A Method for the Computation of Reliability Bounds for Non-repairable Fault-tolerant Systems*

Víctor Suñé and Juan A. Carrasco
Departament d'Enginyeria Electrònica, UPC
Diagonal 647, plta. 9, 08028 Barcelona, Spain
{sunye, carrasco}@eel.upc.es

Abstract

A realistic modeling of fault-tolerant systems requires to take into account phenomena such as the dependence of component failure rates and coverage parameters on the operational configuration of the system, which cannot be properly captured using combinatoric techniques. Such dependencies can be modeled with detail using continuous-time Markov chains (CTMC's). However, the use of CTMC models is limited by the well-known state space exploition problem. In this paper we develop a method for the computation of bounds for the reliability of non-repairable fault-tolerant systems which requires the generation of only a subset of states. The tightness of the bounds increases as more detailed states are generated. The method uses the failure distance concept and is illustrated using an example of a quite complex fault-tolerant system whose failure behavior has the above mentioned types of dependencies.

1. Introduction

The increasing demand on dependability has fostered interest in fault-tolerant systems. The evaluation of such systems requires the combination of fault injection techniques, either on the real system or in a simulated model of it, and modeling techniques. Fault-injection experiments are aimed at achieving estimates for the coverage of the system to several types of faults. These coverage parameters are then combined with estimates for failure rates and, for repairable systems, repair times to obtain an estimate for the overall dependability of the system. Continuous-time Markov chains (CTMC's) are the most common modeling formalism. The use of CTMC models is however limited by the well-known state space exploition problem. A general approach to attack the problem is the use of methods which obtain bounds for the dependability measure of interest using detailed knowledge of the CTMC in a subset of its state space (the generated portion). Computing bounds for the steady-state availability and similar measures is a problem which has received recently a great deal of attention and several bounding methods are currently available [4], [5], [6], [11], [12], [13], [18]. Bounding transient measures has received relatively less attention.

In this paper we develop a method to obtain bounds for the reliability of non-repairable fault-tolerant systems, which gives significantly tighter bounds than the trivial approach (see, for instance, [2]) in which lower and upper bounds are obtained by assuming the system, respectively, operational or down whenever the model exits the generated state space. The method uses the failure distance concept which has been proved useful to obtain tight bounds for the steady-state availability [4], [6]. The method allows to obtain accurate estimates for the reliability of systems with dependencies which cannot be managed in hierarchical solution methods [10], [17] or refined combinatoric methods [7] recently developed to attack the state space exploition problem. The rest of the paper is organized as follows. Section 2 describes the bounding method, which has the useful property that the bounds can be expressed in terms of transient solutions of an augmented CTMC model in which the non-generated state space is represented by a "bounding" part added to the detailed CTMC model in the generated state space. Section 3 includes the proof of the non-trivial bound. Section 4 reviews the algorithms used for the computation of the failure distances required by the method. Section 5 illustrates the application of the method and analyzes its typical performance using an example exhibiting dependencies which prevent the use of combinatoric or hierarchical solutions. Section 6 concludes the paper, and suggests future research directions.

2. Description of the method

We consider CTMC models of non-repairable fault-tolerant systems. The system is assumed made up of components which can be grouped in classes, being all components in the same class indistinguishable from a dependability point of view. The operational/down state of the system is assumed determined from the unfailed/failed state of its components by a coherent structure function [1] which, without lost of generality, is assumed defined by a logic expression involving AND/OR operators acting over atoms of the form $c[n]$, which have the logic value true if and only

*This work was supported by the "Comisión Interministerial de Ciencia y Tecnologfa" (CICYT) under the research grant TIC95-0707-C02-02.

0-8186-7758-9/97 $10.00 © 1997 IEEE

if n or more components of class c are unfailed. Components fail following a set of patterns (called *failure events*) E, where each $e \in E$ is a bag[1] of components which can fail simultaneously. Failure events with more than one component allow to model failure propagation and lack of coverage. Failure events may have state dependent rates, allowing the modeling of complex dependencies resulting in state dependent failure rates and coverages. The resulting CTMC $X = \{X(t); t \geq 0\}$ is acyclic, has a finite state space $\Omega \cup \{f\}$, where f is an absorbing state which represents the failure of the system and Ω is the set of states in which the system is operational, and transition rates associated to failure events. Given $a \in \Omega$, $b \in \Omega \cup \{f\}$ we will denote by $\lambda_{a,b}$ the transition rate of X from state a to state b and by $\lambda_a = \sum_{b \in \Omega \cup \{f\}} \lambda_{a,b}$ the output rate of X from state a. Being B a subset of states, we will denote by $\lambda_{a,B} = \sum_{b \in B} \lambda_{a,b}$ the transition rate from state a to B.

The bounding method exploits the *failure distance* concept. The failure distance from a state a, $d(a)$, is defined as the minimum number of components which have to fail in addition to those already failed in a to take the system to a failed state. Since the system is down if and only if the bag of failed components contains some minimal cut, $d(a)$ can be expressed as:

$$d(a) = \min_{m \in MC} |m - F(a)|, \qquad (1)$$

where MC is the set of minimal cuts of the structure function of the system (see, for instance, [1]), $F(a)$ denotes the bag of components failed in a, and $|s|$ denotes the cardinality of bag s. Note that a minimal cut is also a bag of components. The computation of the rates λ_{a,U_d} (U_d denotes the subset of non-generated states with failure distance $d > 0$) used in our method requires the computation of the failure distances from the states in the frontier of the non-generated state space. Trivial modifications to well-known algorithms [9], [15] allow the computation of the minimal cuts given the structure function of the system when classes of components are considered. However, the use of (1) for the computation of failure distances is costly when the number of minimal cuts is large. In [6] more efficient algorithms are proposed for the computation of the failure distances from the states reached from a given state by considering all failure events of the model. Those algorithms are briefly reviewed in Section 5.

