Reliability Modeling of Hard Real-Time Systems

Hagbae Kim
Dept. of Elect. Eng.
Yonsei Univ.
Seoul, Korea

Allan L. White
Mail Stop 132
NASA LaRC
Hampton, VA 23681

Kang G. Shin
Real-Time Computing Lab.
Dept. of Elect. Eng. and Comput. Sci.
The Univ. of Michigan
Ann Arbor, MI 48109-2122

Abstract

A hard real-time control system, such as a fly-by-wire system, fails catastrophically (e.g., lose stability) if its control input is not updated by its digital controller computer within a certain time limit called the the hard deadline. To assess and validate system reliability by using a semi-Markov model that explicitly contains the deadline information, we propose a path-space approach deriving the upper and lower bounds of the probability of system failure. These bounds are derived by using only simple parameters, and they are especially suitable for highly-reliable systems which must recover quickly. Analytical bounds are derived for both exponential and Weibull failure distributions, which have proven effective through numerical examples, while considering three repair strategies: repair-as-good-as-new, repair-as-good-as-old, and repair-better-than-old.

1 Introduction

A "hard" real-time system is characterized by a stringent timing requirement, which should be met to avoid any catastrophe [7]. This timing information must, therefore, be accounted for when the reliability of a hard real-time system is modeled or measured. By embedding this timing information, the reliability of a hard real-time system can also handle temporary malfunctions caused, for example, by electromagnetic interference. One class of examples is real-time control systems where the dynamics of the controlled plant (aircraft, robot, or paper mill) keep the plant within a safe region if the controller malfunction does not last too long. In a real-time control system such as aircraft or satellite, the system should be directed by an appropriate controller computer in a timely manner; that is, its control input must be updated by the controller computer within a time limit called the *hard deadline* [6]. For safety-critical applications this has led to highly- redundant/reconfigurable controllers.

Most conventional reliability models assumed that the (perfect) controller must always be failure-free and must be in control of the underlying controlled plant. Previous reliability models have captured the details of such systems, and focused only on the states of fault-tolerant computers treating a temporary controller failure as a total system failure regardless of the requirements of the controlled plant [2, 10]. That is, they erred on the safe side by ignoring the "system inertia" or system resilience in tolerating temporary loss of the controller.

In contrast, in this paper the system failure is to be caused by a slow recovery taking more than the hard deadline that depends on the plant dynamics [6], where neither of the inter-arrival time of controller failures nor the recovery time is always exponentially-distributed and the failure rate depends on the holding time in the state of controller failure(s). Note that the failure rate is also dependent on the "global time" (the total operating time of the system) in more general systems.

There has been some previous work that considered the deadline information for reliability modeling. In [9], a Markov model, which not only describes component-failure behaviors but also incorporates deadline violations as simple transitions, was used to measure system reliability by deriving only the probability of missing a deadline, while needing another computation in a different 'lower-level' model. The authors of [3] considered non-failure-critical cases, where some system-down time can be tolerated if it is recovered within a certain deadline. They derived the mean value of the system lifetime and the cumulative

The work reported was supported in part by the Office of Naval Research (ONR) under Grant N00014-94-1-0229. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the view of the ONR.

operational time for the case of bounded repair time (restricted by the deadline). However, it is difficult to derive the distribution from the Laplace-Stieltjes transform of the system lifetime, although it is easy to compute the mean value. Hence, it is intractable to derive system reliability using these results. Moreover, none of these considered such general cases as when the time-to-failure and/or time-for-repair are not exponentially-distributed. Although these general cases were modeled by a time-non-homogeneous Markov chain [1], a semi-Markov process [4], or a Markov regenerative process [8], none of these dealt with the case when the failure rate depends on the total operation time of the system (implying that the model is not semi-Markov). These general models can be computed by the Monte Carlo method, but, since the Monte Carlo method is just a statistical estimation, it is computationally very expensive.

To overcome these obstacles, we consider a *path-space* approach which has proven useful in solving other reliability modeling problems [11, 12, 13]. Our goal is to derive tight upper and lower bounds for the probability of system failure in terms of two simple parameters: (i) the probability of k $(k > 0)$ interruptions during the operating period T, and (ii) the probability of successful recovery (before the hard deadline) given an interruption. For the first parameter, computing the probability of k events during a time period is straightforward, and there are analytical formulas for some of the more popular probability distributions [5]. For the second parameter, using the probability of successful recovery has three advantages: (i) it is mathematically more tractable than the density function for the recovery time that is required by the Chapman-Kolmogorov equations; (ii) it is experimentally and statistically less demanding to obtain the binomial parameters of failures than to do curve fitting for a density function; and (iii) it permits model reduction because it reduces complicated, multi-state recovery models to a single state with jump probabilities to successful recovery or unsuccessful recovery. Despite all of these simplifications, it will be shown by examples that this approach yields tight bounds for a wide variety of models. It is especially suitable for the stiff models of highly-reliable systems.

The recovery/repair procedure begins at the start of an interruption. There can be a time lag between the occurrence of an interruption and the beginning of the actual repair, but this time lag is included in the repair-time distribution. Hence, in the models recovery begins when the system enters a "down" state, often called the *recovery/repair state*. The probability distribution for the recovery time is also fixed for a given model. That is, it is assumed that recovery is either an automated procedure or done by a repair crew that does not become either more proficient or fatigued. These properties of the recovery/repair procedures imply that the time to recovery depends only on the time since entering the recovery/repair state. Hence, recovery/repair is a semi-Markov process for all the models described below, even if the distribution for system malfunction is dependent on the global time.

