NASA Applications and Lessons Learned in Reliability Engineering

Fayssal M. Safie, PhD, NASA Marshall Space Flight Center

Raymond P. Fuller, PhD, NASA Marshall Space Flight Center

Key words: reliability, probabilistic, design, process, operational, risk

SUMMARY & CONCLUSIONS

Since the Shuttle Challenger accident in 1986, communities across NASA have been developing and extensively using quantitative reliability and risk assessment methods in their decision making process. This paper discusses several reliability engineering applications that NASA has used over the year to support the design, development, and operation of critical space flight hardware. Specifically, the paper discusses several reliability engineering applications used by NASA in areas such as risk management, inspection policies, components upgrades, reliability growth, integrated failure analysis, and physics based probabilistic engineering analysis. In each of these areas, the paper provides a brief discussion of a case study to demonstrate the value added and the criticality of reliability engineering in supporting NASA project and program decisions to fly safely. Examples of these case studies discussed are reliability based life limit extension of Shuttle Space Main Engine (SSME) hardware, Reliability based inspection policies for Auxiliary Power Unit (APU) turbine disc, probabilistic structural engineering analysis for reliability prediction of the SSME alternate turbo-pump development, impact of ET foam reliability on the Space Shuttle System risk, and reliability based Space Shuttle upgrade for safety.

Special attention is given in this paper to the physics based probabilistic engineering analysis applications and their critical role in evaluating the reliability of NASA development hardware including their potential use in a research and technology development environment.

1 *INTRODUCTION*

Reliability is the probability that an item will perform its intended function for a specified mission profile. High reliability means design it right and build it right. To achieve high reliability one must:

- Establish a reliability requirement.
- Use qualitative and quantitative analysis methods and tools to verify the requirement is met.
- Analyze the manufacturing, assembly, and test procedures concurrent with the design process.
- Use concurrent engineering to get everybody involved upfront.

As shown in Figure 1, reliability is defined in terms of design reliability [1] and process reliability. Design reliability is analyzed in many different ways. One way of evaluating design reliability is shown in Figure 2. In Figure 2, reliability is derived using design information. Specifically, reliability is defined as load and environment (performance) versus capability. On the other hand, in Figure 3, process reliability, is concerned with mapping the critical design parameters to processing, process characterization, and process control. This paper discusses several case studies that address both the design reliability and process reliability.

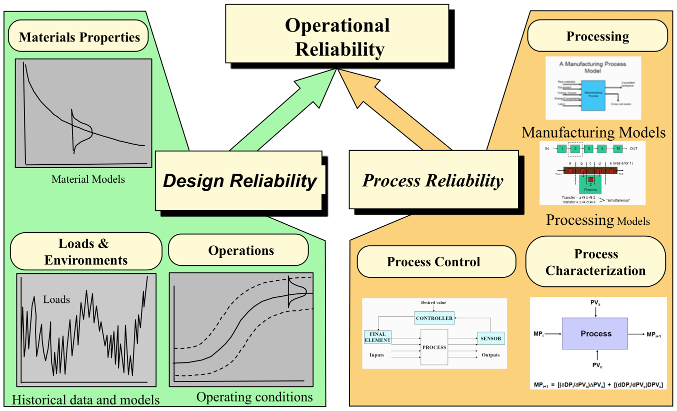

Figure 1 Operational Reliability.

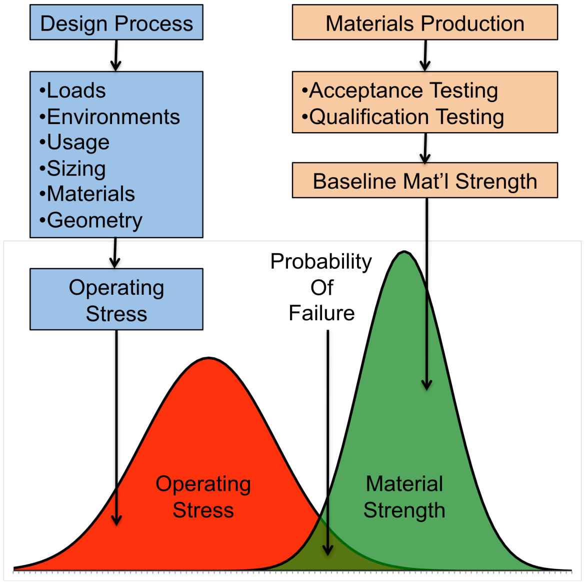

Figure 2 Design reliability.

