NASA-CR-172,340

NASA Contractor Report 172340

UPPER AND LOWER BOUNDS FOR SEMI-MARK
RELIABILITY MODELS OF RECONFIGURABLE SYSTEMS

Allan L. White

KENTRON INTERNATIONAL, INC.
Kentron Technical Center
Hampton, Virginia 23666

Contract NAS1-16000
April 1984

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23665

ABSTRACT

This paper determines the information required about system recovery to compute the reliability of a class of reconfigurable systems. Upper and lower reliability bounds are derived for these systems. The class consists of those systems satisfying five assumptions: the individual components fail independently at a low constant rate, fault occurrence and system reconfiguration are independent processes, the reliability model is semi-Markov, the recovery functions which describe system reconfiguration have small means and variances, and the system is well designed. The derivation proceeds by considering paths through the reliability model from the initial, fault-free, state to the absorbing, system-failure, states. Since the probability of system failure is the sum of the probabilities of traversing these fatal paths, it suffices to obtain bounds on traversing a path by a given time. The bounds involve the component failure rates and the means and variances of the recovery functions. They are easy to compute, and illustrative examples are included.

1. INTRODUCTION

This paper determines the information needed about fault recovery to compute the reliability of a class of reconfigurable systems.

Reconfigurable systems can identify a faulty component, remove it from the working group, and replace it with a spare if available. Typically, building the system is only justified if the reliability requirement is high--often high enough that natural life testing is impossible, and system reliability must be computed from a mathematical model that includes descriptions of component failure and system recovery. Hence the modeling problem consists of a complex system whose reliability requires careful computation. This combination suggests delicate experiments with hard statistical analyses to get a description of system fault recovery, followed by difficult calculations to get an estimate of system reliability. Even more important, it may not be clear what needs to be observed in the experiments and included in the calculations.

Given certain assumptions about component and system behavior, this paper derives upper and lower bounds for the probability of system failure in terms of system operating time, component fault rates, and the means and variances of system fault recovery times. The assumptions used are common (see references [1], [2], and [3]), and their plausibility is discussed below. However, their plausibility and common use do not mean the assumptions are valid, and more investigation is required before the derived bounds can be confidently applied to a reconfigurable system.

The derivation of the bounds requires five assumptions: 1) components fail independently at a low constant rate; 2) component failure and system recovery are independent processes; 3) the system quickly recovers from all faults; 4) fault recovery depends only on time elapsed since fault occurrence; 5) the system is well designed. The first assumption is appropriate for high quality components operating for a short period of time in a benign environment, but may not be applicable otherwise. The second assumption is reasonable if failure is an instantaneous event--a component's imminent failure does not affect its current performance. The third assumption on quick recovery describes a desirable property for reconfigurable systems since these systems fail if too many faults accumulate in the working group of components. If recovery is quick then the reconfiguration process has a small mean. If recovery is quick for all faults then the reconfiguration process has a small deviation from the mean, measured by the variance. Hence the third assumption has a mathematical version: 3') any system fault recovery has a small mean and variance. The fourth assumption, together with the first on constant rates, says the reliability model is semi-Markov. The major objection against a semi-Markov model is that fault recovery may depend on what the system is doing at the time of fault occurrence. A later section considers time dependent recovery and shows the same upper bound is still valid. Because the mathematics is more complicated for the time dependent case no attempt is made to derive a lower bound. The fifth assumption about the system being well designed means the system only fails when overwhelmed by faulty components. Conceivably, a system can fail to operate properly even if all the components are fault free.

The next section presents an arbitrary path from the initial state to a failure state in a semi-Markov reliability model and derives upper and lower bounds for traversing the path by a given time. The probability of system failure is the probability of traversing all such fatal paths which means an upper bound for system failure is the sum of the upper bounds for all the paths, while a lower bound for system failure is the sum of the lower bounds for all the paths. Simple addition of the probabilities suffices because traversing one path is a disjoint event compared to traversing another path. The bounds established in the next section are partly numerical and partly algebraic. The numerical part consists of solving the simultaneous linear differential equations associated with a constant rate Markov model where all the rates are fairly close--an easy exercise for a computer numerical package. The algebraic part consists of expressions involving component fault rates and the means and variances of system recovery times. Section four derives purely algebraic bounds and discusses their accuracy. The algebraic upper bound is particularly easy to use, and it shows the influence of fault rates and recovery times on system reliability. Each of these sections is followed by a section containing an example. Section six shows that the same upper bound is still valid even if system fault recovery is time dependent.

