The Role of Probabilistic Design Analysis Methods in Safety and Affordability

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

Key Words: NASA, Probabilistic Design Analysis, Reliability, Safety, and affordability

SUMMARY & CONCLUSIONS

For the last several years, NASA and its contractors have been working together to build space launch systems to commercialize space. Developing commercial affordable and safe launch systems becomes very important and requires a paradigm shift. This paradigm shift enforces the need for an integrated systems engineering environment where cost, safety, reliability, and performance need to be considered to optimize the launch system design. In such an environment, rule based and deterministic engineering design practices alone may not be sufficient to optimize margins and fault tolerance to reduce cost. As a result, introduction of Probabilistic Design Analysis (PDA) methods to support the current deterministic engineering design practices becomes a necessity to reduce cost without compromising reliability and safety.

This paper discusses the importance of PDA methods in NASA's new commercial environment, their applications, and the key role they can play in designing reliable, safe, and affordable launch systems. More specifically, this paper discusses:

1) The involvement of NASA in PDA
2) Why PDA is needed
3) A PDA model structure
4) A PDA example application
5) PDA link to safety and affordability

1 INTRODUCTION

Since the Space Shuttle Challenger accident in 1986, NASA has extensively used Probabilistic Risk Assessment (PRA) to assess, understand, and communicate Loss of Mission (LOM) and Loss of Crew (LOC) risk of space launch vehicles [1, 2, and 3]. However, PDA methods, which could play a key role in designing reliable and affordable launch systems, have not been extensively used at NASA and its contractors. Given the new commercial environment which calls for high safety and low cost launch systems, it is important for NASA and its contractors to consider PDA in conjunction with the traditional engineering deterministic practices to better understand design uncertainties to optimize safety factors, and reduce conservatism (i.e. worst-on-worst design) to save weight and reduce cost. The following section discusses the need for PDA as a complimentary analysis to the deterministic approach. To optimize the design for safety/reliability and affordability.

2 THE NEED FOR PROBABILISTIC ENGINEERING DESIGN ANALYSIS

Conventional deterministic design considers single values for each design input variable (such as material properties, geometrical variables, temperatures, speeds, pressures, etc.) and, therefore, provides a single-valued estimate for a design output variable (such as Low Cycle Fatigue (LCF) life, burst margin, deflection, stress, etc.). The conventional approach to assessing the effects of the input variables is to assume or estimate "worst case" values for them and calculate the design output variable accordingly by standard engineering methods. Commonly used engineering methods include Finite Element Models, company proprietary design codes, engineering handbook, etc. Although commonly used, it is not known whether this single point "worst case" estimate is close to being unacceptable or a fair distance away from being a concern. In fact, it is possible for two deterministic designs to have the same "worst case" value for a design output variable and yet to have one design be much more reliable than the other one. This deterministic method, besides being costly, provides no way to estimate risk or determine failure probability and, thus, requires the use of heuristic safety factor in an attempt to avoid in-service failures. It is interesting to note that when determining the factor of safety for a design, the designer traditionally assumes a single value for stress that is equal to some maximum or nominal value, *So*, depending on how the individual defines the factor of safety for a particular application. Similarly, the strength is assumed to be deterministic and equal to some nominal or minimum value, *Ro*. As shown in Fig. 1, if nominal values are used, we can end with two different designs that have the same factor of safety, but different reliabilities. This illustrates why a PDA approach is recommended in conjunction with the conventional deterministic approach to account for the uncertainty in the design parameters [4, 5, 6, and 7].

PDA methods can also provide an assessment of the design reliability and help in performing design sensitivity analysis to investigate what is important and, potentially, optimize the design for safety and performance. PDA is extremely important in the NASA new environment and can play a key role in designing reliable, safe, and affordable launch systems.

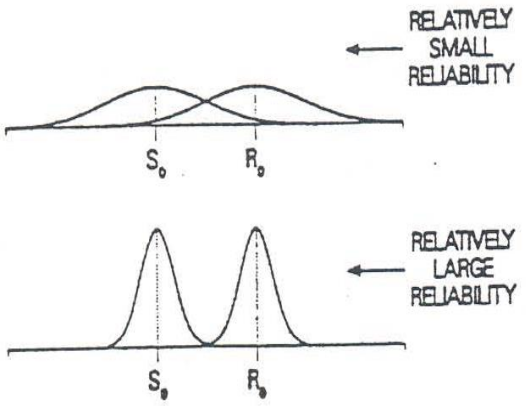

Figure 1. Situation Where Factors of Safety are the same but Reliabilities are Different

2.1 The PDA Structure

A generalized probabilistic design analysis model structure is shown in Fig. 2. Although no two probabilistic models are identical, all of them contain similar elements to the ones shown in Fig. 2. As shown in Fig 2, each parameter controlling design life can be defined and treated as a random variable. These life-controlling parameters are uncertain for two reasons. First, it is known that there will be some amount of variability, regardless of how well the parameter is known. Secondly, it is not known at this phase how well the engineering analyses and models being used will correlate with the actual component parameters. Both of these uncertainties contribute to variability. This would mandate the use of engineering safety factors in traditional deterministic design. PDA, on the other hand, permits the assessment of the actual distributions of these life-controlling factors and the interactions with each other, thus providing an evaluation of component risk.

For example, if it were desired to calculate the low cycle fatigue (LCF) life of a specific feature of an impeller rotor, it would be a function of rotor geometry and material properties (e.g., density, modulus of elasticity, and coefficient of thermal expansion) and the cyclic stress from rotor speed and other loads. In simplistic terms, it is necessary to assign distributions to each of these basic life drivers, (e.g., modulus of elasticity, coefficient of thermal expansion, rotor speed), have a set of equations to map these basic life drivers into the high level life-controlling parameters (e.g., crack growth rate), transform the high level life controlling parameters into an LCF life via a failure model, and then iterate through these steps several times until a distribution of lifetimes is constructed.

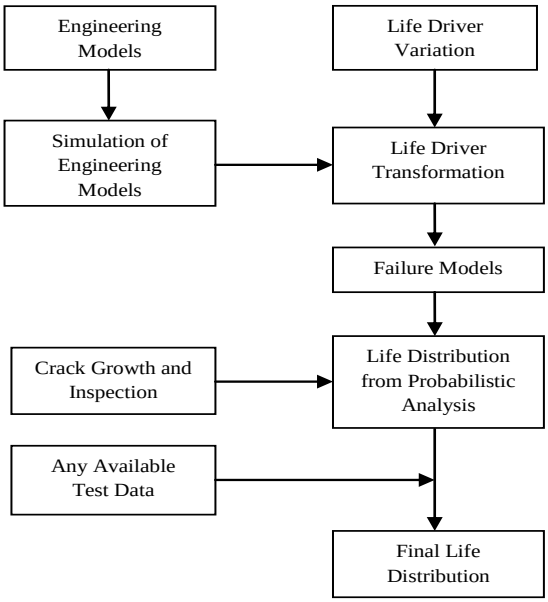

Figure 2. Generalized Probabilistic Design Analysis Model Structure

As indicated by the life driver variation element, all important parameters which affect life are assigned a range or distribution of realistic values rather than some "worst case" value. Note that several different probability/statistical distributions exist, such as Weibull, normal, lognormal, beta, uniform, etc., for describing the pattern of variation of life drivers.

3 A PDA APPLICATION

PDA methods and techniques can be applied at the various phases of a design whenever design data become available [8 and 9]. Generally, this would be during the preliminary design (PD) phase forward. PDA can be used when failure data is not available and the design is characterized by complex geometry or is sensitive to loads, material properties, and environments. For instance, during the subsystem and component design and development, PDA can be used to assist the designer in making decisions on the best material or on the best balanced design with respect to several design criteria. At the hardware certification stage, probabilistic design can be used to determine if a component meets its life requirements. Finally, PDA can be used to manage the risk of a product or system put into service. In the late 1990s, NASA made a decision to make significant upgrades to the Space Shuttle Main Engine (SSME) to improve the Space Shuttle reliability and safety, and reduce cost through life limit extension of the various SSME components [10]. As part of their support to the Space Shuttle upgrade activity, Pratt &Whitney developed PDA models for about 30 SSME turbopumps failure modes to assess the reliability and safety of the new pump for an extended life relative to the old pumps [11]. Many other applications of PDA can be found in [8].

The following example discusses a PDA case that had a significant impact on reliability, safety, and cost during the design and development phase of the SSME upgraded turbopumps that were flown on the Space Shuttle program. The example represents a case where PDA was used to make a decision for selection of a better material for the bearing cage inner race of the High Pressure Fuel Turbopump (HPFTP) of the SSME during the upgrade process. More specifically, this example application addresses the fracture failure mode of the inner race on the roller bearing of the SSME High Pressure Fuel Turbopump (HPFTP). The inner race fracture location is shown in Fig. 3.

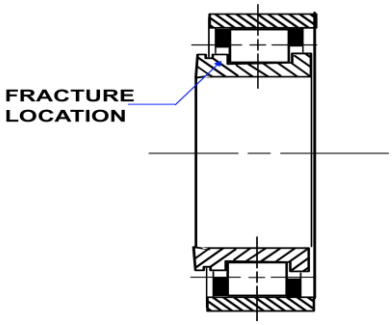

Figure 3. Roller Bearing Inner Race Fracture Location

The analysis intent was to estimate the probability of fracture due to the hoop stress exceeding the material strength. A Monte Carlo simulation model of the failure logic was developed with probabilistic models applied to the stress contributors and material capability, expressed as allowable loads. Fig. 4 illustrates the model.

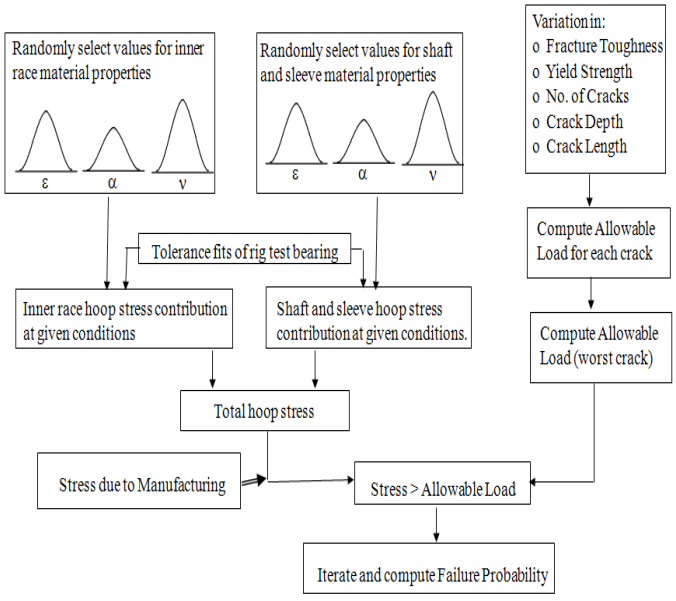

Figure 4. HPFTP Roller Bearing Inner Race PDA Model

In order to calculate the hoop stress, it was necessary to determine materials properties variability. Of those materials properties that affected the total inner race hoop stress, a series of equations was derived which mapped these life drivers (such as the modulus of elasticity and the coefficient of thermal expansion, etc.) into the total inner race hoop stress. Similarly, a distribution on the materials capability was derived. In this case, life drivers such as fracture toughness, crack depth and length, and yield strength, among others, were important. The resulting materials strength distribution was then obtained through a series of similar equations. A Monte Carlo simulation was then used to calculate a random hoop stress and random materials strength. If the stress exceeded the strength in the simulation, a failure was assigned to the simulation run. Otherwise, a success was recorded. After a large number of simulation runs were conducted, a failure distribution was established for the inner race.

To summarize, engineering information with statistical models can be used to probabilistically characterize design parameters and determine design reliability. The probabilistic models can be used for both prediction as well as performing sensitivity analyses to identify design improvements. In fact, the analysis detailed above led to uncovering a major material capability problem for the turbopump bearing cage caused by induced manufacturing stresses. The material could not withstand the predicted flight loads, which resulted in a crack in the bearing cage. A material with different properties was used which reduced the probability of a crack to near zero and significantly improved the reliability of the turbopump bearing cage. Reliability improvement for turbopumps led to a better SSME safety and lower sustainment cost.

4 THE PDA LINK TO SAFETY AND AFFORDABILITY

The consistent pressure to reduce the budget and the commercial industry involvement in space flight provide a compelling incentive to design for safety and affordability. In System design, the assumption is that the total life cycle cost will be justified according to how well the system performs its intended function over time. This assumption cannot be justified when a system fails to perform upon demand or fails to perform repeatedly. History has shown us that good reliability engineering upfront can pay off in terms of mission success and affordability. PDA involves understanding design uncertainties and physics of failure can play a key role in the development of high reliability and cost-effective systems. Lessons learned from the Space Shuttle Program accidents demonstrated that the lack of understanding of the physics of failure can have a major impact on reliability, safety, and affordability of space flight systems. The reliability and safety impact is due to Loss of Crew (LOC)/Loss of Mission (LOM); while the affordability impact is a result of the cost of failure in terms loss of assets and the cost of redesign expressed in terms of cost of development testing, certification, and sustaining engineering.

Lack of understanding of the physics of failure of the Space Shuttle Thermal Protection System (TPS) foam was a major contributor to the Columbia accident (Fig. 5).

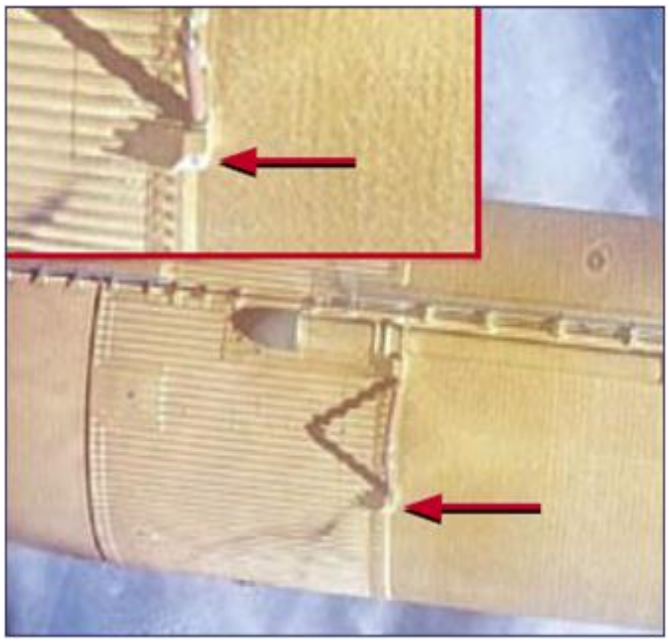

Figure 5. Bipod ramp foam loss

Similarly, lack of understanding of the impact of the loads and environment on the field joint O-ring material was a major contributor to the Challenger accident (Fig. 6).

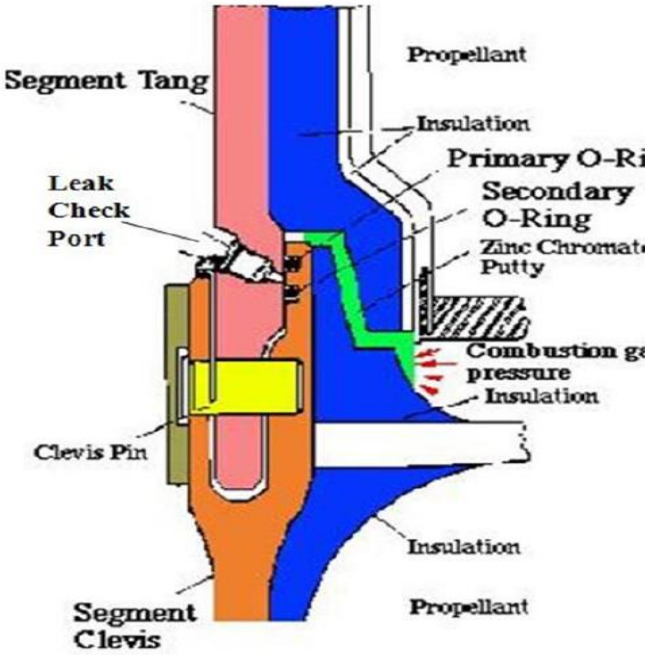

Figure 6. Solid Rocket Motor Field Joint

5 CONCLUDING REMARKS

Both the Columbia and Challenger cases provide a lesson learned for the potential impact of lack of understanding of design uncertainties and physics of failure on both safety and cost of space flight systems. PDA methods can help in understanding design uncertainties and physics of failure.
A PDA approach is recommended in conjunction with the conventional deterministic approach to better understand design uncertainties and optimize the design for performance, reliability, safety, and affordability.

6 ACKNOWLEDGMENT

The authors would like to thank Mr. Richard Stutts and Mr. Steve Broussard of the Marshall Space Flight Center for their contribution to this paper.

7 REFERENCES

1. Planning Research Corporation, "Independent Assessment of Shuttle Accident Scenario Probabilities for Galileo Mission" 1989
2. Science Applications International Corporation, *Probabilistic Risk Assessment of the Space Shuttle*, 1995
3. Safie F. M., *An Overview of Quantitative Risk Assessment for the Space Shuttle Propulsion Elements*, The fourth Probabilistic Safety Assessment and Management (PSAM4), NY City, 1998.
4. F.M. Safie and E.P. Fox, "A Probabilistic Design Analysis Approach for Launch Systems," AIAA/SAE/ASME 27th Joint Propulsion Conference, 1991.
5. Hoffman C.R., Pugh R., Safie F.M., *Methods and Techniques for Risk Prediction of Space Shuttle Upgrades*. AIAA, 1998.
6. Moore, N.R., Et al, *An Improved Approach for Flight Readiness Certification – Methodology for Failure Risk Assessment and Application Examples*, Jet Propulsion Laboratory Report under NASA RTOP 553-02-01, May 1992.
7. Fox, Eric P. and Safie, Fayssal, Statistical Characterization of Life Drivers for a Probabilistic Design Analysis, AIAA/SAE/ASME/ASEE 28th Joint Propulsion Conference and Exhibit, Nashville, TN, 1992
8. Townsend, John S. Et al, Review *of Probabilistic Failure Analysis Methodology and Other Probabilistic Approaches for Application in Aerospace Structural Design*, NASA Technical Paper 3434, 1993.
9. Townsend, John S. *Reliability Analysis of the SRB Aft Skirt Critical Weld*, 8thASCE Specialty Conference on Probabilistic Mechanics and Structural Reliability PMC2000-044.
10. F.M. Safie and B.L. Rebecca, "NASA New Approach for Evaluating Risk Reductions Due to Space Shuttle Upgrades," Proceedings of the Annual Reliability and Maintainability Symposium, January 2000, pp. 288-291.

11. Fox E.P., *SSME Alternate Turbopump Development Program*—Probabilistic Failure Methodology Interim Report. FR-20904-02, 1990.

8 BIOGRAPHIES

Fayssal M. Safie, Ph.D., CRE
NASA Marshall Space Flight Center/QD01
Huntsville, Alabama 35812 USA

Internet (e-mail): fayssal.safie@msfc.nasa.gov

Dr. F. Safie is currently serving as The NASA Reliability and Maintainability (R&M) Technical Fellow. 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 and a Bachelor, a Master, and a Doctorate in engineering.