Reliability Modeling of Complex Components Using Simulation

Todd Paulos, Ph.D.[a], Curtis Smith, Ph. D.[b], and Andrew H. Ho[c]
[a] Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, USA, tpaulos@jpl.nasa.gov
[b] Idaho National Laboratory, Idaho Falls, ID, USA, curtis.smith@inl.gov
[c] Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, USA, andrew.h.ho@jpl.nasa.gov

Abstract:

This paper is a continuation of papers presented at the 13th and 15th Probabilistic Safety Assessment and Management Conferences [1, 2]. The previous work presented discussions of modeling failure modes of complex components and the effects of censor bias. The first paper demonstrated how the typical method of treating failure modes as exponential gives optimistic predictions when predicting how improvements to subcomponents will perform. Instead of relying on traditional analytical methods, a more accurate approach is to model the failure modes as a race in time. Unfortunately, this does not give a closed-form solution and requires a more advanced solution. A simulation with pre-defined component attributes demonstrated the optimistic nature of classical techniques. Unfortunately for complex systems, the simulation routine may become very complex and difficult to implement. The second paper demonstrated the effect of censor bias when dealing with large amounts of success-only testing, and the difference between treating data as "missing" instead of censored.

In the quest for closed-form solutions and simplicity, the world of reliability engineering relies on the exponential distribution. In most cases, it makes the solution closed-form and easy to solve. However, simple models may lead to incorrect results when modeling even something as simple as modeling to the failure mode or component/subassembly level. An excellent real-world example of using exponential distributions in this context is the typical automobile. No one expects a new car to have the same failure intensity as an older car. Obviously a more advanced approach is needed, and not just at the component level.

This paper will use two approaches to analyze a simple system with components that have more than one failure mode. The first is a standard fault tree, and the second is a simulation. In both methods, various data assessment methods will be used to compare the results of both the data assessment method and the solution. A discussion of the results will follow.

Keywords: failure modes, reliability, simulation.

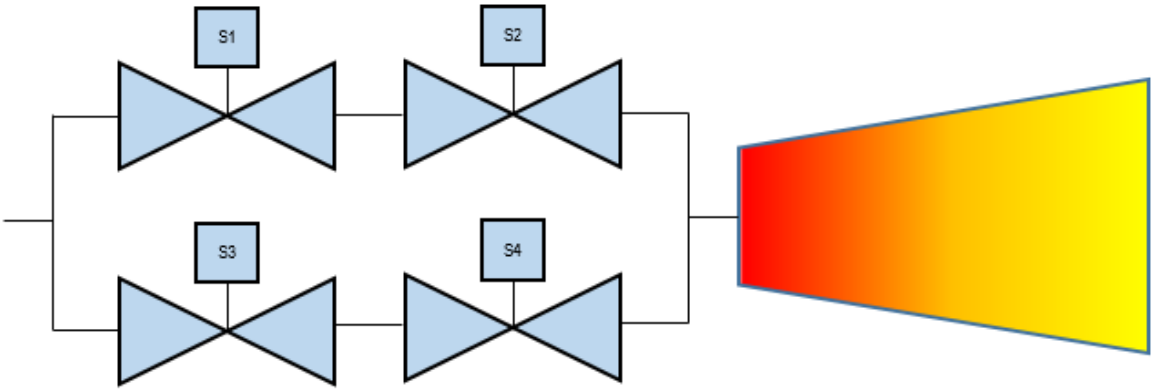
1. INTRODUCTION

As a continuation of the previous efforts, this paper will demonstrate the difference between using traditional reliability methods to simulation when dealing with complex components with multiple failure modes. Traditional methods rely on summing the failure rates of failure modes. The error may be compounded depending on the type of data analysis used, leading to erroneous predictions. Additionally, this paper will examine these issues in the context of having high failure probabilities, as seen comparatively to other industries such as nuclear and oil and gas.

2. PROBLEM STATEMENT

As an elementary example, consider a single monopropellant spacecraft thruster. The thruster is operated through four valves (S1, S2, S3, and S4), as shown in Figure 1. In this configuration, the thruster can only operate when there is propellant flowing in either one of the two flow paths, or both. Additionally, when the thruster is not in use, both flow paths need to be closed to save propellant and prevent the spacecraft from gaining unwanted momentum.

Figure 1: Spacecraft Thruster with Four Control Valves



For simplicity, the only failure modes of the valves considered are Fail Open (FO) and Fail Closed (FC), although, in a more complex model, considerations could be given to Fails Leak (FL), Fails to Open (FTO) or Fails to Close (FTC) as well.

3. FAULT TREE SOLUTIONS

3.1. Fault Tree Analysis

For a traditional model, the authors chose to do a simple Fault Tree Analysis (FTA) using SAPHIRE Version 8.2.5 (https://saphire.inl.gov/#/). The simple FTA is shown in Figure 2, which describes both the FO and FC failure paths through the thruster. The thruster fails when either flow path fails open or when both flow paths fail closed. Note that in Figure 2, the probability display could not be disabled in the graphic. The fault tree has no data populated, and thus probabilities of 1.0 are shown in Figure 2.