Besides determining the information required about system recovery, the material below offers some other benefits. The upper and lower bounds are derived rigorously from the assumptions placing the resulting calculations on firm foundations. The bounds are proved for arbitrary recovery distributions with finite means and variances which eliminates concern over the applicability of a parameteric model. The fault injection experiments to study system recovery need only record the time between fault injection and system recovery with no information required about the intermediate steps. Since different system architectures produce reliability models with different paths to failure, the calculations based on paths to failure reflects the influence of architecture on reliability. (For examples, see references [6] and [7].) The bounds are easy to compute, and they use familiar mathematics and statistics: differential equations, means, and variances. The algebraic upper bound used as an approximation formula allows computation from a mere inspection of the reliability model and reveals the influence of the various parameters on system reliability. The major disadvantage of the approach below is that it may not be able to handle transient and intermittent faults.

Besides the references mentioned before, references [4] and [5] contain the necessary probability theory, while [8] and [9] present other approaches to the reliability of reconfigurable systems.

2. THE APPROXIMATION THEOREM

Upper and lower reliability bounds are obtained by considering the paths in the reliability model that begin at the initial state and proceed to an absorbing state representing system failure. A general path, rearranged for notational convenience, is displayed in figure 1. Any transition on a path is by means of a fault occurrence competing with other fault occurrences, or by means of system recovery competing with fault occurrences, or by means of a fault occurrence competing with system recovery and other fault occurrences. In figure 1, the fault occurrence transitions are labeled by the component failure rates, and the system recovery transitions are labeled by the generalized densities of the recovery distributions. Figure 2 shows the first part of the path, consisting of just fault occurrence transitions with the absorbing state E replacing the non-absorbing state B_1. As the absorbing state of a constant rate Markov process, the probability of being in state E by a given time is easy to compute.

In the first third of figure 1, the λ's are the rates of component failures that stay on the path, while the γ's are those that lead off the path. In the second third, the dF's are the generalized densities of recovery transitions that stay on the path, while the ε's are the rates of component failures that lead off the path. In the final third, the α's are the rates of component failures that stay on the path, while the dG's and β's represent recovery transitions and component failures that lead off the path.

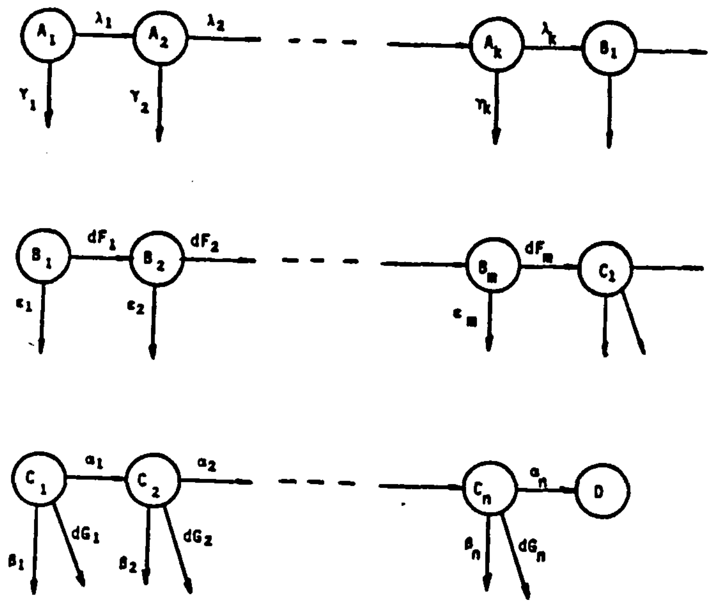

Figure 1: A Path in a Semi-Markov Reliability Model

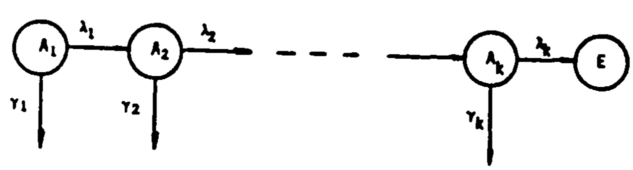

Figure 2: The Constant Rate Markov Part of the Path

Let $D(T)$ and $E(T)$ be the probabilities of being in states D and E by time T. Suppose the distribution F_i has mean μ_i and variance σ_i^2, and G_j has mean η_j and variance τ_j^2. Let

$$\Delta = \mu_1^{1/2} + \ldots + \mu_m^{1/2} + \eta_1^{1/2} + \ldots + \eta_n^{1/2}$$

and assume $\Delta < T$.

