Monte Carlo Simulation of Markov, Semi-Markov, and Generalized Semi-Markov Processes in Probabilistic Risk Assessment

Final Report
NASA Faculty Fellowship Program 2004

Johnson Space Center

Prepared by:	Thomas English
Academic Rank:	Professor
University & Department:	College of the Mainland Department of Mathematics Texas City, TX 77591
NASA/JSC	
Directorate:	Safety and Mission Assurance
Division:	Advanced Programs and Analysis Division
JSC Colleague:	Richard P. Heydorn, PhD
Date Submitted:	August 10, 2004
Contract Number:	NAG 9-1526

INTRODUCTION

A standard tool of reliability analysis used at NASA-JSC is the event tree. An event tree is simply a probability tree, with the probabilities determining the next step through the tree specified at each node. The nodal probabilities are determined by a reliability study of the physical system at work for a particular node. The reliability study performed at a node is typically referred to as a fault tree analysis, with the potential of a fault tree existing for each node on the event tree.

When examining an event tree it is obvious why the event tree/fault tree approach has been adopted. Typical event trees are quite complex in nature, and the event tree/fault tree approach provides a systematic and organized approach to reliability analysis.

The purpose of this study was two fold. Firstly, we wanted to explore the possibility that a semi-Markov process can create dependencies between sojourn times (the times it takes to transition from one state to the next) that can decrease the uncertainty when estimating time to failures. Using a generalized semi-Markov model, we studied a four element reliability model and were able to demonstrate such sojourn time dependencies. Secondly, we wanted to study the use of semi-Markov processes to introduce a time variable into the event tree diagrams that are commonly developed in PRA (Probabilistic Risk Assessment) analyses. Event tree end states which change with time are more representative of failure scenarios than are the usual static probability-derived end states.

BLOCK DIAGRAM ANALYSIS

Our study begins with a look at a four component reliability block diagram. Figure 1 shows the component block diagram.

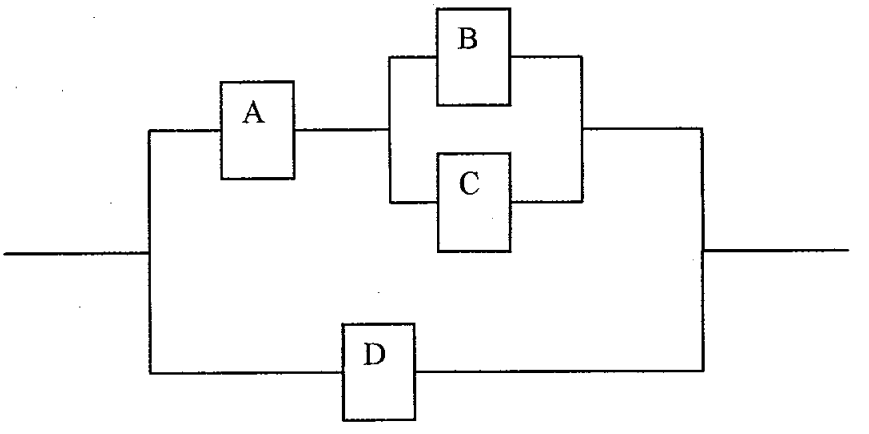

Figure 1: Four Component Block Diagram

This block diagram represents a system in which initially all four components are working independently of each other. Given that there are 4 components in the system, and two possible states for each component (working versus failed), there are a total of 16 possible states in which the system may reside at any given time. These 16 states are related to each other by the flow diagram illustrated in Figure 2. Figure 2 shows the possible paths to overall failure of the system, which is realized at nodes 8, 10, 12, 14, and 16. The 16 nodes of the flow diagram are defined in Table 1. The symbol "**O**" refers to an operating state, and the symbol "**F**" refers to a failed state.