The method assumes the knowledge of upper bounds $\lambda_{ub}(e)$, $e \in E$ for the rates of the failure events and computes bounds for the unreliability of the system $ur(t) = P[X(t) = f]$ using a CTMC $X' = \{X'(t); t \geq 0\}$ with state space $G \cup \{f\} \cup \{u_0, \cdots, u_L\}$, $L = \min_{m \in MC} |m|$. G is the subset of Ω which is generated and the method assumes $P[X(0) \in G] = 1$; f represents the failure of the system from a state belonging to G; the states u_d, $0 \leq d \leq L$ "bound" the behavior of X after it exits G through a non-failed state. Let $U = \Omega - G$. The formal proof of the method assumes that there are not transitions from U to G. For a given partition $\Omega = G \cup U$, depending on G it could well be that X had transitions from U to G, violating the assumption. However, the assumption does not in fact impose any real restriction to the selection of G, since it is enough to redefine X so that U includes copies of the states of G reachable from U to satisfy the assumption. Thus, the only limitation imposed to G is $P[X(0) \in G] = 1$. The transition rates among the states of G are as in X; the transition rates from states $a \in G$ to u_d, $1 \leq d \leq L$ have values λ_{a,U_d}, being U_d the subset of U including the states with failure distance d; finally, denoting by FC the set of different cardinalities of the failure events of the model and by E_i the subset of failure events with cardinality i, and defining $f_i = \sum_{e \in E_i} \lambda_{ub}(e)$, for each $1 \leq d \leq L$, $i \in FC$ there is a transition rate f_i from u_d to $u_{\max\{0,d-i\}}$. Figure 1 illustrates the structure of X'. The initial probability distribution of X' is $P[X'(0) = a] = P[X(0) = a]$, $a \in G$; $P[X'(0) = f] = 0$; $P[X'(0) = u_d] = 0$, $0 \leq d \leq L$.

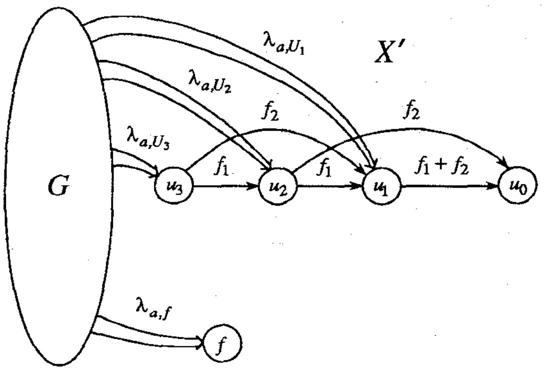

Figure 1. State transition diagram of X' for $L = 3$ and $FC = \{1, 2\}$.

The bounds are:

$$[ur(t)]_{lb} = P[X'(t) = f], \qquad (2)$$

$$[ur(t)]_{ub} = P[X'(t) \in \{u_0, f\}]. \qquad (3)$$

The lower unreliability bound (2) is trivial, since X' enters f when X enters f from G; the upper bound (3) is shown in the next section.

3. Proof of the upper bound

The proof of the upper bound will be done through a lemma, two propositions and a theorem and will make reference to the discrete-time Markov chains (DTMC's) $Y = \{Y_n; n = 0, 1, \ldots\}$ and $Y' = \{Y'_n; n = 0, 1, \ldots\}$ obtained by randomizing, respectively, X and X' with a rate Λ, greater than or equal to the maximum output rate of X (for instance, $\Lambda = \sum_{e \in E} \lambda_{ub}(e)$). Y has the same state space and initial probability distribution as X and transition probabilities $q_{a,b} = \lambda_{a,b}/\Lambda$, $a \neq b$, $q_{a,a} = 1 - \lambda_a/\Lambda$. Y'

[1] A bag is a collection of elements which can be repeated (see, for instance, [14]) and can be described by giving the number of instances for each element included in the bag: in our context, the number of instances of each component class.

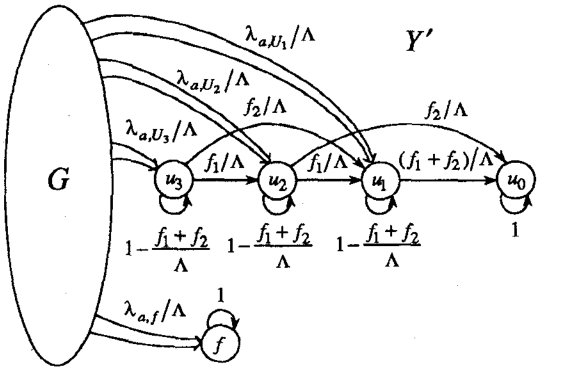
Y'
G
$\lambda_{a,U_1}/\Lambda$
$\lambda_{a,U_2}/\Lambda$
$\lambda_{a,U_3}/\Lambda$
f_2/Λ
f_2/Λ
f_1/Λ
f_1/Λ
$(f_1+f_2)/\Lambda$
u_3
u_2
u_1
u_0
$1-\frac{f_1+f_2}{\Lambda}$
$1-\frac{f_1+f_2}{\Lambda}$
$1-\frac{f_1+f_2}{\Lambda}$
1
$\lambda_{a,f}/\Lambda$
1
f

Figure 2. State transition diagram of DTMC Y' for $L = 3$ and $FC = \{1, 2\}$.

