Aerospace Applications of Weibull and Monte Carlo Simulation with Importance Sampling

Salvatore J. Bavuso; NASA; Hampton

Key Words: Weibull, Reliability, Monte Carlo, simulation, importance sampling, HARP (Hybrid Automated Reliability Prediction), Fault tree, HIRel (HARP integrated Reliability tool system)

Abstract/Summary

Recent developments in reliability modeling and computer technology have made it practical to use the Weibull time to failure distribution to model the system reliability of complex fault-tolerant computer-based systems. These system models are becoming increasingly popular in space systems applications as a result of mounting data that support the decreasing Weibull failure distribution and the expectation of increased system reliability. This presentation introduces the new reliability modeling developments and demonstrates their application to a novel space system application. The application is a proposed guidance, navigation, and control (GN&C) system for use in a long duration manned spacecraft for a possible Mars mission. Comparisons to the constant failure rate model are presented and the ramifications of doing so are discussed.

The combination of modeling spacecraft systems with the Weibull time to failure distribution and the modeling of cold or warm spares to reflect reduced power usage presents the reliability modeler with a very difficult mathematical model to evaluate. Such reliability models are non-Markovian because the model requires multiple clocks. One keeps track of component failures whose clock starts at the initiation of the mission and the others start when cold or warm Weibull spares are fully powered, i.e., when switched on. The general mathematical model which describes these systems is given by the Chapman-Kolmogorov equations.

Presently, the most general solution methodology for such models is the Monte Carlo simulation method. Although very powerful and general, the Monte Carlo simulation method has not been used for highly reliable or long duration systems because of the enormous computer resources required to evaluate these models. Two recent developments have mitigated this shortcoming: The most obvious is the availability of fast and inexpensive microcomputer systems whose computational speed is ever increasing and whose cost is increasing less proportionally. The second development which is less known is the probabilistic modeling technique called importance sampling. Although this technique has been available for at least two decades, its use has been limited. Importance sampling is a variance reduction technique. This technique allows the efficient sampling of failure events that have very long mean times to failure and reduces the spread (variance) of predicted system failure events; thus giving greater confidence for the predicted mean value (system reliability). The increased sampling efficiency reduces computational time and cost and increases the precision of the computed results.

Importance sampling requires the user to specify certain biasing values. In the general application of importance sampling, the best assignment of these biasing values is difficult to derive, and the success of the technique hinges critically on the correct choice. This problem has been an important factor in limiting the use of importance sampling. The Monte Carlo integrated Hybrid Automated Reliability Program (MCI-HARP) has sidestepped this difficulty by requiring a specific system model. The system model is always a Markov chain without repair. The Markov chain can more

generally be semi-Markov with non-constant failure rates. Because Markov chain models can be huge and difficult to specify, MCI-HARP uses the fault tree notation instead. Moreover, the fault tree notation includes order dependent gates to increase the modeling flexibility and power. This notation is completely compatible with HARP; so for fault tree models that HARP can solve, MCI-HARP can also solve them. The dualism of solution techniques can be useful for verification of the model solution.

The Monte Carlo simulation offers one other important feature necessary for modeling today's complex systems that often involve order dependent failures. Because the technique searches through the fault tree to determine the system state, it is unnecessary to store the system transition matrix in memory. The number of elements in the transition matrix is given by 2^{2N} for N system components; and even with sparse matrix techniques, analytical solutions quickly become limited by computer memory resources for modest to large system models. The HARP program has this limitation which it attempts to minimize by using a number of approximation techniques including truncation-bounding and behavioral decomposition.

