NASA CR-178,008

NASA Contractor Report 178008

NASA-CR-178008
19860005577

SYNTHETIC BOUNDS FOR SEMI-MARKOV RELIABILITY MODELS

Allan L. White

PRC Kentron, Inc.
Aerospace Technologies Division
Hampton, Virginia 23666

Contract NAS1-18000
November 1985

NASA
National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23665

INTRODUCTION

We derive upper and lower bounds for the probability of failure for systems that achieve high reliability with architectures that use redundancy and reconfiguration. The engineering assumptions are that individual components fail independently at a low constant rate and that the system quickly recovers from all faults. The mathematical assumption is that the process of component failure and system recovery can be represented by a semi-Markov model where competing events are stochastically independent. The bounds are synthetic in the sense that descriptions of component failure and system recovery are obtained from different sources. The reliability model is constructed (synthesized) under the assumption that the processes are independent.

UPPER AND LOWER BOUNDS

Figure 1 displays a general path in a reliability model that begins at an initial fault-free state and ends at an absorbing system-failure state. The global time-independence of a semi-Markov model permits the rearrangement of states on the path for notational and computational convenience. In the first line of figure 1, successful fault transitions that have rate λ_k compete with fault transitions that have rate γ_k. In the second line, successful recovery transitions that have generalized density $dF_{i,1}$ compete with other recovery transitions $dF_{i,2},\ldots,dF_{i,b_i}$ and fault occurrences ε_i. In the third line, successful fault occurrences α_j compete with recovery transitions $dG_{j,1},\ldots,dG_{j,c_j}$ and other fault occurrences β_j. For notation

$D(T)$ = Probability of traversing the path in figure 1 by time T

$p(F_i)$ = Probability the transition $dF_{i,1}$ is successful when competing against other recovery transitions

$$= \int_0^\infty [1 - F_{i,2}(t)]\ldots[1 - F_{i,b_i}(t)]\, dF_{i,1}(t)$$

$m_1(F_i)$ = First conditional moment of $dF_{i,1}$

$$= \frac{1}{p(F_i)} \int_0^\infty t\, [1 - F_{i,2}(t)]\ldots[1 - F_{i,b_i}(t)]\, dF_{i,1}(t)$$

$m_2(F_i)$ = Second conditional moment of $dF_{i,1}$

$$= \frac{1}{p(F_i)} \int_0^\infty t^2\, [1 - F_{i,2}(t)]\ldots[1 - F_{i,b_i}(t)]\, dF_{i,1}(t)$$

$m_1(C_j)$ = First moment of the holding time in state C_j considering only the recovery transitions

$$= \int_0^\infty [1 - G_{j,1}(t)]\ldots[1 - G_{j,c_j}(t)]\, dt$$

$m_2(C_j)$ = Second moment of the holding time in state C_j considering only the recovery transitions

$$= 2 \int_0^\infty t\, [1 - G_{j,1}(t)]\ldots[1 - G_{j,c_j}(t)]\, dt.$$

There is a relationship between the moments of a holding time for a state and the conditional moments of the transition functions given by

$$m_i(C_j) = \sum_{\ell=1}^{c_j} p(G_{j,\ell})\ m_i(G_{j,\ell})$$

where $p(G_{j,\ell})$ and $m_i(G_{j,\ell})$ are defined just as the probabilities and moments for the F's are.

Continuing to developing the notation, figure 2 displays the constant rate part of the path in figure 1. Let

$E(T)$ = Probability of traversing the path in figure 2 by time T.

Let $V = T - r_1 - \ldots - r_m - s_1 - \ldots - s_n$ where

$$r_i = [m_1(F_i)]^{1/2}$$

$$s_i = [m_1(C_j)]^{1/2}.$$

We assume $r_1 + \ldots + r_m + s_1 + \ldots + s_n < T$.

The proof of the assertions below uses the elementary facts that if H is a distribution such that H(0-) = 0 then

$$\int_0^\infty \lfloor 1-H(t) \rfloor \, dt = m_1(H)$$

$$\int_0^\infty t \lfloor 1-H(t) \rfloor \, dt = \frac{m_2(H)}{2}$$

$$1-H(c) = \int_c^\infty dH(t) \leq \frac{m_2(H)}{c^2} \quad \text{for } c > 0 \text{ (Markov's inequality)}$$

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

$$E(V) \prod_{i=1}^{m} p(F_i) \lfloor 1 - \varepsilon_i m_1(F) - \frac{m_2(F_i)}{m_1(F_i)} \rfloor$$

$$\prod_{j=1}^{n} \alpha_j \, \mu(C_j) \lfloor 1 - \frac{(\alpha_j + \beta_j) m_2(C_j)}{2m_1(C_j)} - \frac{m_2(C_j)}{[m_1(C_j)]^{3/2}} \rfloor$$

$$\leq D(T)$$

$$\leq E(T) \prod_{i=1}^{m} p(F_i) \prod_{j=1}^{n} \alpha_j \, m_1(C_j)$$

Proposition

(i) $\int_0^\infty e^{-\varepsilon_i x_i} [1-F_{i,2}(x_i)]\ldots[1-F_{i,b_i}(x_i)]\, dF_{i,1}(x_i) \leq p(F_i)$

