

binary vector $Z(a_m, a_s)$ at the transition from a_m to a_s. The output vector is set down as a list of binary signals z_i equal to one. If none of them is equal to one, then the corresponding row carries the symbol "$\sim$."

In what follows, consideration is given to the faults of input, output, and state variables. By the faults of variables are meant faults like "suck-at-1" or "suck-at-0" $(x_l/1, x_l/0)$. Additionally, the checker faults are considered as well.

3.1. Distribution of Latent Time under Faults of Input Variables

We use the following notation for the probabilities of values of the input variables x_l:

$$\Pr(x_l = 1) = p_l, \quad \Pr(x_l = 0) = \Pr(\overline{x}_l = 1) = q_l = 1 - p_l, \quad l = 1, \ldots, N_x.$$

Then, in the case of no faults behavior of the automaton obeys the Markov chain with the following matrix of transition probabilities:

$$(p_{ms}) = \begin{pmatrix} p_1q_2q_3 & p_1p_2 & q_1 & p_1q_2p_3 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ p_1p_4 & 0 & 0 & q_1p_4 + q_4 & 0 \\ q_2 & 0 & 0 & 0 & p_2 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{1}$$

Let a fault like $x_1/1$ occur for the input variable x_1. We denote by A the manifestation of occurred fault and by $\overline{A}$ the opposite event. Now, we construct two matrices for the even $\overline{A}$. The first matrix is for the case of $x_1 = 1$, and the second matrix, for $x_1 = 0$. Then, the fault $x_1/1$ coincides with x_1 if $x_1 = 1$, and consequently, in this case it cannot manifest itself. The first matrix is obtained from (1) be substituting 1 and 0, respectively, for p_1 and q_1:

$$\left(p_{ms} \mid \overline{A}, x_1/1, x_1 = 1\right) = \begin{pmatrix} q_2q_3 & p_2 & 0 & q_2p_3 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ p_4 & 0 & 0 & q_4 & 0 \\ q_2 & 0 & 0 & 0 & p_2 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{2}$$

The second matrix corresponds to x_1= 0 and as follows from Table 1 has the form

$$\left(p_{ms} \mid \overline{A},\ x_1/1,\ x_1 = 0\right) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & q_4 & 0 \\ q_2 & 0 & 0 & 0 & p_2 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{3}$$

The matrix of transition probabilities for the cases of $\overline{A}$ and $x_1/1$ is as follows:

$$\left(p_{ms} \mid \overline{A},\ x_1/1\right) = p_1\left(p_{ms}\overline{A}, x_1/1, x_1 = 1\right) + q_1\left(p_{ms} \mid \overline{A}, x_1/1,\ x_1 = 0\right)$$
$$= \begin{pmatrix} p_1q_2q_3 & p_1p_2 & 0 & p_1q_2p_3 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ p_1p_4 & 0 & 0 & q_4 & 0 \\ q_2 & 0 & 0 & 0 & p_2 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{4}$$

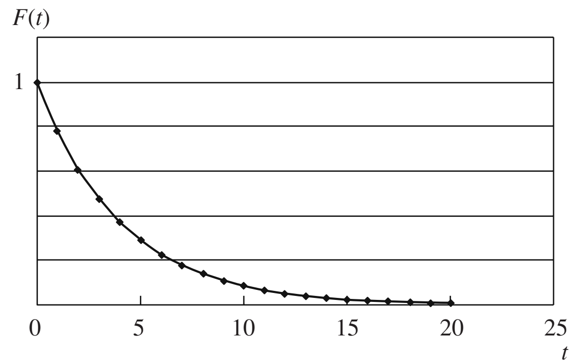

Fig. 2. Graph of the latent time distribution function.

We stress that each of the matrices (2)–(4) describes only those transitions where faults cannot manifest themselves, rather than every possible transition. Therefore, the matrices can be other than only stochastic, that is, the sum of elements in some rows needs not to be equal to one.

