Space Shuttle Main Engine Quantitative Risk Assessment: Illustrating Modeling of a Complex System with a New QRA Software Package

Christian Smart, Ph.D.
Hernandez Engineering, Inc.
Huntsville, USA

1 Introduction

During 1997, a team from Hernandez Engineering, MSFC, Rocketdyne, Thiokol, Pratt & Whitney, and USBI completed the first phase of a two year Quantitative Risk Assessment of the Space Shuttle. The models for the Shuttle systems were entered and analyzed by a new QRA software package. This system, termed the Quantitative Risk Assessment System(QRAS), was designed by NASA and programmed by the University of Maryland. The software is a groundbreaking PC-based risk assessment package that allows the user to model complex systems in a hierarchical fashion. Features of the software include the ability to easily select quantifications of failure modes, draw Event Sequence Diagrams(ESDs) interactively, perform uncertainty and sensitivity analysis, and document the modeling. This paper illustrates both the approach used in modeling and the particular features of the software package. The software is general and can be used in a QRA of any complex engineered system.

The author is the project lead for the modeling of the Space Shuttle Main Engines (SSMEs), and this paper focuses on the modeling completed for the SSMEs during 1997. In particular, the groundrules for the study, the databases used, the way in which ESDs were used to model catastrophic failure of the SSMEs, the methods used to quantify the failure rates, and how QRAS was used in the modeling effort are discussed. Groundrules were necessary to limit the scope of such a complex study, especially with regard to a liquid rocket engine such as the SSME, which can be shut down after ignition either on the pad or in flight. The SSME was divided into its constituent components and subsystems. These were ranked on the basis of the possibility of being upgraded and risk of catastrophic failure. Once this was done the Shuttle program Hazard Analysis and Failure Modes and Effects Analysis (FMEA) were used to create a list of potential failure modes to be modeled. The groundrules and other criteria were used to screen out the many failure modes that did not contribute significantly to the catastrophic risk. The Hazard Analysis and FMEA for the SSME were also used to build ESDs that show the chain of events leading from

the failure mode occurrence to one of the following end states: catastrophic failure, engine shutdown, or successful operation (successful with respect to the failure mode under consideration). The SSME has a long test history that was used to quantify the failure mode and the pivotal events in the ESDs. The quantification of these events consisted of an uncertainty distribution for the probability of each event's occurrence. QRAS was used to build the ESDs for the failure mode models, and also to quantify the uncertainty about each event probability in the ESDs. Features of the software as they apply to the modeling of the SSME are discussed. One of the failure mode models is discussed in detail. It is shown how the ESD for the failure mode was drawn using QRAS, and how uncertainty analysis was performed. Also, the sensitivity analysis module is discussed. The information about QRAS presented here is contained in [1].

2 Modeling and QRAS

2.1 Modeling Process

The SSME has hundreds of potentially catastrophic failure modes. Groundrules were used to limit the scope of the study. The most important groundrule was to focus the SSME QRA analysis on the major risk drivers, while de-emphasizing secondary risk issues, such as aborts. Indeed, abort scenarios were not modeled in the 1997 study. The study only considered those failures which lead to a catastrophic failure of the SSMEs. Initiators occurring outside the Shuttle vehicle (e.g., ground support equipment failures and severe weather) were excluded.

Due to time constraints, the QRA team, after discussions with engineers at MSFC and at Rocketdyne, decided to model four SSME components during the 1997 study. These were the High Pressure Fuel Turbopump, High Pressure Oxidizer Turbopump, Main Combustion Chamber, and the Nozzle. The rest of the engine components are being modeled during 1998. The decision to model these was based upon two interrelated factors: catastrophic risk and upgrade potential. Once the components to be modeled were chosen, a list of potential failure modes was created using the Shuttle program FMEA and Hazard Analysis. Several criteria were used to screen the failure modes to a manageable level. All events in the Hazard Analysis fault tree that are categorized as being an accepted risk but have a catastrophic effect were modeled. Events are classified as accepted risk if there is sufficient doubt about the ability of the control processes to prevent the occurrence of the event[2]. Also, events having a Deviation Approval Request (DAR - a deviation from original specifications) were considered for modeling. For example, the porosity of the turbine blades in the HPFTP was included because such a problem caused an uncontained failure of an SSME on a test stand in 1991. This particular event was classified under accepted risk in the Hazard Analysis and the turbine blades have been life-limited by a DAR to 4300 seconds. Finally, the list of events selected for

modeling was reviewed with engineers at MSFC and Rocketdyne. A few additional events were then added. In all, 50 failure modes were modeled for the SSME.