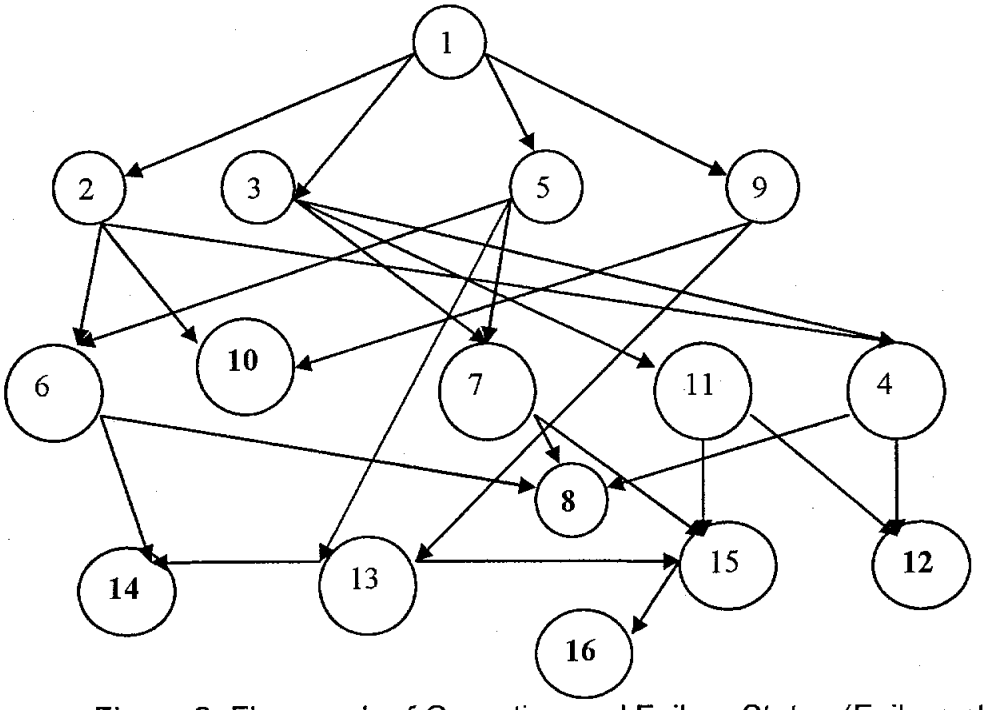

Figure 2: Flowgraph of Operating and Failure States (Failure states in boldface).

TABLE 1: OPERATING AND FAILURE STATES

Component	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
B	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
C	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
D	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
State	O	O	O	O	O	O	O	F	O	F	O	F	O	F	O	F

In effect, this four node diagram has incorporated into it the notion of a generalized semi-Markov process (GSMP), that is, the future node is predicted not only by the present node (as in a Markov Process), but also by a set of time

generators (think stopwatches) running in the present node and indicating the time to transition to a future node. Inherent in a GSMP is the notion of competition among the transition times, with the smallest transition time specifying the future node. A fundamental question is, can we use the node and time components to develop an improved reliability estimate? The first part of our investigation is to explore the concept of path dependence within the flow diagram.

Multiple runs through the flow diagram presented in Figure 2 are simulated using the S programming language with summary statistics presented in Table 2 and Table 3.

Table 2: PATH MEAN TIMES TO FAILURE

	The Weibull Model		
Path	**MTTF**	**S.E.**	**Prob**
1-2-10	0.99	0.01	0.11
1-9-10	1.00	0.01	0.00
1-2-6-14	1.00	0.00	0.12
1-2-6-8	1.00	0.01	0.00
1-2-4-8	0.99	0.01	0.10
1-2-4-12	0.99	0.01	0.10
1-3-4-8	0.99	0.01	0.10
1-3-4-12	0.99	0.01	0.10
1-3-7-8	1.00	0.01	0.00
1-3-11-12	1.00	0.01	0.00
1-5-6-8	1.00	0.00	0.00
1-5-6-14	1.00	0.00	0.00
1-5-7-8	1.00	0.00	0.00
1-5-13-14	1.14	0.11	0.03
1-9-11-12	0.99	0.01	0.00
1-9-13-14	1.13	0.11	0.03
1-3-7-15-16	1.23	0.18	0.11
1-3-11-15-16	1.23	0.18	0.11
1-9-11-15-16	1.22	0.17	0.00
1-5-7-15-16	1.24	0.17	0.00
1-5-13-15-16	1.33	0.18	0.03
1-9-13-15-16	1.33	0.18	0.03
Overall	1.08	0.16	1.00

Table 3: PARTIAL PATH MEAN TMES TO FAILURE

	Weibull Model	
Partial Path	**MTTF**	**S.E.**
1-2-4	0.99	0.01
1-2-6	1.00	0.00
1-2	1.00	0.01
1-9-11-15	1.22	0.17
1-9-13-15	1.33	0.18
1-9-11	1.21	0.18
1-9-13	1.23	0.18
1-9	1.23	0.18
1-3-7-15	1.23	0.18
1-3-11-15	1.23	0.18
1-3-4	0.99	0.01
1-3-7	1.23	0.18
1-3-11	1.23	0.18
1-3	1.12	0.18
1-5-7-15	1.24	0.17
1-5-13-15	1.33	0.18
1-5-6	1.00	0.00
1-5-7	1.23	0.17
1-5-13	1.23	0.18
1-5	1.14	0.18

In this simulation the time to failure of each component is assumed to have a Weibull distribution, with components A and B having their time to failure concentrated at a point by using a shape parameter of 200, while components C and D have their time to failure spread out by using a shape parameter of 3. The purpose for such a choice of shape parameters is to model a system where a specific path occurs with inter-arrival times that are almost fixed, while other

paths contain inter-arrival times with greater variation. This is an attempt to model real-world events where success at a node occurs at precise points in time, while failure can occur over a broader interval of time. The overall system time to failure is estimated by a weighted mixture of each path's time to failure.