Let now

$$p\left(t-1,\overline{A} \mid x_1/1\right)=\left(p_1\left(t-1,\overline{A} \mid x_1/1\right),\ldots,p_{N_Q}\left(t-1,\overline{A} \mid x_1/1\right)\right)$$

be the vector of probabilities of the automaton states at the $(t-1)$st step after fault occurrence, but before its manifestation. We introduce the column vector

$$p^{\mathrm{T}}\left(A \mid x_1/1\right)=\left(p_{ms}\right)\,(1,0,0,1,0)^{\mathrm{T}} \tag{5}$$

with ones at the places of states detecting the fault, T being the sigh of transposition. Vector (5) defines the probabilities of states detecting faults on one step. Then, the probability $P_f(t)$ of detecting $x_1/1$ at the tth step is representable as

$$P_f\left(t\right)=p\left(t-1,\overline{A} \mid x_1/1\right)p^{\mathrm{T}}\left(A \mid x_1/1\right), \tag{6}$$

and the vector $p(t-1,\overline{A} \mid x_1/1)$ is obtained at that using the recurrent formula

$$p\left(t-1,\overline{A} \mid x_1/1\right)=p\left(t-2,\overline{A} \mid x_1/1\right)\left(p_{ms} \mid \overline{A},x_1/1\right), \tag{7}$$

and $p(0,\overline{A} \mid x_1/1)$ is the vector of probabilities of the automaton states at the instant of fault occurrence.

Figure 2 depicts the results of calculating the additional distribution function of the latent time, that is, the probability that the latent time is greater than t,

$$F\left(t\right)=\Pr\left(lat>t\right)=\sum_{k=t+1}^{\infty}P_f\left(k\right)=1-\sum_{k=0}^{t}P_f\left(k\right).$$

We consider the fault $x_4/1$ (see transitions 7 and 8 in Table 1) in order to demonstrate the difference between the potential and real latent times of detection. These transitions initiate the same output vector. We emphasize that the fault $x_4/1$ belongs namely to x_4 (transition 7) and not to its negation (transition 8). For the *accepted fault*, if the (input) literals $x_1=0$ and $x_4=0$, then both corresponding terms are equal to one. Therefore, at the output of the automaton the fault manifestation detected by term 7 will be masked by term 8. An example of difference between

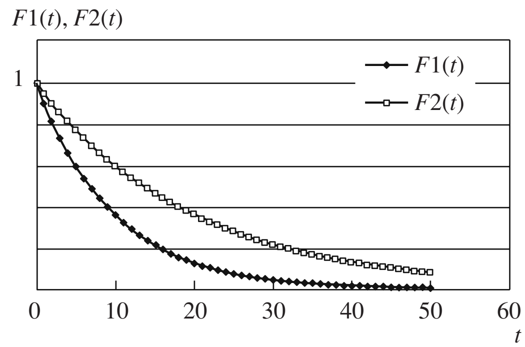

Fig. 3. Graph of the distribution function of the real and potential latent times for the fault $x_4/1$.

the distribution functions of the potential and real (relative to the output) latent times for the fault $x_4/1$ is shown in Fig. 3.

The considered fault can be detected by the architecture using various observation points [7]. In this case, the real (relative to the observation points used) and potential latent times coincide, which means that it is impossible to construct a better checker for the given fault. For other faults, this result in principle can be improved.

As follows from the above example, fault manifestation does not necessarily lead to its detection at the output. Consequently, for this fault the given automaton features FST. However, the architecture of [7] enables one to detect it, although it does not manifest itself at the output.

3.2. Distribution of the Latent Time under Faults of the Output Variables

Let the fault $z_1/1$ occur. It does not manifest itself if the output vector containing the variable z_1 is not initiated (see states a_2, a_3, and a_5 in Table 1). We use the above method to specify on the entire set of trajectories a subset such that it does not allow manifestation of this fault. As is evident from Table 1, the matrix corresponding to this subset is as follows:

$$\left(p_{ms}\left(\overline{A}\right)\right) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ p_1p_4 & 0 & 0 & q_1p_4 + q_4 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The matrix corresponding to the faulty state is as follows:

$$\left(p_{ms}\left(A\right)\right) = \begin{pmatrix} p_1q_2q_3 & p_1p_2 & q_1 & p_1q_2p_3 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ q_2 & 0 & 0 & 0 & p_2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

and $(p_{ms}(\overline{A})) + (p_{ms}(A)) = (p_{ms})$.

