SUMMARY AND CONCLUSIONS

Semi-Markov processes have proved to be an effective and convenient tool to construct models of systems that achieve reliability by redundancy and reconfiguration. These models are able to depict complex system architectures and to capture the dynamics of fault arrival and system recovery. A disadvantage of this approach is that the models can be extremely large, which poses both a model construction and a computational problem. Results are needed that permit a reduction in model size. Because these systems are used in critical applications where failure can be expensive, there must be analytically derived bounds for the error produced by the model reduction techniques. This paper presents three theorems which show that the reliability of a popular class of systems can be computed using small and simple models. These theorems give error bounds for three model reduction and simplification techniques. The error bounds are given in terms of readily available system parameters.

1. INTRODUCTION

Efforts are being made to design reliable digital control systems using redundancy and reconfiguration. The reliability requirement for these systems can be extremely high. An example is the proposed requirement that the flight control system for a commercial aircraft has less than one chance in a billion of failure during a flight. Such requirements are beyond what can be established by natural life testing. An alternate method that is being considered is to compute the probability of system failure with a semi-Markov model that captures the elements of system architecture, component failure, and system recovery from failed components. One obstacle is that an accurate model of a redundant and reconfigurable system presents major model construction and numerical computation problems [1]. A large number of states are necessary to represent the status of all the components in the system. In addition, the behavior of faulty components and system recovery can be complex transactions involving arbitrary probability distributions.

For a popular class of systems, however, the semi-Markov reliability model has features that make the reliability computations easy. A common approach to achieving reliability is to have three or four components perform a majority vote. When a component becomes faulty and disagrees with the majority, it is discarded from the system and replaced by a spare if a spare is available. Almost all systems currently being considered are assemblages of subsystems where each subsystem is such a majority-voting threeplex plus spares or fourplex plus spares. It is also possible to have some (or all) of the spares belong to a common pool. For this class of systems, three theorems are presented that reduce the computational burden. The first theorem (for which one version has already been published [2]) derives an error bound for deleting certain transitions out of the states in which the system is recovering from a fault. The second theorem derives an error bound for deleting most of the coincident-fault failure states. A coincident-fault failure state occurs when two faults occur nearly simultaneously and either overwhelm the majority voter or confuse the system reconfiguration algorithm. The third theorem derives an error bound for estimating the probability of failure-by-exhaustion-of-parts by combinatorial methods.

After section 2 on notation, sections 3 and 4 explain the contents of the three theorems using an illustrative example of two fourplexes. Section 5 contains more comments on the version of the theorems presented in this paper. Section 6 states the three theorems with their assumptions. Because of a lack of space, only a sketch of the proof for the second theorem is presented in section 7. After this sketch, section 8 uses the three theorems to compute the reliability of a large and complex system.

2. NOTATION

The notation used in all the reliability model figures is

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>fault-free state</td>
</tr>
<tr>
<td>R,Q</td>
<td>recovery-mode state</td>
</tr>
<tr>
<td>C</td>
<td>coincident-fault failure state</td>
</tr>
<tr>
<td>E</td>
<td>exhaustion-of-parts failure state</td>
</tr>
<tr>
<td>k, j, l, γ</td>
<td>component failure rates</td>
</tr>
<tr>
<td>δ, p</td>
<td>system recovery rates</td>
</tr>
<tr>
<td>f</td>
<td>semi-Markov recovery density</td>
</tr>
<tr>
<td>F</td>
<td>distribution function for the density f.</td>
</tr>
</tbody>
</table>

Additional notation used in the statement and proofs of the theorems is

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>εx</td>
<td>sum of the failure rates out of state S_x (x can be a vector)</td>
</tr>
<tr>
<td>θ</td>
<td>maximum of the sums of the failure rates out of any state</td>
</tr>
<tr>
<td>µ</td>
<td>maximum average-holding-time in any single-fault recovery-mode state</td>
</tr>
<tr>
<td>T</td>
<td>system operating time</td>
</tr>
<tr>
<td>C*</td>
<td>bound on coincident-failure probability, equal to ε^2 T µ</td>
</tr>
</tbody>
</table>
3. ILLUSTRATIVE EXAMPLE

This section motivates the theorems and illustrates their contents by means of a simple system consisting of two fourplexes. Each fourplex has the reconfiguration sequence fourplex-threeplex-simplex. The system fails if either fourplex fails by a coincident-fault failure or exhaustion-of-parts failure. The initial states for the reliability model of this system are given in Figure 1.