Of interest is the apparent existence of path dependence within Table 2. What appears to be true from Table 2 is that the shorter paths have shorter mean time to failure. Table 3 is a look at the information gained by knowing the nodes passed through as one traverses the flow diagram. Note that passing through node 2 virtually guarantees a mean time to failure of the system of 1. Unfortunately, the standard error associated with the mean time to failure along any path is sufficiently large as to mask general distinctions among time to failure along arbitrary paths.

We examine the correlation among inter-arrival times T_1, T_2, T_3, T_4, and the time to failure TTF, by means of correlation matrices. Inter-arrival times (sojourn times) represent the times the process resides at a particular node before transitioning to the next node. In effect, the inter-arrival times for a particular path through the flow diagram are the differences between the failure times of components failing in sequence, with the first inter-arrival time being the time to failure of the first component. Hence, the time to failure (TTF) for a given path is the sum of the inter-arrival times along the path. Since all paths for the given reliability block diagram must have at least two component failures for the system to fail, there are at least two inter-arrival times on every path. A three by three matrix shows the correlations among the inter-arrival times along all paths (*i.e.* for paths of length 2, 3, or 4),, as well as the time to failure:

$$corr(T_1, T_2, TTF) = \begin{bmatrix} 1 & -.83 & .50 \\ & 1 & -.27 \\ & & 1 \end{bmatrix}.$$

A four by four matrix shows the correlations among the inter-arrival times along all paths containing at least three inter-arrival times (*i.e.* for paths of length 3 or 4),, as well as the time to failure:

$$corr(T_1, T_2, T_3, TTF) = \begin{bmatrix} 1 & -.81 & -.29 & .58 \\ & 1 & -.26 & -.23 \\ & & 1 & -.47 \\ & & & 1 \end{bmatrix}.$$

A five by five matrix shows the correlations among the inter-arrival times along all paths containing four inter-arrival times (*i.e.* for paths of length 4), as well as the time to failure:

$$corr(T_1, T_2, T_3, T_4, TTF) = \begin{bmatrix} 1 & -1 & .39 & -.04 & .78 \\ & 1 & -.39 & .04 & -.78 \\ & & 1 & -.10 & .64 \\ & & & 1 & .43 \\ & & & & 1 \end{bmatrix}.$$

Of interest in these correlation matrices is the exponential decay of correlation that occurs between inter-arrival times. In the last matrix we see that T_4 shares no correlation with the previous inter-arrival times. This loss of correlation will have an interesting consequence in the following section.

In an attempt to utilize the correlations present in the inter-arrival times and the time to failure (TTF) of the system, we construct a series of linear regression models and present the results in Table 4.

Table 4: PREDICTIVE MODELS

Model 1: TTF ~ T.1

	Value	Std. Error	t value	Pr(>|t|)
(Intercept)	2e+000	8e-003	2e+002	0e+000
T.1	2e+000	1e-002	2e+002	0e+000

Residual standard error: 0.8 on 99998 degrees of freedom
Multiple R-Squared: 0.3

Model 2: TTF ~ T.1 + T.2

	Value	Std. Error	t value	Pr(>|t|)
(Intercept)	0.12	0.02	7.40	0.00
T.1	3.35	0.02	186.96	0.00
T.2	1.94	0.02	96.04	0.00

Residual standard error: 0.7 on 99997 degrees of freedom
Multiple R-Squared: 0.3

Model 3: TTF ~ T.1 + T.2 + T.3

	Value		Std. Error	t value	Pr(>|t|)
(Intercept)	-2.04	0.03	-66.64	0.00	
T.1	5.62	0.03	189.95	0.00	
T.2	4.65	0.03	137.68	0.00	
T.3	1.70	0.03	55.98		0.00

Residual standard error: 0.5 on 88225 degrees of freedom
Multiple R-Squared: 0.5

Model 4: TTF ~ T.1 + T.2 + T.3 + T.4

	Value	Std. Error	t value	Pr(>|t|)
(Intercept)	0e+000	0e+000	4e+000	0e+000
T.1	4e+000	0e+000	4e+014	0e+000
T.2	3e+000	0e+000	3e+014	0e+000
T.3	2e+000	0e+000	2e+015	0e+000

ABSTRACT

Most probabilistic risk assessment (PRA) and reliability methods commonly used at Johnson Space Center (JSC) make the assumption that component failures in a system are independent random occurrences. There are some exceptions (e.g. modeling common cause events), but because of the mathematical complications that occur when full dependency is assumed, it is not done by the standard models.