The distribution function of the latent time, that is, the fault manifestation probability at the tth step, is as follows:

$$P_f\left(t\right) = p\left(0, \overline{A} \mid y_1/1\right)\left(p_{ms}\left(\overline{A}\right)\right)^{t-1}\left(p_{ms}\left(B\right)\right)\left(1,1,1,1,1\right)^{\mathrm{T}}, \tag{8}$$

where $p(0, \overline{A} \mid y_1/1)$ is the vector of automaton state at the instant of fault occurrence.

3.3. Distribution of the Fault Latent Time in the Memory of Automaton

If the state of the automaton memory is coded by a nonredundant code, then the fault cannot be detected. In the case of redundant codes, the latent time of detection depends on the code characteristics. We assume by way of example that the unit position code is used. Then, for the state a_r a fault like $y_r/0$ can be detected immediately at the instant of reaching this state, and the fault $y_r/1$ manifests itself at the first step when the memory gets into a state other than a_r.

We put down the matrix of transition probabilities in the general form

$$(p_{ms}) = \begin{pmatrix} p_{1,1} & \cdots & p_{1,r-1} & p_{1,r} & p_{1,r+1} & \cdots & p_{1,N_Q} \\ \multicolumn{7}{c}{\dotfill} \\ p_{r,1} & \cdots & p_{r,r-1} & p_{r,r} & p_{r,r+1} & \cdots & p_{r,N_Q} \\ \multicolumn{7}{c}{\dotfill} \\ p_{N_Q,1} & \cdots & p_{N_Q,r-1} & p_{N_Q,r} & p_{N_Q,r+1} & \cdots & p_{N_Q,N_Q} \end{pmatrix}. \tag{9}$$

The matrix specifying the set of trajectories that do not detect the fault $y_r/0$ has zeros at the rth row and the rth column:

$$\left(p_{ms}^{(f)}\right) = \begin{pmatrix} p_{1,1} & \cdots & p_{1,r-1} & 0 & p_{1,r+1} & \cdots & p_{1,N_Q} \\ \multicolumn{7}{c}{\dotfill} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \multicolumn{7}{c}{\dotfill} \\ p_{N_Q,1} & \cdots & p_{N_Q,r-1} & 0 & p_{N_Q,r+1} & \cdots & p_{N_Q,N_Q} \end{pmatrix}.$$

In the example, matrix (9) has form (1). If the column vector

$$p(0) = \left(p_1(0), \ldots, p_{N_Q}(0)\right)$$

is the probability vector of the initial state (at the instant of fault occurrence), then the distribution of the latent time—the probability that the fault does not manifest itself before the kth step—is representable as

$$\Pr(t > k) = p_r(0) \left(p_{ms}^{(f)}\right)^k (1, \ldots, 1, 0, 1, \ldots, 1)^{\mathrm{T}},$$

with zero at the rth position.

For the fault $y_r/1$, we get

$$\Pr(t = 1) = p(0) \left(p_{ms}^{(f)}\right) (1, \ldots, 0, \ldots, 1)^{\mathrm{T}}, \quad \Pr(t > k) = p_r(0)\, p_{r,r}^k,$$

where $p_r(0)$ is the rth element of the vector $p(0)$ and $p_{r,r}$ is an element of matrix (9).

3.4. Distribution of the Latent Time of Checker Faults

The desired distribution is obtained using the method of construction of the matrices $(p_{ms}(\overline{A}))$ and $(p_{ms}(A))$. According to Table 1, these matrices as follows:

$$\left(p_{ms}\left(\overline{A} \mid R_1/1\right)\right) = \begin{pmatrix} 0 & 0 & q_1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ p_1p_4 & 0 & q_4 & 0 & 0 \\ p_2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \left(p_{ms}\left(A \mid R_1/1\right)\right) = \begin{pmatrix} p_1q_2q_3 & p_1p_2 & q_1 & p_1q_2p_3 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & q_1p_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & q_2 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

In order to determine the distribution function of the latent time, (8) must be applied with the use of $p(0, \overline{A} \mid R_1/1)$.

4. ESTIMATION OF THE LATENT TIME OF FAULT MANIFESTATIONS

The above method for calculation of distributions describes exhaustively the latent time as a random variable. It might seem that it requires a great bulk of computations. Yet if one uses in (6) the recurrent formula (7) and takes into consideration that the matrices of transition probabilities for the generally accepted automata (matrix (1) in the case at hand) usually are very sparse and the reasonably designed programs perform calculations only over the nonzero elements, the time of calculations may prove to be quite acceptable.