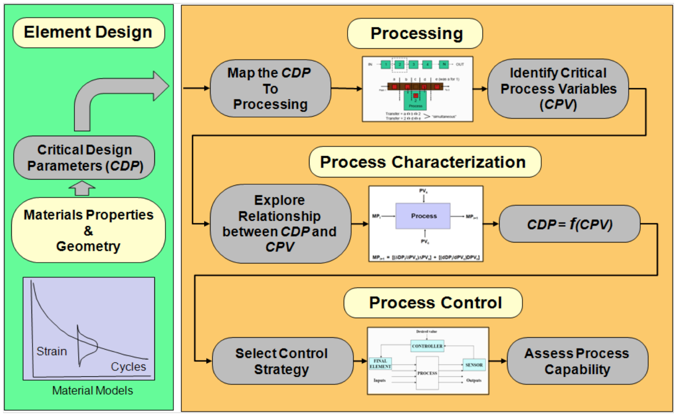
Element Design
Critical Design Parameters (CDP)
Materials Properties & Geometry
Strain
Cycles
Material Models
Processing
Map the CDP To Processing
Identify Critical Process Variables (CPV)
Process Characterization
Explore Relationship between CDP and CPV
Process
CDP = f(CPV)
Process Control
Select Control Strategy
CONTROLLER
FINAL ELEMENT
PROCESS
SENSOR
Inputs
Outputs
Assess Process Capability

Figure 3 Process reliability.

2 RELIABILITY APPLICATIONS

The following sections provide examples of reliability studies that were used to support critical Space Shuttle decisions.

2.1 A Lesson Learned in Process Reliability

This case study discusses the importance of quality in system design, and the relationship between quality, reliability, and system safety for space vehicles.

The difficulties and sensitivities of the Space Shuttle External Tank (ET) Thermal Protection System (TPS) manual spray process is a good demonstration of the impact of process control on component reliability and system risk.

The TPS is a foam type material applied to ET to maintain cryogenic propellant quality, minimize ice/frost formation, and protect the structure from ascent, plume, and re-entry heating. Figure 4 shows the main ET components that have TPS foam sprayed by automated or manual processes.

The reliability of the TPS is broadly defined as its strength versus the stress put on it in flight. High TPS reliability means less debris released and fewer hits to the orbiter, reducing system risk. Process control is a critical factor in achieving high reliability and low system risk. Good process uniformity and high process capability yield fewer process defects, smaller defect sizes, and good material properties that meet the engineering specification—the critical ingredients of high reliability and low system risk. Figure 5 shows the impact of process control on foam process reliability and on system risk. Figure 6 shows the relationship between quality, reliability, and system risk. These relationships were developed and applied as part of the post Columbia accident efforts to return to flight. The clear message from the Columbia accident and the ET TPS foam experience is that inadequate manufacturing and quality control can have a severe negative impact on component reliability and system safety. It is also critical to understand the relationship between process control, component reliability, and system safety up front in the design process.