The model reduction process has three steps. The first step is model-reduction-by-trimming [2]. To illustrate this procedure, consider the recovery-mode state $R_{1,1}$ in Figure 1 where a component of a fourplex has become faulty and the system is recovering to the fault-free state $S_2$ at rate $\delta_1$. The transition $3\lambda_1$ from $R_{1,1}$ to $C_{1,1}$, a system failure state, represents the failure of another component in the same fourplex before system recovery occurs. The transition $4\lambda_2$ from $R_{1,1}$ to RR is a component failure transition during system recovery that does not cause system failure. Since this transition from $R_{1,1}$ to RR has a small probability and it must be followed by other component failures before system failure occurs, it is a reasonable conjecture that this last transition and the subsequent failure states can be eliminated from the model without causing significant error. The model in Figure 2 depicts the model in Figure 1 modified by deleting all component failure transitions out of recovery-mode states that do not cause immediate system failure. For the component failure rates $\lambda_1 = \lambda_2 = 10^{-4}$/hour, the single-fault system recovery rates $\delta_1 = \delta_2 = 3600$/hour, the double-fault system recovery rate $\rho = 360$/hour, and an operating time of 1 hour, the complete model of Figure 1 returns

$$P\{\text{failure from complete model}\} = 7.0634192e-11$$

while the "trimmed" model of Figure 2 returns

$$P\{\text{failure from trimmed model}\} = 7.06340076e-11.$$  

The difference is

$$P\{\text{complete}\} - P\{\text{trimmed}\} = 1.416616.$$  

The error is insignificant.

---

$C_k$ coincident-fault failure given precisely $k+1$ faults have occurred

$C_R$ the sum $C_2 + C_3 + \ldots \text{ Poiss}[n]$ probability that $n$ or more events have occurred before time $T$ in a Poisson renewal process with rate $\delta$.

The mnemonics for the three error bounds and the predicted probability of system failure are

TRMBND the bound on the error due to trimming

COFBND the bound on the error due to considering only $C_1$, the first coincident-fault failure

EXHBND the bound on the error due to ignoring coincident-fault failures when computing the probability of failure by exhaustion of parts.

THMEST estimate of the probability of failure using first coincident-failure and combinatorial exhaustion-of-parts.

---

**Figure 1:** Initial States of the Complete Reliability Model for Two Fourplexes

**Figure 2:** Initial States of the Reliability Model for Two Fourplexes After Trimming
The second step is the elimination of most of the remaining coincident-fault failure states. Motivating this step begins by comparing the coincident-fault failure states \(C_{1,1}\) and \(C_{1,2}\) in the trimmed model in Figure 2. The probability of going from \(R_{1,2}\) to \(C_{1,2}\) is slightly less than the probability of going from \(R_{1,1}\) to \(C_{1,1}\). In addition, arrival at \(C_{1,2}\) requires more failure occurrence than arrival at \(C_{1,1}\). If the system operating time is much shorter than the mean-time-to-failure of the components, then the probability of another fault occurrence is small and it is reasonable to conjecture that \(C_{1,2}\) is much less than \(C_{1,1}\). Let \(C_t\), the first coincident-fault failure, be defined to be system failure by coincident fault when precisely two faults have occurred. Let \(C_R\), the remaining coincident fault failures, be defined to be system failure by coincident fault when more than two failures have occurred. For the trimmed model of the two fourplexes, \(C_t\) consists of the state \(C_{1,1}\) (which is shown in Figure 2) and the symmetric state \(C_{2,1}\) (which is not shown in Figure 2). For the parameter values given above,

\[C_t = 6.668 \times 10^{-11}\]
\[C_R = 2.006 \times 10^{-14}\]

Ignoring \(C_R\) produces an insignificant amount of error. Both \(C_{1,1}\) and \(C_{2,1}\) can be computed using the model displayed in Figure 3(a).