At the same time, another reason must be taken into consideration. Calculation of the distribution function of the latent time requires a rather great amount of initial data which are not always available, especially at the initial stages of design. At that, it is possible to confine oneself to one or another estimate of the latent time. Therefore, despite the aforementioned possibilities of reducing the time required for precise calculations, the question of approximate estimates is of significant interest.

Let us consider two approaches to getting such estimates:

—determination of the upper and lower boundaries of the distribution function of the latent time;

—determination of the upper boundary of the mean value of the latent time.

4.1. The Lower and Upper Boundaries of the Latent Time Distribution

Let the latent time distribution for the fault f obey (6)—example for $f = x_1/1$. Then, (6) and (7) are representable as

$$P_f(t) = p\left(t-2, \overline{A} \mid x_1/1\right)\left(p_{ms} \mid \overline{A}, x_1/1\right) p^{\mathrm{T}}\left(A \mid x_1/1\right). \tag{10}$$

Let us determine

$$p^{\mathrm{T}}\left(A \mid x_1/1\right) = \left(\alpha_1, \ldots, \alpha_{N_Q}\right) \tag{11}$$

and

$$\left(p_{ms} \mid \overline{A}, x_1/1\right) p^{\mathrm{T}}\left(A \mid x_1/1\right) = \left(\beta_1, \ldots, \beta_{N_Q}\right), \tag{12}$$

where α_i is the sum of the probabilities of transition from the state a_i to the state manifesting the fault under consideration.

We rearrange (12) in

$$\left(p_{ms} \mid \overline{A}, x_1/1\right) p^{\mathrm{T}}\left(A \mid x_1/1\right) = (\gamma_1\alpha_1, \ldots, \gamma_{N_Q}\alpha_{N_Q}), \;\; \gamma_i = \beta_i/\alpha_i \le 1, \;\; \alpha_i \ne 0, \tag{13}$$

substitute (13) in (10)

$$P_f(t) = p\left(t-2, \overline{A} \mid x_1/1\right)(\gamma_1\alpha_1, \ldots, \gamma_{N_Q}\alpha_{N_Q}) \left| \begin{array}{l} \le p\left(t-2, \overline{A} \mid x_1/1\right)\gamma_{\max}\left(\alpha_1, \ldots, \alpha_{N_Q}\right) \\ \ge p\left(t-2, \overline{A} \mid x_1/1\right)\gamma_{\min}\left(\alpha_1, \ldots, \alpha_{N_Q}\right), \end{array} \right. \tag{14}$$

$$\gamma_{\max} = \max_i \gamma_i, \quad \gamma_{\min} = \min_i\left(\gamma_i \mid \gamma_i \ne 0\right),$$

and use (10) and (11) to represent (14) as

$$\begin{aligned} P_f(t) &\le \gamma_{\max} P_f(t-1) = P_f^{\max}(t), \\ P_f(t) &\ge \gamma_{\min} P_f(t-1) = P_f^{\min}(t). \end{aligned} \tag{15}$$

Relation (15) enables one to estimate the residual part of the function $P_f(t)$ at any step after precise calculations or to give the following exponential estimates:

$$P_f(t) \leq \gamma_{\max}^t p(0, A \mid x_1/1), \quad P_f(t) \geq \gamma_{\min}^t p(0, A \mid x_1/1). \tag{16}$$

We note that if all γ_i are equal, $\gamma_i = \gamma$, then inequalities (27) turn into equalities, that is, provide the exact expression for the function $P_f(t)$ which is exponential in this case:

$$P_f(t) = \gamma^t p(0, B \mid x_1/1).$$

If $\gamma_{\max} = 1$, then the first formula in (15) becomes trivial and other methods of estimation must be sought.

4.2. Upper Boundary of the Mean Value of Latent Time

To establish the desired estimates, we construct in this case a "worst" automaton and also assume that $\Pr(x_l = 1) = 0.5$ for any x_l.

The set of terms will be said to be the "triangular" set of length $K \leq N_x$ if

$$G_{K+1} = \prod_{l=1}^{K} x_l; \quad G_k = \prod_{l=1}^{k-1} x_l \overline{x}_k, \quad k = 1, \ldots, K. \tag{17}$$

Then, the two following theorems are valid.