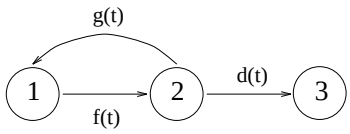

Figure 1: The semi-Markov model for hard deadlines

2 Semi-Markov Model for Hard Deadlines

This section first discusses the assumptions needed for a semi-Markov formulation of modeling the reliability of a hard real-time system, and presents a semi-Markov model and its Chapman-Kolmogorov equations. It then describes the path-space approach and derives the upper and lower bounds for the probability of system failure due to a lengthy interruption.

2.1 The semi-Markov formulation

We begin with a semi-Markov model. (A fixed deadline can be modeled as a semi-Markov transition with zero variance.) Later sections extend the result to models with global-time dependencies. The assumptions for the model are:

- Recovery is as-good-as-new,
- Recovery distribution depends on elapsed time since malfunction,
- Deadline is some fixed time, and
- All the processes (malfunction, recovery, and deadline) are independent of each other.

Let $f(t)$, $g(t)$, and $d(t)$ be the density function for the arrival of the malfunction, the density for recovery, and the density for the deadline, respectively. With the four assumptions above, the model is semi-Markov with three states as given in Fig. 1.

The first assumption is appropriate in case of either perfect replacements or the repair of high-quality equipment (such as electronic components) which has a constant, or nearly-constant, failure rate. Obviously, this assumption is the place to generalize the model in order to handle a wider variety of systems. This is done in later sections, but it requires global-time dependent models. The second assumption says that the repair procedure begins when a breakdown occurs, and that the repair-time distribution remains the same throughout the lifetime of the system. This is true for the automatic recovery of a redundant/reconfigurable electronic system. The assumption that the deadline is fixed is made for convenience, which can be extended for the random deadlines with minor modification. The fourth assumption reflects the fact that the processes (malfunction, recovery, and deadline) arise from different physical causes. Recovery depends on diagnostics and the repair algorithm (for automatic repair) or the repair policy (for a repair crew). The deadline depends on the external demands for the system.

To compute the probability of being in state 3 by time T given the system starts in state 1 at time 0. Chapman-Kolmogorov equations are:

$$P_{13}(t) = \int_0^t f(x)P_{23}(t-x)dx \qquad (2.1)$$

$$P_{23}(t) = \int_0^t g(x)\bar{D}(x)P_{13}(t-x)dx + \int_0^t d(x)\bar{G}(x)dx,$$

where $P_{ij}(t)$ is the probability of being in state j by time t given the system is in state i at time 0, and a bar above a distribution function indicates its complement. These equations require the density functions for system recovery which can be difficult to obtain.

2.2 The path-space approach

The path-space approach considers all possible ways of getting from the initial state to the absorbing state, unwinding the loop in the malfunction-recovery model and producing an infinite collection of paths from the initial state to system failure states to remove loops via structural patterns. The first three paths for the model in Section 2.1 appear in Fig. 2.

Each path is a disjoint event even though they share similar states. The probability of being in state 3 is the sum of the probabilities of traversing each of the paths. Hence, an upper bound for being in state 3 is the sum of the upper bounds for traversing each of the paths; similarly for the lower bound. Initially, the path-space approach appears more complicated,

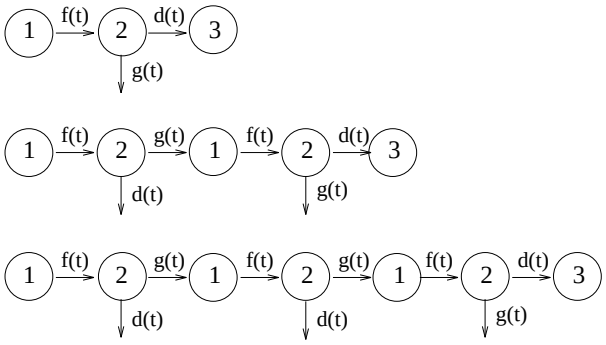

Figure 2: The first three paths for the hard deadline model

but the regular (and repetitive) structure of the paths lets one derive useful formulas. Before deriving the bounds, note that since the density d is for a fixed time of length τ, we can define the probabilities of successful and unsuccessful recoveries as

$$Q = \int_0^\infty g(x)\bar{D}(x)dx = \int_0^\tau g(x)\bar{D}(x)dx \qquad (2.2)$$

$$\bar{Q} = 1 - Q = \int_0^\infty d(x)\bar{G}(x)dx = \int_0^\tau d(x)\bar{G}(x)dx.$$

2.3 Derivation of the bounds

We now derive bounds for traversing the second path above. Derivation of the bounds for longer paths merely requires more bookkeeping. The probability of traversing the second path by time T is given by the convolution integral:

$$\int_0^T f(t_1)\int_0^{T-t_1} g(t_2)\bar{D}(t_2)\int_0^{T-t_1-t_2} f(t_3) * \int_0^{T-t_1-t_2-t_3} d(t_4)\bar{G}(t_4)dt_4dt_3dt_2dt_1$$
$$= \int_0^T f(t_1)\int_0^{T-t_1} f(t_2)\int_0^{T-t_1-t_2} g(t_3)\bar{D}(t_3) * \int_0^{T-t_1-t_2-t_3} d(t_4)\bar{G}(t_4)dt_4dt_3dt_2dt_1.$$