The third step consists of computing the failure due to exhaustion of parts by a simple model that ignores coincident-fault failures. This procedure should produce an overestimation for the probability of failure due to exhaustion of parts since it ignores the possibility that the system may have failed by coincident-faults before reaching exhaustion of parts. For the system of two fourplexes, the model and formula for this third step is displayed in Figure 3(b). Using the parameters above,

\[E_{\text{by complete model in Figure 1}} = 3.9925 \times 10^{-12}\]
\[E_{\text{by ignoring coincident faults}} = 3.9992 \times 10^{-12}\]

This third step introduces a small amount of error.

4. COMPUTATION OF BOUNDS FOR ILLUSTRATIVE EXAMPLE

To complete the example of two fourplexes presented in section 3, this section applies the three theorems to obtain an estimate, along with upper and lower bounds, for the probability of failure. Using the complete model to compute the probability gives

\[\text{Prob}(\text{Failure}) = 7.06341498 \times 10^{-11}\]

The estimate for the probability of system failure using this model reduction approach is the sum of \(C_t\) computed from Figure 3(a) and \(E_t\) computed from Figure 3(b)

\[\text{THMEST} = C_t + E_t\]
\[= 6.66348188 \times 10^{-11} + 3.99920002 \times 10^{-12}\]
\[= 7.06340198 \times 10^{-11}\]

The actual error is

\[\text{Prob}(\text{Failure}) - \text{THMEST} = 1.308 \times 10^{-16}\]

Ignoring \(C_R\) produces an insignificant amount of error. Both \(C_{1,1}\) and \(C_{2,1}\) can be computed using the model displayed in Figure 3(a).

The third step consists of computing the failure due to exhaustion of parts by a simple model that ignores coincident-fault failures. This procedure should produce an overestimation for the probability of failure due to exhaustion of parts since it ignores the possibility that the system may have failed by coincident-faults before reaching exhaustion of parts. For the system of two fourplexes, the model and formula for this third step is displayed in Figure 3(b). Using the parameters above,

\[E_{\text{by complete model in Figure 1}} = 3.99258 \times 10^{-12}\]
\[E_{\text{by ignoring coincident faults}} = 3.99926 \times 10^{-12}\]

This third step introduces a small amount of error.

The maximum amount that \(\text{THMEST}\) can underestimate the probability of failure is given by the sum of the trimming bound, formula (1), and the coincident-fault bound, formula (2). These formulas are in section 6 which states the theorems.

\[\text{TRMBND} = 7.2 \times 10^{-14}\]
\[\text{COFBND} = 1.4 \times 10^{-13}\]

The maximum amount \(\text{THMEST}\) can overestimate the probability of system failure is given by the exhaustion bound, formula (4), which is also in section 6 which states the theorems.

\[\text{EXHBND} = 1.4 \times 10^{-13}\]

Hence,

\[\text{Upper bound} = \text{THMEST} + \text{TRMBND} + \text{COFBND}\]
\[= 7.063 \times 10^{-11} + 2.1 \times 10^{-13}\]
\[= 7.083 \times 10^{-11}\]

1992 PROCEEDINGS Annual RELIABILITY AND MAINTAINABILITY Symposium
Lower bound = THMEST - EXHBND
= 7.063e-11 - 1.4e-13
= 7.048e-11.

These bounds show that THMEST has an error of less than 1 per cent.

5. DISCUSSION OF COINCIDENT-FAULT BOUND

Considering Figure 2 for the example in the sections 3 and 4, it is clear that the probability of a transition to the coincident-fault failure state $C_{1,1}$ out of the recovery-mode state $R_{1,1}$ is greater than the probability of a transition to $C_{1,2}$ out of $R_{1,2}$. A similar inequality holds for $C_{2,1}$. These inequalities are one of the reasons that, for this example, coincident-fault failures are dominated by $C_1$, the first coincident-fault failure. In this example the system is at greater risk in the recovery-mode states for the first coincident-fault than in subsequent recovery-mode states. Not all systems have this property. A system can be at greater risk in later recovery-mode states for a variety of reasons. Three reasons come immediately to mind. (1) Spares can fail, and when a faulty spare is brought into the system the system must begin recovery again. (2) A component brought in as a spare can have a higher failure rate than the initial set of active components. (3) After some equipment has failed, the recovery procedure can be longer and more difficult. For these and other reasons, the bound COFBND in this paper uses $C$ instead of $C_1$. More refined versions of the bound COFBND are being developed.