This study investigates the use of models in which dependencies among the failure states has been considered via a variety of processes. Our study included: 1) analysis of a general block component diagram for path dependence and inter-arrival time correlations; 2) analysis of correlation among inter-arrival times on a small, generic event tree; 3) a semi-Markov approach designed to provide updated reliability predictions for general event trees.

T.4	1e+000	0e+000	3e+015	0e+000

Residual standard error: 1e-014 on 29902 degrees of freedom
Multiple R-Squared: 1

Model 5: T.2 ~ T.1

	Value	Std. Error	t value	Pr(>|t|)
(Intercept)	7e-001	1e-003	6e+002	0e+000
T.1	-7e-001	2e-003	-5e+002	0e+000

Residual standard error: 0.1 on 99998 degrees of freedom
Multiple R-Squared: 0.7

Model 6: T.3 ~ T.1 + T.2

	Value	Std. Error	t value	Pr(>|t|)
(Intercept)	9e-001	1e-003	7e+002	0e+000
T.1	-9e-001	2e-003	-6e+002	0e+000
T.2	-1e+000	2e-003	-6e+002	0e+000

Residual standard error: 0.06 on 88119 degrees of freedom
Multiple R-Squared: 0.8

Table 4 (CONTINUED): PREDICTIVE MODELS

Model 7: T.4 ~ T.1 + T.2 + T.3

	Value	Std. Error	t value	Pr(>|t|)
(Intercept)	6e-001	2e-001	4e+000	2e-004
T.1	-4e-001	2e-001	-2e+000	2e-002
T.2	-4e-001	2e-001	-2e+000	2e-002
T.3	1 -2e-001	2e-002	-1e+001	0e+000

Residual standard error: 0.2 on 30151 degrees of freedom
Multiple R-Squared: 0.009

We have considered models in which TTF is regressed upon the inter-arrival times as well as models in which inter-arrival times are regressed on prior inter-arrival times. In models designed to predict TTF, we see in general that the multiple R-squared values are small and hence we gain poor predictive value from the model. The only model which predicts TTF well is model 4, which says knowing all the inter-arrival times allows one to predict TTF. Since TTF is the sum of all inter-arrival times, one hardly finds this regression model useful. In models 5 and 6, we see more promise in gaining predictive ability, with multiple R-squared values improving. In model 7 we see the artifact of the loss of correlation previously mentioned. The "return to randomness" of the inter-arrival times masks our ability to gain predictive power.

We consider another method of extracting predictive power from the simulation in terms of a simulated reliability curve. Figure 3 presents an empirical reliability curve for the data used in the simulation of the block diagram and the empirical mixture pdf of the distributions for the four components.

In Figure 3 we have plotted a 95% confidence interval on the empirical reliability curve, which appears as a very narrow band about the mean reliability curve. This simulation ran 100,000 tests replicated 50 times (hence 5,000,000 path simulations) to generate the lower and upper confidence intervals. The empirical mixture pdf for the block diagram is calculated using data from one of the 50 replications. We see the reliability curve generated from the simulation is quite accurate in terms of the confidence intervals, and can alleviate the difficulty of analytic calculations when the pdf for the block diagram is a mixture (Figure 3) and hence analytically more difficult to work with.