Theorem 1. *For the automaton with identical probabilities of fault occurrence and the set of transition functions defined by the "triangular" set of terms, the mean probability of manifestation of a single fault is minimal over every possible automaton with the same number of states and equal to*

$$\overline{p}_f = \frac{1}{K}\left(1 - \frac{1}{2^K}\right).$$

Theorem 2. *Among all automata with N_Q states and N_x input variables, the automaton of Fig. 4 has the following maximal latent time per one fault:*

$$\overline{T} = \frac{2N_Q}{N_x}\left(2^{N_x} - 1\right) - \left(\frac{N_Q}{2} + 1\right). \tag{18}$$

We note that the determined estimate $\overline{T}$ is unimprovable because the structure of the automaton where it is reached is given.

Theorems 1 and 2 are proved in the Appendix.

5. PROBABILITY OF RETENTION OF FAULT UNIQUENESS

It may turn out in practice that only the real latent time is of interest because over this period the automaton operates without faults (at outputs) and at appearance of an output fault it must be stopped. Therefore, the potential latent time will be only of theoretical interest as a possible boundary of improvement of checkers.

Until now we followed the generally accepted way and assumed that the fault remains single over the entire time between its occurrence and the instant of its manifestation. However, another fault may occur between the instants of fault occurrence and manifestation. Moreover, this new fault can mask its predecessor so that the automaton will operate erroneously, but this fact will either remain undetected at all or detected much later even relative to the real latent time of the single fault. In this situation the above methodology of estimation of the potential and real latent times proves to be unacceptable. However, to reduce the probability of occurrence of these events in any case it is required to reduce the time of fault detection and, consequently, the potential latent time becomes an essential characteristic.

The following two problems may be posed in the light of this fact: (a) examine the problem of detection of multiple faults, including the case of mutual masking, and (b) determine the probability that a fault remains single until its manifestation and, consequently, the conditions for applicability of the above results remain valid. Now we turn to the second problem and leave the first problem for separate study.

Let us numerate all possible faults and let their number be M. Also, let $P_l(n)$ be the distribution function of the potential latent time for the lth fault and p_m be the probability of occurrence of the mth fault l, $m = 1, \ldots, M$. Assuming that the instants of occurrence of different faults are independent, we can set down the probability that the lth fault remains single over the entire latent time as follows:

$$Q_l = \sum_{n=0}^{\infty} P_l(n) \times \Pr(D) = \sum_{n=0}^{\infty} P_l(n) \prod_{\substack{m=1 \\ m \neq l}}^{M} (1 - p_m)^n,$$

where D is the case where no other fault appears over the entire latent time of occurrence of the lth fault.

For the standard case of $p_m \ll 1$, we obtain to within $o(p_m)$ that

$$Q_l = \sum_{n=0}^{\infty} P_l(n) \prod_{\substack{m=1 \\ m \neq l}}^{M} (1 - np_m) = \sum_{n=0}^{\infty} P_l(n) \left(1 - \sum_{\substack{m=1 \\ m \neq l}}^{M} np_m\right) = 1 - E(n_l) \sum_{\substack{m=1 \\ m \neq l}}^{M} p_m,$$

where $E(n_l)$ is the mean latent time for the lth fault.

We note that Q_l is independent of the distribution of the latent time and depends only on its mean value.

The resulting probability characterizes the lth fault. In essence, it is the conditional probability for the case of fault occurrence. For the unconditional probability we obtain the following:

$$Q = \sum_{l=1}^{M} p_l Q_l = \sum_{l=1}^{M} p_l \left(1 - E(n_l) \sum_{\substack{m=1 \\ m \neq l}}^{M} p_m\right). \tag{19}$$

Now we turn to the probability of masking. Let the lth fault can be masked by the fault numbered l_1. For example, these may be the bit-stuck faults of some literal and its negation. Then, the probability that masking occurs before the instant of manifestation is as follows:

$$R_l = \sum_{n=0}^{\infty} P_l(n) \left[1 - (p_l)\right]^n \prod_{\substack{m=1 \\ m \neq l, l_1}}^{M} (1 - p_m)^n.$$

For small p_m, we obtain with the same precision that

$$R_l = \sum_{n=0}^{\infty} P_l(n)\, np_{l_1} \left(1 - \sum_{\substack{m=1 \\ m \neq l, l_1}}^{M} np_m\right) = E(n_{l_1})\, p_{l_1} - E\left(n_l^2\right) \sum_{\substack{m=1 \\ m \neq l, l_1}}^{M} p_m p_{l_1}. \tag{20}$$

The unconditional probability is obtained by multiplying (20) by p_l summation over all l's.