This paper does not discuss common cause failures, and hence, are not shown in the FTA.

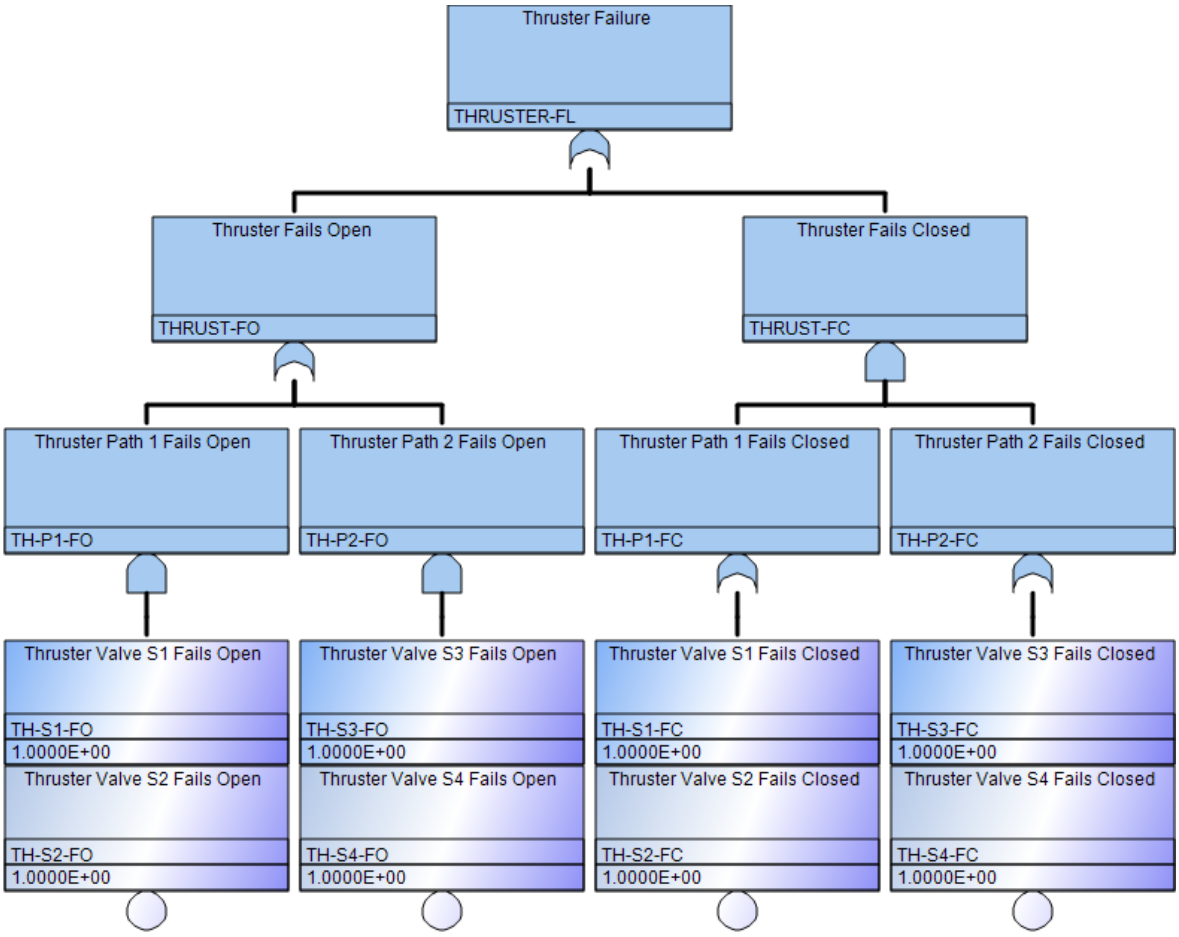
3.2. Data Inputs

In this example, consider that during operational experience, this type of valve has had four failures, two fail open, and two fail closed. Additionally, both the failure modes occurred at 45,000 and 55,000 hours. The failure history is in Table 1.

Table 1: Failure Times to Different Failure Modes

Failure Mode	Time to Failure (Hrs)
Fail Open	45,000
Fail Closed	45,000
Fail Open	55,000
Fail Closed	55,000

Figure 2: Fault Tree for Thruster



3.2.1. Simple Data Analysis Method

The previous two papers described a few data analysis methods [1, 2]. A common yet overly simplistic data analysis would consider each failure mode having two failures (one each at 45,000 and 55,000 hours) in 200,000 hours. The simple data assessment yields a failure rate of (2/200,000)/hr, or a point estimate of $1x10^{-5}$/hr for both failure modes.