MCI-HARP has made it practical to model some complex systems and produce results which at first appear to be counter intuitive. When President Bush proposed that NASA should direct its attention toward a manned mission to Mars, some of us at NASA's Langley Research Center explored the feasibility of state-of-the-art (SOA) fault-tolerant guidance, navigation, and control (GN&C) systems being reliable enough for such a mission. Using SOA constant failure rate data, we concluded that the reliability of the GN&C would be too low to justify such a mission. Although, I was aware at the time of the mounting data to support the use of Weibull decreasing failure rates in spacecraft systems, I had no practical way to model such systems with cold or warm spares. Intuitively I believed that decreasing failure rates and warm spares would increase the predicted system reliability, but whether or not enough reliability gain could be attained was beyond my computational reach. The HARP program is capable of correctly modeling Weibull decreasing failure rates with or without hot spares but not with warm or cold spares.

By the end of 1990, a prototype Monte Carlo HARP was developed by researchers at Northwestern University under the leadership of E.E. Lewis. The idea of structuring the simulation based on the Markov chain was first presented to me by Robert Geist at Clemson University. Under grant to NASA Langley, Northwestern implemented this concept using the HARP program's fault/error-handling models. Mark Boyd (a HARP codeveloper now at NASA's Ames Research Center) further integrated the Monte Carlo simulator with HARP's fault tree notation, and I later reengineered the entire program to be consistent with HARP (now called Monte Carlo integrated HARP, i.e., MCI-HARP). With a working program on hand, Boyd and I used MCI-HARP to explore the effects of decreasing failure rates with warm and cold spares on a Jet Propulsion Laboratory's proposed GN&C system, a 3-dimensional hypercube fault-tolerant system. The details of the study can be found in the 1993 RAMS proceedings; however, some of the results are worth mentioning here.

Although the study examined the system reliability for missions times of 1 to 10 years, 10 years was considered the target mission time. An acceptable GN&C unreliability for a 10 year mission was specified to be less than 50%, i.e., a reliability greater than or equal to 50%. When all components were assigned constant failures rates (CFR) and all spares were hot, the system unreliability was computed to be 63%, confirming our previous studies which also predicted an unacceptable unreliability. Using decreasing failure rates (DFR) with hot spares and a conservative shape value of 0.5, a three orders of magnitude improvement was computed with an unreliability of 0.078%, clearly demonstrating the beneficial effect of DFRs. That's not to say that such an improvement can actually be obtained. The important point to note here is the potential for reliability gain when using DFRs. Actual gains will depend on the accuracy of the DFR data. In this study, we assumed the initial instantaneous failure rate was equal to a component's CFR; thus the instantaneous failure rate of the DFR will always be lower than the CFR after the initial mission time. Whether or not this assumption is reasonable, is yet to be determined.

When the spares are allowed to be cold, the CFR model produced an unreliability of 57%, about a 10% improvement over the hot CFR spare model, an expected trend but still unacceptable. This outcome is expected because, hot spares can fail before they can be used to replace failed operational components; where as

cold spares cannot fail until they are powered up. By comparison, the cold spare DFR model produced an unreliability of 0.079% , about a 1% improvement over the hot spare DFR model, and this small improvement was not expected. The implication is that there is little to gain by using cold DFR spares from a reliability point of view. In fact, some of our results (see RAMS proceedings 1993) have shown that cold DFRs produce a higher unreliability than with hot DFRs. If power conservation is not a design factor, these results suggest that DFR spares should be powered up throughout the mission in order to enhance fault detection (not addressed in these reported results). These results make even a stronger argument for using hot DFR spares if the shape value is less than 0.5 as suggested by Hecht at Sohar INC.

Why do these results run counter to one's intuition? In the CFR cold spare model, a spare is mathematically considered to be brand new on switch-in **with the same failure rate** as the hot spares. With DFR spares, the cold DFR spare is also considered to be brand new, but its instantaneous failure rate at switch-in is at its maximum while the hot operating components (including hot operational spares) have lower instantaneous failure rates. Another interesting observation results from this study - although using cold CFR spares are not physically realistic, models using them produce an optimistic reliability prediction - the best possible reliability prediction. This property, however, does not apply to cold DFR spare models because the instantaneous failure rate of a warm spare will be less than that of a cold DFR spare when it becomes operational.

One concludes from these studies that DFR models predict substantially greater reliability than do CFR models and that the use of Monte Carlo simulation with importance sampling makes it possible to examine these trade-offs. Moreover, the reliability analyst must be mindful of the counter intuitive properties of DFR models and attempt to model such systems with warm spares in lieu of cold spare models to obtain accurate predictions.

With recent renewed interest in a manned mission to Mars, proposed GN&C systems for this type of application should include DFR models, and capabilities like MCI-HARP will make the reliability evaluation practical and meaningful.

Salvatore J. Bavuso

WORK: NASA Langley Research Center
MS 130
Hampton, VA 23681-0001, USA
(757) 864-6189
FAX: (757) 864-4234

Salvatore J. Bavuso is a senior researcher at NASA Langley Research Center in Hampton, Virginia. He received the BS degree in mathematics from the Florida State University in 1964 and the MS degree in applied mathematics from the North Carolina State University at Raleigh in 1971. He has been instrumental in the development of advanced reliability modeling technology for over two decades. He was the NASA project manager for and a codeveloper of the HiRel, HARP, and CARE III programs.

Aerospace Applications of Weibull and Monte Carlo Simulation with Importance Sampling

Salvatore J. Bavuso; NASA; Hampton

Monte Carlo Simulation

General modeling technique applies to modeling notations:

- Reliability Block Diagrams
- Fault trees
- Markov chains

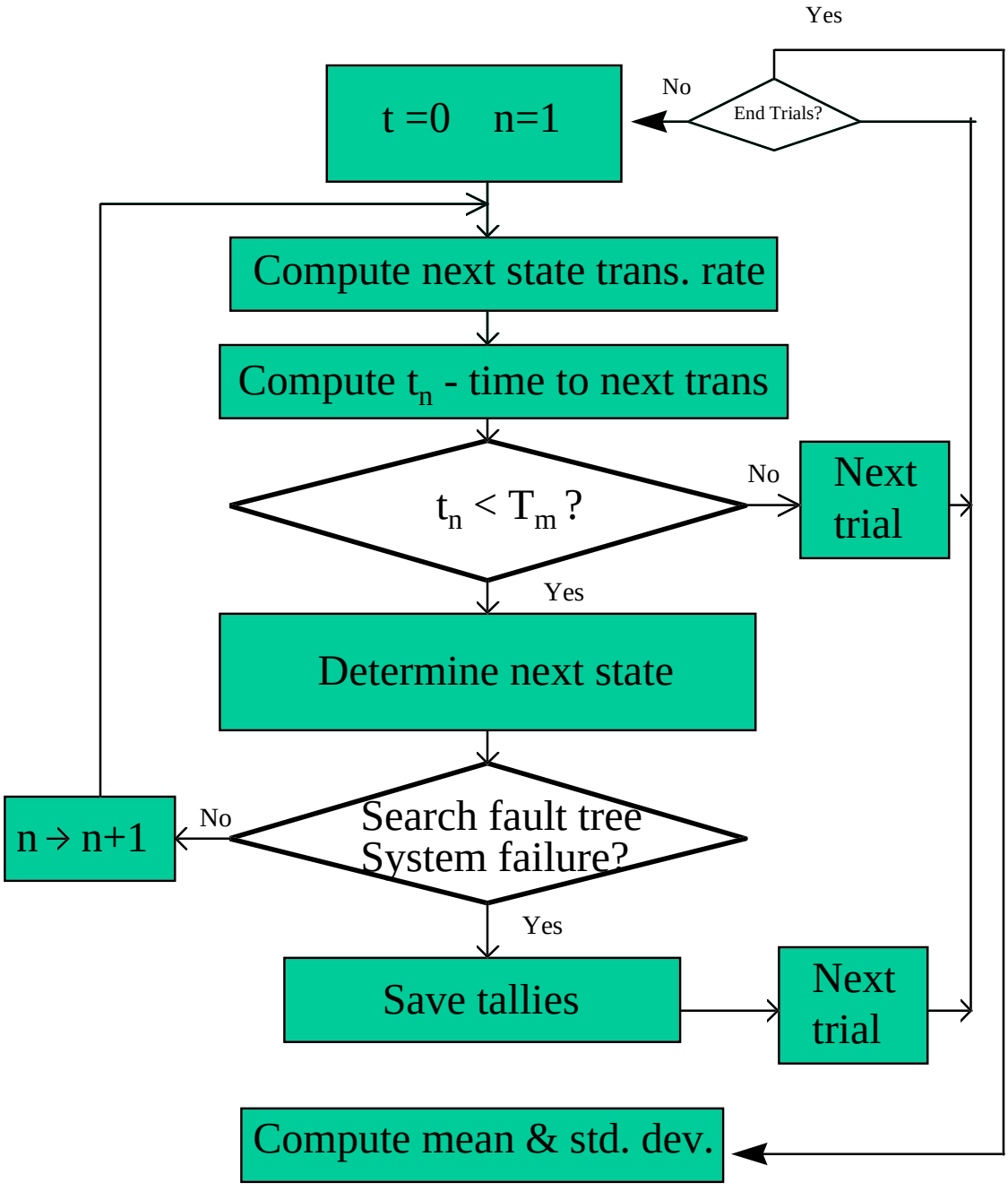
Allows:

- Order dependency
- Time varying lambdas
- Hot, cold, & warm spares with above

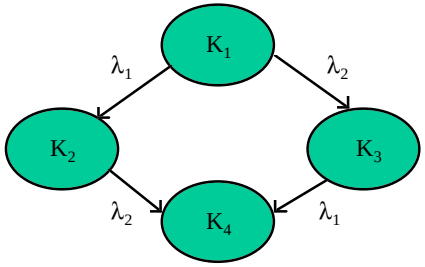
Fault tree notation most used:

- Flexible
- Compact

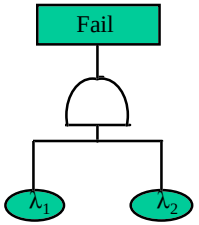
Monte Carlo Algorithm



Markov chain

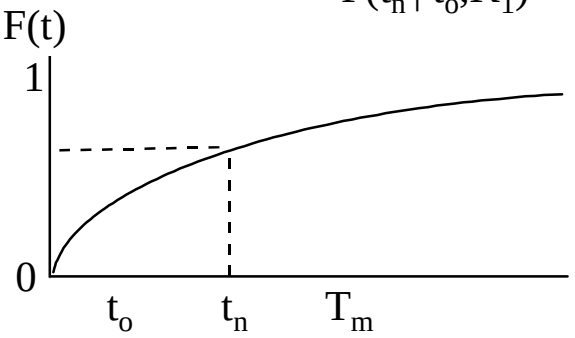


Fault tree



State transition rate => $Y_{K_1} = \lambda_1 + \lambda_2$

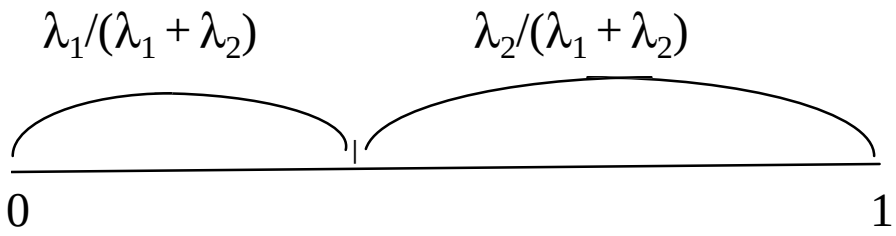
State CDF => $F(t_n \mid t_o, K_1) = 1 - e^{-Y_{K1}(tn - to)}$



Transition time to leave state K_1 : $t_n = t_o - (1/Y_{K_1})\mathrm{Ln}(1 - \zeta)$

Determine which comp. failed:

Divide unit interval into sub-intervals proportional to operational comp. & use random number to pick an interval corresponding to failed comp.