Adjusting the limits of integration gives an upper bound of

$$\int_0^T f(t_1)\int_0^{T-t_1} f(t_2)\int_0^\infty g(t_3)\bar{D}(t_3) * \int_0^\infty d(t_4)\bar{G}(t_4)dt_4dt_3dt_2dt_1$$
$$= \int_0^T f(t_1)\int_0^{T-t_1} f(t_2)Q\bar{Q}dt_4dt_3dt_2dt_1$$

and a lower bound of

$$\int_0^{T-2\tau} f(t_1) \int_0^{T-2\tau-t_1} f(t_2) \int_0^{\tau} g(t_3)\bar{D}(t_3) * \int_0^{\tau} d(t_4)\bar{G}(t_4)dt_4 dt_3 dt_2 dt_1 = \int_0^{T-2\tau} f(t_1) \int_0^{T-2\tau-t_1} f(t_2) Q\bar{Q} dt_4 dt_3 dt_2 dt_1 .$$

The two dimensional convolution integral that appears in both bounds is the probability that two or more events occur by time T.

For the general case, let $P\{n \geq k;\ T\}$ be the probability that k or more events have occurred by time T. An upper bound for being in state 3 of Fig. 1 by time T is

$$UB = \sum_{k=1}^{\infty} P\{n \geq k;\ T\} Q^{k-1}\bar{Q} \qquad (2.3)$$

and a lower bound is

$$LB = \sum_{k=1}^{\lfloor T/\tau \rfloor} P\{n \geq k;\ T - k\tau\} Q^{k-1}\bar{Q}. \qquad (2.4)$$

The upper limit of summation for the lower bound is the largest integer less than, or equal to, the quotient. These sums converge faster than a geometric series since $P\{n \geq k;\ T\} \leq [P\{n \geq 1;\ T\}]^k$.

2.4 Numerical examples

We now consider a variety of demonstrative examples: an assembly line where the reliability is moderate, an aircraft where the operating time is short and the reliability is high, and a satellite where the operating period is long and the reliability is fairly high. The parameter values are chosen to yield "stress" cases for the formulas (and may not reflect the ultimate in realism). Each example uses both an exponential density $f_1(t) = \lambda e^{-\lambda t}$ and a gamma density $f_2(t) = \alpha^2 t e^{-\alpha t}$ for the occurrences of malfunctions. For each example, the parameters are chosen so that the exponential and gamma distributions have the same mean, i.e., $\alpha = 2\lambda$. For the assembly line, the operating period is 1 day, the hard deadline is 15 minutes, the probability of successful recovery is 0.95, and the expected time to malfunction is 10 days. For the exponential distribution,

$$LB = 0.004931, \quad UB = 0.004988$$
$$Relative\ Error = (UB - LB)/UB = 0.01134,$$

and for the gamma distribution,

$$LB = 0.000879, \quad UB = 0.000862$$
$$Relative\ Error = (UB - LB)/UB = 0.01954.$$

For the aircraft with a highly-reliable redundant/reconfigurable controller, the operating time is 1 hour, the hard deadline is 1 second, the probability of recovery is 0.99, and the expected time to malfunction is 10^8 hours. For the exponential distribution,

$$LB = 5.00000 \times 10^{-10}, \quad UB = 4.99972 \times 10^{-10},$$
$$Relative\ Error = (UB - LB)/UB = 5.5525 \times 10^{-5},$$

and for the gamma distribution, $LB = 4.99600 \times 10^{-17}$, $UB = 4.99600 \times 10^{-17}$. This example demonstrates that the path-space approach with its upper and lower bounds is suitable for extremely stiff problems.

For the satellite with a long mission time and reliable controllers, let the operating time be 20,000 hours, the hard deadline be 30 minutes, the probability of successful recovery be 0.97, and the expected time to malfunction be 10^4 hours. For the exponential distribution,

$$LB = 0.058236, \quad UB = 0.058236,$$
$$Relative\ Error = (UB - LB)/UB = 7.5048 \times 10^{-7},$$

and for the gamma distribution,

$$LB = 0.051445, \quad UB = 0.051442,$$
$$Relative\ Error = (UB - LB)/UB = 6.8839 \times 10^{-5}.$$

2.5 An analytic upper bound for the exponential distribution

For an exponential distribution with a parameter λ, the probability of exactly k events in time T is $P_k = (\lambda T)^k e^{-\lambda T}/(k!)$. Hence, the upper bound

$$\sum_{k=1}^{\infty} P\{n \geq k;\ T\} Q^{k-1}\bar{Q}$$

can be displayed as the sum of $\bar{Q}$ times the rows

$$\begin{bmatrix} 1 & -P_0 & & & \\ Q & -QP_0 & -QP_1 & & \\ Q^2 & -Q^2P_0 & -Q^2P_1 & -Q^2P_2 & \\ Q^3 & -Q^3P_0 & -Q^3P_1 & -Q^3P_2 & -Q^3P_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}.$$

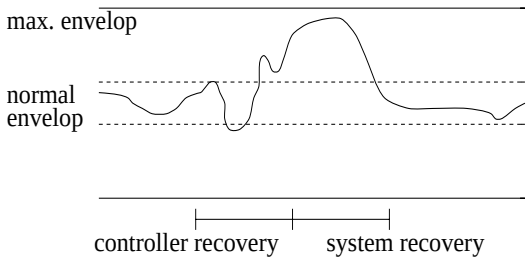

Figure 3: Control scenario with two envelops

Temporarily ignore the first column. The top diagonal is

$$-\sum_{i=0}^{\infty} Q^i P_i = -\sum_{i=0}^{\infty} \frac{Q^i(\lambda T)^i e^{-\lambda T}}{i!} = -e^{-\lambda T} e^{Q\lambda T}.$$