3.2.2. Alternative Data Analysis Method 1

Now consider the data analysis discussed in the previous papers [1, 2], where the data is treated as *missing*. In this case, each failure mode has failures at 45,000 and 55,000 hours, the other two failures are considered incomplete and missing, and thus the failure rate prediction simplifies 2/(45,000+55,000) or (2/100,000)/hr, which equals $2x10^{-5}$/hr for each failure mode. Note that the authors assumed there is no state-of-knowledge correlation between failure modes or failure rates in this paper. For more information on this type of correlation, see Chapter 12 of [3].

State-of-knowledge correlations are used in uncertainty analyses to correlate identical components' failure rates or probabilities. Although applying the correlation in that fashion makes sense, from an engineer's perspective, it does not make sense to have all of the identical components fail simultaneously. That would defeat the redundancy concept and make the inclusion of common cause factors relatively easy. Hence, simulation trials are run for identical components individually.

3.2.3. Alternative Data Analysis Method 2

In the second alternative data analysis method, consider the common Bayesian solution described in the literature [4, p. 6-12 and 6-13]. In this case, the prior distribution for the failure rate λ is a gamma(α_{prior}, β_{prior}), and the data is considered a Poisson with x events in time t. The posterior gamma distribution for λ is thus,

$$\text{gamma}(\alpha_{posterior}, \beta_{posterrior}) \quad (1)$$

$$\alpha_{posterior} = \alpha_{prior} + x \quad (2)$$

$$\beta_{posterior} = \beta_{prior} + t \quad (3)$$

In this example we will use a Jeffreys' noninformative prior, gamma(½, 0) [4, p. 6-14 and 5], which yields for Equations (2) and (3)

$$\alpha_{posterior} = x + ½ \quad (4)$$

$$\beta_{posterior} = t + 0 \quad (5)$$

In this method, the Alternative Data Analysis Method 1 is used to determine the x and t. Thus, for each failure mode, the point estimate result is 2.5/100,000, which equals 2.5×10^{-5}.

3.3. Minimal Cut Sets and Results

For the fault tree shown in Figure 2, the Minimal Cut Sets are in Table 2.

Table 2: Minimal Cut Sets of Example Problem

Minimal Cut Set	Event Description	Boolean Designator
1	Thruster Valve S1 Fails Open Thruster Valve S2 Fails Open	TH-S1-FO TH-S2-FO
2	Thruster Valve S3 Fails Open Thruster Valve S4 Fails Open	TH-S3-FO TH-S4-FO
3	Thruster Valve S1 Fails Closed Thruster Valve S3 Fails Closed	TH-S1-FC TH-S3-FC
4	Thruster Valve S2 Fails Closed Thruster Valve S3 Fails Closed	TH-S2-FC TH-S3-FC
5	Thruster Valve S1 Fails Closed Thruster Valve S4 Fails Closed	TH-S1-FC TH-S4-FC
6	Thruster Valve S2 Fails Closed Thruster Valve S4 Fails Closed	TH-S2-FC TH-S4-FC

The mission times for this problem are three years (26,281 hours), five years (43,801 hours), and ten years (87,603 hours). The results for the three-year mission using the simple data analysis method described in Section 3.2.1 (each failure mode has a failure rate of 1×10^{-5}/hr) are in Table 3.

Similarly, results for the three time frames (3, 5, and 10 years) using the previously derived failure rates for each failure mode (1×10^{-5}, 2×10^{-5}, and 2.5×10^{-5} per hour) are in Table 4.

3.4. Fault Tree Results Discussion

As seen in Table 4, using the typical data analysis method, where failure rates are summed for failure modes of a complex component, leads to an optimistic prediction when compared to the other failure rate analysis methods. The values in Table 4 are the probabilities of failure using a Minimal Cut Set (MSC) approximation for the fault tree. These differences among the three methods of data analysis are reasonably consistent as the failure rate drops to 1×10^{-7}. When using a Binary Decision Digraph (BDD) solution within SAPHIRE, these values change very little.

Table 3: Minimal Cut Sets for 3 Year Mission

Minimal Cut Set	Probability	Basic Events	Event Probability
1	$5.35x10^{-2}$	TH-S1-FO TH-S2-FO	$2.31x10^{-1}$ $2.31x10^{-1}$
2	$5.35x10^{-2}$	TH-S3-FO TH-S4-FO	$2.31x10^{-1}$ $2.31x10^{-1}$
3	$5.35x10^{-2}$	TH-S1-FC TH-S3-FC	$2.31x10^{-1}$ $2.31x10^{-1}$
4	$5.35x10^{-2}$	TH-S2-FC TH-S3-FC	$2.31x10^{-1}$ $2.31x10^{-1}$
5	$5.35x10^{-2}$	TH-S1-FC TH-S4-FC	$2.31x10^{-1}$ $2.31x10^{-1}$
6	$5.35x10^{-2}$	TH-S2-FC TH-S4-FC	$2.31x10^{-1}$ $2.31x10^{-1}$
Min Cut Set Upper Bound		**$2.81x10^{-1}$**	