<u>Theorem</u> With the notation as above,

$$E(T) \left\{ \prod_{j=1}^{n} \alpha_j \eta_j \right\}$$

$$\geq D(T)$$

$$\geq E(T-\Delta) \left\{ \prod_{i=1}^{m} \left[1 - \varepsilon_i \mu_i - \frac{(\sigma_i^2 + \mu_i^2)}{\mu_i}\right] \prod_{j=1}^{n} \alpha_j \left[\eta_j - \frac{(\alpha_j + \beta_j)(\tau_j^2 + \eta_j^2)}{2} - \frac{(\tau_j^2 + \eta_j^2)}{\eta_j^{1/2}}\right] \right\}.$$

<u>Proposition</u> Suppose H is a distribution function, $H(x) = 0$ for $x < 0$, and H has finite mean μ and variance σ^2. Then, for $\varepsilon, \alpha, \beta \geq 0$,

(i) $$\int_0^\infty \alpha e^{-(\alpha+\beta)x}[1-H(x)]dx \leq \alpha \mu$$

(ii) $$\int_0^\infty e^{-\varepsilon x} dH(x) \leq 1$$

(iii) $$\int_0^{\mu^{1/2}} e^{-\varepsilon x} dH(x) \geq 1 - \varepsilon \mu - \frac{\sigma^2 + \mu^2}{\mu}$$

(iv) $$\int_0^{\mu^{1/2}} \alpha e^{-(\alpha+\beta)x}[1-H(x)]dx \geq \alpha \left[\mu - \frac{(\alpha+\beta)(\sigma^2+\mu^2)}{2} - \frac{\sigma^2 + \mu^2}{\mu^{1/2}}\right]$$

Proof of the Proposition

The derivation uses the standard results

$$1 - x \leq e^{-x} \leq 1 \qquad \text{for } x \geq 0$$

$$\int_0^\infty [1 - H(x)]\, dx = \mu$$

$$\int_0^\infty x[1 - H(x)]\, dx = \frac{\sigma^2 + \mu^2}{2}$$

$$1 - H(c) = \int_c^\infty dH(x) \leq \frac{\sigma^2 + \mu^2}{c^2} \qquad \text{for } c > 0.$$

The proof of (iii) is

$$\int_0^{\mu^{1/2}} e^{-\varepsilon x}\, dH(x) = \int_0^\infty e^{-\varepsilon x}\, dH(x) - \int_{\mu^{1/2}}^\infty e^{-\varepsilon x}\, dH(x)$$

$$\geq \int_0^\infty (1 - \varepsilon x)\, dH(x) - \int_{\mu^{1/2}}^\infty dH(x)$$

$$\geq 1 - \varepsilon\, \mu - \frac{\sigma^2+\mu^2}{\mu}.$$

The proof of (iv) is

$$\int_0^{\mu^{1/2}} \alpha\, e^{-(\alpha+\beta)x}\,[1-H(x)]\,dx = \int_0^{\infty} \alpha\, e^{-(\alpha+\beta)x}[1-H(x)]\,dx$$

$$-\int_{\mu^{1/2}}^{\infty} \alpha\, e^{-(\alpha+\beta)x}[1-H(x)]\,dx$$

$$\geq \alpha \int_0^{\infty} [1-(\alpha+\beta)x]\,[1-H(x)]\,dx$$

$$-\alpha \int_{\mu^{1/2}}^{\infty} \frac{\sigma^2+\mu^2}{x^2}\,dx$$

$$\geq \alpha\left[\mu - \frac{(\alpha+\beta)(\sigma^2+\mu^2)}{2} - \frac{\sigma^2+\mu^2}{\mu^{1/2}}\right].$$

Proof of the Theorem

Let $q(t)$ be the density function of $E(t)$. Since the path in figure 1 is from a semi-Markov process.