has the same state space and initial probability distribution as X' and transition probabilities $q'_{a,b} = \lambda'_{a,b}/\Lambda$, $a \neq b$, $q'_{a,a} = 1 - \lambda'_a/\Lambda$, where $\lambda'_{a,b}$ and λ'_a are, respectively, the transition and output rates of X'. Figure 2 illustrates the state transition diagram of Y'. It is well-known (see, for instance, [16]) that $X(t) = Y_{N(t)}$ and $X'(t) = Y'_{N(t)}$, where $N = \{N(t); t \geq 0\}$ is a Poisson process with rate Λ. These results allow to express the transient solution of X (X') in terms of the transient solution of Y (Y'):

$$P[X(t) = a] = \sum_{n=0}^{\infty} \frac{(\Lambda t)^n}{n!} e^{-\Lambda t} P[Y_n = a], \qquad (4)$$

$$P[X'(t) = a] = \sum_{n=0}^{\infty} \frac{(\Lambda t)^n}{n!} e^{-\Lambda t} P[Y'_n = a]. \qquad (5)$$

Intuitively, it is clear that the probability that Y' will reach the absorbing state u_0 from u_d, $d \geq 0$ in m steps decreases with d. The result is established in the following lemma. Let

$$R'_m(d) = P[Y'_m = u_0 | Y'_0 = u_d].$$

Lemma 1 *$R'_m(d), m > 0, d \geq 0$ is decreasing with d.*

Proof From the structure of Y' we can write:

$$R'_m(0) = 1,\ m > 0\,, \qquad (6)$$

$$R'_1(d) = \sum_{\substack{i \in FC \\ i \geq d}} \frac{f_i}{\Lambda},\ d > 0\,, \qquad (7)$$

and for $m > 1\,, d > 0$:

$$\begin{aligned} R'_m(d) \;&=\; \Big(1 - \frac{1}{\Lambda} \sum_{i \in FC} f_i\Big) R'_{m-1}(d) \\ &+ \sum_{i \in FC} \frac{f_i}{\Lambda} R'_{m-1}(\max\{0, d-i\})\,. \end{aligned} \qquad (8)$$

The proof is by induction on m.

<u>Base case ($m = 1$)</u>: We show $R'_1(d) \leq R'_1(d-1)\,,\ d > 0$. For $d = 1$, using (7) and (6) we have:

$$R'_1(1) = \sum_{i \in FC} \frac{f_i}{\Lambda} \leq 1 = R'_1(0)\,.$$

For $d > 1$, using (7):

$$R'_1(d) = \sum_{\substack{i \in FC \\ i \geq d}} \frac{f_i}{\Lambda} \leq \sum_{\substack{i \in FC \\ i \geq d-1}} \frac{f_i}{\Lambda} = R'_1(d-1)\,.$$

<u>Induction step</u>: Let $m > 0$; we will assume $R'_m(d)$, $d \geq 0$ decreasing with d and will show $R'_{m+1}(d) \leq R'_{m+1}(d-1)$, $d > 0$. For $d = 1$, using (8), $R'_m(1) \leq 1$ and (6) we have:

$$\begin{aligned} R'_{m+1}(1) \;&=\; \Big(1 - \frac{1}{\Lambda} \sum_{i \in FC} f_i\Big) R'_m(1) + \sum_{i \in FC} \frac{f_i}{\Lambda} R'_m(0) \\ &\leq\; 1 - \frac{1}{\Lambda} \sum_{i \in FC} f_i + \sum_{i \in FC} \frac{f_i}{\Lambda} \;=\; 1 \;=\; R'_{m+1}(0)\,. \end{aligned}$$

For $d > 1$, using (8) and the induction hypothesis:

$$\begin{aligned} R'_{m+1} \;&=\; \Big(1 - \frac{1}{\Lambda} \sum_{i \in FC} f_i\Big) R'_m(d) \\ &\quad + \sum_{i \in FC} \frac{f_i}{\Lambda} R'_m(\max\{0, d-i\}) \\ &\leq\; \Big(1 - \frac{1}{\Lambda} \sum_{i \in FC} f_i\Big) R'_m(d-1) \\ &\quad + \sum_{i \in FC} \frac{f_i}{\Lambda} R'_m(\max\{0, d-i-1\}) \\ &=\; R'_{m+1}(d-1).\ \square \end{aligned}$$

Let us define $R_m(a) = P[Y_m = f | Y_0 = a]$. We have:

Proposition 1 $R_m(a) \leq R'_m(d), a \in U_d, m > 0, d > 0\,.$

Proof Let $\lambda^i_{a,f}$ be the contribution to $\lambda_{a,f}$ associated to failure events $e \in E_i$. We have $\lambda^i_{a,f} \leq f_i$. Since a failure event $e \in E_i$ reduces the failure distance at most by i, $\lambda_{a,f}$ will not have contributions $\lambda^i_{a,f}$ for $i < d$, and:

$$R_1(a) = \sum_{\substack{i \in FC \\ i \geq d}} \frac{\lambda^i_{a,f}}{\Lambda}\,. \qquad (9)$$

Let us denote by $U_{k,d}$ the subset of U including the states with k failed components and failure distance d. For $m > 1$, taking into account that f is absorbing, we can write:

$$\begin{aligned} R_m(a) \;&=\; \Big(1 - \frac{\lambda_a}{\Lambda}\Big) R_{m-1}(a) \\ &+ \sum_{\substack{i \in FC \\ i \geq d}} \Big[\frac{\lambda^i_{a,f}}{\Lambda} + \sum_{d'=1}^{d} \sum_{b \in U_{k+i,d'}} \frac{\lambda_{a,b}}{\Lambda} R_{m-1}(b)\Big] \\ &+ \sum_{\substack{i \in FC \\ i < d}} \sum_{d'=d-i}^{d} \sum_{b \in U_{k+i,d'}} \frac{\lambda_{a,b}}{\Lambda} R_{m-1}(b)\,. \end{aligned} \qquad (10)$$

The proof is by induction on m.