Table 4: MCS Results of Sample Problem for Various Mission Lengths and Failure Rates

Minimal Cut Set Upper Bound Approximation (Probability of Failure)	Baseline Failure Rate /Hr ($1x10^{-5}$)	Alt Method 1 Failure Rate /Hr ($2x10^{-5}$)	Alt Method 2 Failure Rate /Hr ($2.5x10^{-5}$)
3 Year Mission (26,281 hrs)	$2.8x10^{-1}$	$6.7x10^{-1}$	$8.0x10^{-1}$
5 Year Mission (43,801 hrs)	$5.5x10^{-1}$	$9.2x10^{-1}$	$9.7x10^{-1}$
10 Year Mission (87,603 hrs)	$9.2x10^{-1}$	$9.990x10^{-1}$	$9.991x10^{-1}$

4. SIMULATION MODEL

4.1. Simulation Algorithm

There are many software programs available in which to develop a simulation. Matlab (Version R2019a) was chosen due to the author's familiarity and the commonality of the software. We also used Excel to validate some of the simulation-based calculations performed in Matlab. Before developing the code, the team worked out an algorithm to solve this problem that considers the competition between the failure modes and that a component cannot fail twice. Considerations were given to allow common cause failures of the hardware to be added in future work.

The algorithm follows these steps.

Step 1 Establish parameters
- Input mission time in hours
- Input the gamma distribution parameters for each component failure mode based on the input parameters determined in Section 3.2
- Input k number of trials
- Determine a random seed value (or use a common seed from trial to trial to narrow down the number of unknowns)

Step 2 Establish failure criteria for the system. For this simulation, the results from Table 2 were used to establish the failure criteria for the system. Although the inspection is easy enough for simple examples, such as in this paper, more complex systems or configurations may require an alternative method to determine the success/failure criteria.

Step 3 Simulate component failure mode times by:
- Drawing random values given input distributions from Step 1
- Taking the reciprocal of failure rate to simulate the mean time to failure (MTTF) vector

Determine the failure mode times (fail open and fail close) for each valve (S1, S2, S3, S4)

Determine the failure mode for each valve, i.e., which component failure mode occurred first and at what time

Does the simulated component time to failure survive mission time, i.e., is time to failure greater than mission time?

Step 4 Determine if a system failure occurred in the mission time

Determine if any of the six system failures defined in Step 2 (Table 2) occurred during Step 3

The system failure time taken is the 2nd of the two failure modes.

Record this MTTF and the specific system failure path

If more than one system mode fails, take the earlier system failure time

Step 5 Track success and failure statistics and report

4.2. Simulation Results

Similar to the results in Table 4, the simulation utilized the same failure rates and mission times as discussed previously for comparison purposes. Each data set was run initially for 10,000 trials; lower probability simulations required 100,000 trials to obtain a result.

A single simulation trial is shown in Table 5 and Table 6 using a three-year mission and Alternative Data Method 1.

Table 5: Component Failure Mode Simulation

Comp FM	**S1C**	**S1O**	**S2C**	**S2O**	**S3C**	**S3O**	**S4C**	**S4O**
Sim Time to Failure	96,268	**23,501**	106,845	**25,894**	**20,048**	139,391	55,960	89,436
Survives 3 Year Mission?	TRUE	**FALSE**	TRUE	**FALSE**	**FALSE**	TRUE	TRUE	TRUE
1st FM	FALSE	**TRUE**	FALSE	**TRUE**	**TRUE**	FALSE	TRUE	FALSE

In Table 5, each column represents the simulation time that the failure mode was seen. Due to the diffuse gamma distribution used to draw these failure modes, there is a wide range of values (25,894 hours to 139,391 hours) for the failure modes. For the simulation trial, S1C occurred at 96,268 hours. Since the life time of 96,268 hours is greater than the 3 year mission time of 26,281 hours, a "TRUE" is shown that it survived the mission. Under S1O, the time to failure is 23,501 hours. This time is less than the required mission time, so a **FALSE** is placed for not surviving the mission. Since S1O happened before S1C, S1O is labeled as **TRUE** for which failure mode occurred first, S1C is labeled FALSE, and the time value in S1O (**23,501**) is in bold as it was the failure mode that occurred first. The items denoted in **BOLD** depict the failure modes that are carried through to the system analysis described in Table 6.