Once this list was agreed upon, the system decomposition (called the "hierarchy") could be constructed using QRAS, as shown in Figure 1. For the SSME, the hierarchy consists of subsystems, components, and failure modes. The failure modes are grouped by component, and the components are grouped by subsystem. As shown in Figure 1, one of the SSME subsystems is the Fuel Turbopumps, and one of its components is the HPFTP. One of the failure modes in the HPFTP is Thermal Shield Failure.

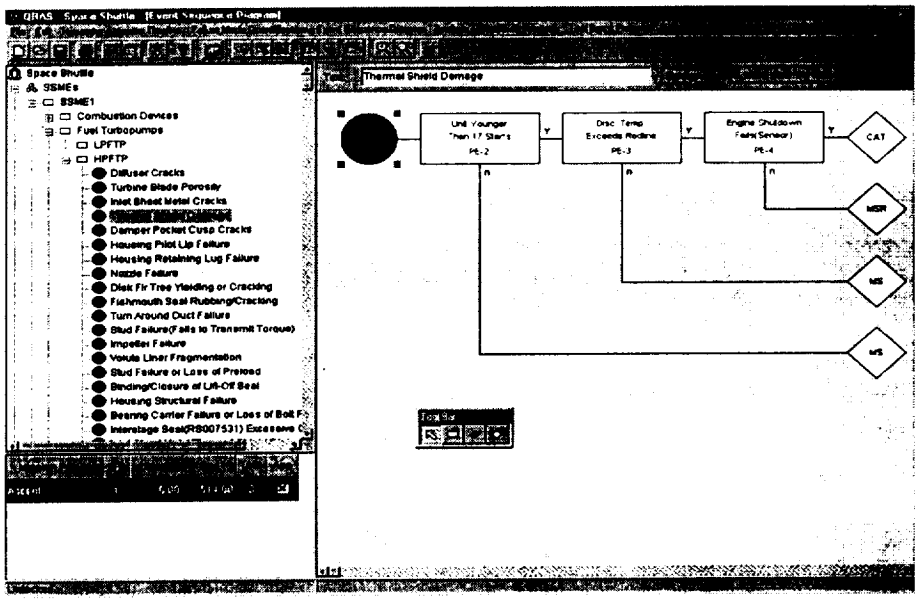

Figure 1. SSME Hierarchy and ESD in QRAS.

2.2 Event Sequence Diagrams

Once selected for modeling, each failure mode was extensively analyzed. The first step in this process was the creation of an Event Sequence Diagram(ESD). An ESD explains how a failure mode (which is the initiating event in some ESD) can lead to an end state of interest (e.g., catastrophic failure). An example of an ESD is shown in Figure 1.

The ESD was drawn in QRAS using the ESD editor, which has an easy to use point-and-click interface. A circle, representing the initiating event, is drawn automatically after the failure mode is created. Once this is done, the user can add pivotal events (represented by rectangles), comment boxes (represented by parallelograms), and

end states (represented by diamonds). This is done by depressing the appropriate button in the floating tool bar.

The ESD in Figure 1 is for the Thermal Shield Damage failure mode in the HPFTP. The concern is that thermal shield damage may cause flow blockage, resulting in loss of turbine power. This will lead to a reduction in turbopump speed. The worst consequence is the increase of the HPFTP discharge temperature to such an extent that it exceeds the redline limit protected by two dual output sensors.

In the ESD, once Thermal Shield Damage has occurred, the first pivotal event asks whether the thermal shield has experienced fewer than 17 starts. Due to previous problems with the thermal shield, it has been life-limited to 17 starts. Thus, if the thermal shield has seen at least 17 starts, it will be removed. A new thermal shield will replace it, which will result in mission success (with respect to this failure mode). Mission success is denoted in the figure by "MS." However, if the unit has experienced fewer than 17 starts, it will be flown. This event was included in the ESD because most of the failure data available for analysis occurred on thermal shields that had experienced more than 17 starts. Including this pivotal event is a way to use all the available data in the analysis of the failure mode while incorporating the increase in the reliability due to the life limit. The next pivotal event is exceedance of the HPFTP discharge temperature redline (limit). If this occurs, the engine will attempt to shutdown. The assumption was made here that the only way in which this can fail is for the sensor output to fail. Failure of the engine to shutdown leads to catastrophic failure of the engine, which is an end state denoted by "CAT." Since aborts were not modeled, it was assumed that an engine shutdown would not lead to a catastrophic failure. Thus, once engine shutdown occurs, the mission continues but without the use of one of the three SSMEs. That is, "mission success" (with respect to this failure mode) occurs, but with the loss of a redundant item. This end state is denoted "MSR."