$$D(T) = \int_0^T \int_0^{T-t} \cdots \int_0^{T-t-x_1-\cdots-x_{m-1}} \int_0^{T-t-x_1-\cdots-x_m} \cdots \int_0^{T-t-x_1-\cdots-y_{n-1}}$$

$$q(t)$$

$$e^{-\varepsilon_1 x_1} \cdots e^{-\varepsilon_m x_m}$$

$$\alpha_1\, e^{-(\alpha_1+\beta_1)y_1}[1-G_1(y_1)] \cdots \alpha_n e^{-(\alpha_n+\beta_n)y_n}[1-G_n(y_n)]$$

$$dy_n \cdots dy_1\, dF_m(x_m) \cdots dF_1(x_1)\, dt.$$

Working with just the limits of integration

$$D(T) \le \int_0^T \int_0^\infty \cdots \int_0^\infty \int_0^\infty \cdots \int_0^\infty$$

and

$$D(T) \ge \int_0^{T-\Delta} \int_0^{\mu_1^{1/2}} \cdots \int_0^{\mu_m^{1/2}} \int_0^{\eta_1^{1/2}} \cdots \int_0^{\eta_n^{1/2}} .$$

To complete the proof write the multiple integrals as iterated integrals, and apply the inequalities in the proposition to the integrands.

3. EXAMPLE

One of the simplest reconfigurable systems consists of a working triad plus a spare. The majority voting lets the triad detect a faulty member and maintain process control while replacing it with the spare. Figure 3 displays the first two failure states of the system. The mnemonics are I for the initial state, Q for a faulty component in the triad, R for system recovery, and D for system failure because of two faulty components in the triad. The transitions are labeled with either component failure rates or generalized densities of recovery functions. The vertical transitions refer to failure of the spare.

There is one path to state D_1 and one path to state D_2. The constant rate Markov part of these paths are given in figure 4 with E_1 and E_2 as the absorbing states.

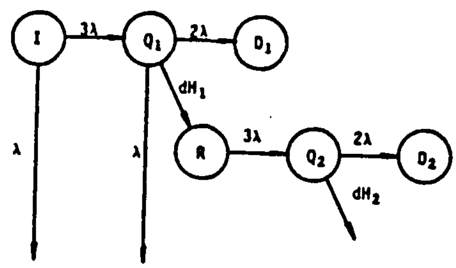

Figure 3: The First Failure States of a Triad Plus a Spare

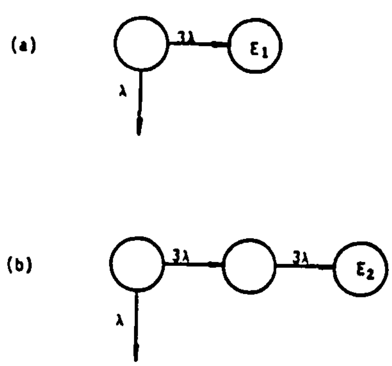

Figure 4: (a) The Constant Rate Part of the First Path

(b) The Constant Rate Part of the Second Path

Let H_i have mean μ_i and variance σ_i^2. The inequalities are

$$E_1(T)\{2\lambda\mu_1\}$$

$$\geq D_1(T)$$

$$\geq E_1(T - \mu_1^{1/2})\{2\lambda\left(\mu_1 - \frac{3\lambda(\sigma_1^2 + \mu_1^2)}{2} - \frac{\sigma_1^2 + \mu_1^2}{\mu_1^{1/2}}\right)\}$$

and

$$E_2(T)\{2\lambda\mu_2\}$$

$$\geq D_2(T)$$

$$\geq E_2(T - \mu_1^{1/2} - \mu_2^{1/2})$$

$$X\{2\lambda\left[1 - 3\lambda\mu_1 - \frac{\sigma_1^2 + \mu_1^2}{\mu_1}\right]\left[\mu_2 - \lambda(\sigma_2^2 + \mu_2^2) - \frac{(\sigma_2^2 + \mu_2^2)}{\mu_2^{1/2}}\right]\}$$

For a numerical comparison suppose H_1 represents a fixed time recovery that takes one second, and suppose H_2 is the uniform distribution from zero to one second. In terms of hours the means and variances are

$$\mu_1 = 2.78 \times 10^{-4} \qquad \sigma_1^2 = 0$$
$$\mu_2 = 1.39 \times 10^{-4} \qquad \sigma_2^2 = 6.43 \times 10^{-9}$$