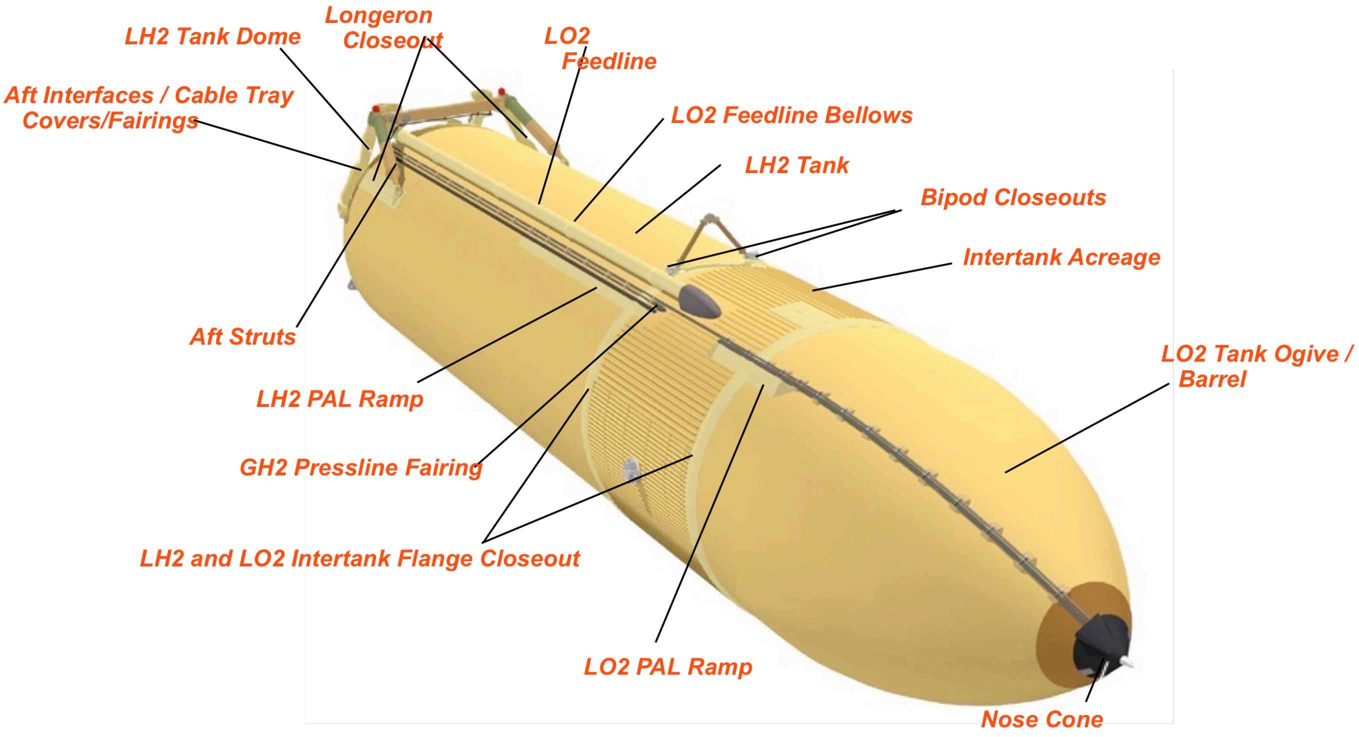

Figure 4 Space Shuttle External Tank (ET).

