An Overview of Quantitative Risk Assessment of Space Shuttle Propulsion Elements

Fayssal M. Safie, Ph.D., CRE
Marshall Space Flight Center
Huntsville, Alabama

Abstract

This paper presents an overview of the application of the quantitative risk assessment (QRA) methods to the NASA Space Shuttle system. The NASA QRA application involves the development of a risk model for the overall Space Shuttle system. The model is intended to provide a tool to estimate Space Shuttle risk and to perform sensitivity analyses/trade studies, including the evaluation of Shuttle upgrades. Marshall Space Flight Center (MSFC) is part of the NASA team conducting the QRA study; MSFC responsibility involves modeling the propulsion elements of the Space Shuttle.

1 Introduction

1.1 Application of Probabilistic Methods to NASA Programs

Since the Space Shuttle *Challenger* accident in 1986, NASA has begun incorporating QRA in decisions concerning the Space Shuttle and other NASA projects. At MSFC, for example, QRA has been extensively used in areas such as risk management of flight hardware, trade studies, and reliability prediction of new hardware. In the risk management area, life limits based on QRA are being used in the Space Shuttle main engine (SSME) program [1]. QRA has also been incorporated to support flight issues on the SSME as well as other MSFC elements. With regard to trade studies, QRA has been used as the basis to evaluate the elimination of unnecessary inspections, procedures, and other program costs. For example, an extensive study was conducted in 1994 to determine whether to eliminate the preproof test x-ray inspections on the Space Shuttle external tank (ET) [2]. In the reliability prediction area, similarity analysis and probabilistic structural models have been used by MSFC to predict the reliability of newly developed hardware such as X-33 and X-34 engines (discussed in Ref. 3).

1.2 Space Shuttle QRA Studies

In addition to the ongoing QRA effort at the various NASA centers, NASA Headquarters has led several studies to predict the overall Space Shuttle risk. These studies are the most extensive QRA studies that have been conducted by NASA. The first of these Space Shuttle QRA studies was conducted in 1988 by Planning Research Corporation (PRC). Per NASA's request, PRC conducted a QRA study to determine the Space Shuttle risk for the Galileo mission [4]. In 1993, Science

Applications International Corporation (SAIC) updated the Galileo study using Bayesian techniques [5]. In 1995, SAIC conducted a comprehensive QRA study [6]. In July 1996, the NASA Administrator requested an independent QRA to be conducted by NASA QRA experts. Before July 1996, all the QRA studies performed on the Space Shuttle system have been conducted by independent consultants outside of NASA. In response to the Administrator's request, NASA is conducting a two year study (October 1996 - September 1998) to develop a model that will provide an overall Space Shuttle risk and estimates of risk changes due to proposed Shuttle upgrades. The development of the model consists of two major efforts. One is the development of the risk model and the other is the development of the computer software to run the model. The risk model is being developed by MSFC and JSC (Johnson Space Center) and the computer software, QRAS (Quantitative Risk Assessment System), is being developed by NASA Headquarters.

This paper discusses the approach that MSFC is using in the risk model development of its Space Shuttle elements, including insights obtained from this experience in modeling large scale, highly complex systems with a varying availability of success/failure data. Insights, which are applicable to any QRA study, pertain to organizing the modeling effort, obtaining customer buy-in, preparing documentation, and using varied modeling methods and data sources.

2 MSFC Approach to QRA

The MSFC QRA study involves modeling the Space Shuttle propulsion elements. This includes the SSMEs, reusable solid rocket motors (RSRM), solid rocket boosters (SRB), and the ET. Modeling the four propulsion elements is a large and complex task which requires a good strategy for conducting the study, a sound step-by-step technical approach, and innovative quantification methods and techniques. Section 2.1 addresses the overall MSFC strategy in conducting the study, Section 2.2 addresses the step-by-step technical approach, and Section 2.3 addresses the quantification methods and techniques.