Case base ($m = 1$): We will show $R_1(a) \leq R'_1(d)$, $a \in U_d, d > 0$. Using (9), $\lambda^i_{a,f} \leq f_i$, and (7):

$$R_1(a) = \sum_{\substack{i \in FC \\ i \geq d}} \frac{\lambda^i_{a,f}}{\Lambda} \leq \sum_{\substack{i \in FC \\ i \geq d}} \frac{f_i}{\Lambda} = R'_1(d)\,.$$

Induction step: Let $m > 0$; we will assume $R_m(a) \leq R'_m(d), a \in U_d, d > 0$ and show $R_{m+1}(a) \leq R'_{m+1}(d), a \in U_d, d > 0$. Using (10) and the induction hypothesis:

$$\begin{aligned} R_{m+1}(a) \quad &\leq \quad \left(1 - \frac{\lambda_a}{\Lambda}\right) R'_m(d) \\ &+ \sum_{\substack{i \in FC \\ i \geq d}} \left[\frac{\lambda^i_{a,f}}{\Lambda} + \sum_{d'=1}^{d} \sum_{b \in U_{k+i,d'}} \frac{\lambda_{a,b}}{\Lambda} R'_m(d')\right] \\ &+ \sum_{\substack{i \in FC \\ i < d}} \sum_{d'=d-i}^{d} \sum_{b \in U_{k+i,d'}} \frac{\lambda_{a,b}}{\Lambda} R'_m(d')\,. \end{aligned}$$

Taking into account that $R'_m(d') \leq 1$, $\sum_{b \in U_{k+i,d'}} \lambda_{a,b} = \lambda_{a,U_{k+i,d'}}$, and using Lemma 1:

$$\begin{aligned} R_{m+1}(a) \;&\leq\; \left(1 - \frac{\lambda_a}{\Lambda}\right) R'_m(d) \\ &+ \sum_{\substack{i \in FC \\ i \geq d}} \frac{\lambda^i_{a,f} + \sum_{d'=1}^{d} \lambda_{a,U_{k+i,d'}}}{\Lambda} \\ &+ \sum_{\substack{i \in FC \\ i < d}} R'_m(d-i) \sum_{d'=d-i}^{d} \frac{\lambda_{a,U_{k+i,d'}}}{\Lambda}\,. \quad (11) \end{aligned}$$

Let U^k be the subset of U including the states with k failed components, (11) can be written as:

$$\begin{aligned} R_{m+1}(a) \quad &\leq \quad \left(1 - \frac{\lambda_a}{\Lambda}\right) R'_m(d) + \sum_{\substack{i \in FC \\ i \geq d}} \frac{\lambda^i_{a,f} + \lambda_{a,U^{k+i}}}{\Lambda} \\ &+ \sum_{\substack{i \in FC \\ i < d}} R'_m(d-i) \, \frac{\lambda_{a,U^{k+i}}}{\Lambda}\,. \qquad (12) \end{aligned}$$

Taking into account that $\lambda_a = \lambda_{a,f} + \sum_{i \in FC} \lambda_{a,U^{k+i}}$, we have:

$$\frac{\lambda_a}{\Lambda} = \sum_{\substack{i \in FC \\ i \geq d}} \frac{\lambda^i_{a,f} + \lambda_{a,U^{k+i}}}{\Lambda} + \sum_{\substack{i \in FC \\ i < d}} \frac{\lambda_{a,U^{k+i}}}{\Lambda}\,. \qquad (13)$$

Combining (12) and (13):

$$\begin{aligned} R_{m+1}(a) \quad &\leq \quad R'_m(d) + \sum_{\substack{i \in FC \\ i \geq d}} \left[1 - R'_m(d)\right] \frac{\lambda^i_{a,f} + \lambda_{a,U^{k+i}}}{\Lambda} \\ &+ \sum_{\substack{i \in FC \\ i < d}} \left[R'_m(d-i) - R'_m(d)\right] \frac{\lambda_{a,U^{k+i}}}{\Lambda}\,. \end{aligned}$$

Noting that, for $i \geq d$, $\lambda^i_{a,f} + \lambda_{a,U^{k+i}} \leq f_i$ and that, for $i < d$, $\lambda_{a,U^{k+i}} \leq f_i$, and using (6) and (8):

$$\begin{aligned} R_{m+1}(a) \quad &\leq \quad R'_m(d) + \sum_{\substack{i \in FC \\ i \geq d}} \left[1 - R'_m(d)\right] \frac{f_i}{\Lambda} \\ &+ \sum_{\substack{i \in FC \\ i < d}} \left[R'_m(d-i) - R'_m(d)\right] \frac{f_i}{\Lambda} \\ &= \quad \left(1 - \frac{1}{\Lambda} \sum_{i \in FC} f_i\right) R'_m(d) \\ &+ \sum_{i \in FC} \frac{f_i}{\Lambda} R'_m(\max\{0, d-i\}) \\ &= \quad R'_{m+1}(d). \;\square \end{aligned}$$

Using Proposition 1 it is possible to show:

Proposition 2 $P[Y_n = f] \leq P[Y'_n \in \{u_0, f\}], n > 0\,.$

Proof Y can enter f through U or directly from G. Taking into account that f is absorbing and conditioning the entry of Y in f through U to the step in which Y leaves G and the entry state in U, we have:

$$\begin{aligned} P[Y_n = f] \;&=\; \sum_{m=1}^{n-1} \sum_{d=1}^{L} \sum_{a \in U_d} P[Y_{m-1} \in G \wedge Y_m = a] \\ &\qquad\qquad P[Y_n = f | Y_m = a] \\ &+ \sum_{m=1}^{n} P[Y_{m-1} \in G \wedge Y_m = f] \\ &= \sum_{m=1}^{n-1} \sum_{d=1}^{L} \sum_{a \in U_d} P[Y_{m-1} \in G \wedge Y_m = a] R_{n-m}(a) \\ &+ \sum_{m=1}^{n} P[Y_{m-1} \in G \wedge Y_m = f]\,. \end{aligned}$$

Invoking Proposition 1 and using the relationships between Y and Y' we have:

$$\begin{aligned} &P[Y_n = f] \;\leq \\ &\leq \sum_{m=1}^{n-1} \sum_{d=1}^{L} \sum_{a \in U_d} P[Y_{m-1} \in G \wedge Y_m = a] R'_{n-m}(d) \\ &+ \sum_{m=1}^{n} P[Y_{m-1} \in G \wedge Y_m = f] \\ &= \sum_{m=1}^{n-1} \sum_{d=1}^{L} P[Y'_{m-1} \in G \wedge Y'_m = u_d] R'_{n-m}(d) \\ &+ \sum_{m=1}^{n} P[Y'_{m-1} \in G \wedge Y'_m = f] \\ &= \sum_{m=1}^{n-1} \sum_{d=1}^{L} P[Y'_{m-1} \in G \wedge Y'_m = u_d] \end{aligned}$$

$$P[Y'_n = u_o | Y'_m = u_d] + \sum_{m=1}^{n} P[Y'_{m-1} \in G \wedge Y'_m = f] = P[Y'_n = u_0] + P[Y'_n = f] = P[Y'_n \in \{u_0, f\}]. \ \square$$

Finally:

Theorem 1 $ur(t) \leq [ur(t)]_{ub}$.

Proof Since Y is the result of randomizing X, using (4), taking into account that $P[Y_0 = f] = P[X(0) = f] = 0$, we have:

$$ur(t) = P[X(t) = f] = \sum_{n=1}^{\infty} \frac{(\Lambda t)^n}{n!} e^{-\Lambda t} P[Y_n = f].$$

Invoking Proposition 2 and using (5), taking into account that $P[Y'_0 \in \{u_0, f\}] = P[X'(0) \in \{u_0, f\}] = 0$, we have (3):

$$\begin{aligned} ur(t) &\leq \sum_{n=1}^{\infty} \frac{(\Lambda t)^n}{n!} e^{-\Lambda t} P[Y'_n \in \{u_0, f\}] \\ &= P[X'(t) \in \{u_0, f\}] \ = \ [ur(t)]_{ub}. \ \square \end{aligned}$$

4. Computation of failure distances

In order to obtain the transition rates λ_{a,U_d}, $a \in G$ required by the bounding method, it is necessary to compute the failure distances from the successors out of G of the states in the frontier of G. Use of (1) can be expensive if the number of minimal cuts is large. In this section we review the algorithms described in [6] which typically are much less expensive when the number of minimal cuts is large.

We start by introducing the concept of *after minimal cut.* The after minimal cut associated to a minimal cut m and a failure event $e \in E$, $m \cap e \neq \emptyset$ is $m' = m - e$. Let AMC_e be the set of after minimal cuts associated to failure event e, i.e., $AMC_e = \{m' \mid m' = m - e, m \in MC, m \cap e \neq \emptyset\}$. Then, the failure distance from any state reached from a through a failure transition with failure event e, $ad(a, e)$, can be obtained as:

$$ad(a, e) = \min\{d(a), \min_{m \in AMC_e} |m - F(a)|\}. \qquad (14)$$

Thus, we can obtain $ad(a, e)$, $e \in E$ computing $d(a)$ by (1) and using (14). In this way the total number of minimal or after minimal cuts which are "touched" to compute $ad(a, e)$, $e \in E$ is $|MC| + \sum_{e \in E} |AMC_e|$, which is typically much smaller than the number of minimal cuts which would be touched ($|E||MC|$) if the failure distances from all the successor states were computed using (1). Further reduction in the number of minimal cut "touches" and the associated overhead can be obtained by examining only minimal cuts or after minimal cuts which may reduce a known upper bound for, respectively, $d(a)$ or $ad(a, e)$, $e \in E$. We assume that minimal cuts are indexed by their cardinality and selectors of up to a given cardinality R included in some minimal cut. The parameter R allows to control the degree of selection in the access to minimal cuts. Larger values of R yield smaller number of minimal cut "touches" but more potential selectors have to be tested. We have found $R = 2$ to be a good tradeoff in general. We assume the same indexing structure for the collection of after minimal cuts. We describe next two algorithms: the first one computes $d(a)$; the second one computes $ad(a, e)$, $e \in E$, assuming $d(a)$ known.

```
Algorithm Compute_d(F(a), L, d(a))
$d(a) = L$;
for (increasing minimal cut cardinality $c$ while
    $c < d(a) + |F(a)|$){
  $q = \min\{R, c - d(a) + 1\}$;
  for (each bag $p$ of cardinality $q$ included in $F(a)$)
    if ($p$ is a selector of some minimal cut of
        cardinality $c$)
      for (each minimal cut $m$ with $|m| = c$ and $p \subset m$)
        $d(a) = \min\{d(a), |m - F(a)|\}$;
}
```

Figure 3. Algorithm to compute failure distances.