(ii) $\int_0^\infty \alpha_j\, e^{-\alpha_j y_j}\, e^{-\beta_j y_j} [1 - G_{j,1}(y_j)]\ldots[1 - G_{j,c_j}(y_j)]\, dy_j \leq \alpha_j\, m_1(C_j)$

(iii) $\int_0^{r_i} e^{-\varepsilon_i x_i} [1 - F_{i,2}(x_i)]\ldots[1 - F_{i,b_i}(x_i)]\, dF_{i,1}(x_i)$

$$\geq p(F_i) \left[1 - \varepsilon_i\, m_1(F_i) - \frac{m_2(F_i)}{r_i^2}\right]$$

(iv) $\int_0^{s_j} \alpha_j\, e^{-\alpha_j y_j}\, e^{-\beta_j y_j} [1 - G_{j,1}(y_j)]\ldots[1 - G_{j,c_j}(y_j)]\, dy_j$

$$\geq \alpha_j m_1(C_j) \left[1 - \frac{(\alpha_j+\beta_j)\, m_2(C_j)}{2m_1(C_j)} - \frac{m_2(C_j)}{s_j m_1(C_j)}\right]$$

Proof of the proposition

Assertions (i) and (ii) follow from the inequality $e^{-a} \leq 1$ for $a \geq 0$.

Assertions (iii) and (iv) require more work and use the equation $\int_0^c = \int_0^\infty - \int_c^\infty$ and the inequalities $1-a \le e^{-a} \le 1$ for $a \ge 0$.

To prove (iii) note that the integral is bigger than or equal to

$$\int_0^\infty (1 - \varepsilon_i x_i)[1 - F_{i,2}(x_i)]\ldots[1 - F_{i,b_i}(x_i)]\, dF_{i,1}(x_i)$$

$$- \int_{r_i}^\infty [1 - F_{i,2}(x_i)]\ldots[1 - F_{i,b_i}(x_i)]\, dF_{i,1}(x_i)$$

which is bigger than or equal to

$$p(F_i) - \varepsilon_i p(F_i)\, m_1(F_i) - p(F_i)\,\frac{m_2(F_i)}{r_i^2}$$

when the last integral is replaced by Markov's inequality.

To prove (iv) note that the integral is bigger than or equal to

$$\alpha_j \int_0^\infty (1-(\alpha_j + \beta_j)y_j)[1 - G_{j,1}(y_j)]\ldots[1 - G_{j,c_j}(y_j)]\, dy_j$$

$$- \alpha_j \int_{s_j}^{\infty} [1 - G_{j,1}(y_j)]\ldots[1 - G_{j,c_j}(y_j)]\, dy_j.$$

The integrand in the last integral is equal to one minus the probability of being in state C_j at time y_j and by Markov's inequality is less than or equal to $\frac{m_2(C_j)}{y_j^2}$.

Hence (iv) is bigger than or equal to

$$\alpha_j m_1(C_j) - \frac{\alpha_j(\alpha_j + \beta_j)\, m_2(C_j)}{2} - \frac{\alpha_j m_2(C_j)}{s_j}.$$

Proof of the theorem

Let q(t) be the density function for traversing the path in figure 2 by time t.

The probability of reaching state D in figure 1 before time T is

$$D(T) = \int_0^T q(t)$$

$$\int_0^{T-t} e^{-\varepsilon_1 x_1} [1 - F_{1,2}(x_1)]\ldots[1 - F_{1,b_1}(x_1)]$$

$$\vdots$$

$$\int_0^{T-t-x_1-\ldots x_{m-1}} e^{-\varepsilon_m x_m} [1 - F_{m,2}(x_m)]\ldots[1 - F_{m,b_m}(x_m)]$$

$$\int_0^{T-t-x_1-\cdots-x_m} e^{-(\alpha_1+\beta_1)y_1} [1 - G_{1,2}(y_1)]\cdots[1 - G_{1,c_1}(y_1)]$$

$$\vdots$$

$$\int_0^{T-t-x_1-\cdots-y_{n-1}} \alpha_n e^{-(\alpha_n+\beta_n)y_n} [1 - G_{n,1}(y_n)]\cdots[1 - G_{n,c_n}(y_n)]$$

$$dy_n \cdots dy_1 \, dF_{m,1}(x_m)\cdots dF_{1,1}(x_1) \, dt$$

Working with just the limits of integration

$$\int_0^V \int_0^{r_1} \cdots \int_0^{r_m} \int_0^{s_1} \cdots \int_0^{s_n} \leq D(T) \leq \int_0^T \int_0^\infty \cdots \int_0^\infty \int_0^\infty \cdots \int_0^\infty .$$

The theorem is proved by applying the inequalities in the proposition to the integrals in the above inequality for D(T).