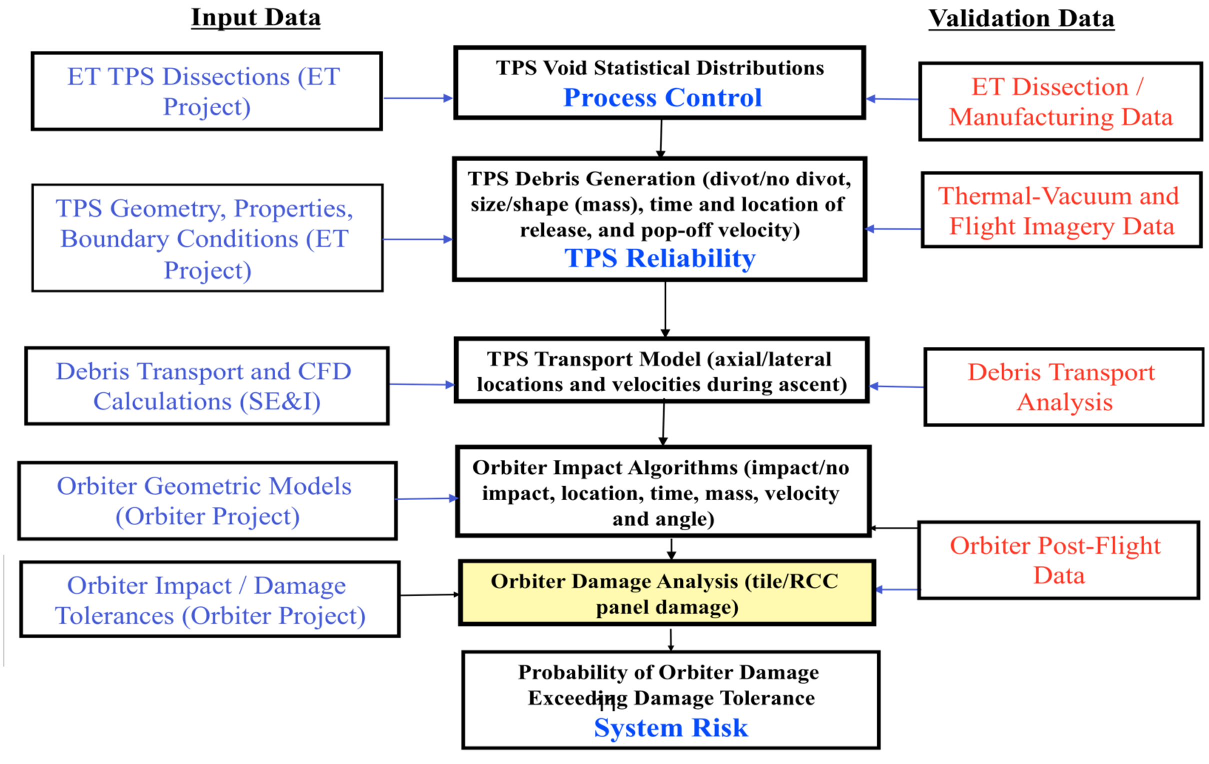
Input Data
Validation Data
ET TPS Dissections (ET Project)
TPS Void Statistical Distributions
Process Control
ET Dissection / Manufacturing Data
TPS Geometry, Properties, Boundary Conditions (ET Project)
TPS Debris Generation (divot/no divot, size/shape (mass), time and location of release, and pop-off velocity)
TPS Reliability
Thermal-Vacuum and Flight Imagery Data
Debris Transport and CFD Calculations (SE&I)
TPS Transport Model (axial/lateral locations and velocities during ascent)
Debris Transport Analysis
Orbiter Geometric Models (Orbiter Project)
Orbiter Impact Algorithms (impact/no impact, location, time, mass, velocity and angle)
Orbiter Post-Flight Data
Orbiter Impact / Damage Tolerances (Orbiter Project)
Orbiter Damage Analysis (tile/RCC panel damage)
Probability of Orbiter Damage Exceeding Damage Tolerance
System Risk

Figure 5 Impact of process control on system risk.

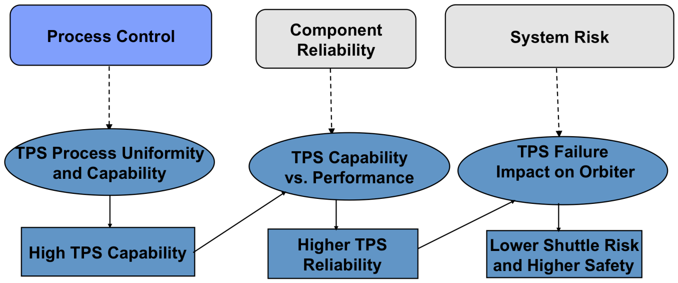
Process Control
Component Reliability
System Risk
TPS Process Uniformity and Capability
TPS Capability vs. Performance
TPS Failure Impact on Orbiter
High TPS Capability
Higher TPS Reliability
Lower Shuttle Risk and Higher Safety

Figure 6 Relationships between process control, reliability, and system risk.

The clear message from the Columbia accident and the ET TPS foam experience is that inadequate manufacturing and quality control can have a severe negative impact on component reliability and system safety. It is also critical to understand the relationship between process control, component reliability, and system safety up front in the design process.

2.2 A Reliability-Based Inspection Policy

Post Challenger Accident, a major simulation modeling effort (shown in Figure 7) was conducted to evaluate the reliability of the Shuttle APU turbine wheel [2]. The simulation model was designed to determine the probability of failure of the APU turbine wheel due to critical blade crack (shown in Figure 8) given that the wheel has to operate for some specified life limit during which a given inspection policy is imposed. The simulation model also allows the analyst to study the trade-offs between wheel reliability, wheel life, inspection interval, and rejection crack size.

Using the simulation model, analysis results showed that for a wheel life limit of 100 Hot Gas Starts (HGS's), an inspection interval of 16 HGS, and a rejection flaw size of 90 mils, the APU reliability is estimated to be 0.99994. Based on these result, the program decision was to establish a 16-starts inspection interval and 100 starts life limit. Inspection intervals could have a major impact on reliability.