2.1 Strategy for Conducting the QRA Study

The MSFC strategy for conducting the QRA study focused on a team approach. The team approach involved both Government and Industry, with team members representing various technical disciplines. This includes design engineers, safety engineers, statisticians, and QRA experts. The MSFC team approach has proven to be very effective in capturing the knowledge, data, and expertise required in conducting a complex task such as the Space Shuttle QRA study. This approach has also proven to facilitate the customer buy-in and improve the fidelity of the analyses results.

2.2 Technical Approach

The first step in the MSFC technical approach is the identification of the most critical failure modes or events to be modeled. This can be accomplished using

various methods. One method is using a Master Logic Diagram (MLD) as shown on the upper left-hand side of Figure 1. The MLD is basically a Fault Tree with its basic events being the failure modes/causes to be modeled. Other methods involve using Failure Modes and Effects Analyses (FMEA) and Hazard Analyses combined with a screening criteria to identify the most critical failure modes/causes to be modeled. In QRA terminology, the identified failure modes/causes are called initiating events.

The second step in the MSFC technical approach is the development of a Functional Event Sequence Diagram (FESD) for each initiating event identified in Step 1. The FESD shown in Figure 1 describes how failures could propagate through the system along various scenarios leading to mission success, loss of vehicle/crew, or other end states; or how mitigating factors could prevent the initial failure from propagating to undesirable end states, thereby protecting the higher level system. Note that a circle represents an initiating event, a rectangle represents a pivotal event, a parallelogram represents a comment, and a diamond represents an end state.

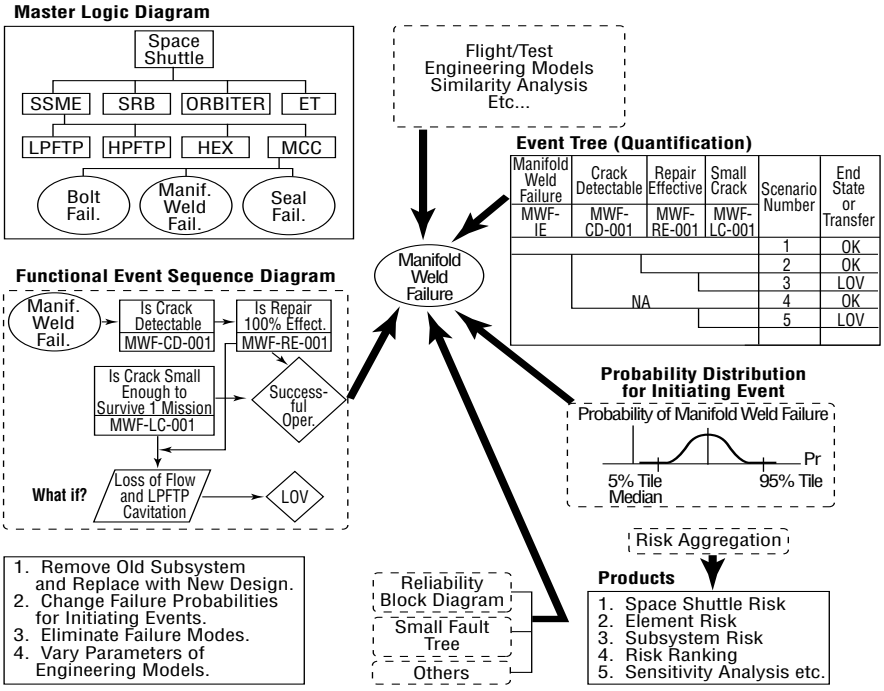

Figure 1. MSFC Technical Approach to QRA

The third step in the MSFC technical approach is to translate each FESD to an Event Tree to determine the probability of Space Shuttle failure due to the FESD initiating event. The event tree probabilities require the quantification of the initiating and pivotal events (described in Section 2.3).

The final step in the MSFC technical approach is to aggregate the probabilities of all initiating events to obtain the probability of catastrophic failure at the failure mode, component, subsystem, element, and Shuttle level.