If the component fault rate and operating time are

$$\lambda = 5 \times 10^{-4} \text{ per hour}$$
$$T = 1 \text{ hour}$$

then the inequalities are

$$4.16 \times 10^{-10} \geq D_1(1) \geq 4.02 \times 10^{-10}$$
$$1.56 \times 10^{-13} \geq D_2(1) \geq 1.45 \times 10^{-13}.$$

4. ALGEBRAIC BOUNDS

The upper and lower bounds derived in section two become completely algebraic when algebraic bounds are provided for E(S), the probability of traversing the path in figure 2 by time S. Jumping ahead to the next theorem and using the notation in figure 2, these bounds are

$$\frac{\lambda_1 \ldots \lambda_k S^k}{k!} \geq E(S) \geq \frac{\lambda_1 \ldots \lambda_k S^k}{k!} \left[1 - \frac{S(\lambda_1 + \gamma_1 + \ldots + \lambda_k + \gamma_k)}{k+1}\right]$$

Letting

$$\text{Error} = \frac{\text{Upper Bound - Lower Bound}}{\text{Upper Bound}} = \frac{S\,(\lambda_1 + \gamma_1 + \ldots + \lambda_k + \gamma_k)}{k+1}$$

it can be seen that the algebraic bounds for E(S) are accurate when the product of the operating time and the sum of the fault rates is small.

<u>Theorem</u> With the notation in figure 2,

$$\frac{\lambda_1 \ldots \lambda_k S^k}{k!} \geq E(S) \geq \frac{\lambda_1 \ldots \lambda_k S^k}{k!} \left[1 - \frac{S(\lambda_1 + \gamma_1 + \ldots + \lambda_k + \gamma_k)}{k+1}\right]$$

Proof

The upper bound is the easier.

$$E(S) = \int_0^S \ldots \int_0^{S-x_1-\ldots-x_{k-1}} \lambda_1 \; e^{-(\lambda_1+\gamma_1)x_1} \ldots \lambda_k e^{-(\lambda_k+\gamma_k)x_k} dx_k \ldots \; dx_1$$

$$\leq \lambda_1 \ldots \lambda_k \quad \int_0^S \ldots \int_0^{S-x_1-\ldots-x_{k-1}} dx_k \ldots dx_1$$

$$= \frac{\lambda_1 \ldots \lambda_k \; S^k}{k!} .$$

For the lower bound, begin with k = 1.

$$E_1(S) = \frac{\lambda_1}{\lambda_1 + \gamma_1}(1 - e^{-(\lambda_1 + \gamma_1)S})$$

$$\geq \frac{\lambda_1}{\lambda_1 + \gamma_1}(1 - 1 + (\lambda_1 + \gamma_1)S - \frac{(\lambda_1 + \gamma_1)^2 S}{2})$$

$$= \frac{\lambda_1 S}{1!}\left[1 - \frac{S(\lambda_1 + \gamma_1)}{2}\right]$$

Assume the lower bound is true for k = n.

$$E_{n+1}(S) = \int_0^S \lambda_1 e^{-(\lambda_1+\gamma_1)x_1} \int_0^{S-x_1} \cdots \int^{S-x_1-\cdots-x_{n+1}}$$

$$\lambda_2 e^{-(\lambda_2+\gamma_2)x_2} \cdots \lambda_{n+1} e^{-(\lambda_{n+1} + \gamma_{n+1})x_{n+1}}$$

$$dx_{n+1} \cdots dx_2\, dx_1$$

$$\geq \int_0^S \lambda_1 \frac{\lambda_2 \cdots \lambda_{n+1}(S-x_1)^n}{n!}\left[1 - \frac{(S-x_1)(\lambda_2+\gamma_2 + \cdots + \lambda_{n+1}\gamma_{n+1})}{n!}\right] dx_1$$

$$- \int_0^S \lambda_1 (\lambda_1 + \gamma_1)x_1 \frac{\lambda_2 \cdots \lambda_{n+1} (S - x_1)^n}{n!} dx_1$$

$$= \frac{\lambda_1 \lambda_2 \cdots \lambda_{n+1} S^{n+1}}{(n+1)!}$$

$$- \frac{\lambda_1 \lambda_2 \cdots \lambda_{n+1} (\lambda_2 + \gamma_2 + \cdots + \lambda_{n+1} + \gamma_{n+1}) S^{n+2}}{(n+2)!}$$

$$- \frac{\lambda_1 \lambda_2 \cdots \lambda_{n+1} (\lambda_1 + \gamma_1) S^{n+2}}{n!\,(n+1)\,(n+2)}$$

$$= \frac{\lambda_1 \cdots \lambda_{n+1} S^{n+1}}{(n+1)!}\left[1 - \frac{S(\lambda_1 + \gamma_1 + \cdots + \lambda_{n+1} + \gamma_{n+1})}{n+2}\right].$$

The theorem is proved.