The algorithm to compute $d(a)$ initializes the upper bound for $d(a)$, ub, to $L = \min_{m \in MC} |m|$. Since at most $|F(a)|$ components can be failed in any minimal cut we only need to consider the minimal cuts m with cardinality $|m|$ satisfying $|m| - |F(a)| < ub$, i.e., $|m| < ub + |F(a)|$. The minimal cuts to be considered can be further restricted considering that $|m - F(a)|$ cannot be $< ub$ unless m contains a selector $p \subset F(a)$ and $|m| - |p| < ub$, i.e., $|p| \geq |m| - ub + 1$. Thus, for each possible minimal cut cardinality c we can restrict our attention to the minimal cuts of cardinality c containing selectors $p \subset F(a)$ and $|p| = \min\{R, c - ub + 1\} = q$. Possible selectors $p \subset F(a)$ can be obtained by generating all bags of cardinality q included in $F(a)$. Then, if the selectors are kept in a hash table or a similarly efficient structure, it is possible to test whether each possible selector p is in fact a selector and, with the appropriate data structures, visit all minimal cuts of cardinality c including p. The discussion justifies the algorithm given in Figure 3.

Assuming $d(a)$ known, similar ideas can be used to reduce the number of after minimal cuts which have to be examined to obtain $ad(a, e)$, $e \in E$. To reduce the overhead associated to the control of the algorithm only an upper bound **adub** for all $ad(a, e)$, $e \in E$ is used. The after failure distances $ad(x, e)$ are initialized to $min\{d(a), L_e\}$, where $L_e = \min_{m \in AMC_e} |m|$. The upper bound **adub** can be initialized to the maximum of the initial after failure distances. $d(a)$ and L_e, $e \in E$ are passed to the algorithm. The algorithm is given in Figure 4.

These algorithms are used as follows. For each state a in the frontier of G, $d(a)$ is computed using *Compute_d*().

```
Algorithm $Compute\_all\_ad(F(a),\ d(a),\ L_e,\ ad(a,e))$
for (each $e \in E$) $ad(a,e) = \min\{d(a), L_e\}$;
$adub = \max_{e \in E}\{ad(a,e)\}$;
for (increasing after minimal cut cardinality $c$ while
      $c < adub + |F(a)|$){
  $q = \min\{R, c - adub + 1\}$;
  for (each bag $p$ of cardinality $q$ included in $F(a)$)
    if ($p$ is a selector of some after minimal cut of
        cardinality $c$)
      for (each after minimal cut $m$ with $|m| = c$ and
          $p \subset m$){
        Let $e$ be the failure event associated to $m$;
        $ad(a,e) = \min\{ad(a,e), |m - F(a)|\}$;
      }
}
```

Figure 4. Algorithm to compute after failure distances.

Then, the failure distances $ad(a,e)$, $e \in E$ are computed using *Compute_all_ad*(). Using these failure distances, it is easy to obtain the rates λ_{a,U_d} by simply adding the rates of the failure events e leading to states with failure distance d.

5. Analysis and comparison

In this section we analyze the behavior of the proposed bounding method using a complex example with dependencies which prevent the use of combinatoric and hierarchical solution methods, and compare the quality of the bounds obtained with the proposed method with the bounds obtained using the trivial method in which the upper bound assumes that the system fails when the model exits G. That bound can be expressed in terms of the transient regime of X' as:

$$[ur(t)]'_{ub} = P[X'(t) \in \{u_0, \cdots, u_L, f\}].$$

The results have been obtained using a prototype implementation of the method which has used the production rules based language available in METFAC [3] as interface for model specification. The transient regime of X' has been solved using the randomization method [8].

The example is a system made up of 38 components. The architecture of the system is shown in Figure 5. The system includes a cluster of redundant master units M1, M2 communicated with five clusters of redundant slave units Si.1, Si.2. Communication is done through two redundant busses to which the master and slave units are connected through dedicated interfaces. The system is operational if some fault-free master unit can communicate directly (i.e., through a bus and an interface) with at least a fault-free slave unit of each slave cluster. The active configuration of the system includes a master unit, all fault-free slave units which can communicate with the active master unit, and the busses and interfaces among these units and the active master unit. In configuring the system priority is given to master unit M1 over master unit M2; M2 is activated only if M1 is faulty or it is impossible to build up an operational configuration with M1 (for instance, because both interfaces associated to M1 are faulty).

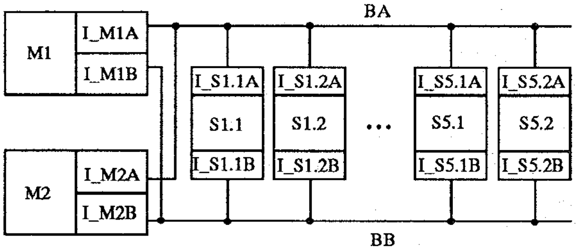

Figure 5. Architecture of the example.

Active master units, slave units, interfaces and busses fail with rates λ_M, λ_S, λ_I, and λ_B, respectively. Passive components fail with rates $\delta_M\lambda_M$, $\delta_S\lambda_S$, $\delta_I\lambda_I$, and $\delta_B\lambda_B$, respectively, being δ_M, δ_S, δ_I, and δ_B dormancy coefficients < 1. The fault of an active or passive interface is propagated to the bus to which the interface is connected with probability ν.