The above described approach is based on Fault Trees, FESDs, and Event Trees. Although MSFC used logic trees, which have historically been used in all large scale QRA studies, the application of these tools and the quantification methods used in the MSFC approach are different. For instance, in order to be able to evaluate Shuttle upgrades, all logic trees used in the MSFC study are developed with a high level of modularity. In the quantification area, advanced probabilistic structural models [7,8,9] are extensively used to account for lack of data, especially when modeling redesigned hardware.

2.3 Quantification Methods and Techniques

The quantification of the initiating and pivotal events is done in two steps. The first step is establishing a failure distribution for the initiating/pivotal events. The second step is establishing an uncertainty distribution on the probability of failure. The most commonly used models for characterizing failure distributions are Binomial, Exponential, Weibull, Lognormal, Normal, and reliability growth. The selection of the distribution depends on the nature of the failure and the data. Numerical/frequency distributions can also be used to characterize the failure distribution where failures are generated by simulation. With regard to the uncertainty distribution on the probability of failure, the most commonly used distributions are the Lognormal, Weibull, and the Beta distribution. Since validation of an uncertainty distribution is difficult, in most cases, the selection of the uncertainty distribution is arbitrary.

It is obvious from the above discussion that the quantification of the initiating and pivotal events requires a large amount of data given all the failure modes that need to be modeled in the Shuttle study. This, in some cases, has the potential to be a problem. However, this data problem can be overcome by using similarity analysis, engineering models such as probabilistic structural models [7], and utilizing good engineering judgment. The effect of lack of data can also be minimized by the one-time construction of a well-documented, maintainable, "living" model that can be easily updated as more data become available.

3 Example Application

Following the first step in the approach discussed in the previous section, 22 failure modes were selected for QRA modeling on the SSME High Pressure Fuel Turbopump (HPFTP). The most important of which is Turbine Blade Porosity.

A network of porosity in the blade material can lead to embrittlement due to the HPFTP's hydrogen environment, which can in turn lead to cracks in the blade. Cracks in the fir tree above the first two lobes can lead to blade separation from the wheel, which can result in the loss of the Shuttle. A network of porosity in a 2nd stage blade resulted in a major engine failure on the test stand.

Figure 2 shows the FESD for the turbine blade porosity. The FESD starts with the initiating event, turbine blade porosity. Given that porosity is present, the next step is to check if inspection is effective enough to catch it. If the inspection catches the porosity, the result is a mission success (MS). If the inspection misses the porosity, then the next step is to check if porosity is present in critical locations. If porosity is not present in critical locations, the result is a mission success. If porosity is present in critical locations, then the next step is to check if porosity can lead to a crack before retiring the blade at 4300 seconds (life limit). If a crack does not occur before 4300 seconds, then the result is a mission success. If a crack occurs before 4300 seconds, then the next step is to check if a turbine blade failure occurs. If no blade failure occurs, the result is mission success. If a blade failure occurs, the result is loss of vehicle.

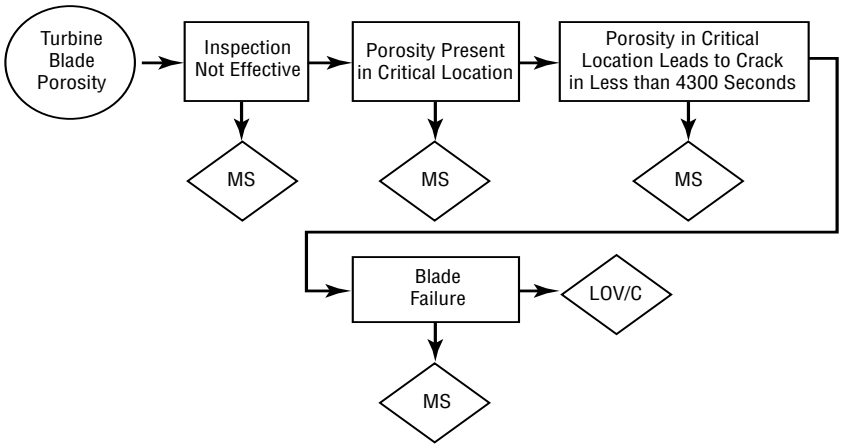

Figure 2. Functional Event Sequence Diagram

The FESD described above shows how the system could fail or how mitigation factors could protect the system from failing.