5. ALGEBRAIC EXAMPLE

This section illustrates using the algebraic upper bound as an approximation formula. Consider the first two failure states for a triad plus a spare depicted in figure 3. The algebraic upper bounds are

$$D_1(T) \approx 6\ \lambda^2\ T\ \mu_1$$

$$D_2(T) \approx 9\ \lambda^3\ T^2 \mu_2$$

where λ is the component fault rate, T is the operating time, and μ_i is the mean of the ith system recovery. The first failure is linear in operating time, linear in average recovery time, and quadratic in component fault rate. The ratio

$$\frac{D_2(T)}{D_1(T)} = \frac{3\ \lambda\ T\ \mu_2}{2\ \mu_1}$$

says that if μ_2 is approximately equal to μ_1 then D_2 is smaller than D_1 by a factor of about λT. For common values of λ and T, D_2 is several orders of magnitude smaller than D_1.

The technique above can be applied to a complete reliability model to identify the dominant failure modes and the important parameters.

6. TIME DEPENDENT RECOVERY

This section shows that the upper bound established for semi-Markov models in section two is still an upper bound when system fault recovery is time dependent. The algebraic upper bound derived in section four also remains valid. All the assumptions remain the same except that fault recovery is time and path dependent.

Consider state j on a path. Let $F(t_1,\ldots,t_{j-1})$ be the probability that the holding time in state i is less than or equal to t_i for $1 \le i \le j - 1$. Let $H[t_1,\ldots,t_{j-1}](t_j)$ be the distribution function for fault recovery in state j given the holding time in state i is t_i for $1 \le i \le j - 1$. The item of interest is the conditional mean

$$\mu_j = \frac{\int_0^T \left[\int_0^\infty t_j \, d\, H[t_1,\ldots,t_{j-1}](t_j)\right] d\, F(t_1,\ldots,t_{j-1})}{\int_0^T d\, F(t_1,\ldots,t_{j-1})}$$

which is the average recovery time for state j given the system reaches state j on the path being considered by time T. Note that recovery time in state j can depend not only on the time of entry into state j, which is $t_1 + \ldots + t_{j-1}$, but also on the intermediate states and the holding time in each of the intermediate states.

The demonstration that the same upper bound remains valid proceeds inductively by removing expressions containing recovery distributions from the integral giving the probability of traversing a path by time T. The expression containing a recovery distribution is replaced by a factor of 1 if the transition is a recovery competing with component failures. It is replaced by a factor of $\alpha_j \mu_j$ if the transition is a component failure with rate α_j competing with other component failures and with a recovery that has conditional mean μ_j. The general case in the inductive step where the transition on the path at state j is a recovery is described by the iterated integral

$$\int_0^T d\,F\,(t_1,\ldots,t_{j-1})$$

$$\int_0^{T-t_1-\ldots-t_{j-1}} e^{-\varepsilon_j t_j}\, d\,H\,[t_1,\ldots,t_{j-1}](t_j)$$

$$\int_0^{T-t_1-\ldots-t_j} d\,G\,(t_{j+1})$$

where F and H are as described above and G is a composition of constant failure rate transitions competing with other constant failure rate transitions. As a distribution representing the sum of sojourn times associated with component failures, G is time independent. At this point in the induction, the transitions involving a recovery that have occurred after state j have been replaced by their upper bounds. Clearly the last expression is less than or equal to

$$\int_0^T d\,F\,(t_1,\ldots,t_{j-1}) \int_0^{T-t_1-\ldots-t_{j-1}} d\,G(t_j).$$

Consider the general case in the inductive step where the transition at state j that is on the path is a component failure with rate α_j. It competes with a recovery, dH, and other component failures, rate β_j. The iterated integral is

