PSAM16 Paper TP76

Reliability Modeling of Complex Components Using Simulation

Todd Paulos, Ph.D. and Andrew Ho.
Jet Propulsion Laboratory, California Institute of Technology, USA

Curtis Smith, Ph.D.
Idaho National Laboratory, USA

Jet Propulsion Laboratory
California Institute of Technology

Acknowledgement

- Thanks to Caltech/JPL, NASA, Lockheed Martin and Parker Hannifin for inspiration on this topic over the years

- “Be quick, be quiet, and be on time” – Kelly Johnson

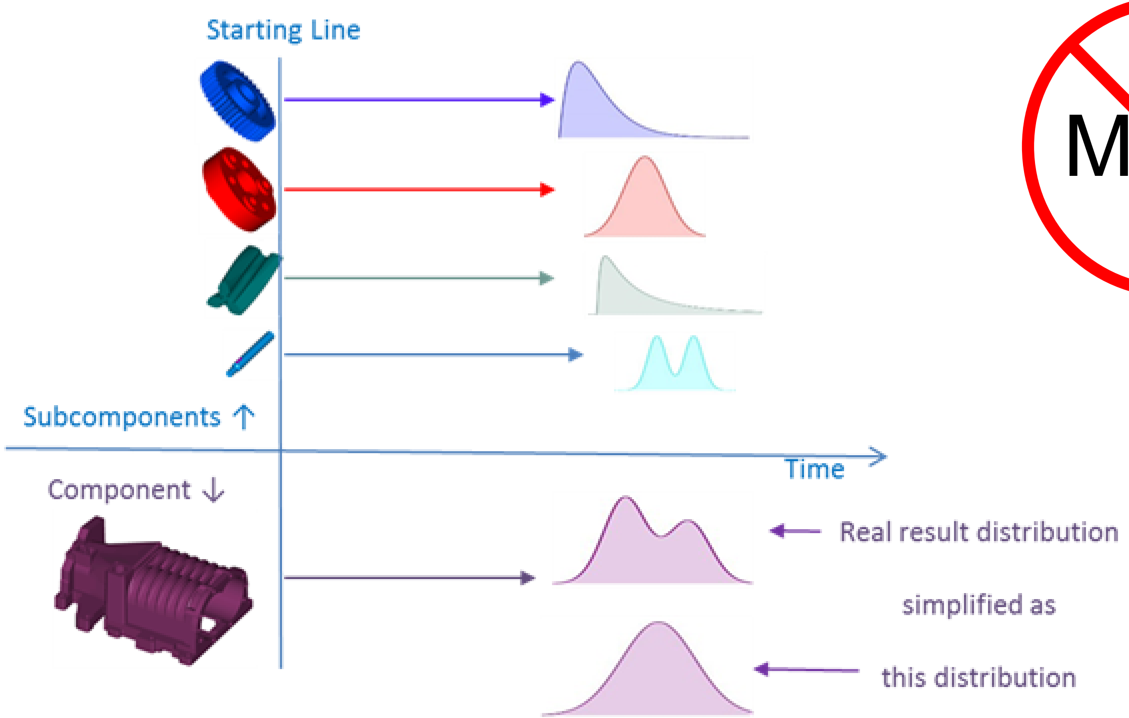
- “I believe in the golden rule: he who has the gold makes the rules” – Ben Rich

- “Do not go where the path may lead, go instead where there is no path and leave a trail” – Emerson

Topics

- Review of previous papers
  - "A Discussion of Failure Mode Modeling of Complex Components and Overall Component Reliability" presented at PSAM 13
  - "Continued Discussion of Failure Mode Modeling and Overall Component Reliability: Are the Data Missing or Censored?" presented at ESREL 2020 / PSAM 15
- Basics of Failure Mode simulation
- FTA vs. Simulation Comparisons
- Results Discussion