6. EXPERIMENTAL RESULTS

Five automata describing each operation of some microprocessor were used as experimental benchmarks whose parameters and the calculated latent times are compiled in Table 2, where N_x is the number of inputs, N_y is the number of outputs, N_Q is the number of states, h is the number of the transition, and t and $\overline{T}$ are the precise and maximal values of the mean latent time, respectively, as calculated from the ordinary formulas of expectation using (8) for t and (19) for $\overline{T}$, time being measured in cycles. Analysis of the results demonstrated utility of both methods for estimation of the latent time.

Table 2

Name	N_x	N_y	N_Q	h	$\bar{t}$	$\overline{T}$
big	18	28	17	185	747	2420
bs	19	13	17	185	247	903
acdl	16	27	22	214	456	1742
cow	49	24	24	261	366	1486
v1_6	14	18	17	169	237	608
v1_10	15	18	18	264	300	907
v11_20	14	29	18	367	360	1630

7. CONCLUSIONS

The above results may be summed up as follows.

(1) The paper analyzed the latent time of manifestation of the occurring faults. This analysis is valid for the case where the automaton is tested in the course of its real operation.

(2) Introduced was the concept of the potential and real latent times. Their difference is indicative of the potentiality of checker improvement, which is important for reduction of the fault detection time and the probability of mutual masking in the case of multiple faults.

(3) A precise expression for calculation of the distribution of the potential and real latent times, as well as their upper boundaries, was established.

(4) An expression for the upper (worst) estimate of the mean latent time was obtained from the analysis of the proposed construction of the "worst" automaton. The precise value of the mean latent time is about 30% of the established upper boundary, which may be regarded as satisfactory taking into consideration the fact that $\overline{T}$ is intended for estimation at that stage of design where the volume of data is limited.

APPENDIX

Proof of Theorem 1. Let us expand the "triangular" set of terms (17) as follows:

$$\begin{array}{lllllll} G_{K+1} & = x_1 & x_2 & \cdots & x_l & \cdots & x_{K-1} \quad x_K, \\ G_K & = x_1 & x_2 & \cdots & x_l & \cdots & x_{K-1} \quad \overline{x_K}, \\ G_{K-1} & = x_1 & x_2 & \cdots & x_l & \cdots & \overline{x_{K-1}}, \\ \cdots & & & & & & \\ G_l & = x_1 & x_2 & \cdots & \overline{x_l}, & & \\ \cdots & & & & & & \\ G_2 & = x_1 & \overline{x_2}, & & & & \\ G_1 & = \overline{x_1}. & & & & & \end{array} \tag{A.1}$$

We first determine the initial probability of fault manifestation for a variable in (A.1). For example, let it be the variable x_1 with a fault like $x_1/1$, which means that all literals x_1 in (A.1) are equal to one. If now the variable itself $x_1 = 0$, then its value and those of its corresponding literals in (18) are distinct. Therefore, the fault can manifest itself with the probability 0.5. For the same reason, the probabilities of the fault $x_1/0$ and the same faults for the literals corresponding to the negation of x_1 are equal to 0.5 as well.

Now we consider the fault $x_l/1$. As follows from (12), it can manifest itself only if $\prod x_k = 1$, where the product is taken over all $k < l$. In this case we obtain the conditional and unconditional manifestation probabilities

$$p_f\left(x_l \,\middle|\, \prod_{k=1}^{l-1} x_k = 1\right) = \frac{1}{2},$$

$$p_f\left(x_l\right) = \Pr\left(\prod_{k=1}^{l-1} x_k = 1\right) p_f\left(x_l \,\middle|\, \prod_{k=1}^{l-1} x_k = 1\right) = \left(\frac{1}{2}\right)^l.$$

The probability of fault manifestation averaged over set (A.1) is as follows:

$$\overline{p}_f = \frac{1}{K}\sum_{l=1}^{K} p_f\left(x_l\right) = \frac{1}{K}\left(1 - \frac{1}{2^K}\right).$$

It is assumed at that that the occurrence probabilities of all faults are the same.