The conceptual framework assumed by the bounding method allows to model coverage failures by introducing "recovery" components which do not fail on their own and to which non covered failures of other components are propagated. For the example, two "recovery" components were introduced and the structure function was defined so that both components had to be unfailed for the system to be operational. In this way, the failure distances from the operational states are not affected by the presence of the "recovery" components and the performance of the bounding method (which increases with increasing failure distances) is not degradated. The coverage model of the example includes the parameters C_M, coverage to the failure of M1, C_S^H, C_B^H, C_I^H, and C_{IB}^H, coverages to the failures of, respectively, a slave unit, a bus, an interface whose failure is not propagated to the bus, and an interface whose failure is propagated to the bus, when the reconfiguration of the system does not involve the activation of M2, and C_S^L, C_B^L, C_I^L, and C_{IB}^L, homologous coverages when the reconfiguration involves the activation of M2.

For the example, $FC = \{1, 2, 3, 4\}$ and for the upper bounds f_i we can take:

$$\begin{aligned}
f_1 &= \max\{\lambda_M C_M, \lambda_M \delta_M\} + \lambda_M \\
&\quad + 10\max\{\lambda_S C_S^H, \lambda_S C_S^L, \lambda_S \delta_S\} \\
&\quad + 2\max\{\lambda_B C_B^H, \lambda_B C_B^L, \lambda_B \delta_B\} \\
&\quad + 24(1-\nu)\max\{\lambda_I C_I^H, \lambda_I C_I^L, \lambda_I \delta_I\}, \\
f_2 &= 24\nu\max\{\lambda_I C_{IB}^H, \lambda_I C_{IB}^L\}, \\
f_3 &= \lambda_M(1-C_M) + 10\max\{\lambda_S(1-C_S^H), \lambda_S(1-C_S^L)\} \\
&\quad +2\max\{\lambda_B(1-C_B^H), \lambda_B(1-C_B^L)\} \\
&\quad +24(1-\nu)\max\{\lambda_I(1-C_I^H), \lambda_I(1-C_I^L)\},
\end{aligned}$$

Table 1. Relative bands for several mission times obtained with the proposed method (top) and the trivial method (down).

time	K (states)		
	1 (39)	2 (735)	3 (8,871)
1 month	0.007761	3.213×10^{-5}	6.665×10^{-8}
	1.887	1134×10^{-5}	3118×10^{-8}
2 months	0.01637	1.295×10^{-4}	5.300×10^{-7}
	2.063	230.7×10^{-4}	1245×10^{-7}
6 months	0.05846	1.197×10^{-3}	1.400×10^{-5}
	2.711	73.45×10^{-3}	111.1×10^{-5}
1 year	0.1408	4.930×10^{-3}	1.084×10^{-4}
	3.548	157.2×10^{-3}	43.80×10^{-4}
2 years	0.3545	0.02032	8.114×10^{-4}
	4.860	0.3424	169.2×10^{-4}
5 years	1.187	0.1249	0.01043
	7.202	0.9228	0.09300
10 years	2.724	0.4339	0.06110
	8.987	1.740	0.2926

$$f_4 = 24\nu \max\{\lambda_I(1 - C_{IB}^H), \lambda_I(1 - C_{IB}^L)\}.$$

The numerical results have been obtained for $\lambda_M = 1.2 \times 10^{-6}\,\mathrm{h}^{-1}$, $\lambda_S = 6 \times 10^{-7}\,\mathrm{h}^{-1}$, $\lambda_B = 6 \times 10^{-8}\,\mathrm{h}^{-1}$, $\lambda_I = 1.2 \times 10^{-7}\,\mathrm{h}^{-1}$, $\delta_M = \delta_S = \delta_B = \delta_I = 0.2$, $\nu = 0.1$, $C_M = 0.95$, $C_S^H = C_B^H = C_I^H = 0.99$, $C_S^L = C_B^L = C_I^L = 0.95$, $C_{IB}^H = 0.97$ and $C_{IB}^L = 0.93$. The corresponding values of the bounds f_i are $f_1 = 1.096488 \times 10^{-5}\,\mathrm{h}^{-1}$, $f_2 = 2.7936 \times 10^{-7}\,\mathrm{h}^{-1}$, $f_3 = 4.956 \times 10^{-7}\,\mathrm{h}^{-1}$ and $f_4 = 2.016 \times 10^{-8}\,\mathrm{h}^{-1}$. As initial state we have assumed the state in which no component is failed. As subset of generated states G we have taken the set including all operational states with up to K failed components, with $K = 1, 2, 3$. The cardinality $|G|$ of the generated state space was 39 for $K = 1$, 735 for $K = 2$, and 8,871 for $K = 3$. The structure function of the system has 512 minimal cuts: 8 of cardinality 2, 48 of cardinality 3, 96 of cardinality 4 and 360 of cardinality 6. For the computation of the failure distances we have used the algorithms described in Section 4, resulting in an overhead in time due to the computation of the failure distances of about 10 %. However, the part of that overhead which depends on the number of minimal cuts was only 0.3 % and, thus, we feel that systems with of the order of tens of thousands of states could be dealt without significant overhead.

Figure 6 shows the unreliability bounds as a function of the time t for the three values of K considered. It can be shown that very tight bounds are obtained with a reasonable number of states (8,871 for $K = 3$) even for large times. The tightness of the bounds increases for decreasing times. Table 1 shows, for several mission times, the relative band obtained by the proposed method, $([ur(t)]_{ub} - [ur(t)]_{lb})/[ur(t)]_{lb}$, and the relative band obtained with the trivial method, $([ur(t)]'_{ub} - [ur(t)]_{lb})/[ur(t)]_{lb}$. The proposed bounding method outperforms significantly the trivial method, specially for short and medium mission times.