Each diagonal is Q times the diagonal above. Hence, the sum of all the diagonals is

$$-\sum_{j=0}^{\infty} Q^j [e^{-\lambda T} e^{Q\lambda T}] = -\frac{e^{-\lambda T} e^{Q\lambda T}}{1-Q}.$$

Adding the sum of the first column gives

$$\frac{1}{1-Q} - \frac{e^{-\lambda T} e^{Q\lambda T}}{1-Q}.$$

Multiplying by small $\bar{Q} = 1-Q$ gives an upper bound of $1-e^{-\lambda T\bar{Q}}$. Summing the terms in a different order gives the correct answer since the series converges absolutely.

2.6 A rough-and-ready upper bound

When $\lambda T\bar{Q}$ is small, an approximation to the analytic upper bound for the exponential is $1-e^{-\lambda T\bar{Q}} \leq \lambda T\bar{Q}$, which is $\bar{Q}$ times the expected number of events. In general, if Q is close to 1, the upper bound

$$\sum_{k=1}^{\infty} P\{n \geq k;\ T\} Q^{k-1}\bar{Q} \approx \bar{Q} \sum_{k=1}^{\infty} P\{n \geq k;\ T\}, \quad (2.5)$$

which, once again, is $\bar{Q}$ times the expected number of events.

2.7 A state aggregation example

The three state model in Fig. 1 is more general than it appears because of the technique of state aggregation in semi-Markov models. As an example, consider the control scenario where there is a normal operating envelop inside a safe operating envelop. This is illustrated in Fig. 3. In this scenario the system is vulnerable even after the controller has recovered because the system is close to the edge of its maximum safe envelop. A worst-case analysis assumes that the system needs the time for the controller to bring it within its normal operating envelop before it can survive another malfunction.

A simple approach considers two fixed time intervals: (i) the maximum time the controller should recover before the system leaves the outer envelop given it begins within the inner envelop, and (ii) the maximum time needed by the controller to bring the system within the inner envelop given the system is inside the outer envelop. Given these two time intervals, a semi-Markov model is displayed in Fig. 4, where state 2 is the controller-recovery state. The density h is a fixed time jump of length τ_1 representing the maximum time the controller should recover. The density u represents controller recovery. State 4 is the system-recovery state where the controller has recovered but the system is not yet back within its normal operating envelop. Using the worst-case analysis, another malfunction in state 4 (after the controller has recovered, but before it can bring the system back within the normal envelop) yields a system failure, and this is represented by the density function f. In state 4, the density function v is a fixed time jump of length τ_2 accounting for the maximum time required for system recovery (bringing the system back within its normal operating envelop). States 2 and 4 inside the dashed box will be combined into a single state. To begin this process, let

$$\begin{aligned} Q_1 &= \int_0^{\infty} u(t)\bar{H}(t)dt = \int_0^{\tau_1} u(t)\bar{H}(t)dt \\ Q_2 &= \int_0^{\infty} v(t)\bar{F}(t)dt = \int_0^{\tau_2} v(t)\bar{F}(t)dt, \end{aligned}$$

and let

$$G(t) = \int_0^t u(t_1)\bar{H}(t_1) \int_0^{t-t_1} v(t_2)\bar{F}(t_2)dt_2dt_1 = \int_0^t g(x)dx.$$

Then, Q is equal to $G(\infty)$, computed as follows:

$$\begin{aligned} &\int_0^{\infty} u(t_1)\bar{H}(t_1) \int_0^{\infty} v(t_2)\bar{F}(t_2)dt_2dt_1 \\ &\quad = \int_0^{\tau_1} u(t_1)\bar{H}(t_1) \int_0^{\tau_2} v(t_2)\bar{F}(t_2)dt_2dt_1 = Q_1Q_2 \\ &\quad = \int_0^{\tau_1} u(t_1)\bar{H}(t_1) \int_0^{\tau_2} v(t_2)\bar{F}(t_2)dt_2dt_1 + 0 + 0 \\ &\quad = \int_0^{\tau_1} u(t_1)\bar{H}(t_1) \int_0^{\tau_2} v(t_2)\bar{F}(t_2)dt_2dt_1 \\ &\quad + \int_{\tau_1^+}^{\tau_1+\tau_2} u(t_1)\bar{H}(t_1) \int_0^{\tau_1+\tau_2-t_1} v(t_2)\bar{F}(t_2)dt_2dt_1 \end{aligned}$$

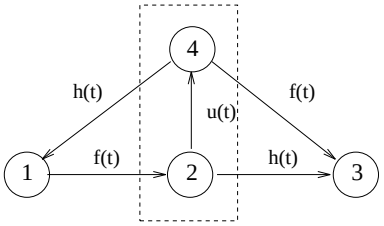

Figure 4: Semi-Markov model for a control scenario

$$+ \int_0^{\tau_1} u(t_1)\bar{H}(t_1) \int_{\tau_2^+}^{\tau_1+\tau_2-t_1} v(t_2)\bar{F}(t_2)dt_2dt_1$$
$$= \int_0^{\tau_1+\tau_2} u(t_1)\bar{H}(t_1) \int_0^{\tau_1+\tau_2-t_1} v(t_2)\bar{F}(t_2)dt_2dt_1$$
$$= G(\tau_1+\tau_2).$$

To continue the state aggregation process, let

$$D(t) = \int_0^t h(t_1)\bar{U}(t_1)dt_1 + \int_0^t u(t_1)\bar{H}(t_1) * \int_0^{t-t_1} f(t_2)\bar{V}(t_2)dt_2dt_1 = \int_0^t d(x)dx.$$

Likewise, it results in

$$D(\infty) = D(\tau_1+\tau_2) = 1-Q. \qquad (2.6)$$

Hence, the four state model in Fig. 3 can be reduced to the three-state model in Fig. 1 in a manner that preserves the parameters for the upper and lower bounds.

A general method for obtaining the probabilities and moments for state aggregation in semi-Markov models is developed in [12].

3 Global Time-Dependent Models

We now modify the assumption that repair is as-good-as-new. This introduces global-time dependent models which are beyond the reach of semi-Markov models, but can be similarly analyzed by path-space techniques. The first (and easier) case is as-good-as-old. It turns out that this assumption is well-suited to the Weibull distribution, and it is possible to derive an analytic upper bound. The general case is that repair is better-than-old. Repair induces conditional probability distributions as explained below. Several numerical examples are given.

3.1 Repair is as-good-as-old

The opposite of repair as-good-as-new is as-good-as-old. This is a reasonable approximation if the system under consideration consists of a large number of parts. Replacing one part as-good-as-new has little effect on the overall failure rate of the system. If the part is replaced not-as-good-as-new, then the approximation is even better. Furthermore, recovery may consist of a simple restart with no repair. The system is wearing out, which is less and less able to handle incoming perturbations. In this case repair as-good-as-old is an exact model. The assumptions for the model are:

- Recovery is as-good-as-old,
- System does not age during recovery,
- Recovery is semi-Markov (it depends only on the time since malfunction), and
- The hard deadline is fixed at τ.

It is assumed that the system does not age during recovery since it will not be operating while it is being repaired. If there is some use or wear-out during the repair time, then the assumption of no wear-out will be a close approximation because repair time is small compared to the lifetime of the system. Recovery is still assumed to begin when the system enters the malfunction state and to be an automatic procedure or a steady-state phenomenon as before. Hence, recovery is semi-Markov. A subtle point in the analysis is that repair as-good-as-old induces a conditional probability. After the repair, it is as if the failure had not happened. Hence, the probability of failure at some future time must be conditioned by the assumption that (immediately after repair) no failure has yet occurred (as far as the system can tell because it has been repaired as-good-as-old). Once again, consider a typical path from the initial state to the failure state. The probability of traversing this path by time T is given by the integral expression

$$\int_0^T f(t_1)\int_{t_1}^T g(t_2-t_1)\bar{D}(t_2-t_1)\int_{t_1}^{T-(t_2-t_1)} \frac{f(t_3)}{1-F(t_1)} * \int_{t_3}^{T-(t_2-t_1)} d(t_4-t_3)\bar{G}(t_4-t_3)dt_4dt_3dt_2dt_1.$$

The first integral gives the occurrence of the first malfunction. The second integral has a lower limit of t_1, because the expression must track the global-time. Since recovery is a semi-Markov process, the functions in the second integral are adjusted to begin at (their) time equal to zero. The lower limit for the third integral is t_1 because there is no system wear-out during recovery. The upper limit is correspondingly decremented by the time spent in recovery. The integrand

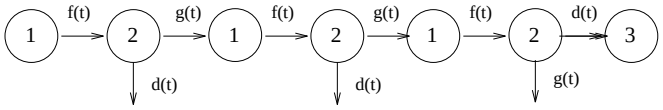

Figure 5: A typical path form the initial state to failure

in the third integral is the conditional density function. The fourth integral describes the semi-Markov transition to the failure state.

3.2 The upper and lower bounds for repair-as-good-as-old

As the first step the upper limit for the third integral can be changed into T. If this is done, the third integral does not depend on the parameter t_2, which means the order of integration can be changed to:

$$\int_0^T f(t_1)\int_{t_1}^T \frac{f(t_3)}{1-F(t_1)}\int_{t_1}^T g(t_2-t_1)\bar{D}(t_2-t_1) * \int_{t_3}^{T-(t_2-t_1)} d(t_4-t_3)\bar{G}(t_4-t_3)dt_4dt_3dt_2dt_1.$$

Using the above equation, the lower bound is successively obtained by giving the semi-Markov transition time τ to occur. Beginning with the last semi-Markov transition on the path, the original expression is greater than, or equal to

$$\int_0^{T-\tau} f(t_1)\int_{t_1}^{T-\tau} g(t_2-t_1)\bar{D}(t_2-t_1)\int_{t_1}^{T-\tau-(t_2-t_1)} \frac{f(t_3)}{1-F(t_1)}\int_{t_3}^{t_3+\tau} d(t_4-t_3)\bar{G}(t_4-t_3)dt_4dt_3dt_2dt_1.$$

Adjusting for the first semi-Markov transition, the expression above is greater than, or equal to

$$\int_0^{T-2\tau} f(t_1)\int_{t_1}^{t_1+\tau} g(t_2-t_1)\bar{D}(t_2-t_1)\int_{t_1}^{T-\tau-(t_2-t_1)} \frac{f(t_3)}{1-F(t_1)}\int_{t_3}^{t_3+\tau} d(t_4-t_3)\bar{G}(t_4-t_3)dt_4dt_3dt_2dt_1.$$

Since $t_1 \le t_2 \le t_1+\tau$, we have $T-\tau-(t_2-t_1) \ge T-2\tau$. Making this replacement for the upper limit of the third integral decreases the numerical value of the expression. This replacement also eliminates the dependence of the third integral on t_2. Hence, the last expression is greater than, or equal to

$$\int_0^{T-2\tau} f(t_1)\int_{t_1}^{T-2\tau} \frac{f(t_3)}{1-F(t_1)}\int_0^{\tau} g(t_2)\bar{D}(t_2)\int_0^{\tau} d(t_4)\bar{G}(t_4)dt_4dt_3dt_2dt_1 = \int_0^{T-2\tau} f(t_1)\int_{t_1}^{T-2\tau} \frac{f(t_3)}{1-F(t_1)}dt_3dt_1\, Q\bar{Q}.$$

The bounds for all the paths are similar to the bounds for the path of length four. The derivations just require more bookkeeping. Hence, once again, an upper bound for system failure is

$$\sum_{k=1}^{\infty} P\{n \ge k;\ T\}Q^{k-1}\bar{Q}, \tag{3.1}$$

and a lower bound is

$$\sum_{k=1}^{\lfloor T/\tau \rfloor} P\{n \ge k;\ T-k\tau\}Q^{k-1}\bar{Q}, \tag{3.2}$$

where $\sum_{k=1}^{\infty} P\{n \ge k;\ T\}$ is the probability of k or more events given recovery-as-good-as-old.

3.3 The Weibull distribution

We use the Weibull density in the form $f(t) = \alpha\lambda t^{\alpha-1}e^{-\lambda t^{\alpha}}$. The first result for the Weibull is that with repair-as-good-as-old, the probability of exactly k events by time T is

$$\frac{(-\lambda t^{\alpha})^k e^{-\lambda t^{\alpha}}}{k!}.$$

To derive this formula, the integral expression for exactly k events is

$$\int_0^T f(t_1)\int_{t_1}^T \frac{f(t_2)}{1-F(t_1)}\cdots\int_{t_{k-1}}^T \frac{f(t_k)}{1-F(t_{k-1})}\int_T^{\infty}\frac{f(t_{k+1})}{1-F(t_k)}dt_k\cdots dt_1 = \int_0^T \alpha\lambda t_1^{\alpha-1}\int_{t_1}^T \alpha\lambda t_2^{\alpha-1}\cdots\int_{t_{k-1}}^T \alpha\lambda t_k^{\alpha-1}\int_T^{\infty}\alpha\lambda t_{k+1}^{\alpha-1}e^{-\lambda t_{k+1}^{\alpha}}dt_k\cdots dt_1$$
$$= \lambda^k e^{-\lambda T^{\alpha}}\int_0^T \alpha t_1^{\alpha-1}\int_{t_1}^T \alpha t_2^{\alpha-1}\cdots\int_{t_{k-1}}^T \alpha t_k^{\alpha-1}dt_k\cdots dt_1.$$

$(\times 10^{-2})$	$\alpha = 0.5$	$\alpha = 1.5$	$\alpha = 2.0$
UB	0.2237	1.1118	2.4689
LB	0.2230	1.1112	2.4680
Rel Error	0.149	0.0513	0.0376

Table 1: Upper and lower bounds for various α when $\tau = 1$ day and $G(\tau) = 0.99$

	$\alpha = 0.5$	$\alpha = 1.5$	$\alpha = 2.0$
UB	0.03658	0.17001	0.34057
LB	0.03657	0.17000	0.34056
Rel Error	1.3×10^{-4}	4.97×10^{-5}	3.45×10^{-5}

Table 2: Upper and lower bounds for various α when $\tau = 2$ hours and $G(\tau) = 0.90$

An induction argument yields

$$\lambda^k e^{-\lambda T^\alpha} \frac{(T^\alpha)^k}{k!}. \tag{3.3}$$

Using this expression for exactly k events and the techniques of Section 2, an analytic upper bound for the Weibull distribution is $1 - e^{-\lambda T^\alpha}$. The expected number of events in time T (which is used in the rough-and-ready upper bound) is λT^α.

3.4 Examples for repair-as-good-as-old

Consider an industrial process with Weibull failure density $f(t) = \alpha\lambda t^{\alpha-1} e^{-\lambda t^\alpha}$. If the process uses machinery, it is likely that the failure rate is increasing ($\alpha > 1$). If the process uses software, it is likely that the failure rate is decreasing because of program improvements ($\alpha < 1$). Suppose the process has a lifetime of five years. Let $\lambda = 1/6$ per year. (If α were equal to one, this would give an expected time to malfunction of two months.)

Suppose the hard deadline is 1 day and the probability of recovery is 0.99. The results for various α values are given in Table 1. Assuming the hard deadline is 2 hours and the probability of recovery is 0.90, Table 2 describes the cases for various α.

3.5 Repair is better-than-old

In this scenario, recovery includes partial restoration. The system is possibly better-than-old but not necessarily as-good-as-new. If the i-th incident occurs at time t_i, then after recovery the system is as good as it was at time $r_i t_i$, where $0 \le r_i \le 1$. The r_i's need not be equal for different i's. We continue to model recovery as a semi-Markov process. Once again, for the path of length four, the integral expression is

$$\int_0^T f(t_1) \int_{t_1}^T g(t_2 - t_1)\bar{D}(t_2 - t_1) * \int_{r_1 t_1}^{T-(t_2-t_1)-(t_1-r_1 t_1)} \frac{f(t_3)}{1 - F(r_1 t_1)} * \int_{t_3}^{T-(t_2-t_1)-(t_1-r_1 t_1)} d(t_4 - t_3)\bar{G}(t_4 - t_3) dt_4 dt_3 dt_2 dt_1.$$

As before, the upper and lower bounds are based on inclusion for the sets of integration. Consider the three sets determined by the inequalities:

$$A: \begin{cases} 0 \le t_1 \le T \\ t_1 \le t_2 \le T \\ r_1 t_1 \le t_3 \le T - (t_2 - t_1) - (t_1 - r_1 t_1), \\ t_3 \le t_4 \le T - (t_2 - t_1) - (t_1 - r_1 t_1) \end{cases}$$

$$B: \begin{cases} 0 \le t_1 \le T \\ 0 \le t_2 - t_1 \le \infty \\ r_1 t_1 \le t_3 \le T - (t_1 - r_1 t_1) \\ 0 \le t_4 - t_3 \le \infty \end{cases}$$

$$C: \begin{cases} 0 \le t_1 \le T - 2\delta \\ 0 \le t_2 - t_1 \le \delta \\ r_1 t_1 \le t_3 \le T - 2\delta(t_1 - r_1 t_1) \\ 0 \le t_4 - t_3 \le \delta, \end{cases}$$

where δ is the hard deadline. It can be shown that $C \subseteq A \subseteq B$, establishing the associated upper bound

$$\int_0^T f(t_1) \int_{r_1 t_1}^{T-(t_1-r_1 t_1)} \frac{f(t_3)}{1 - F(r_1 t_1)} \int_0^\infty g(t_2)\bar{D}(t_2) * \int_0^\infty d(t_4)\bar{G}(t_4) dt_4 dt_3 dt_2 dt_1,$$

and lower bound

$$\int_0^{T-2\delta} f(t_1) \int_{r_1 t_1}^{T-2\delta-(t_1-r_1 t_1)} \frac{f(t_3)}{1 - F(r_1 t_1)} \int_0^\delta g(t_2)\bar{D}(t_2) * \int_0^\delta d(t_4)\bar{G}(t_4) dt_4 dt_3 dt_2 dt_1$$

for the original integral expression.

The bounds for paths of other lengths are handled similarly. Computing the bounds is straightforward using numerical routines for multiple integrals.

3.6 Example for repair-better-than-old

Let the failure density function be $f(t) = \alpha\lambda t^{\alpha-1} e^{-\lambda t^\alpha}$ where $\lambda = 0.01$ and $\alpha = 1.5$, and let

the operating time T be 5 years. Suppose (i) the recovery period is 1 day, (ii) there is a 99% chance of successful recovery, and (iii) the repair is progressively less effective with $r_i = 1-(1/2)^i$. The upper and lower bounds, then, are

$$UB = 0.001105953 \quad \text{and} \quad LB = 0.001104978$$

with the relative error of $(UB - LB)/UB = 8.816 \times 10^{-4}$.

4 Random Hard Deadlines

The hard deadline can be thought of as the maximum controller "think time," which may depend on the time needed to "actuate" the plant. This actuation time is a random variable due to, for example, random environmental perturbations like wind gusts in case of the plant being an aircraft. (See [9] for detailed examples showing that the hard deadline is a random variable.) As another example, let's consider a relay station where messages arrive and are instantly retransmitted. The station is subjected to random down-times due to perturbations (power outages, external noises, or equipment malfunctions). If the perturbation and its effects are not removed before the next message arrives (at some random time), then the station will suffer a system failure.

The case of random deadlines uses the same mathematical formulation as the case of fixed deadlines. We carry out the analysis in terms of repair-better-than-old because this case includes both as-good-as-new and as-good-as-old. Repair-as-good-as-new is recovered by letting the r_i's equal zero, while repair-as-good-as-old is recovered by letting them equal one. As before, the integral for traversing the path of length four by time T is

$$\int_0^T f(t_1) \int_{t_1}^T g(t_2 - t_1)\bar{D}(t_2 - t_1) * \int_{r_1 t_1}^{T-(t_2-t_1)-(t_1-r_1 t_1)} \frac{f(t_3)}{1 - F(r_1 t_1)} * \int_{t_3}^{T-(t_2-t_1)-(t_1-r_1 t_1)} d(t_4 - t_3)\bar{G}(t_4 - t_3)dt_4 dt_3 dt_2 dt_1.$$

The upper and lower bounds

$$\int_0^T f(t_1) \int_{r_1 t_1}^{T-(t_1-r_1 t_1)} \frac{f(t_3)}{1 - F(r_1 t_1)} \int_0^\infty g(t_2)\bar{D}(t_2) * \int_0^\infty d(t_4)\bar{G}(t_4)dt_4 dt_3 dt_2 dt_1$$

and

$$\int_0^{T-2\delta} f(t_1) \int_{r_1 t_1}^{T-2\delta-(t_1-r_1 t_1)} \frac{f(t_3)}{1 - F(r_1 t_1)} \int_0^\delta g(t_2)\bar{D}(t_2) * \int_0^\delta d(t_4)\bar{G}(t_4)dt_4 dt_3 dt_2 dt_1$$

are obtained by merely adjusting the set over which the integral is taken. The fact that δ is a fixed deadline does not play any role in establishing that the last two integrals bound the original. The upper bound does not depend on δ. For the lower bound the choice of δ depends on making a tradeoff. Using the equation for a path of length four as an example, the factor for the occurrence of two or more perturbations

$$\int_0^{T-2\delta} f(t_1) \int_{r_1 t_1}^{T-2\delta-(t_1-r_1 t_1)} \frac{f(t_3)}{1 - F(r_1 t_1)} dt_3 dt_1$$

decreases as δ increases, while the factor for recovery or failure

$$\int_0^\delta g(t_2)\bar{D}(t_2) \int_0^\delta d(t_4)\bar{G}(t_4)dt_4 dt_2$$

increases as δ increases.