$$\int_0^T d\,F\,(t_1,\ldots,t_{j-1})$$

$$\int_0^{T-t_1-\ldots-t_{j-1}} \alpha_j e^{-(\alpha_j+\beta_j)t_j}\,[1 - H[t_1,\ldots,t_{j-1}](t_j)]\, dt_j$$

$$\int_0^{T-t_1-\ldots-t_j} d\,G\,(t_{j+1})$$

The theorem at the end of this section shows that the last iterated integral is less than or equal to

$$\int_0^T d\,F\,(\omega_1,\ldots,\omega_{j-1}) \int_0^{T-\omega_1-\ldots\omega_{j-1}} d\,G\,(t_{j+1})$$

$$\times \left\{ \frac{\int_0^T d\,F\,(t_1,\ldots t_{j-1}) \int_0^\infty \alpha_j e^{-(\alpha_j+\beta_j)t_j} [1 - H[t_1,\ldots,t_{j-1}](t_j)]\,dt_j}{\int_0^T d\,F\,(w_1,\ldots,w_{j-1})} \right\}$$

The expression in the braces is less than or equal to $\alpha_j\,\mu_j$.

Hence the reliability model with the time dependent recovery has the same upper bound as the semi-Markov reliability model.

<u>Theorem</u> With the notation as above

$$\int_0^T d\,F\,(\omega_1,\ldots,\omega_{j-1}) \int_0^T d\,F\,(t_1,\ldots,t_{j-1}) \int_0^{T-t_1-\ldots-t_{j-1}} \alpha_j e^{-(\alpha_j+\beta_j)t_j}[1 - H[t_1,\ldots t_{j-1}](t_j)]\,d\,t_j \int_0^{T-t_1-\ldots t_j} d\,G\,(t_{j+1})$$

$$\leq \int_0^T d\,F\,(\omega_1,\ldots,\omega_{j-1}) \int_0^{T-\omega_1-\ldots-\omega_{j-1}} d\,G(t_{j+1}) \int_0^T d\,F\,(t_1,\ldots,t_{j-1}) \int_0^\infty \alpha_j e^{-(\alpha_j+\beta_j)t_j} [1 - H[t_1,\ldots t_{j-1}](t_j)]\,d\,t_j$$

Proof

Let

$$\nu\ (x_1,\ldots,x_{j-1}) = \int_0^\infty \alpha_j e^{-(\alpha_j+\beta_j)t_j}[1 - H\ [x_1,\ldots x_{j-1}](t_j)]\ d\ t_j$$

and note that $\nu\ (x_1,\ldots,x_{j-1}) \leq 1$.

Consider the difference

$$\int_0^T d\ F\ (\omega_1,\ldots,\omega_{j-1})$$

$$\int_0^{T-\omega_1-\ldots-\omega_{j-1}} d\ G\ (t_{j+1})$$

$$\int_0^T d\ F\ (t_1,\ldots,t_{j-1})$$

$$\int_0^\infty \alpha_j e^{-(\alpha_j+\beta_j)t_j}\ [1 - H[t_1,\ldots t_{j-1}](t_j)]\ d\ t_j$$

$$- \int_0^T d\ F\ (\omega_1,\ldots,\omega_{j-1})$$

$$\int_0^T d\ F\ (t_1,\ldots,t_{j-1})$$

$$\int_0^{T-t_1-\ldots-t_{j-1}} \alpha_j e^{-(\alpha_j+\beta_j)t_j}[1 - H[t_1,\ldots t_{j-1}](t_j)]\ d\ t_j$$