The next step in the QRA process is the quantification of the FESD. Quantification of the FESD requires the use of the methods and techniques described in Section 2.3. For example, to quantify the initiating event, turbine blade porosity, data on 1000 inspected blades were used in a Binomial model to characterize the probability of having porosity in a blade. Out of the 1000 blades inspected, 40 blades were found to have significant porosity. This translates to a Binomial characterization of 40 failures out of 1000 trials. Assuming a Uniform prior on the interval [0,1] and using Bayesian methods results in a Beta distribution (uncertainty distribution) with parameters 41 and 961. Using the Beta distribution, the 5^{th}, 50^{th}, and 95^{th} percentiles of the probability of having porosity in the blade were calculated as 3.118E-02, 4.016E-02, and 5.170E-02, respectively. The remaining events in the FESD are quantified similarly. In order to calculate the probability of Loss of Vehicle (LOV) due to turbine blade porosity, the uncertainty distributions for all FESD events are aggregated using event tree logic through simulation.

4 Conclusions

As described in the paper, MSFC has successfully developed a sound technical approach for conducting QRA studies. The approach developed represents a systematic and well-documented process to evaluate the risk of the Space Shuttle propulsion elements, and to evaluate the risk reduction due to the Shuttle upgrades. Also, through conducting the Shuttle QRA study, MSFC has demonstrated the effectiveness of using the multiple discipline strategy in obtaining customer buy-in and improving the fidelity of the QRA results.

5 Recommendations

Large scale QRA studies are very complex, therefore they require a large amount of data, assumptions, and modeling. It is recommended that when conducting a QRA study, to follow a well defined documented systematic procedure and assemble the right team including design and systems engineers. In fact, the high level of success of this NASA led QRA study is attributed to the process followed in conducting the study, the participation of various disciplines, and the use of all Shuttle generated data including test, flight, and engineering analyses.

Acknowledgment

The author acknowledges and appreciates the contribution of all the QRA team members involved in this project. A special thanks to Rebecca Belyeu of HEI for her contribution as a team member and her support in the preparation of this paper.

References

1. Safie FM. A Statistical Approach for Risk Management of Space Shuttle Main Engine Components. Probabilistic Safety Assessment and Management, 1991
2. Safie FM. A Risk Assessment Methodology for the Space Shuttle External Tank Welds. Reliability and Maintainability Symposium, 1994
3. Safie FM. Use of Probabilistic Design Methods for NASA Applications. ASME Symposium on Reliability Technology, 1992
4. Planning Research Corporation, Independent Assessment of Shuttle Accident Scenario Probabilities for Galileo Mission and Comparison with NSTS Program Assessment, 1989
5. Science Applications International Corporation, Probabilistic Risk Assessment of the Space Shuttle Phase 1: Space Shuttle Catastrophic Failure Frequency Final Report, 1993
6. Science Applications International Corporation, Probabilistic Risk Assessment of the Space Shuttle, 1995
7. Hoffman CR, Pugh R, Safie FM. Methods and Techniques for Risk Prediction of Space Shuttle Upgrades. AIAA, 1998
8. Fox EP. SSME Alternate Turbopump Development Program—Probabilistic Failure Methodology Interim Report. FR-20904-02, 1990
9. Safie FM, Fox EP. A Probabilistic Design Analysis Approach for Launch Systems. AIAA/SAE/ASME 27th Joint Propulsion Conference, 1991