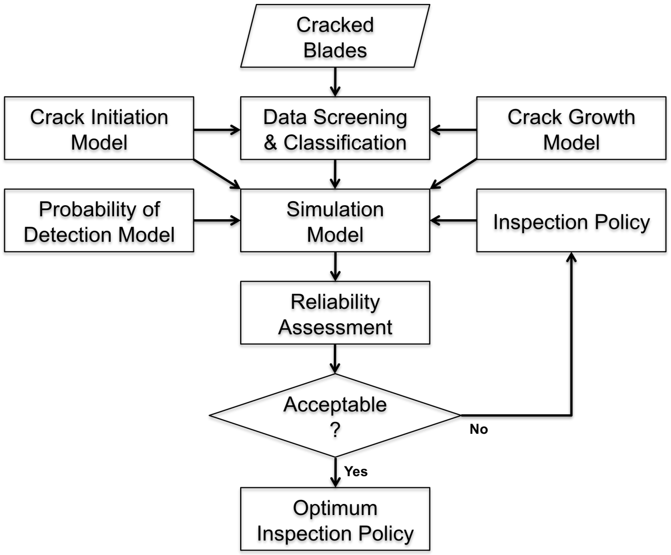

Figure 7 Shuttle APU blade crack model.

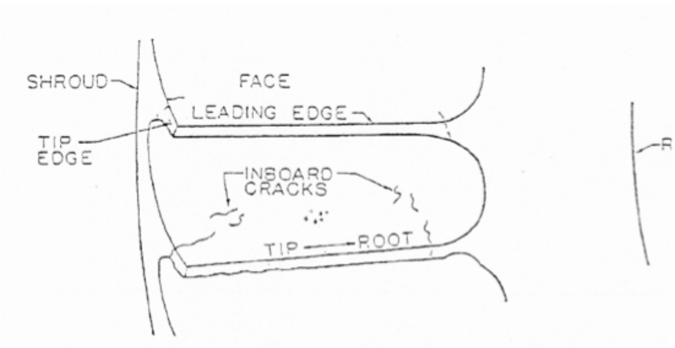

Figure 8 Typical APU blade cracks.

2.3 Reliability Based Risk Management

As part of the National Aeronautics and Space Administration (NASA) effort to introduce the use of probabilistic models in managing the risk for the critical Space Shuttle hardware, a tool was developed [3] to derive a life limit for a given component subject to a specified reliability and confidence level requirement. The statistical tool developed is based on Weibull time to failure distribution, combined with an optimization technique used to derive the minimum life limit that meets the reliability requirement. The model that applies to components with no failure data is called the Weibayes. The Weibayes, which was used in this study, is basically a Weibull with an assumed Beta. In this study, since the shape parameter of the Weibull distribution varies for different components, an optimization technique is used in combination with the statistical technique to derive a life limit, which does not require knowledge of the shape parameter value. The life limit derived is constrained by a specified reliability and confidence level.

The steps to determine the life limits are as follows:

1) Make sure "no failures or major Material Review Board (MRB) history"
2) Collect fleet hot fire history
    - Seconds for High Cycle Fatigue (HCF) failure mode application
    - Starts for Low-Cycle Fatigue (LCF) failure mode application (or transients for some nozzle applications)
3) Make sure units for SFR calculation are from the same configuration or present strong argument that prior configurations have lower or equal reliability
4) Input fleet data (time history) into the SFR computer program
5) Run the computer program to obtain results (4 values)
    - 25th percentile fleet leader
    - 50th percentile fleet leader
    - 6th highest unit
    - SFR math model value
6) Pick the minimum of the 50th percentile, the 6th highest, and the SFR math model value.
7) If the minimum is less than the 25th percentile, use the 25th percentile as the life limit.
8) If the minimum is greater than the 50th percentile use the 50th percentile as the life limit.

Figure 9 is an example application of the above process to a fuel bleed duct of the Space Shuttle Main Engine. The life limit derived in this case was 34th percentile.

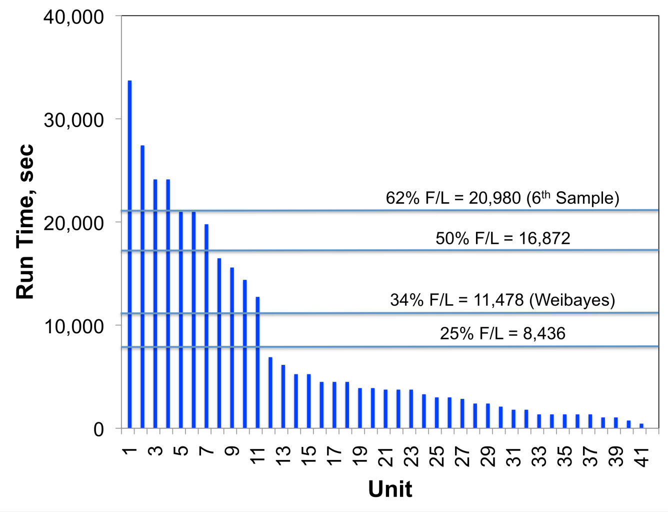

Figure 9 Life limits of a fuel bleed duct.

In summary, this case study provides a dynamic risk management tool to consistently and effectively determine the life limit of specified SSME hardware based on the fleet operational history. The tool developed, combined with other engineering considerations, is being used as part of a general life limit specification for the SSME.

2.4 Reliability Tracking

The reliability growth of a system takes place due to changes introduced into the system structure. These changes make it difficult to estimate the system reliability using a classical model such as the binomial model. Thus, it is desirable to model the growth by a "growth model." A reliability growth model is an analytical tool used to monitor the reliability progress during the developmental program, and to establish a test plan to demonstrate acceptable system reliability. Some of the advantages of using a reliability growth model are:

- Determining the intensity of Test, Analyze, and Fix (TAAF) to reach reliability objectives.
- Predicting whether stated reliability objectives will be achieved.
- Correlating reliability changes with reliability activities and tracking progress.
- Planning for a reliability demonstration test.

The most widely used reliability growth model is the AMSAA. The AMSAA reliability growth model was developed by Crow and is reported in MIL HDBK 189. The AMSAA model is designed for tracking the reliability within a test phase and not across tests phases. The model assumes that within a test phase, reliability growth can be modeled as a non-homogeneous Poisson process (NHPP). The model assumes that within a test phase, the cumulative failure rate is linear on log-log-scale. The AMSAA model evaluates the reliability growth that results from the introduction of design fixes into the system and not the reliability growth that may occur at the end of a test phase due to delayed fixes.

The AMSAA model assumes that the intensity function can be approximated by a continuous parametric function, i.e.

$$\rho(t) = \lambda\beta t^{\beta-1} \quad t > 0, \lambda > 0, \beta > 0, \tag{1}$$

which is the Weibull failure rate function where λ is the scale parameter and β is the shape parameter. Thus, the mean value function is

$$E(N(t)) = \theta(t) = \lambda t^{\beta}. \tag{2}$$

For β = 1, $\rho(t)$ is constant, indicating an homogeneous Poisson process (HPP). For β < 1, $\rho(t)$ is decreasing, indicating reliability growth. For β > 1, $\rho(t)$ is increasing, indicating deterioration in system reliability. It should be noted that the model assumes that $\rho(t)$ is approximated by a Weibull intensity function and not the Weibull distribution. Thus, statistical techniques used for the Weibull distribution are not applicable to $\rho(t)$.

To estimate the parameters of the AMSAA model, two procedures exist. One procedure is used for time terminated testing, and the second one is for failure terminated testing. The SSME used the time-terminated testing procedure. For time terminated testing β is estimated by

$$\hat{\beta} = \frac{N}{N \ln T - \sum_{i=1}^{N} \ln x_i}, \tag{3}$$

where N = number of failures, T = accumulated test time, and x_{i} = failure times. Using β, the estimate of λ is

$$\hat{\lambda} = N / T^{\beta}. \tag{4}$$

Using both parameter estimates, the instantaneous failure rate is given by:

$$m(T) = 1/\hat{\rho}(T), \tag{5}$$

Where,

$$\hat{\rho}(T) = \hat{\lambda}\hat{\beta}T^{\hat{\beta}-1}. \tag{6}$$

Based on the data shown in Table 1 the following is an example from the SSME program. Using the equations above for the SSME data, the SSME instantaneous Mean Time Between Failures (MTBF) and the engine mission reliability are calculated and the total time of T = 373,868 sec. The β and λ are determined using Equations 3 and 4:

$$\hat{\beta} = 0.4228 \quad \text{and} \quad \hat{\lambda} = 0.05725.$$

Notice that a β of 0.4278 indicates a growth. Using these λ and β, the instantaneous MTBF is 68,021. The MTBF is then used to calculate the engine reliability for a mission time of 520 sec,

$$R(520) = e^{-\text{mission duration / inst.MTBF}} = 0.9924.$$

Table 1 Cumulative Test Time Versus Failures.

Failure i	Cumulative Failure Time x_{i}, sec
1	505
2	10,348
3	10,872
4	15,516
5	15,844
6	48,168
7	48,476
8	55,606
9	78,724
10	97,648
11	158,674
12	206,712
13	270,242

and the total time of T = 373,868 sec. The β and λ are determined using Equations 3 and 4:

$$\hat{\beta} = 0.4228 \quad \text{and} \quad \hat{\lambda} = 0.05725.$$

Notice that a β of 0.4278 indicates a growth. Using these λ and β, the instantaneous MTBF is 68,021. The MTBF is then used to calculate the engine reliability for a mission time of 520 sec,

$$R(520) = e^{-\text{mission duration / inst.MTBF}} = 0.9924.$$

The SSME reliability growth analysis was developed after the Challenger accident and has been used since then. It has provided a tool to evaluate and track reliability, evaluate the effectiveness of the test program, and evaluate the effectiveness of design and process changes.

2.5 Physics-Based Reliability

Probabilistic engineering analysis is used when failure data is not available and the design is characterized by complex geometry or is sensitive to loads, material properties, and environments. The following is an example of a reliability application to an SSME bearing inner race crack problem (shown in Figure 10) that was solved using physics-based probabilistic analysis.

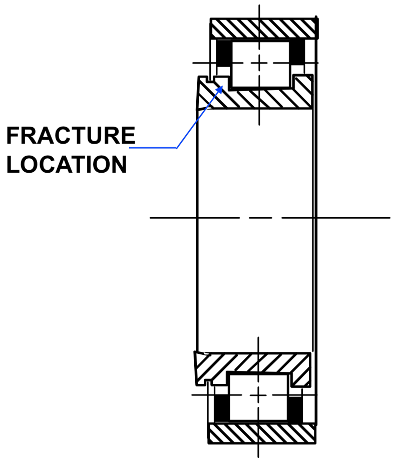

Figure 10 SSME Turbo-pump bearing fracture location.

The objective of the study [4] was to predict the probability of inner race over-stress under conditions experienced in the test rig and to estimate the effect of manufacturing stresses on the fracture probability. The simulation model used is shown in Figure 11.

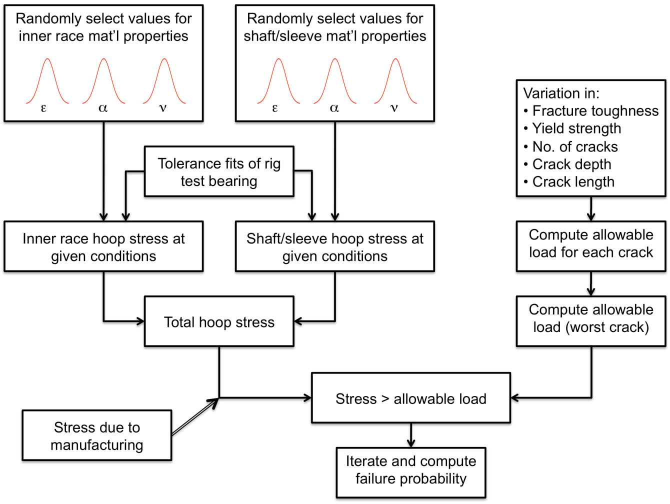
Randomly select values for inner race mat'l properties
ε
α
ν
Randomly select values for shaft/sleeve mat'l properties
ε
α
ν
Variation in:
• Fracture toughness
• Yield strength
• No. of cracks
• Crack depth
• Crack length
Tolerance fits of rig test bearing
Inner race hoop stress at given conditions
Shaft/sleeve hoop stress at given conditions
Compute allowable load for each crack
Total hoop stress
Compute allowable load (worst crack)
Stress > allowable load
Stress due to manufacturing
Iterate and compute failure probability

Figure 11 SSME Turbo-pump bearing simulation model.

The result from the simulation model shown in Table 2 led to a change in the material of the bearing inner race from 440C to the 9310. Justification for the change in material is explained in Table 2.

Table 2 Turbo-pump Bearing Analysis Results

Test Failures	Race Configuration	Failures in 100,000 firings**
3 of 4	440C w/ actual* mfg. stresses	68,000
N/A	440C w/ no mfg. stresses	1,500
N/A	440C w/ ideal mfg. stresses	27,000
0 of 15	9310 w/ ideal mfg. stresses	10

*ideal + abusive grinding

**Probabilistic Structural Analysis

3 CONCLUDING REMARKS

Quantitative reliability engineering analysis:

- Involves more than just reliability predictions and reliability demonstration that are performed against a given program or project requirements.
- Can play a key role in supporting abroad range of applications such as risk management, inspection policies, life limits, and design trades.
- Analysis is critical to addressing design and manufacturing deficiencies.

REFERENCES

1. Safie, F. M., "Design for Reliability," *Presentation at the 39th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics & Materials Conference*, April 1998.
2. Safie, F. M., Hage, R. T., and Smith, W. C., "A Simulation Model for Reliability Evaluation of Turbine Wheels," *Proceedings of the First Annual Symposium on Mechanical System Design in a Concurrent Engineering Environment: Concurrent Engineering of Mechanical Systems Volume I*, edited by E. J. Haug, 1989, pp. 143-151.
3. Safie, F. M., "A Statistical Approach for Risk Management of Space Shuttle Main Engine Components," *Probabilistic Safety and Management*, edited by G. Apostolakis, Elsevier Science Publishing Co., Inc., 1991, pp. 1437-1443
4. Safie, F. M. and Fox, E. P., "A Probabilistic Design Analysis Approach for Launch Systems," AIAA Paper 91-3372, June 1991.

BIOGRAPHIES

Fayssal M. Safie, PhD, CRE
NASA Marshall Space Flight Center / QD30
Huntsville, Alabama 35812 USA

e-mail: fayssal.safie@msfc.nasa.gov

Dr. F. Safie is currently serving as The NASA Reliability and Maintainability (R&M) Technical Fellow lead. He joined NASA in 1986 as a reliability and quality engineer at Marshall Space Flight Center (MSFC). He received Over 50 honors and Awards including the NASA Exceptional Engineering Achievement Medal, the NASA Flight Safety Award, the NASA Quality Assurance Special Achievement Recognition (QASAR) Award, and the NASA Silver Snoopy Award. He published over 40 papers in R&M Engineering, Probabilistic Risk Assessment, System Safety, Quality Engineering, and Computer Simulation. Besides his responsibility as a NASA Tech Fellow, Dr. Safie is serving as an Adjunct Professor in the Systems Engineering Department at the University of Alabama in Huntsville (UAH). He has a Bachelor degree in science, a Bachelor, a Master, and a Doctorate in engineering.

Raymond P. Fuller, Ph.D.
NASA Marshall Space Flight Center / QD30
Huntsville, Alabama 35812 USA

e-mail: ray.fuller@nasa.gov

Dr. Raymond Fuller is a Flight Systems Engineer specializing in Risk and Reliability for the NASA Marshall Space Flight Center (MSFC) Safety & Mission Assurance (S&MA) Directorate. He has over 15 years of aerospace engineering experience in academia, industry, and government. Dr. Fuller joined NASA in 2006 before which he worked at Northrop Grumman Space Technology as a Project Reliability Manager. His technical interests include Probabilistic Design Analysis (PDA), Reliability-Based Design (RBD) and Design Optimization (RBDO), Probabilistic Risk Assessment (PRA), and Failure Analysis. He has a B.S. in aerospace engineering from the University of Michigan (1992), and a M.S and Ph.D. in aerospace engineering from Virginia Tech (1994, 1996).