6. STATEMENT OF THEOREMS

Theorem (Statement of the three theorems -- the three error bounds)

Suppose a system has the following four properties

(i) The system is an assemblage of subsystems, where each subsystem achieves fault tolerance by a three-way or four-way majority voter.
(ii) Components fail at a constant rate.
(iii) Fault recovery depends only on the time since fault occurrence.
(iv) All transitions to system failure are component failure transitions. (This assumption eliminates pathological cases.)

Then an error bound for the model reduction technique of trimming is given by

$$TRMBND = \mu \cdot (\exp(\theta T) - \theta T - 1).$$

(1)

The first coincident fault states are the coincident-fault failure states when precisely two component failures have occurred. An error bound for considering only the first coincident-fault states is

$$COFBND = \theta^2 T^2 \mu.$$  

(2)

An error bound for ignoring coincident-fault failures when computing failure by exhaustion of parts is

$$EXHBND = \theta \mu \left[ 2\theta T \exp(\theta T) - \exp(\theta T) + 1 \right].$$

(3)

If the system has enough components that there is no failure-by-exhaustion-of-parts until at least $N_2 \geq 3$ components fail, then the last error bound becomes

$$EXHBND = \theta \mu \left[ 2\theta T \exp(\theta T) - \exp(\theta T) + 1 \right] - \theta \mu \sum_{k=1}^{N-2} k \left[ \theta^{k+1} T^{k+1/(k+1)} + \theta^k T^k/k! \right].$$

(4)

Corollary (Statement of the estimate and its bounds)

Assume the system has the same four properties as listed in the result above.

Let $C_1$ be the probability of coincident-fault failure when precisely two fault have occurred, and let $E'$ be failure-by-exhaustion-of-parts computed by ignoring coincident-fault failures. Then an estimate for the probability of system failure is

$$THMEST = C_1 + E'.$$

An upper bound for the probability of system failure is

$$Upper \; Bound = THMEST + TRMBND + COFBND.$$

A lower bound for the probability of system failure is

$$Lower \; Bound = THMEST - EXHBND.$$

7. SKETCH OF THE PROOF FOR THE COINCIDENT-FAULT BOUND

This material below sketches the derivation for COFBND, the error bound for ignoring all coincident-fault failures except for the first one. The general model needed for the derivation is displayed in Figure 4. It is assumed that trimming has already occurred, which means the only failure transitions out of recovery-mode states (R's) are those into system-failure states (C's).
The proof proceeds by considering paths from the initial state to the absorbing states representing system failure. Considering such paths is a common procedure for obtaining error bounds[3]. From the model in Figure 4, we have

\[
C_2 = \sum_{i=1}^{m} \sum_{j=1}^{m} \int_{0}^{T} \alpha_i \exp(-\epsilon_0 t_1) dt_1
\]

\[
\int_{0}^{T-t_1} \alpha_i \exp(-\epsilon_1 t_2) dt_2
\]

\[
\int_{0}^{T-t_1-t_2} \beta_{ij} \exp(-\epsilon_2 t_3) [1-F_{ij}(t_3)] dt_3 dt_1
\]

The first step is to replace each integral that has a factor of \(f(t)\) in the integrand. Each such integral is replaced by a factor of \(1\). This replacement and an adjustment of the variables of integration give the inequality

\[
C_2 \leq \sum_{i=1}^{m} \sum_{j=1}^{m} \int_{0}^{T} \alpha_i \exp(-\epsilon_0 t_1) dt_1
\]

\[
\int_{0}^{T-t_1} \alpha_i \exp(-\epsilon_1 t_2) dt_2
\]

\[
\int_{0}^{T-t_1-t_2} \beta_{ij} \exp(-\epsilon_2 t_3) [1-F_{ij}(t_3)] dt_3 dt_1
\]