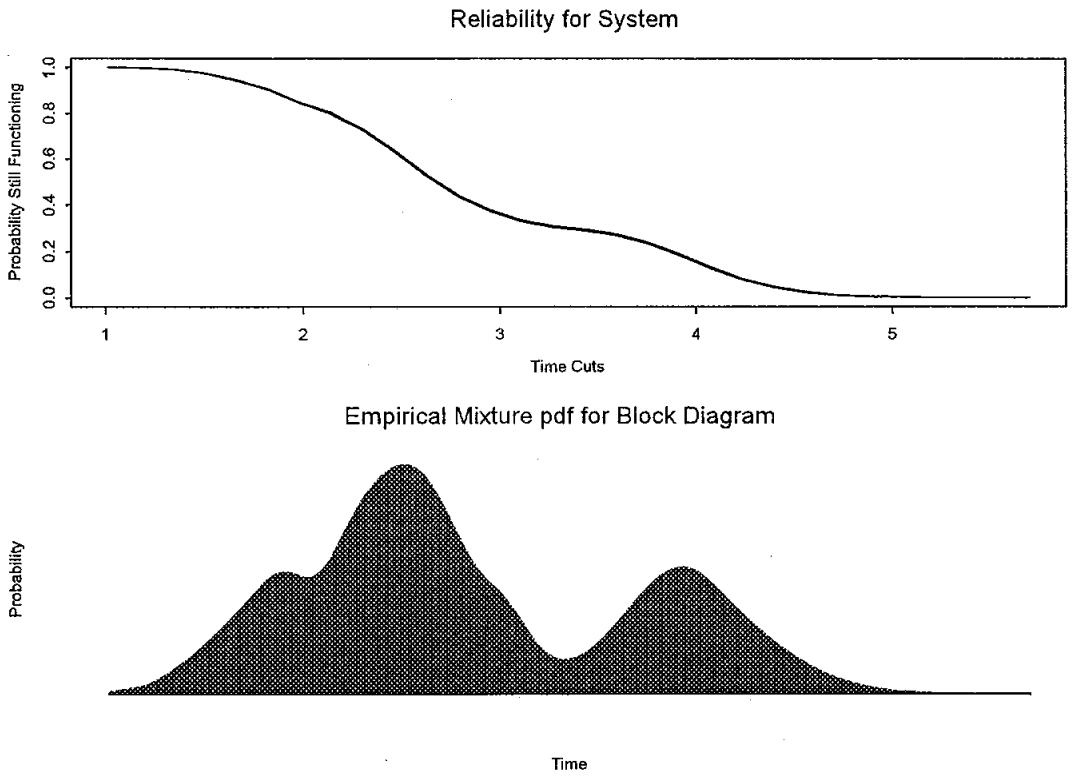

Figure 3: Reliability Curve for Block Diagram; pdf for Block Diagram

SIMPLE EVENT TREES

We began the study of the application of semi-Markov processes to event tees with the simple flow diagram shown in Figure 4.

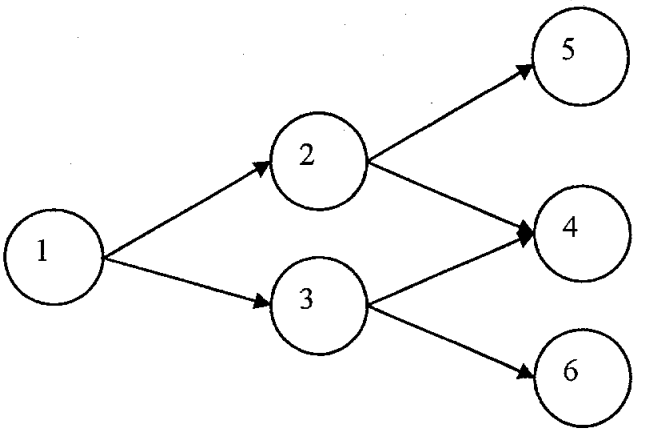

Figure 4: The simple event tree flowdiagram.

Event tree models are such that there are two primary paths through the flow diagram: a success path and a failure path. The transition times for the success path are not random, whereas the transition times for the failure paths are random. The study of correlation among inter-arrival times for the flow diagram shown in Figure 4 is carried out both as a semi-Markov process (SMP) in which the path is chosen by binomial distributions located at each node, while the inter-arrival times are Weibull in nature, and a generalized semi-Markov Process (GSMP) in which case the inter-arrival times compete to transition at each node. In both cases the inter-arrival times for these models do not show dependencies between inter-arrival times. This result indicates that there is a fundamental difference between the block diagram and the event tree, and motivates our desire to try a different approach to analyzing event trees.

A SIMPLE NASA EVENT TREE

We turn our focus to the analysis of a simple NASA-JSC event tree representing a lunar mission (Figure 5, Table 5), and show how Monte-Carlo simulation techniques can provide a more dynamic view of the probability associated with each path, as well as capture underlying information associated with node and inter-arrival time values.

TABLE 5: EVENT TREE TIMES

Node	Mission Events	Time (min)	Explanation of Event Times
1	Booster Launch With Payload	0.167	From engine ignition to clearing the tower
2	Booster Ascent With Payload	8.5	Tower clear to engine cutoff
3	Launch Abort	10	From abort declaration to descent (abort declaration could be anywhere during ascent)
4	Payload Orbit Insertion	2	Orbital engine burn time
5	Mission In Orbit	7200	

6	Mission Abort And Return	90	Maximum time from declaration of abort to orbital engine burn
7	Deorbit Burn	2	Orbital engine burn time (deorbit)
8	Vehicle Entry	60	Vehicle entry from engine burn to below Mach 1
9	Vehicle Descent	10	Mach 1 to final approach
10	Vehicle Landing	2	Final approach, landing, and rollout