Simple Example: Supercharger



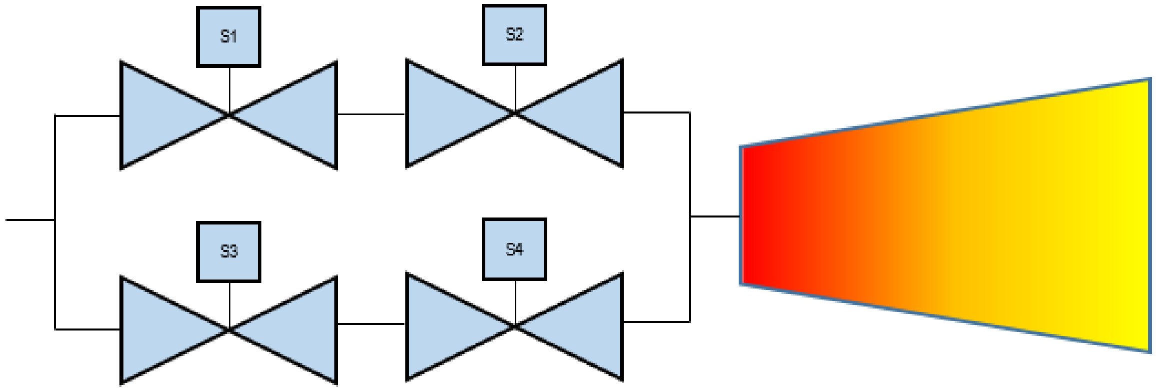
This methodology is useful in industries where there is repair data at the subassembly level, such as automotive, industrial, or aircraft Maintenance, Repair and Overhaul (MRO)

Exponential vs. Censored vs. Missing Data

Failure Mode	Exponential (Hrs)	Censored (Hrs)	Missing (Hrs)
A	367	176	100
B	367	174	125
C	367	166	144

Trial	A	B	C
1	100	>100	>100
2	>75	75	>75
3	>125	>125	125
4	75	>75	>75
5	>100	100	>100
6	>150	>150	150
7	125	>125	>125
8	>200	200	>200
9	>150	>150	150

Simple Monoprop Thruster (1/2)



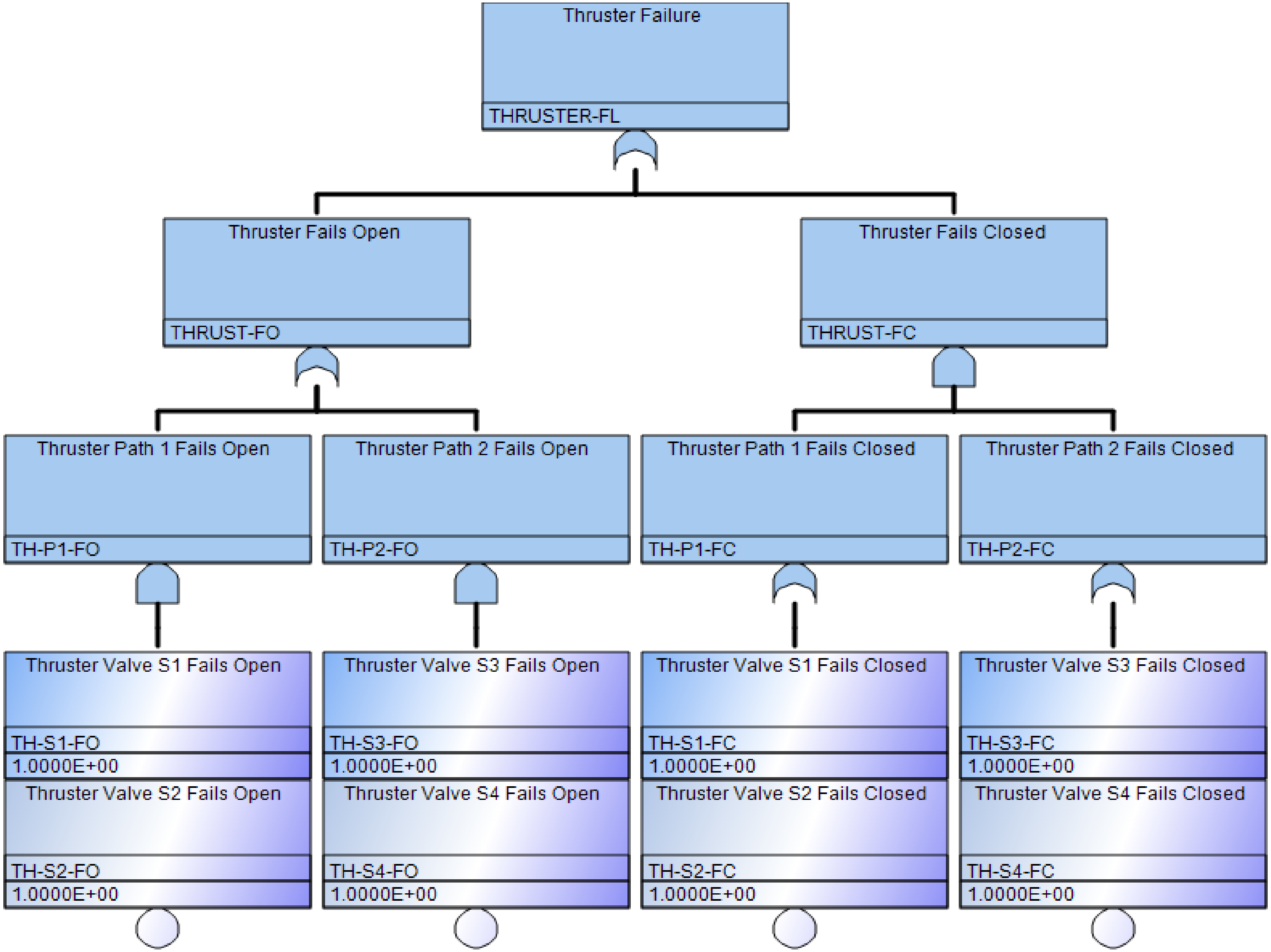
- Compare traditional FTA vs. simulation solution
  - Valves can fail open or closed, but not both
- Success criteria
  - Need at least on flow pathway to operate, need both pathways to close to conserve fuel
- Compare various data assessment methods for failure modes and the effect on the results