2.3 Quantification

Once the ESD is drawn the initiating and pivotal events must be quantified. This involves not merely a point estimate, but an uncertainty distribution for the probability of occurrence of each event in the ESD. There are several options available for quantification of the ESD events. One of these is the specification of an uncertainty distribution that has been obtained via analysis completed off-line. The distributions available for this choice are: Uniform, Normal, Lognormal, Triangular, Beta, Gamma, Weibull, and Tabular. The user can also define a function of physical variables; create a predefined function for the failure probability via logistic regression; create a limit state function; or specify a reliability function. Several other options will be added to this list in the next version of the software (some of the future enhancements that will be included in the next version are mentioned in section 2.5).

Not all of the quantitative analysis was completed using QRAS. Several methods were used to quantify events off-line, including reliability growth models, Weibull analysis, and Bayesian techniques.

Most SSME events modeled had sufficient data in the form of problem reports for tests and flights. However, for some events little failure data existed. Where possible, The QRA team avoided the use of expert opinion to quantify events. In the cases where data was scarce, generic SSME data was sometimes used, as was Probabilistic Design Analysis. All failure modes for the Pratt&Whitney High Pressure Oxidizer Turbopump were analyzed using probabilistic design methods.

All quantification was fully documented in QRAS, including the assumptions made, the data and methods used, and the results for each event quantified. The user can view the modeling documentation by right-clicking the mouse on any event in any ESD, and then choosing the documentation option.

Once all events in an ESD are quantified, QRAS calculates the probability of each end state. For the ESD in Figure 1, the probability of occurrence of catastrophic failure can be calculated as Pr(CAT)=Pr(IE)*Pr(PE2)*Pr(PE3)*Pr(PE4). This type of calculation is done for all ESDs (for more information about ESDs, see [3]). Since all dependencies and redundancies are currently handled in the ESDs, the results are added and the cross-products are subtracted to get the results for the subsystem, element, and project level. Note that the results are stored for the failure mode, subsystem, and element level. This aggregation can be performed via Monte Carlo simulation or by using only the means of the distributions.

While the current version allows the user to define limit state functions, additional probabilistic engineering reliability methods will be included in Version 2. These include the incorporation of Fast Probability Integration techniques, and a Monte Carlo routine for handling hyper-distributions.

2.4 Analysis Results

The analysis results can be viewed at the failure mode, subsystem, element, or project level. For an end state, such as catastrophic failure, the results can be ranked by mean risk. There are two ways to do this: by failure mode or by scenario (path to an end state). This can be done at any level: for a subsystem, an element, or a project.

Once an analysis has been run, sensitivity analyses can be performed in QRAS. The most salient advantage of this feature is that it easily allows a comparison of risks between an existing system and the same system after a proposed upgrade has been implemented. This option allows the user to replace a subsystem with a subsystem from another project. Other options include the ability to modify the quantification of a failure mode, remove a subsystem, remove a failure mode, add a failure mode, and modify an ESD.

2.5 QRAS Enhancements

Various limitations exist in the current version of QRAS. For example, all system dependencies and redundancies must be incorporated in the ESDs. To rectify this, fault tree and reliability block diagram support will be included in version 2. Also, other modifications will be made to the current configuration to help the user in the modeling of multiple failure modes, subsystems, etc. For example, in Version 1, one of the failure modes is turbine blade cracking. Due to the nature of the data available, the analysis was performed at the individual blade level. However, there are 122 blades per pump. To incorporate this explicitly in QRAS, one would have to enter the ESD 122 times.

In Version 2, the capability allowing the user to indicate multiple items per failure mode, per subsystem, and per element will be included. Also, the ability to explicitly model common cause failures and the failure of multiple but redundant items will be included.

Several other features will be added, such as the capability to rank risk results not only by the means, but by several different criteria, including the medians.

References

1. NASA, Quantitative Risk Assessment System(QRAS) User's Guide. Unpublished, January 15, 1998.
2. NASA, Methodology for Conduct of Space Shuttle Program Hazard Analyses, NSTS 22254, Revision B, Change No. 4. 1993.
3. Kumamoto H, Henley EJ. Probabilistic Risk Assessment and Management for Engineers and Scientists, 2nd ed. IEEE Press, 1996.