Table 6: System Failure Simulation

System Failure MCS	**1** **TH-S1-FO** **TH-S2-FO**	**2** TH-S3-FO TH-S4-FO	**3** TH-S1-FC TH-S3-FC	**4** TH-S2-FC **TH-S3-FC**	**5** TH-S1-FC TH-S4-FC	**6** TH-S2-FC TH-S4-FC
Sys Failure?	**TRUE**	FALSE	FALSE	FALSE	FALSE	FALSE
Sys Failure Time	25,894	139,391	96,268	106,845	96,268	106,845

Table 6 depicts the comparison of component and failure mode failure times to the system level criteria to determine if a failure has occurred in the trial or not. In the various columns, the MCS is shown. Under MCS 1, the events TH-S1-FO and TH-S2-FO are both in bold because they are shown failed in Table 5. Additionally, the system failure is labeled as **TRUE**, and the system failure time is listed as 25,894 since it is the later failure mode between the two basic events (TH-S2-FO). Also shown failed is event TH-S3-FC, but it is only one half of the MCS, so the system failure is labeled as FALSE. If

there were multiple paths to failure in the simulation, the time to the first system MCS will be declared the "winner" of the simulation.

This is one trial, which reports MCS 1 as the system failure occurring at 25,894 hours. It is possible that a trial reports no system failures. This process is repeated for each of the k trials in the simulation. In the end, the probability of failure is calculated as the ratio of system failures to total trials through all k trials.

Table 7 shows a comparison between the simulation results and the fault tree approach for all three failure rates from Section 3.2, and all three mission times. As shown in Table 7, there is a difference between the fault tree and simulation results.

Table 7: Comparison of Fault Tree Analysis to Simulation Results

Probability of Failure	FT or Sim	Baseline Failure Rate ($1x10^{-5}$ /Hr) or Gamma(2, 200000)	Alt Method 1 Failure Rate ($2x10^{-5}$ /Hr) or Gamma(2, 100000)	Alt Method 2 Failure Rate ($2.5x10^{-5}$ /Hr) or Gamma(2.5, 100000)
3-Year Mission (26,281 hrs)	FT	$2.8x10^{-1}$	$6.7x10^{-1}$	$8.0x10^{-1}$
	Sim	**$7x10^{-5}$ (100k trials)**	$5.7x10^{-2}$	$1.4x10^{-1}$
5-Year Mission (43,801 hrs)	FT	$5.5x10^{-1}$	$9.2x10^{-1}$	$9.7x10^{-1}$
	Sim	$1.8x10^{-2}$	$3.9x10^{-1}$	$6.0x10^{-1}$
10-Year Mission (87,603 hrs)	FT	$9.2x10^{-1}$	$9.990x10^{-1}$	$9.991x10^{-1}$
	Sim	$3.8x10^{-1}$	$8.5x10^{-1}$	$9.5x10^{-1}$

The main focus of this paper is to compare the results from a typical FTA using a typical data analysis (shown in yellow) to a simulation routine using missing data approaches (shown in green). The results for a 3-year mission show a failure probability of $2.8x10^{-1}$ while the alternative data approach presented in [2] yields a failure probability of $5.7x10^{-2}$. Despite having half the failure rate, the fault tree analysis resulted in a failure probability that is almost 5 times larger.

Of additional interest is the box shown in orange, which is a comparison between the FTA and simulation with the same typical data approach. This comparison shows more than four orders of magnitude difference in the results, where the failure probability of the fault tree solution was 4000 times larger than the simulation. The simulation needed 100,000 trials to obtain results for this value, as 10,000 trials did not produce a single failure. When using the same failure rate, all simulations produced a failure probability that is less than the FTA solution.

4.3. Simulation to Fault Tree Comparison

In order to evaluate the differences between our two analysis methods, let us look at a small part of the model. We will first focus on just one failure mode, represented by Cut Set #1 from Table 2:

Thruster Valve S1 Fails Open AND Thruster Valve S2 Fails Open

For the 3-year mission case, this cut set is quantified as:

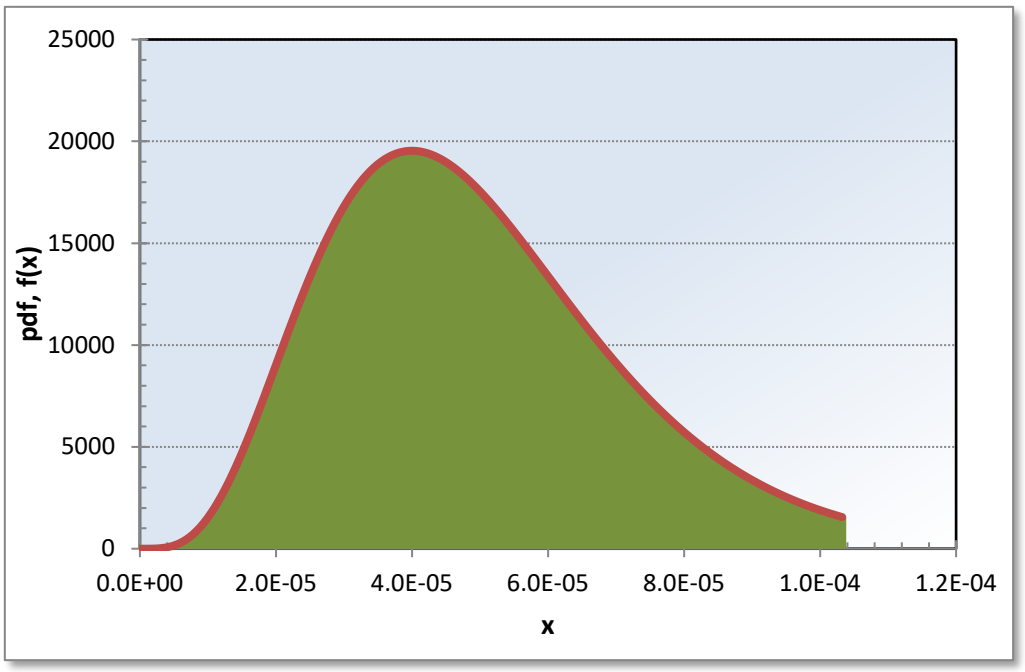
$$\begin{aligned} \text{Cut\_Set1} &= \text{TH-S1-FO} * \text{TH-S2-FO} \\ &= [1-\exp(-1.0x10^{-5}*26{,}281)]* [1-\exp(-1.0x10^{-5}*26{,}281)] \\ &= 2.31x10^{-1} * 2.31x10^{-1} \\ &= 5.35x10^{-2} \end{aligned}$$

However, the simulation results in Excel show that this failure mode occurs only a few times (0 to 5) for every 100,000 trials, giving a failure probability of between $2x10^{-5}$ to $3x10^{-5}$ for every simulation. The question then arises, why is the simulation much different than the fault tree approach? One part

of the answer is that the model of the world in the simulation is looking at useful component life based upon taking the reciprocal of diffusely defined failure rate, while the other part is modeling the complement of minimum reliability and treating it as an average reliability.

Recall that the gamma(2, 200000) distribution represents our knowledge of the failure rate for a thruster to fail open. It has a mean value of 1.0×10^{-5}. However, it is a distribution with a long tail to the right and portions near zero, as seen in Figure 3.

Figure 3: Gamma(2, 20000) Distribution



Cut Set #1 represents the situation with two thrusters that have failed open prior to 26,281 hrs (for the 3-year mission case). One question to ask is given the gamma distribution in Figure 3, what percentage of the distribution is greater than a failure rate represented by 1/26,281 or 3.8×10^{-5}? The answer to that question is 0.0043, which is at the 99.57^{th} percentile of the distribution! In other words, there is only a 0.0043 chance that one of the thrusters will fail open in less than 26,281 hours, given the failure rate of the failure modes are defined by gamma(2, 200000), and that failures can be represented via an exponential model which allows us to translate from failure rate to mean time to failure. Thus, the chance that two thrusters both fail before 26,281 hours is 0.0043 * 0.0043, or 1.8×10^{-5}. This is a large difference compared to the FTA derived failure probability of 2.8×10^{-1}, which is based upon computing average failure probabilities from very broad distributions.

4.4. Simulation Sanity Check

Although there was much cross-checking of the simulation routine in Matlab among the authors, as a sanity check, a second independent simulation was performed using Excel. This comparison used the baseline failure rate described in Section 3.2.1. and 100,000 trials. The results of this second simulation are shown in Table 8, along with the earlier results. The simulation results are reasonable when compared to each other, and both simulation results differ significantly from the fault tree results. Additionally, the time to failure statistics were compiled and compared, as shown in Table 9. Table 9 depicts the minimum, maximum, mean, and various percentile values for the times to failure given a gamma(2, 200000) distribution for both failure modes.

Although these values are correct in the mathematical sense, from an engineer's perspective, they are problematic. Dividing by a distribution with large tails has caused some large times to fail to appear in

the simulation. The mean time to failure of 200,000 hours is 22.8 years, which far exceeds any of the data points of failures at around six years. A time to failure of 193 million hours is more than 22,000 years. Again, this is the issue with using a gamma distribution with little information to represent failure times. At the lower end, engineers do all they can to limit premature failures, such as qualification testing, design margins, use of heritage parts, even building multiple components, and using the best builds.