Monoprop Thruster Failure Data

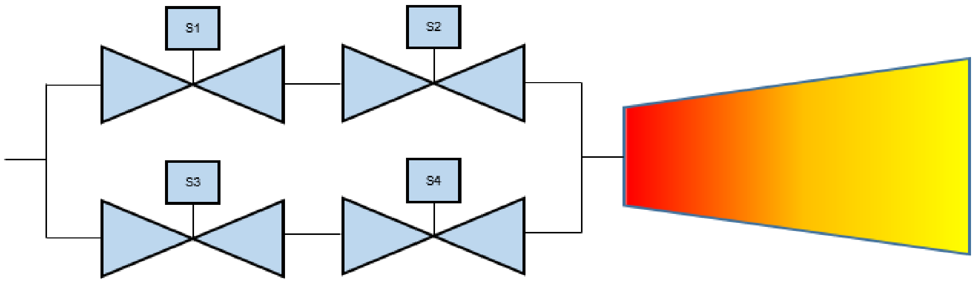
Failure Mode	Time to Failure (Hrs)
Fail Open	45,000
Fail Closed	45,000
Fail Open	55,000
Fail Closed	55,000

- Consider failure modes caused by different and unique hardware subassemblies
- Method 1: Simple Data Analysis Method
  - Failure Modes are exponential
  - Each failure mode has a failure rate estimated as 2/200,000 hrs (1E-5 /hr)
- Alternative Data Analysis Method 1
  - Failure modes are treated as missing data
  - Each failure mode has a failure rate estimated as 2/100,000 hrs (2E-5 /hr)
- Alternative Data Analysis Method 2
  - Bayesian solution with missing data using Jefferys' non-informative prior (ref: HOPE)
  - Each failure mode has a failure rate estimated as 2.5/100,000 hrs (2.5E-5 /hr)

Thruster Fault Tree Analysis



FTA Minimal Cut Sets



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

Simulation Algorithm

- Step 1 Establish parameters
  - Input mission time in hours
  - Input the gamma distribution parameters for each component failure mode
  - Input number of desired trials k
  - 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 MCS 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.

Simulation Algorithm

- 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?

Simulation Algorithm

- Step 4 Determine if a system failure occurred in the mission time
  - Determine if any of the six system failures 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

One Simulation Trial (No SOK Correlation)

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

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

FTA Vs. Simulation Results Comparison

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	$3.8x10^{-1}$	$8.5x10^{-1}$	$9.5x10^{-1}$

Discussion of Results

- PRA community has been looking at simulation for some time, but no standard state-of-the-practice exists
- Simulations are very different models of the world than traditional models
  - Model of life vs. probability of failure give different results
  - Simulation trials can give very odd (e.g., unrealistic) life values
- Simulations seem better for large failure probability system based upon experience; small probabilities are difficult to compare (some industries have little failure statistics)
- Difference between small vs. large statistics, but doesn't appear to be the main driver