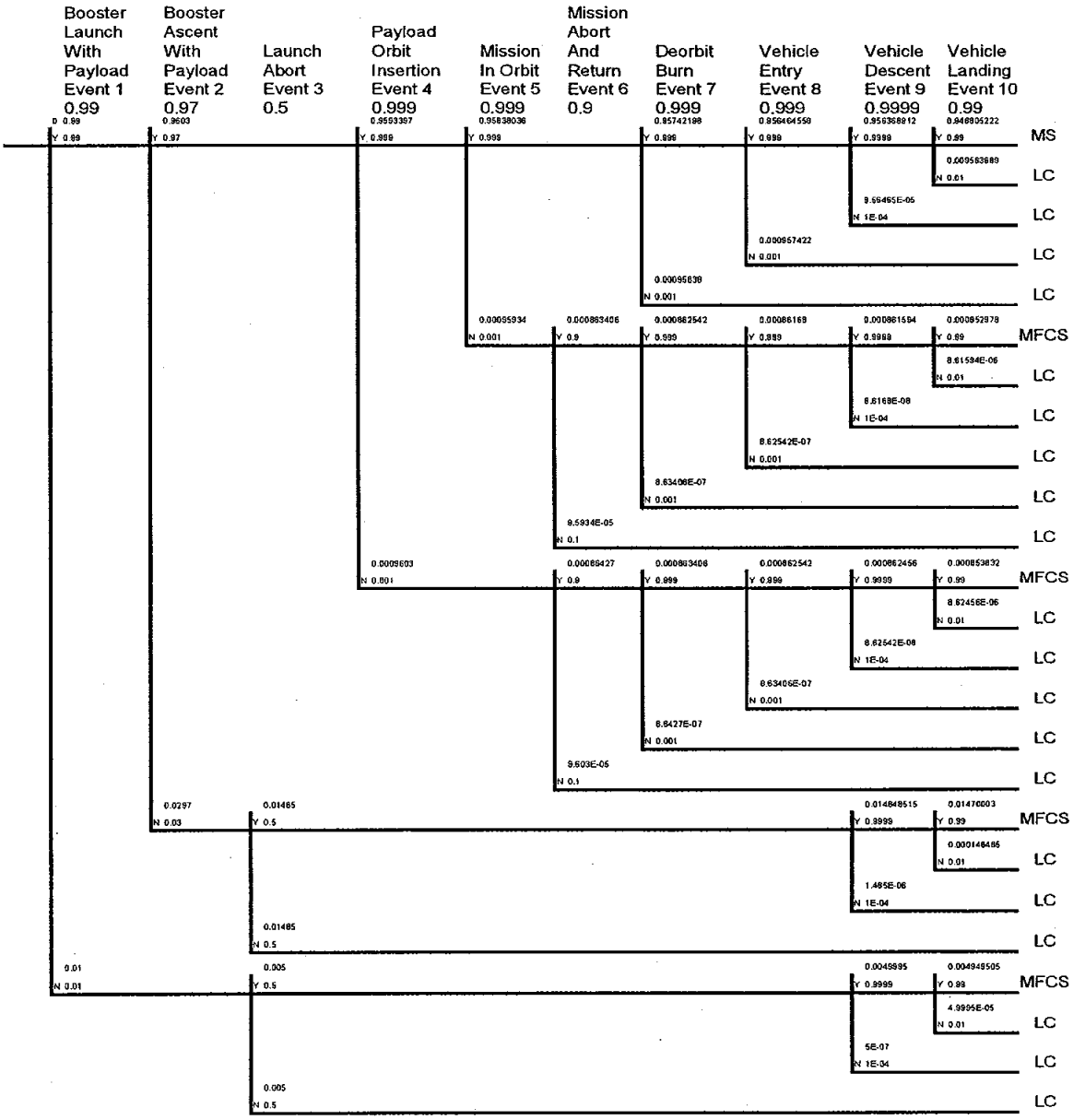

Figure 5: A simple NASA event tree; MS = mission success, LC = loss of crew, MFCS = mission fails, crew survives.

The interpretation of the event tree as a flowgraph results in figure 6.