Bringing the summation over \(j\) inside the first integration yields

\[
C_2 \leq \sum_{i=1}^{m} \int_{0}^{T} \alpha_i \exp(-\epsilon_0 t_1) dt_1
\]

\[
\int_{0}^{T-t_1} \alpha_i \exp(-\epsilon_2 t_2) dt_2
\]

\[
\int_{0}^{T-t_1-t_2} \beta_{ij} \exp(-\epsilon_2 t_3) [1-F_{ij}(t_3)] dt_3 dt_1
\]

It can be shown that the expression inside the brackets is less than or equal to

\[
C^* = e^2 T \mu.
\]

Hence,

\[
C_2 \leq C^* \sum_{i=1}^{m} \int_{0}^{T} \alpha_i \exp(-\epsilon_0 t_1) dt_1.
\]

It can also be shown that since

\[
\sum_{i=1}^{m} \alpha_i \leq \epsilon_0 \leq \Theta,
\]

brining the sum over \(i\) inside the integral gives the inequality

\[
C_2 \leq C^* \int_{0}^{T} \Theta \exp(-\Theta t_1) dt_1 = C^* \Theta \Phi(1).
\]

Proceeding in a similar manner gives, for \(k \geq 2\),

\[
C_k \leq C^* \Phi(k-1).
\]

Summing over \(k\) gives the coincident-fault bound of

\[
\text{COFBND} \leq C^* \sum_{k=2}^{\infty} \Phi(k) = C^* \sum_{k=1}^{\infty} \Phi(k) = C^* \Theta T = e^2 T \mu.
\]

This completes the sketch of the proof for COFBND, the error bound for ignoring all coincident-fault failures except the first one.
Figure 4: General Model for the Proof of the Coincident-Fault Bound

Figure 5: The AIPS for IAPSA System
8. NUMERICAL EXAMPLE

This section applies the three theorems to a system that has been used as an example that generates extremely large reliability models [4]. The system considered is one version of AIPS (Advanced Information Processing System) for IAPSA (Integrated Airframe Propulsion System Architecture) [7]. Figure 5 illustrates the system configuration. In Figure 5, the mnemonics are CH for a computational channel (computer), NI for a network element, L for a link, and D for a device interface. The nodes in the two networks are numbered circles. The devices are labeled DA, DB, DC, and DD.

The system contains numerous dependencies. For example, if the first computational channel (computer) CH1 fails, then the network interface NI1 also fails. In addition, if the first network is connected to the computers through NI1, then the failure of CH1 temporarily removes the first network from the system. In this case, the system can fail by a coincident-fault failure if any component associated with the second network fails before the first network is reconnected. This dependency also creates a failure condition known as temporary exhaustion. For example, if both sensors of type A have failed on the first network and if the second network goes temporarily down for any reason, then the system is, at least temporarily, without any sensors of type A which creates an exhaustion of parts failure. A detailed description can be found in the references [4,7].

The large number of components and their complex interaction produce a large reliability model. The complete model is estimated to have 27 million states [4]. Using the results stated in theorems 1 and 2 in section 6, it is possible to compute the reliability using a 19 state Markov model for the coincident-fault failures, a 30 gate fault tree for the standard failure by exhaustion of parts, and a 32 gate fault tree for the temporary exhaustion of parts failure condition. The predicted reliability and bounds, using the parameters found in the references [4,7], are

Prob(Failure) = 4.12 x 10^-9
Upper Bound = 4.73 x 10^-9
Lower Bound = 3.83 x 10^-9

The theorems return an answer within 12 per cent using small models.

9. CONCLUDING REMARKS

This paper presents three results that simplify reliability prediction for a common class of systems. This class consists of systems that are assemblages of subsystems where each subsystem is a majority-voting threplex plus spares or majority-voting fourplex plus spares. The theorems are error bounds for model reduction and simplification. The material in this paper presents simple versions of these theorems. More refined versions with more scope and accuracy are being developed. The content of the theorems is illustrated by a small example and numerical comparisons. The power of the theorems is indicated by applying them to a large and complex system. For this system, the three theorems easily computed the probability of failure with tight bounds.

REFERENCES


BIOGRAPHY

Allan L. White received a Ph.D. in mathematics from New Mexico State University. He has taught at the University of Colorado. He was an applied mathematician at Kentron International, Inc. He is now at NASA Langley Research Center. His interests include the design and analysis of reliable process control systems.