$$\int_0^{T-t_1-\ldots t_j} d\ G\ (t_{j+1})$$

$$
\begin{aligned}
&\geq \int_0^T d\,F\,(\omega_1,\ldots,\omega_{j-1}) \qquad \int_0^T d\,F\,(t_1,\ldots,t_{j-1}) \\
&\qquad \left\{ \int_0^\infty \alpha_j e^{-(\alpha_j+\beta_j)t_j} \, [1 - H[t_1,\ldots,t_{j-1}](t_j)] \, dt_j \right. \\
&\qquad\qquad \int_0^{T-\omega_1-\ldots-\omega_{j-1}} d\,G\,(t_{j+1}) \\
&\qquad\qquad - \int_0^\infty \alpha_j e^{-(\alpha_j+\beta_j)t_j} \, [1 - H[t_1,\ldots,t_{j-1}](t_j)] \, dt_j \\
&\qquad\qquad\qquad \left. \int_0^{T-t_1-\ldots-t_{j-1}} d\,G\,(t_{j+1}) \right\} \\
&\geq \int_0^T \nu\,(\omega_1,\ldots,\omega_{j-1}) \quad d\,F\,(\omega_1,\ldots,\omega_{j-1}) \\
&\qquad \int_0^T \nu\,(t_1,\ldots,t_{j-1}) \, d\,F\,(t_1,\ldots,t_{j-1}) \\
&\qquad\quad \left\{ \int_0^{T-\omega_1-\ldots-\omega_{j-1}} d\,G\,(t_{j+1}) - \int_0^{T-t_1-\ldots-t_{j-1}} d\,G\,(t_{j+1}) \right\} \\
&= 0.
\end{aligned}
$$

The theorem is proved.

7. ACKNOWLEDGEMENTS

The algebraic lower bound in section four is due to Paul Peterson at Kentron International. Rick Butler and Dan Palumbo at NASA Langley Research Center have an interactive computer program and graphics package for the algebraic bounds which they call SURE for semi-Markov unreliability range evaluator.

REFERENCES

1. T. B. Smith and J. H. Lala, "Development and Evaluation of a Fault-Tolerant Multi-Processor (FTMP) Computer," Vol. I, "FTMP Principles of Operation," NASA CR-166073; Vol. II, "FTMP Software," NASA CR-166072; Vol. III, "FTMP Test and Evaluation," NASA CR-166073; 1983.

2. J. Goldberg, M. Green, W. Kautz, K. Levitt, P. M. Melliar-Smith, R. Schwartz, C. Weinstock, "Development and Analysis of the Software Implemented Fault-Tolerance (SIFT) Computer," NASA CR-182146, 1983.

3. J. H. LaLa, "Fault Detection, Isolation, and Reconfiguration in FTMP: Methods and Experimental Results," Proceedings of the Fifth Digital Avionics System Conference, 1983.

4. K. L. Chung, <u>A Course in Probability Theory</u>, Second Edition, Academic Press, New York, 1974.

5. W. Feller, <u>An Introduction to Probability Theory and Its Applications</u>, Volume II, Second Edition, Wiley, New York, 1971.

6. A. White, "Quick Sensitivity Analysis by Approximation Formulas," Proceedings of the Fifth Digital Avionics System Conference, 1983.

7. A. White, "An Approximation Formula for a Class of Markov Reliability Models," NASA CR-172290, 1983.

8. J. McGough, "Effects of Near Coincident Faults in Multiprocessor Systems," Proceedings of the Fifth Digital Avionics System Conference, 1983.

9. L. Lee, "Some Methods of Estimating a Coverage Parameter," Proceedings of the Sixteenth Annual Electronics and Aerospace Conference, 1983.

1. Report No. NASA CR-172340	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle UPPER AND LOWER BOUNDS FOR SEMI-MARKOV RELIABILITY MODELS OF RECONFIGURABLE SYSTEMS		5. Report Date April 1984
		6. Performing Organization Code
7. Author(s) Allan L. White		8. Performing Organization Report No.
9. Performing Organization Name and Address Kentron International, Inc. Kentron Technical Center, Aerospace Technologies Div. Hampton, VA 23666		10. Work Unit No.
		11. Contract or Grant No. NAS1-16000
12. Sponsoring Agency Name and Address National Aeronautics and Space Administration Washington, DC 20546		13. Type of Report and Period Covered Contractor Report
		14. Sponsoring Agency Code
15. Supplementary Notes Langley Technical Monitor: Charles W. Meissner, Jr.		

16. Abstract

This paper determines the information required about system recovery to compute the reliability of a class of reconfigurable systems. Upper and lower bounds are derived for these systems. The class consists of those systems that satisfy five assumptions: the components fail independently at a low constant rate, fault occurrence and system reconfiguration are independent processes, the reliability model is semi-Markov, the recovery functions which describe system reconfiguration have small means and variances, and the system is well designed. The bounds are easy to compute, and examples are included.

17. Key Words (Suggested by Author(s)) Reliability estimation, Fault tolerance, Digital process control		18. Distribution Statement Unclassified - Unlimited. Subject Category 66	
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 26	22. Price A03