Proof of Theorem 2. Let the variable x_l fail. As is evident from Fig. 4, the automaton structure admits its manifestation only on the transition from a_1 to a_2, and $p_f(x_l) = 1/2^l$ is the probability of this manifestation.

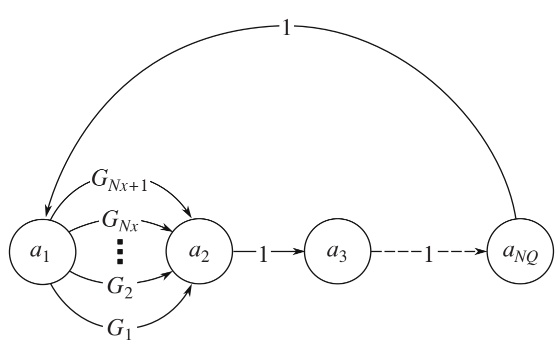

Fig. 4. Graph of the "worst" automaton, that is, the automaton with the maximum mean latent time.

If there was no fault manifestation, conditions for its manifestation will appear only after $N_Q - 1$ step when the automaton again returns to the state a_1. Under the accepted conditions, the number r of cycles before manifestation is a random variable obeying the geometrical distribution

$$P_l(r) = (1 - p_f(x_l))^{r-1} p_f(x_l).$$

The mean number of states to be passed by the automaton from the instant of fault occurrence to that of its manifestation, provided that the fault occurs at the instant where the automaton is in the state a_1, is as follows:

$$\overline{T_l}(a_1) = \sum_{r=1}^{\infty} [(r-1) N_Q + 1] P_l(r) = N_Q \sum_{r=1}^{\infty} r q_f^{r-1}(x_l) p_f(x_l)$$
$$= N_Q \left(\frac{1}{p_f(x_l)} - 1 \right) - 1 = N_Q \left(2^l - 1 \right) - 1.$$

If we assume now that a fault arises with equal probability at the instant when the automaton is in any state, then the unconditional mean latent time of manifestation will be as follows:

$$\overline{T}_l = \overline{T}_l(a_1) + \frac{N_Q}{2}.$$

Finally, by averaging over all feasible single faults and assuming that all faults are equiprobable, we obtain the following mean latent time

$$\overline{T} = \frac{1}{N_x} \sum_{l=1}^{N_Q} \overline{T}_l = \frac{N_Q}{N_x} \sum_{l=1}^{L} 2^l - \left(\frac{N_Q}{2} - 1 \right) = \frac{2N_Q}{N_x} \left(2^{N_x} - 1 \right) - \left(\frac{N_Q}{2} - 1 \right).$$

REFERENCES

1. Lala, P., *Self-Checking and Fault Tolerant Digital Design*, San Francisco: Morgan Kaufman, 2000.
2. Shedletsky, J. and McCluskey, E., The Error Latency of Fault in a Sequential Digital Circuit, *IEEE Trans. Comput.*, 1976, vol. 25, no. 6, pp. 655–659.
3. Goot, R., Levin, I., and Ostanin, S., Fault Latencies of Concurrent Checking FSMs, in *Proc. DSD 2002 Euromicro Sympos. Digital Syst. Design Architectures, Methods and Tools*, Dortmund, pp. 174–179.
4. Feller, W., *An Introduction to Probability Theory and Its Applications*, New York: Wiley, 1971.
5. Kemeny, J. and Snell, J., *Finite Markov Chains*, Princeton: Van Nostrand, 1967.
6. Nicolaidis, M. and Zorian, Y., On-line Testing for VLSI—A Compendium of Approaches, *J. Electron. Testing: Theory Appl.*, 1998, no. 12, pp. 7–20.
7. Levin, I. and Sinelnikov, V., Self-checking of FPGA based Control Units, in *Proc. Great Lakes Sympos. VLSI*, Ann Arbor: IEEE Press, 1999, pp. 292–295.

This paper was recommended for publication by P.P. Parkhomenko, a member of the Editorial Board