Table 8: Simulation Comparison Results for Baseline Failure Rate

Probability of Failure (10k trials)	Matlab	Excel	FT
3-Year Mission (26,281 hrs)	**$7x10^{-5}$ (100k trials)**	$2.0x10^{-4}$	$2.8x10^{-1}$
5-Year Mission (43,801 hrs)	$1.8x10^{-2}$	$2.0x10^{-2}$	$5.5x10^{-1}$
10-Year Mission (87,603 hrs)	$3.8x10^{-1}$	$4.6x10^{-1}$	$9.2x10^{-1}$

Table 9: Times to Failure for Both Failure Modes Using Gamma(2, 200000)

Time to Failure (Hrs)	Excel 10k Sims	Excel 100k Sims	Matlab 10k Sims	Matlab 100k Sims
Minimum	13,501	12,221	12,373	12,373
Maximum	76,195,156	152,957,049	56,303,798	193,562,605
Mean	200,889	199,939	199,444	198,751
5th Percentile	42,230	42,173	42,390	42,167
10th Percentile	51,421	51,334	51,553	51,402
50th Percentile	119,369	119,218	119,904	119,045
90th Percentile	376,653	378,419	374,035	375,212
95th Percentile	563,599	564,195	561,875	562,016

4.5. Fault Tree Statistics

Statistics on fault tree results are quite common in the current state-of-the-practice. Although presented here for completeness, for certain applications, it is felt that the expected life statistics are of more use to a mission planner than the predicted reliability statistics. For example, telling a spacecraft operations team that the expected life is x hours at 90% confidence would allow them to plan activities accordingly, even potentially reduce the wear and tear of certain items if possible to meet other mission objectives. However, presenting a range of potentially high probability failure numbers is less valuable and likely ignored. In either case, it should always be emphasized that both the development of the model and the prioritization of relative risk drivers are more important than the absolute number.

The FTA statistics are presented in Table 10 for no correlation, correlation at the failure mode level, and complete correlation for both failure modes. This is for the baseline failure rate and a three-year mission. Table 10 shows that although there are differences in using correlation and at what level, this has a much lower effect on the results than the model of the world framework (simulation vs. fault tree).

Table 10: Fault Tree Statistics

FTA Results (Probability of Failure)	No Correlation	Correlation at Failure Mode	Correlation of All Failure Modes
Point Estimate	$2.8x10^{-1}$	$2.8x10^{-1}$	$2.8x10^{-1}$
Minimum	$1.8x10^{-2}$	$4.7x10^{-4}$	$6.2x10^{-6}$
Maximum	$8.2x10^{-1}$	$9.94x10^{-1}$	$9.997x10^{-1}$
Mean	$2.5x10^{-1}$	$3.0x10^{-1}$	$2.8x10^{-1}$
5th Percentile	$1.1x10^{-1}$	$4.7x10^{-1}$	$1.2x10^{-2}$
50th Percentile	$2.4x10^{-1}$	$2.7x10^{-1}$	$2.1x10^{-1}$
95th Percentile	$4.4x10^{-1}$	$7.0x10^{-1}$	$7.6x10^{-1}$

4.6. Simulation Convergence

Given that the simulations produced similar results for this simple model for both the 10,000 and 100,000 trial sets, the convergence of the results was examined for the case of gamma(2.5, 100000). The results are shown in Table 11. The result of this experiment is to show that in terms of obtaining reasonable results quickly, the simulation can produce reasonable results with a small number of iterations, as least for the failure rate to time ratios considered in these examples.

Table 11: Simulation Convergence for Gamma(2.5, 100000)

Alpha	Beta	Time	K Trials	System Reliability
2.5	100,000	3 Years	100	0.84
2.5	100,000	3 Years	500	0.89
2.5	100,000	3 Years	1000	0.849
2.5	100,000	3 Years	5000	0.8482
2.5	100,000	3 Years	10,000	0.8594
2.5	100,000	3 Years	50,000	0.85714
2.5	100,000	3 Years	100,000	0.8576
2.5	100,000	3 Years	500,000	0.857464
2.5	100,000	3 Years	1,000,000	0.857028
2.5	100,000	3 Years	10,000,000	0.857558

4.7. Potential Simulation Enhancements

Examination of the failure times in the simulation clearly demonstrates that using the reciprocal of a failure rate is an obvious issue and a major difference between the simulation and fault tree results. For a simple demonstration, Table 12 describes various gamma distributions that have the same mean, but with different parameters.

Table 12: Effects of Gamma Distribution Parameters in Sampling

Gamma (G)	G(1, 100,000)	G(2, 200,000)	G(10, 1,000,000)	G(20, 2,000,000)
Mean FR (/hr)	$1.0x10^{-5}$	$1.0x10^{-5}$	$1.0x10^{-5}$	$1.0x10^{-5}$
1/(Distribution Mean) (hrs)	100,000	100,000	100,000	100,000
1/(Sampling Mean) (hrs)	~1,400,000	~200,000	~111,000	~100,000
P_f(3 years)	0.003	0.0001	0	0
P_f(5 years)	0.06	0.02	0	0
P_f(10 years)	0.4	0.5	0.4	0

As the gamma distribution becomes more certain, the sampled times to failure become narrower. It is not until the gamma(20, 2,000,000) that the approximate sampling mean of 1 over the failure rate is seen. However, that narrower sampled time to failure distribution does not always result in a lower simulation failure probability, as shown in the gamma(2, 200,000) versus gamma(1, 100,000) simulation.. Modeling a distribution based on actual times to failure would give tighter results with much less data, as was shown in [1, 2].