One consequence of this approach is that the formulas for the upper and lower bounds use different Q and $\bar{Q}$. The upper bound is

$$\sum_{k=1}^{\infty} P[n \geq k;\ T] Q_U^{k-1} \bar{Q}_U, \tag{4.1}$$

where Q_U and $\bar{Q}_U$ are computed by integrating from zero to infinity. The lower bound is

$$\sum_{k=1}^{\lfloor T/\tau \rfloor} P[n \geq k;\ T - k\tau] Q_L^{k-1} \bar{Q}_L, \tag{4.2}$$

where Q_U and $\bar{Q}_U$ are computed by integrating from zero to some δ.

5 On Tightness of Bounds

We have obtained tight bounds with a simple procedure by taking advantage of the features of the problem that (at first) appear to create computational problems. These features are: (i) the systems are highly reliable which means the probability of failure is a small number that must be computed accurately; (ii) recovery rates are fast compared to the component failure rates which yields a stiff numerical problem;

and (iii) recovery can be an extremely complex procedure the response is as follows. First, since the system must be extremely reliable it uses components with low failure rates, which means the series (for the upper and lower bounds) converge rapidly. Second, the major difference between the upper and lower bound terms is that the probabilities for the lower bound must be computed over intervals decremented by repair time. Since repair is fast, this introduces only a small inaccuracy. Third, since repair is fast, the details of the repair procedure (the density function)is unimportant. The probabilities of repair success or failure appear to be sufficient. We expect the bounds to diverge if these conditions are violated. On the other hand, if these conditions are violated, we expect a less reliable system whose reliability computation is not as critical.

6 Conclusion

This paper proposes a path-space approach to the problem of modeling the reliability of hard real-time systems embedded with the deadline information. The path-space approach in combination with the repetitive nature of the semi-Markov model yields convenient formulas and straightforward computational techniques. The main results are the upper and lower bounds for the probability of system failure that use only simple parameters dealing with complicated models through a simple canonical form for analysis. An important feature of the path-space approach is that it can be extended to handle global-time dependent failure distributions, which are beyond the reach of semi-Markov models and the associated Chapman-Kolmogorov equations. We considered a spectrum of repair strategies: repair-as-good-as-new, repair-as-good-as-old, and the general repair-better-than-old, where both deterministic and random hard deadlines are considered as well. A variety of examples are presented to demonstrate the effectiveness of the path-space approach. Because of the reliance on only simple parameters and the ease of reducing semi-Markov models, this approach is suitable for very complex models.

References

[1] R. Geist, M. Smotherman, J. Dugan, and K. Trivedi, "Hybrid reliability modeling for fault-tolerant computer systems," *Computers and Lectrical Engineering*, vol. 11, no. 2, pp. 87–108, 1984.

[2] R. M. Geist and K. S. Trivedi, "Ultrahigh reliability prediction for fault–tolerant computer systems," *IEEE Trans. on Computer.*, vol. C-32, no. 12, pp. 1118–1127, December 1983.

[3] A. Goyal, V. Nocola, A. N. Tantawi, and K. S. Trividi, "Reliability of systems with limited repairs," *IEEE Trans. on Reliability*, vol. R-36, no. 2, pp. 202–207, June 1987.

[4] P. Haase and G. Shedler, "Stochstic petri net representation of discrete event simulations," *IEEE Trans. on Soft. Eng.*, vol. 15, no. 4, , April 1989.

[5] S. Karlin and H. Taylor, *A first course in stochastic processes*, Academic Press, New York, 1975.

[6] H. Kim and K. G. Shin, "On the maximum feedback delay in a linear/nonlinear control system with input disturbances caused by controller-computer failures," *IEEE Trans. on Control Systems Technology*, vol. 2, no. 2, pp. 110–122, June 1994.

[7] C. M. Krishna and K. G. Shin, *Real-Time Systems*, McGraw-Hill Companies, New York, 1997.

[8] V. G. Kulkarni, *Modeling and Analysis of Stochastic Systems*, Chapman Hall, 1995.

[9] K. G. Shin and C. Krishna, "New performance measures for design and evaluation of real-time multiprocessors," *Int'l J. Computer Science & Engineering*, vol. 1, no. 4, pp. 179–191, October 1986.

[10] A. K. Somani and T. R. Sarnaik, "Reliability analysis techniques for complex multiple fault-tolerant computer architectures," *IEEE Trans. on Reliability*, vol. 39, no. 5, pp. 547–556, December 1990.

[11] A. L. White, "Reliability estimation for reconfigurable systems with fast recovery," *Microelectron. Reliab.*, vol. 26, no. 6, , 1986.

[12] A. L. White, "Simplifying semi-markov fault recovery models," in *Proc. 11st IEEE/AIAA Digital Avionics Systems Conf.*, 1992.

[13] A. L. White, "Reliability prediction for a class of highly reliable digital systems," *Advanced in ultra-dependable distributed systems*, vol. edited by N. Suri, C. Walter, and M. Hugue, no. IEEE Computer Society, 1995.