Further Discussions Continued in the Paper

- Comparison of Simulation Routines (Matlab vs. Excel)
- Effects of using a diffuse gamma distribution
  - 1/distribution sample for time to failure
  - Maximum life values
- Convergence of simulations
- State of Knowledge correlations
- Additional uses of simulation
  - Maintenance
  - Useful life or other life statistics
  - Mission operation decisions
- Further improvements
  - More complex components
  - Common cause failures
  - Better modeling of life times

Reminders

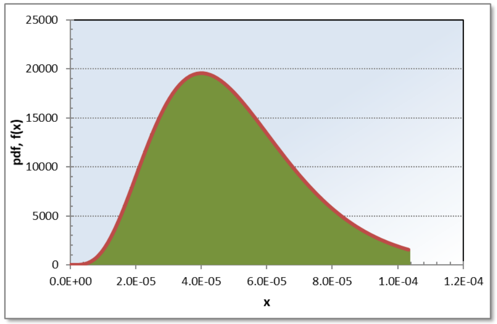
$$R_{Min}(X_1, X_2, \cdots, X_n) = e^{-[(\sum_i^n \lambda_n)t]}$$

$$P_f \stackrel{?}{=} 1 - R_{Min}$$

Sum of two exponential distributions is

$$f(t) = x = \frac{\lambda_1 \lambda_2}{\lambda_2 - \lambda_1}\left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right)$$

Gamma distributions with small data sets have large uncertainty bounds can be large

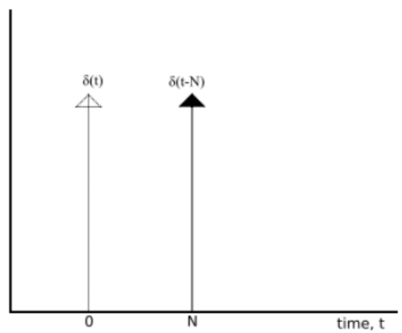


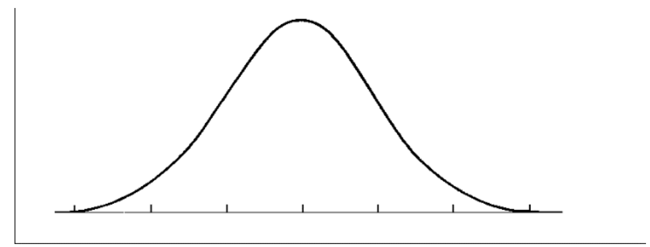
Questions?

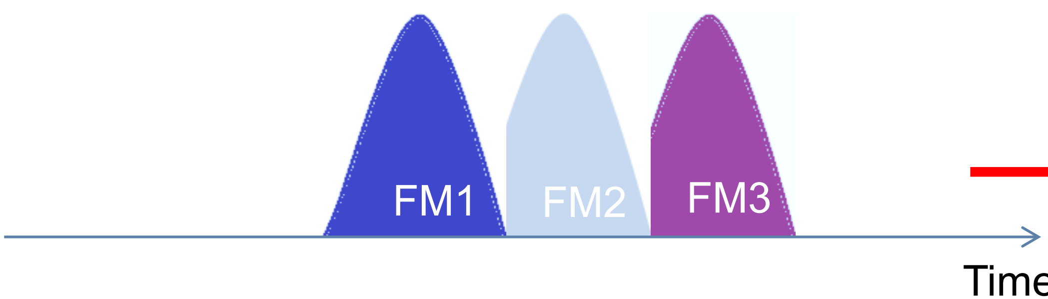
Backup

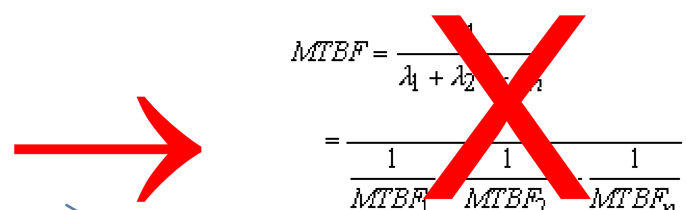
Failure Modes of Complex Assemblies

Components vs.
Assemblies vs.
Subassemblies vs. …









OpenBUGS Simulation with Censored Data

Node	mean	5th	50th	95th
T.TE	118	30	125	182
TA	176	52	167	327
TB	174	67	167	304
TC	166	104	163	235
mu.A	176	127	167	254
mu.B	174	131	167	239
mu.C	166	140	163	200
tau.A	3.3E-04	5.1E-05	2.7E-04	8.2E-04
tau.B	4.1E-04	7.5E-05	3.4E-04	9.6E-04
tau.C	1.3E-03	2.5E-04	1.1E-03	3.0E-03

Vs.