Unfortunately, the amount of data available in certain industries is just not available to drive the bounds tighter, nor is there an expectation that data will become available. This is one of the problems faced with analysts in those industries. Additionally, there are several other areas that could use enhancements in future work. Simple additions to the methodology and simulation could be:

- The incorporation of truncated distributions to reduce the wildly spread times to failure, or the use of a reciprocal gamma distribution;
- Common cause failures;

- Inclusion of additional failure modes and their effect on the simulation to FTA comparison;
- Ranking of risk scenarios from the simulation;
- Dealing with lower probability system events, such as through failure rate*time transformations
- Creating more complex simulations with more components and failure modes to see the differences in the solutions

As the Probabilistic Risk Assessment (PRA) community looks to expand beyond traditional event tree and fault tree approaches, particularly into the use of simulation and other dynamic routines, considerations need to be given into modeling complex components with multiple failure modes and the effect that little data can have on the solutions. Although understanding and modeling the system is always of paramount importance, the use of simulation routines may be helpful in providing additional information, such as predicting useful or remaining system life, mission operations planning, maintenance models, and others, that the current state-of-the-practice methods do not easily provide.

5. CONCLUSIONS

The purpose of this work was to demonstrate the differences between using traditional fault tree (and by extension, event tree) models to assess components with multiple failure modes, and dealing with lack of data situations. The results showed that modeling complex components using traditional FTA models with lower failure rates yielded higher failure probabilities than simulation models with higher failure rates. The effects of both the modeling approach and the lack of data information in the failure rate predictions have a significant impact on the results. There is a clear difference in the results on using an average probability in time versus modeling time to failure. In comparison to the previous bodies of work [1, 2], doing simulations based on times to failure provided more realistic life values versus using 1/failure rate as a mean life; components typically do not survive to 100,000,000 hours, but that is the result of dividing by a distribution.

Additionally, as discussed in the previous work [1, 2] and presentations was the implication of what is meant by $R = e^{-\lambda t}$. Although this is typically called reliability, it is really the *minimum* reliability, from which the probability of failure, P_f, is calculated as

$$P_f = 1 - R_{min} = 1 - e^{-\lambda t} \quad (6)$$

The logical complement of minimum reliability is usually treated as an average in reliability software and applications, although this value could be construed as the maximum failure probability given Eqn. 6.

Although the predicted failure probabilities presented in this paper may seem high, failure probabilities of these levels are common in the space industry due to the lack of observed failures. Every space mission pushes the boundaries of what has been done before, and this results in failure rate predictions that are based on a non-informative prior and operational experience. The next Mars rover will exceed the planned and realized life of the past rover, the next satellite is expected to last at least as long as current technology, and space agencies are examining mission concepts of 20 to 50-year missions. Obviously, there is no data set that can provide statistical confidence in the component reliability of such missions as that boundary is continually pushed.

Unfortunately, these high failure probability predictions (high when compared to real-world experience that seems to have much better success than predicted) have long been a criticism of current methods and the state-of-the-practice. It is hoped that simulation routines will help bring the state-of-the-practice to a new level, closing the gap between predictions and future reality. Future work examining more sophisticated system models will shed light on the differences between these two methods in more detail. More importantly, the analysis is not just about the number, it is about the risk drivers. Comparisons between risk drivers from the two methods on more substantial models are

needed, in particular those that involve complex components. It is suspected that the risk driver will change as well, particularly those involving complex components with multiple failure modes.

Acknowledgments

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

References

[1] T. Paulos and C. Smith, C. "A Discussion of Failure Mode Modeling of Complex Components and Overall Component Reliability," Proceedings of the 13th International Conference On Probabilistic Safety Assessment and Management (PSAM 13), 2016. Available at https://iapsam.org/PSAM13/program/Abstract/Oral/A-558.pdf.

[2] T. Paulos, A. Ho and C. Smith, C. "Continued Discussion of Failure Mode Modeling and Overall Component Reliability: Are the Data Missing or Censored?", Proceedings of the 15th International Conference On Probabilistic Safety Assessment and Management (PSAM 15), 2020.

[3] D. Kelly and C. Smith, *Bayesian Inference for Probabilistic Risk Assessment*, 2011, ISBN 978-1-84996-187-5, Springer London.

[4] C.L. Atwood et al., "*Handbook of Parameter Estimation for Probabilistic Risk Assessment*," NUREG/CR-6823, 2003. Available at https://www.nrc.gov/docs/ML0329/ML032900131.pdf.

[5] GEP Box and GC Tiao, "*Bayesian Inference in Statistical Analysis*," John Wiley & Sons, New York, 2011.