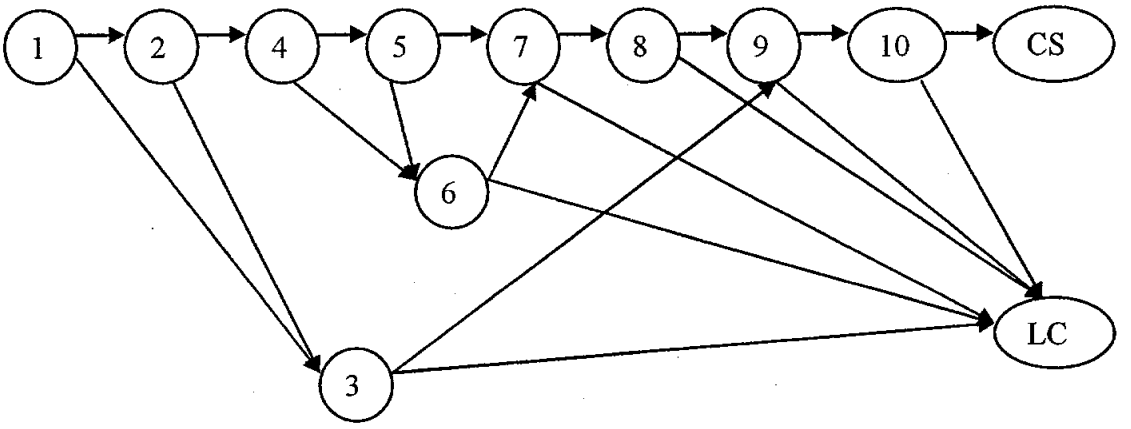

Figure 6: Flowgraph of Event Tree

The 25 paths (Table 6) associated with the flowgraph of the event tree are simulated in a process by which the probabilities provided on the tree diagram are used to calculate the number of simulations needed for each path. Note that 12 millions simulations are required to ensure that the relatively unlikely paths (path 8 and path 14) will be represented at least once in the simulation.

TABLE 6: PATHS THROUGH THE FLOW DIAGRAM

Path	Nodes										Number Simulations
1	1	2	4	5		7	8	9	10	CS	11,361,663
2	1	2	4	5		7	8	9	10	LC	114,764
3	1	2	4	5		7	8	9		LC	1,148
4	1	2	4	5		7	8			LC	11,489
5	1	2	4	5		7				LC	11,501
6	1	2	4	5	6	7	8	9	10	CS	10,236
7	1	2	4	5	6	7	8	9	10	LC	103
8	1	2	4	5	6	7	8	9		LC	1
9	1	2	4	5	6	7	8			LC	10
10	1	2	4	5	6	7				LC	10
11	1	2	4	5	6					LC	1,151
12	1	2	4		6	7	8	9	10	CS	10,246
13	1	2	4		6	7	8	9	10	LC	103
14	1	2	4		6	7	8	9		LC	1
15	1	2	4		6	7	8			LC	10
16	1	2	4		6	7				LC	10
17	1	2	4		6					LC	1,152

18	1	2	3	9	10	CS	176,400
19	1	2	3	9	10	LC	1,782
20	1	2	3	9		LC	18
21	1	2	3			LC	178,200
22	1		3	9	10	CS	59,394
23	1		3	9	10	LC	600
24	1		3	9		LC	6
25	1		3			LC	60,000

Furthermore, the event tree times provided in Table 5 are used to construct shape and scale parameters for the inter-arrival times along each path. The shape parameters are chosen to either be 2 along an event to failure (such as a mission abort) or 200 along an event to success. The scale parameter for inter-arrival times associated with success were taken to be the time to events in Table 5, or ½ the time to events in Table 5 for failure events. This was done in order to concentrate the mass of the success distribution more or less at the point in time at which success is to occur, while failure is more spread out over the entire time interval.

The simulation program uses the inter-arrival times, in conjunction with the present node location to construct the probability mass function (pmf) for the distribution of end states, MS = Mission Success, LC = Loss of Crew, MFCS = Mission Fails, Crew Survives, along 10 equally spaced time slices of the possible inter-arrival times for a given node. Given that there are 10 time slices, we generate 10 pmf's for each of the 10 nodes and display the pmf's as a continuum for each node. For sake of brevity in this report, we only show the results for a particular node – node 1. Figure 6 shows the change in the pmf for the 10 time slices along the inter-arrival times for node 1. We see a re-apportionment of the total probability among the three end states as time evolved. Practically speaking, this means that if we can accurately construct the distributions of failure times along a tree diagram, then this dynamic approach to risk assessment will allow us to update our probability of success based on two observations – the present node, and the time elapsed since entering the present node.