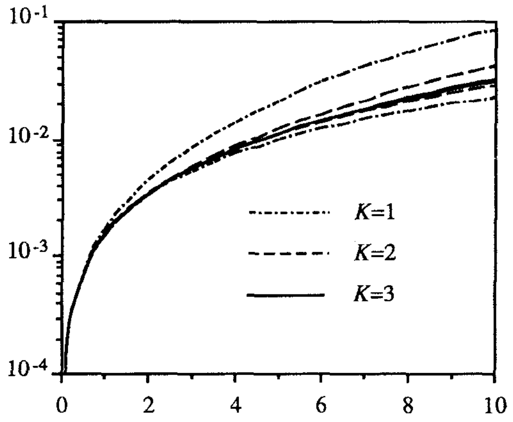

Figure 6. Unreliability bounds obtained with the proposed method as a function of the time in years for $K = 1, 2, 3$.

6. Conclusions and future work

The bounding method which has been developed gives bounds significantly tighter than the bounds obtained by the trivial method. Obviously, the quality of the bounds increases with the size of G. It also decreases for increasing mission times. In the future we want to investigate the possibility of introducing in an efficient way more sophisticated heuristics for the selection of the subset G of generated states such as it has been recently shown for steady-state availability bounding methods [6], [18]. The goal would be to select G so that the required $|G|$ to achieve a given accuracy in the bounds were minimized. We are also investigating the possibility of refining the method in the sense of using partitions of the non-generated state space U based on the parameters k (number of failed components) and d (failure distance), as it has been done for the steady-state availability [4].

References

[1] R.E. Barlow and F. Proschan, *Statistical Theory of Reliability and Life Testing. Probability Models*, McArdle Press, Silver Spring, 1981.

[2] M. A. Boyd, M. Veeraraghavan, J. B. Dugan, and K. S. Trivedi, "An Approach to Solving large Reliability Models," in *Proc. of the AIAA/IEEE 8th Conf. on Embedded Digital Avionics*, 1988, pp. 243–250.

[3] J.A. Carrasco and J. Figueras, "METFAC: Design and Implementation of a Software Tool for Modeling and Evaluation of Complex Fault-Tolerant Computing System", in *Proc. 16th IEEE Int. Symp. on Fault-Tolerant Computing FTCS-16*, 1986, pp. 424–429.

[4] J. A. Carrasco, "Improving Availability Bounds using the Failure Distance Concept," in *Dependable Computing and Fault-Tolerant Systems*, vol. 5, Springer-Verlag, 1995, pp. 479–497.

[5] J. A. Carrasco, A. Calderón and J. Escribá, "Two New Algorithms to Compute Steady-state Bounds for Markov Models with Slow Forward and Fast Backward Transitions," in *Proc. 4th IEEE Int. Workshop on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS'96)*, February 1996. pp. 89–96.

[6] J.A. Carrasco, J. Escribá and A. Calderón, "Efficient Exploration of Availability Models Guided by Failure distances", *Performance Evaluation Review*, vol. 24, no. 1, May 1996.

[7] J. B. Dugan, "Fault trees and imperfect coverage," *IEEE Trans. on Reliability*, vol. 38, no. 2, June 1989, pp. 177–185.

[8] D. Gross and D. Miller, "The randomization technique as a modeling tool and solution procedure for transient Markov processes", *Operations Research*, vol. 38, no. 2, 1984, pp 334–361

[9] W.S. Lee, D.L. Grosh, F.A. Tillman, and C.H. Lie, " Fault Tree Analysis, Methods and Applications –A Review," *IEEE Trans. on Reliability*, vol. R-34, no. 3, August 1985, pp. 194–203.

[10] D. Lee, J. Abraham, D. Rennels, and G. Gilley, "A Numerical Technique for the Hierarchical Evaluation of Large, Closed Fault-Tolerant Systems," in *Dependable Computing for Critical Applications*, Springer-Verlag, 1992, pp. 95–114.

[11] J. C. S. Lui and R. R. Muntz, "Evaluating Bounds on Steady-State Availability of Repairable Systems from Markov Models," in *Numerical Solution of Markov Chains*, Marcel Dekker, New York, 1991, pp. 435–454.

[12] J. C. S. Lui and R. R. Muntz. "Computing Bounds on Steady-State Availability of Repairable Computer Systems," *Journal of the ACM*, vol. 41, no. 4, July 1994, pp. 676–707.

[13] R. R. Muntz, E. de Souza e Silva and A. Goyal, "Bounding Availability of Repairable Computer Systems," *IEEE Trans. on Computers*, vol. 38, no. 12, December 1989, pp. 1714–1723.

[14] J. L. Patterson, *Petri Net Theory and the Modeling of Systems*, Prentice-Hall, 1981.

[15] D.M. Rasmuson and N.H. Marshall, " FATRAM-A Core Efficient Cut-Set Algorithm," *IEEE Trans. on Reliability*, vol. R-27, no. 4, October 1978, pp. 250–253.

[16] S.M. Ross, *Stochastic Processes*, John Wiley & Sons, New York, 1983.

[17] R. A. Sahner and K. S. Trivedi, "Reliability Modeling Using SHARPE," *IEEE Trans. on Reliability*, vol. R-36, no. 2, June 1987, pp. 186–193.

[18] E. de Souza e Silva and P. M. Ochoa, "State Space Exploration in Markov Models," *Performance Evaluation Review*, vol. 20, no. 1, June 1992, pp. 152–166.