When $\lambda_1 < \lambda_2$

$\hat{\xi} < \lambda_1/(\lambda_1 + \lambda_2)$ => λ_1 caused failure

else λ_2 caused failure

Determine if System Failure:

- •Traverse F.T. with depth first search.
- •If top event occurs, start new history & drop tally in bucket

Else

- •Continue sampling from new state Ki using

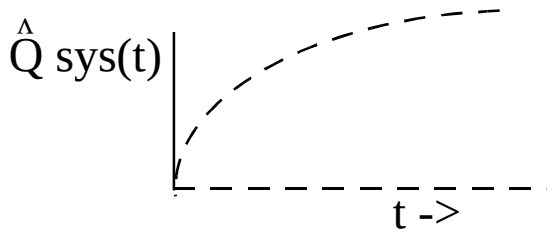
$t_n \Rightarrow t_o$

$t_n = t_o - (1/Y_{ki})\mathrm{Ln}(1 - \zeta)$

History end if $t_n >= T_m$ irrespective of failures remaining

System failure occurs - top event of F.T. occurs

$\hat{Q}$ sys(t) = $\Sigma N_f / N_H$ -> for point estimate



Highly Reliable Systems cause Monte Carlo simulations problems

$$t_n = t_o - (1/Y_{K_i})\mathrm{Ln}(1 - \zeta)$$

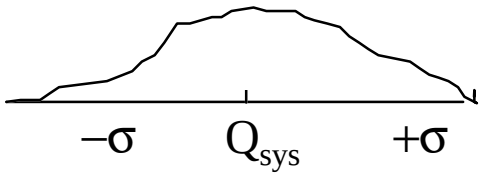
$$Y_{K_i} <<< 1 \quad => \quad - (1/Y_{K_i})\mathrm{Ln}(1 - \zeta) \quad >> \quad T_m$$

$$\text{So} \qquad t_n >> T_m$$

Means:

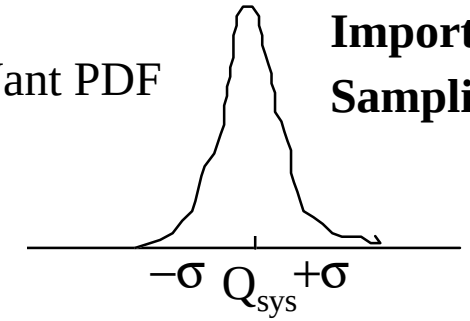
* most trials will be dropped & not contribute
* very wide variance

Get PDF



Want PDF

Importance Sampling



An Importance Sampling Technique

From state CDF : $F(t_n \mid t_o, K_i) = 1 - e^{-Y_{Ki}(tn - to)}$

Define new CDF:

$$\bar{F}(t_n \mid t_o, K_i) = F(t_n \mid t_o, K_i) / F(T_m \mid t_o, K_i)$$

$$= \{1 - e^{-Y_{Ki}(tn - to)}\} / \{1 - e^{-Y_{Ki}(Tm - to)}\}$$

Let $\bar{F}(t_n \mid t_o, K_i) = \bar{\zeta}$ and solve for t_n

$$t_n = t_o - (1/Y_{K_i}) \mathrm{Ln}\{1 - \bar{\zeta}[1 - e^{-Y_{Ki}(Tm - to)}]\}$$

****** $t_o < t_n < T_m$ ******

Unbias tallies with weight w_i for each trial i

where $w_i = 1$ initially

$$w_{i+1} \rightarrow w_i [1 - e^{- Y_{Ki}(Tm - to)}]$$

$$Q_{sys} \sim 1/N \, \Sigma \, w_i = \mu \qquad \text{for} \qquad \bar{t}_n =< T_m$$

$$Var = 1/N\text{-}1 \, \Sigma^{N}_{n=1} [w_n - \mu]^2$$