CONCLUDING REMARKS

A new method for bounding the probability of entering an absorbing state of a semi-Markov model has been presented. The method is based on a path analysis of the model, and reduces the calculation of an absorbing state probability to a single algebraic computation. The bounds are typically close and consequently represent a practical solution to the analysis of a class of semi-Markov reliability models.

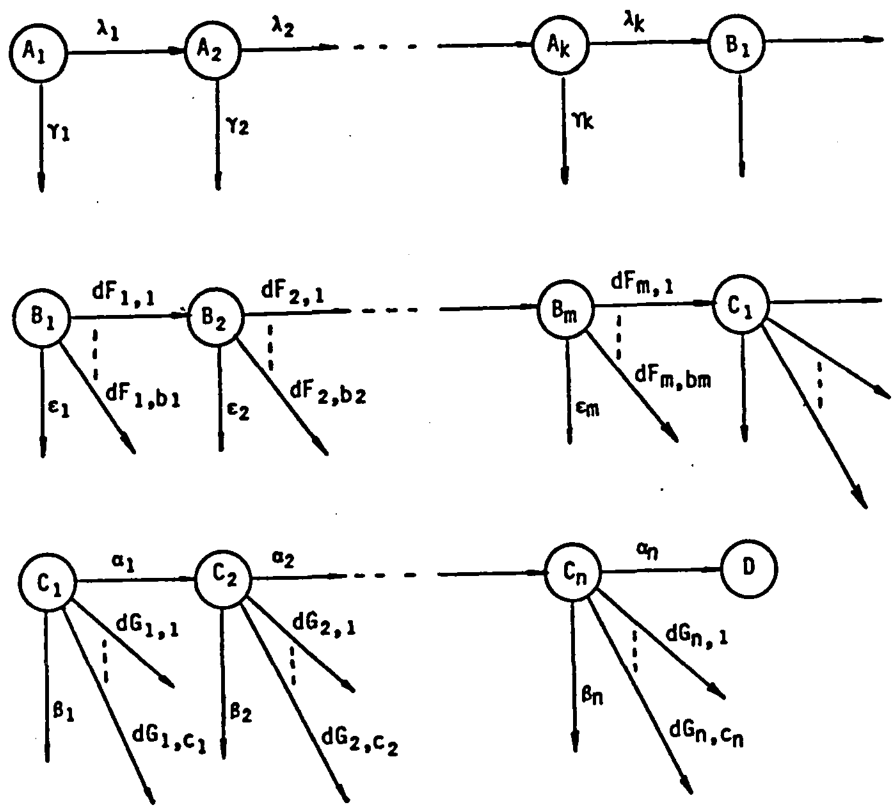

Figure 1: General Path in a Semi-Markov Model

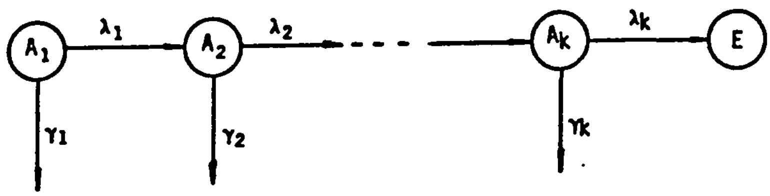

Figure 2: Constant Rate Part of the Path

Standard Bibliographic Page

1. Report No. NASA CR-178008	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Synthetic Bounds for Semi-Markov Reliability Models		5. Report Date November 1985
		6. Performing Organization Code
7. Author(s) Allan L. White		8. Performing Organization Report No.
9. Performing Organization Name and Address PRC Kentron, Inc. Aerospace Technologies Division 3221 N. Armistead Avenue Hampton, VA 23666		10. Work Unit No.
		11. Contract or Grant No. NAS1-18000
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 505-34-13-33
15. Supplementary Notes Langley Technical Monitor: Charles W. Meissner, Jr.		

16. Abstract

Upper and lower bounds are derived for the probability of failure for a class of highly reliable process control computers. The bounds are synthetic in the sense that the descriptions of component failure and system recovery are assumed to be obtained from different sources. The reliability model is constructed under the assumption that the processes are independent.

17. Key Words (Suggested by Authors(s)) Reliability estimation; Fault-tolerant computers	18. Distribution Statement Unclassified - Unlimited; Subject Category 66

19. Security Classif.(of this report)	20. Security Classif.(of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	11	A02

For sale by the National Technical Information Service, Springfield, Virginia 22161

NASA Langley Form 63 (June 1985)