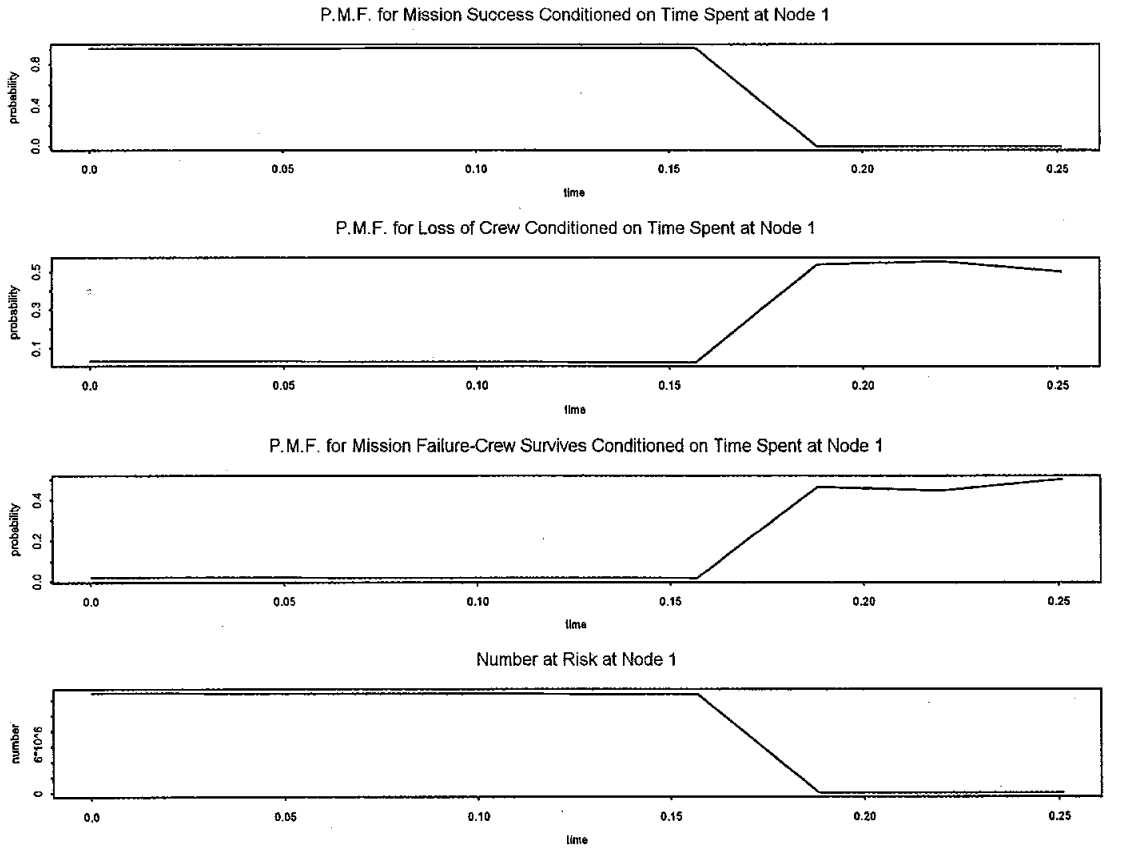

Figure 6: Simulation of pmf for node 1 as time evolves.

The simulation that generated Figure 6 is one in which the probability of ending at a particular node is empirically computed for 10 discrete time intervals, t_i, i = 1, ..., 10, on the range of inter-arrival times for node 1 by considering only those simulations that have not failed at t_i. In effect,

$\Pr(MS \mid t_{i+1} > t > t_i, node\ \ 1) = n(MS \mid t_i)\ \ /\ \ [n(MS \mid t_i) + n(MFCS \mid t_i) + n(LC \mid t_i)],\ \ i = 1,...,9.$

Graphics for the other 9 nodes are constructed in a similar manner.

The simulation performed is somewhat contrived in that it requires the distribution of inter-arrival times be known, and if these inter-arrival times are known, then the pmf can be computed analytically as

$\Pr(MS \mid t_{1,2} > t_i) = \Pr(T > t_{1,2} > t_i) P_{2,4} P_{4,5} P_{5,7} P_{7,8} P_{8,9} P_{9,10} P_{10,MS}$,

where $t_{1,2}$ = the fixed time for the node 2 to be achieved along the path to mission success,

T = the Weibull distributed random variable for the time to failure at node 1,

$P_{i,j}$ = the specified probability of transfer between nodes i and j.

Although contrived, the simulation does carry out two important tasks in that it lays the foundation for a simulation of a GSMP, and it shows the effect of time in the analysis of reliability of the event tree.

The improvement one gets by using the semi-Markov model for an event tree diagram is that the end states now depend upon time. This means that the end state probabilities fluctuate with time and so, for example, if one end state is "loss of crew", then it can happen that the probability that the crew is lost can be high early in the mission, but small late in the mission.

CONCLUSIONS

The study has shown several results of interest to reliability studies at NASA-JSC:

1) Evidence is found to show that correlation between inter-arrival times exists for the general block diagram. This correlation is shown to be difficult to exploit using classical predictive models, and therefore it is suggested that simulation will provide a superior estimate of the distribution of time to failure for the system. It is suggested that each fault tree component of an event tree may be analyzed by the simulation technique, which would provide an empirical pdf for each node of the event tree.

2) Attempts should be made to incorporate the GSMP approach to modeling the event tree. Unless all success events within an event tree are precisely timed and executed such that they effectively have no variance in time, then the GSMP is a more natural modeling assumption.

3) The event tree simulation should be replicated, say 50 times, in order to allow confidence intervals to be placed on the time dependent pmf presented in the study.

REFERENCES

Nilsen, Frode B, 1998. GMSim: A tool for compositional GSMP modeling. Proceedings of the 1998 Winter Simulation Conference. P555-562.

Haas, Peter J. Simulation (Class notes). Retrieved July 9, 2004, from Stanford University website:
http://www.stanford.edu/class/msande223/