Failure Mode	Number	Total Time	Failure Rate (/hrs)	MTBF
A	3	1100	0.0027	367
B	3	1100	0.0027	367
C	3	1100	0.0027	367

```
model                    {
# Loop through the observed and censored times
for (i in 1:N)           {
T.A[i] ~ dnorm(mu.A, tau.A)C(lowerA[i], )
T.B[i] ~ dnorm(mu.B, tau.B)C(lowerB[i], )
T.C[i] ~ dnorm(mu.C, tau.C)C(lowerC[i], )
}
# Replicate the posterior model for failure times
TA ~ dnorm(mu.A, tau.A)
TB ~ dnorm(mu.B, tau.B)
TC ~ dnorm(mu.C, tau.C)
# Find the minimum times
AB <- min(TA, TB)
T.TE <- min(AB, TC)
# diffuse priors
mu.A ~ dflat()
mu.B ~ dflat()
mu.C ~ dflat()
tau.A ~ dunif(0,100)
tau.B ~ dunif(0,100)
tau.C ~ dunif(0,100)
}
data
list(T.A=c(100,NA,NA,75,NA,NA,125,NA,NA), T.B=c(NA,75,NA,NA,100,NA,NA,200,NA),
T.C=c(NA,NA,125,NA,NA,150,NA,NA,150),
lowerA=c(100,75,125,75,100,150,125,200,150), lowerB=c(100,75,125,75,100,150,125,200,150),
lowerC=c(100,75,125,75,100,150,125,200,150), N=9)

inits
          list(mu.A=367, mu.B=367, mu.C=367, tau.A=2, tau.B=2, tau.C=2)
          list(mu.A=300, mu.B=300, mu.C=300, tau.A=2, tau.B=2, tau.C=2)
```

New for this paper: Use of Python script to generate OpenBUGS code to reduce errors

Missing and censored versions of the script

Three Failure Modes Example

Trial	A	B	C
1	100	>100	>100
2	>75	75	>75
3	>125	>125	125
4	75	>75	>75
5	>100	100	>100
6	>150	>150	150
7	125	>125	>125
8	>200	200	>200
9	>150	>150	150

Failure Mode	Number	Total Time	Failure Rate (/hrs)	MTBF
A	3	1100	0.0027	367
B	3	1100	0.0027	367
C	3	1100	0.0027	367

From “A Discussion of Failure Mode Modeling of Complex Components and Overall Component Reliability”

Simulation Results Comparison

Data Set Size = 100

	FM1 (8,000 Hrs)	FM2 (10,000 Hrs)	FM3 (12,000 Hrs)
Known	8,000	10,000	12,000
Exponential	8,530	38,387	76,773
Exp Diff	6.6%	283.9%	539.8%
Censored	13,340	12,800	12,790
Cens Diff	66.8%	28.0%	6.6%
Missing	8,012	9,978	11,610
Miss Diff	0.1%	0.2%	3.3%

The “missing” data approach has reduced all three failure modes to less than 4% error for each

Censored vs. Missing Data

- Likelihood is the product of the probability density functions given the observed data, so in general

$$L(\theta) = \prod_{i=1}^{N} f_i\,(t_i) = \prod_{i=1}^{N} L_i(\theta;\ t_i)$$

- Likelihood of a failure

$$L_i(\theta;\ t_i) = \int_{-\infty}^{t_i} f_i(x)dx = F(t_i) - F(0) = F(t_i)$$

- Survival, with right censored data

$$L_i(\theta;\ t_i) = \int_{t_i}^{\infty} f_i(x)dx = F(\infty) - F(t_i) = 1 - F(t_i)$$

- Missing data ignores the likelihood term altogether

Censored vs. Missing Data Example

- Three failure modes: A, B, and C
- Failure mode A occurs, and B and C are still operational
- Censored treatment of data

$$L_i(\theta;\ t_i) = F_A(t_A)[1 - F_B(t_A)][1 - F_C(t_A)]$$

- Missing treatment of data

$$L_i(\theta;\ t_i) = F_A(t_A)$$

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov