Reliability and Probabilistic Risk Assessment - How They Play Together

Fayssal M. Safie Ph.D, NASA/MSFC

Richard G. Stutts, NASA/MSFC

Zhaofeng Huang, Ph.D, Aerojet Rocketdyne

Key Words: Probabilistic Risk Assessment (PRA), Reliability Engineering, Design

SUMMARY & CONCLUSIONS

Since the Space Shuttle Challenger accident in 1986, NASA and aerospace industry has extensively used Probabilistic Risk Assessment (PRA) methods to assess, understand, and communicate the risk of space launch vehicles, especially manned space flight missions. Another area that was given a lot of emphasis at NASA is reliability engineering. Both PRA and reliability are probabilistic in nature; however; the reliability engineering is a broad design discipline that deals with loss of function, while PRA is a system scenario based risk assessment process that deals with Loss of Mission (LOM), Loss of Vehicle (LOV), and Loss of Crew (LOC). This paper discusses the PRA process and the reliability engineering discipline in details. It discusses their differences and similarities and how they are used as complementary analyses to support design and flight decisions. In summary:

- Reliability Engineering is a discipline that involves the application of engineering principles to the design and processing of products; both hardware and software intended to minimize the loss of functions.
- PRA at NASA is a process that deals with system risk focusing on understanding the system risk scenarios that could lead to LOM, LOV, and LOC.
- PRA and reliability engineering are two different areas serving different functions in supporting the design and operation of launch vehicles. However, PRA as a risk assessment, and reliability as a metric could play together in a complementary manner in assessing the risk and reliability of launch vehicles.
- In general, reliability analyses should be used as a critical data source for PRA.

1 INTRODUCTION

PRA methodology is one of the probabilistic analysis methods that NASA brought from the nuclear industry to assess the risk of LOM, LOV and LOC for launch vehicles. PRA is a system scenario based risk assessment that uses a combination of fault trees, event trees, event sequence diagrams, and probability and statistical data to analyze the risk of a system, a process, or an activity. It is a process designed to answer three basic questions: What can go wrong? How likely is it? What is the severity of the degradation?

Since 1986, NASA, along with industry partners, has conducted a number of PRA studies to predict the overall launch vehicles risks. Planning Research Corporation [1] conducted the first of these studies in 1988. In 1995, Science Applications International Corporation (SAIC) conducted a comprehensive PRA study [2]. In July 1996, NASA conducted a two-year study (October 1996 - September 1998) to develop a model that provided the overall Space Shuttle risk and estimates of risk changes due to proposed Space Shuttle upgrades [3].

After the Columbia accident, NASA conducted a PRA on the Shuttle External Tank (ET) foam. This study was the most focused and extensive risk assessment that NASA has conducted in recent years. It used a dynamic, physics-based, integrated system analysis approach to understand the integrated system risk due to ET foam loss in flight [4].
Most recently, a PRA for Ares I launch vehicle has been performed in support of the Constellation program.

Reliability, on the other hand, addresses the loss of functions. In a broader sense, reliability engineering is a discipline that involves the application of engineering principles to the design and processing of products, both hardware and software, for meeting product reliability requirements or goals. It is a very broad design-support discipline. It has important interfaces with many other engineering disciplines. Reliability as a figure of merit (i.e. the metric) is the probability that an item will perform its intended function(s) for a specified mission profile. In general, the reliability metric can be calculated through the analyses using reliability demonstration and reliability prediction methodologies. Reliability analysis is very critical for understanding component failure mechanisms and in identifying reliability critical design and process drivers.

The following sections discuss the PRA process and reliability engineering in detail and provide an application where reliability analysis and PRA were jointly used in a complementary manner to support a Space Shuttle flight risk assessment.

2 THE PRA PROCESS

PRA is a systematic process of analyzing a system, a process, or an activity to answer three basic questions:

- What can go wrong that would lead to loss or degraded performance (i.e., scenarios involving undesired consequences of interest)?
- How likely is it (probabilities)?
- What is the severity of the degradation (consequences)?

In a PRA process, risk assessment is the task of generating the triplet set:

$$R \equiv RISK \equiv \{\langle S_i, P_i, C_i \rangle\},$$

Where S is the scenario, P is the likelihood of the scenario, and

C is the consequence of the scenario respectively as shown in Fig. 1.

Scenario	Likelihood (Probability)	Consequence
S_1	p_1	C_1
S_2	p_2	C_2
S_3	p_3	C_3
⋮	⋮	⋮
S_N	p_N	C_N

Figure 1. The Risk Triplet Set

Following the steps shown in Fig 2, the first step in a PRA process is to understand the system under consideration. The second step is to develop a Master Logic Diagram (MLD) to identify all the scenarios for a given system undesirable event called the top event. The MLD logically traces the different events that can lead to the top event. In general, the events are expanded using event trees, fault trees, or event sequence diagrams. These logic models are used to identify the failures needed in order for an event to propagate to the undesirable event.

Event trees and event sequence diagrams are inductive models that start with an initiating event and then trace through the intermediate events (pivotal events) that occur because of the initiating event. The intermediate events include failures and successes of functions and systems that are called upon as a result of the initiating event. Fault trees are deductive models that start with a top undesirable event and then trace through intermediate events that can result in the top event. The fault tree stops at suitably defined basic events.

Once the event trees, event sequence diagrams, and fault trees are completed, the next step is to quantify the risk. The quantification involves assigning probabilities to basic events in the models and then propagating these probabilities to determine the probability of the consequence occurring. The basic events in the models are generally component failures, human errors, etc. The probabilities for the basic events are estimated using PRA databases and expert opinions. Uncertainties associated with the estimates are also determined. The probabilities and their uncertainties are propagated through the models using the logics defined by the models. This propagation results in an estimate of the probability and associated uncertainty for the consequence occurring.

The results of the PRA are used to identify the major contributing elements (i.e. initiating events, pivotal events, and basic events) to the overall risk and quantify the risk significance of these contributing elements, helping focus on where improvements will be effective. For further details on PRA and PRA applications, see [1-3].

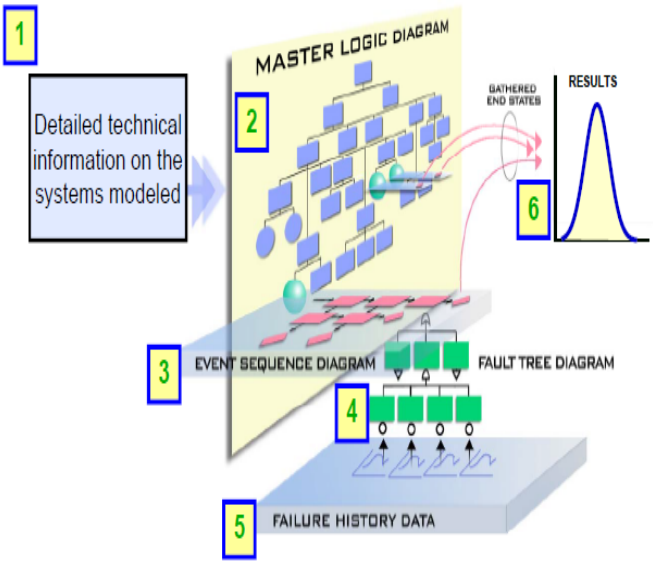

Figure 2. The PRA Process

It is worth noting that a PRA process is complex in nature and requires analysts with special expertise. As shown in Fig. 3, in order to perform a PRA exercise, PRA team members should have a good understanding of engineering science, an understanding of the product being analyzed, an understanding of logic structures, and an understanding of probability and statistics.

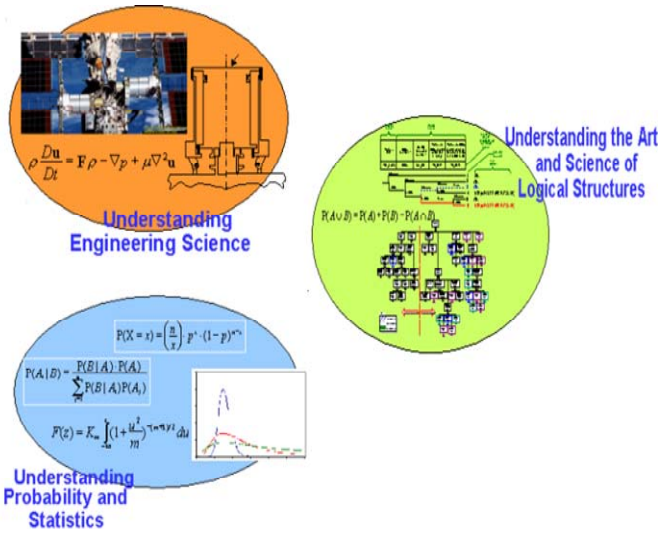

Figure 3. The Skill Set Needed Performing PRA

3 RELIABILITY ENGINEERING AND THE RELIABILITY METRIC

As discussed earlier, reliability engineering is a discipline that involves the application of engineering principles to the design and processing of products, both hardware and software, for meeting product reliability requirements or goals. The reliability figure of merit is the probability that an item will perform its intended function for a specified mission profile. The following sections discuss reliability engineering as a design discipline and the reliability metric in terms of reliability

demonstration and reliability predictions.

3.1 *Reliability Engineering – The Design Function*

To discuss reliability engineering as a design function, we need to get into what constitute a reliability case as part of "design for reliability". Fig. 4 shows examples of the techniques used to build the foundation for a reliability case.

The principle aim of the reliability case shown in Fig. 4 is to generate the data and the supporting evidence to ensure that the product will meet the reliability requirements and achieve mission success. The choice of the techniques is primarily dependent upon the quality and quantity of information available and is tailored to fit the project or program under consideration. These reliability engineering analyses and design techniques are used throughout the design process to be effective and to achieve the performance and reliability goals set by the program.

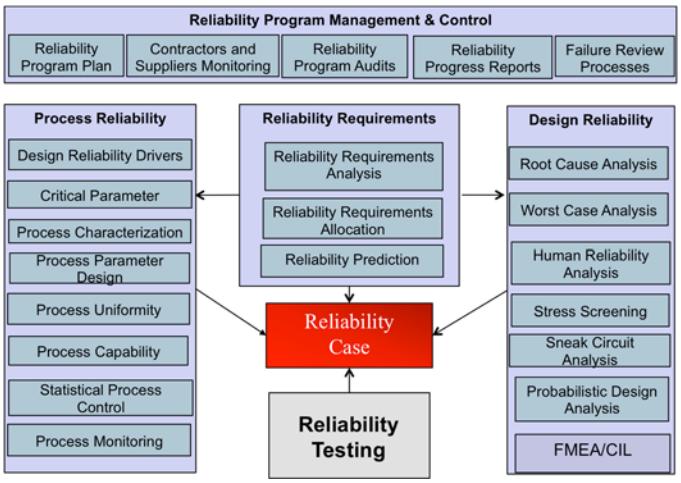

Figure 4. The Reliability Case

It is worth noting that Fig. 4 clearly indicates that designing reliable systems requires addressing both the design reliability and the process reliability [4, 5]; or in other words, "design it right and build it right". It is possible that a good design could be hard to build or manufacture due to process challenges. Many examples were experienced in the Space Shuttle Program (SSP). The most recent example is the Space Shuttle External Tank (ET) Thermal Protection System (TPS) reliability issues that contributed to the Columbia accident. The following examples are provided to illustrate the importance of considering both design and process reliability in designing and building future launch vehicles.

The SSP was a very successful program in terms of reliability and mission success given its complexity; however, two major accidents occurred in the life of the program due to design and process unreliability. They were the Challenger and the Columbia accidents. For the Challenger accident case, Fig. 5 shows the field joint design flown on the Challenger and previous Shuttle flights. According to a published report about the Challenger accident, the main causes and contributing factors were:

- The zinc chromate putty frequently failed and permitted the gas to erode the primary O-rings.
- The particular material used in the manufacture of the shuttle O-rings was the wrong material to use at low temperatures. The elastomers become brittle at low temperatures.

All the accident-contributing factors indicate a design reliability problem.

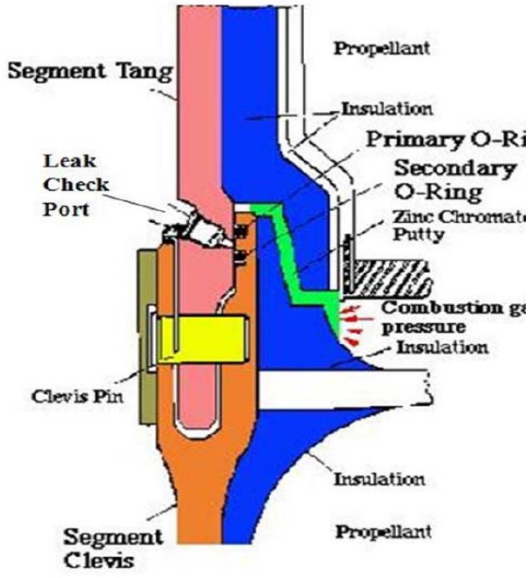

Figure 5. Solid Rocket Motor Field Joint

The problem in the Columbia accident was both design and process reliability. Fig. 6 shows the area of the ET foam loss that contributed to the Columbia accident. According to a published report about the Columbia accident, the causes and contributing factors are:

- A breach in the TPS caused by the left bipod ramp foam insulation from the ET striking the left wing leading edge.
- There were large gaps in NASA's knowledge about the foam.
- Cryopumping and cryoingestion were experienced during tanking, launch, and ascent.
- Dissections of foam revealed subsurface flaws and defects as contributing to the loss of foam.

Unlike the Challenger accident, the Columbia accident failure causes were both process and design related allowing cryopumping and cryoingestion leading to a breach in the TPS.

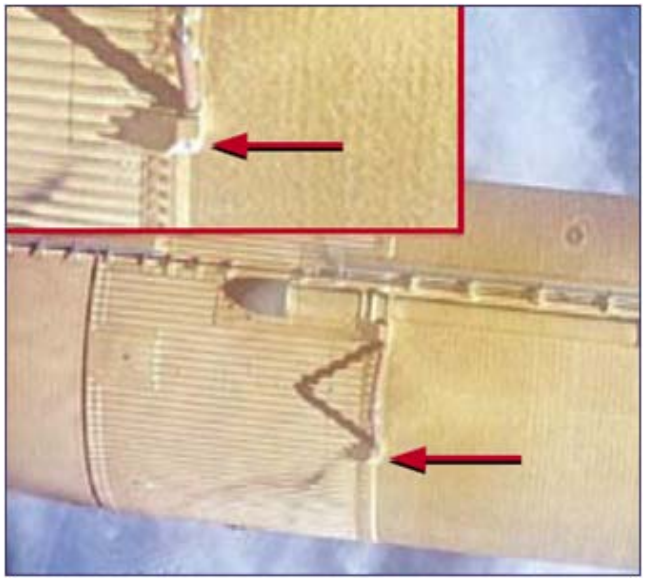

Figure 6. Bipod ramp foam loss

3.2 *The Reliability Metric*

As discussed earlier, the reliability figure of merit or metric is the probability that an item will perform its intended function for a specified mission profile. This probability can be calculated using reliability prediction or reliability demonstration. Reliability prediction is the process of quantitatively estimating the reliability of a system using both objective and subjective data. Reliability prediction is performed to the lowest level for which data is available. Reliability prediction techniques are dependent on the degree of the design definition and the availability of historical data. Examples are:

- Similarity analysis techniques: Reliability of a new design is predicted using reliability of similar parts, where failure rates are adjusted for the operating environment, geometry, material change, etc.
- Physics-based techniques: Reliability is predicted using probabilistic engineering models expressed as loads and environment vs. capability
- Techniques that utilize generic failure rates such as MIL-HDBK 217, Reliability Prediction of Electronic Equipment.

Reliability Demonstration is the process of quantitatively estimating the reliability of a system using objective data at the level intended for demonstration. Statistical formulas are used to calculate the demonstrated reliability at some confidence level. Models and techniques used in reliability demonstration include Binomial, Exponential, Weibull models, etc.. Due to the high cost and schedule impact of reliability demonstration, most programs can only use this method to demonstrate a limited reliability comfort level. For example, a reliability goal of .99 at 95% confidence level requires conducting 298 successful tests with no failures.

4 THE LINK BETWEEN RELIABILITY AND PRA

Given the PRA and the reliability discussions above it is clear PRA and reliability engineering are two different areas serving different functions in supporting the design and operation of launch vehicles. However, PRA as a risk assessment, and reliability as a metric could play together in a complementary manner in assessing the risk and reliability of launch vehicles. A good example is the ET TPS risk assessment shown in Fig. 7. This assessment was used to assess the risk of the foam debris hitting the Orbiter and leading to a LOC. Starting from the top, the risk assessment, which is simulation based, used the ET TPS void distributions derived from the dissection data of the ET components under consideration as the initial input. The void distributions were then used in a fracture mechanics model to generate divots. The divots generated were then transported to evaluate the damage impact on the orbiter. The output of the model was the probability of Orbiter damage exceeding a specified tolerance limit set for the Orbiter. The risk assessment model, although limited in scope, was very critical in understanding and communicating the risk of the ET TPS in flight. The results of the risk assessment were used as part of the rationale to Return-to-Flight (RTF) after the Columbia accident.

It is important to note that the reliability of the foam generated using fracture mechanics was a key input to the probabilistic risk assessment. Although this example does not represent a full-blown system PRA exercise, the foam failure scenario leading to a LOC, was part of the overall Shuttle PRA model. This application represents a good illustration of the complementary nature of probabilistic risk assessments and reliability analyses.

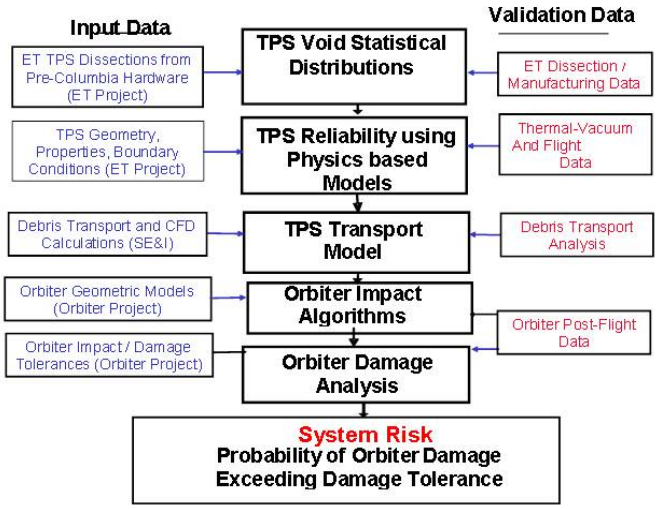

Figure 7. ET TPS Foam Risk Assessment Logic

REFERENCES

1. Planning Research Corporation, "Independent Assessment of Shuttle Accident Scenario Probabilities for Galileo Mission and Comparison with NSTS Program Assessment," 1989 Mission and Comparison with NSTS Program Assessment, 1989
2. Science Applications International Corporation,

"Probabilistic Risk Assessment of the Space Shuttle," 1995
3. 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.
4. F.M. Safie, "Role of Process Control in Improving Space Vehicle Safety A Space Shuttle External Tank Example," 1st IAASS Conference, Nice, France, 2005
5. F.M. Safie and E.P. Fox, "A Probabilistic Design Analysis Approach for Launch Systems," AIAA/SAE/ASME 27th Joint Propulsion Conference, 1991.

BIOGRAPHIES

Fayssal M. Safie, Ph.D., 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.

Richard Stutts
NASA Safety Center/ NA01
Huntsville, Alabama 35812 USA

e-mail:richard.g.stutts@nasa.gov

Mr. Stutts is currently serving as The NASA Reliability and Maintainability (R&M) Technical Discipline Lead for the NASA Safety Center. He joined NASA in 2005 as a Reliability and Maintainability Engineer at Marshall Space Flight Center (MSFC). He has over 25 years experience in Reliability and Maintainability Engineering design within commercial, military and NASA Projects and Programs. He has received several honors and Awards during his time at NASA. He has Bachelor degrees in both Mechanical and Civil Engineering and is currently working on a Masters in Systems Engineering.

Zhaofeng Huang, Ph.D.
Aerojet Rocketdyne
P.O. Box 7922, RFA45, 8900 De Soto Ave.
Canoga Park, CA 91309 USA

Email: zhaofeng.huang@rocket.com

Dr. Zhaofeng Huang is a Technical Fellow at Aerojet Rocketdyne in the areas of Reliability Engineering and Probabilistic analysis under Systems Engineering. Zhao has been working at Aerojet Rocketdyne for 26 years and supported (is supporting) many past and on-going propulsion and energy programs in developing and implementing advanced reliability methods, design-for-reliability approaches, and probabilistic risk assessment for reliability and safety enhancement. Zhao holds a Ph.D. and MS in Mechanical Engineering from University of Southern California, MS in Statistics from Iowa State University, MA in Math from Temple University, and BS in Computational Math from Shanghai University of Science & Technology. Zhao is a Certified Reliability Engineer and Certified Quality Engineer from American Society for Quality, and has Manufacturing Engineering Certificates from UCLA and Society of Manufacturing Engineers.