Use of System Safety Risk Assessments for the Space Shuttle Reusable Solid Rocket Motor

Phillip O. Greenhalgh, CSP; Principal Engineer, ATK Thiokol Propulsion

Keywords: Space Shuttle, Reusable Solid Rocket Motors, Risk Assessment, Assessing Change, Risk Matrix

Abstract

This paper discusses the System Safety approach used to assess risk for the Space Shuttle Reusable Solid Rocket Motor (RSRM). Previous to the first RSRM flight in the fall of 1988, all systems were analyzed extensively to assure that hazards were identified, assessed and that the baseline risk was understood and appropriately communicated. Since the original RSRM baseline was established, Thiokol and NASA have implemented a number of initiatives that have further improved the RSRM. The robust design, completion of rigorous testing and flight success of the RSRM has resulted in a wise reluctance to make changes. One of the primary assessments required to accompany the documentation of each proposed change and aid in the decision making process is a risk assessment. Documentation supporting proposed changes, including the risk assessments from System Safety, are reviewed and assessed by Thiokol and NASA technical management. After thorough consideration, approved changes are implemented adding improvements to and reducing risk of the Space Shuttle RSRM.

Introduction

After the Challenger accident and subsequent investigation in 1986, an extensive redesign of the Space Shuttle Solid Rocket Motor was required. During the redesign period, one of the most extensive efforts for any system was undertaken to identify, understand and control risk for the new Reusable Solid Rocket Motor (RSRM). The risk assessment effort for concepts of the redesigned motor began at the initial design inception stage and included System Safety assessments of hand drawn sketches of potential design concepts. At first, the assessments provided by System Safety simply addressed the pros and cons of each concept. Later, the best design concept was addressed with an overall trade study including input from System Safety. As the best design was selected, all components were analyzed extensively to assure that hazards were identified, mitigated to the extent possible, and the risks of these hazards were understood and controlled to an acceptable level. Fault Tree Analyses, Hazard Analyses, Failure Modes and Effects Analyses/Critical Items List (FMEA/CIL) and the Certificate Of Qualification (COQ) were used in the identification and establishment of baseline risk. The documentation of the System Safety analyses were reviewed, critiqued and approved by all levels of technical management at Thiokol and at NASA assuring an understanding and appropriate mitigation of risk. Prior to flight, the RSRM was tested extensively with a most exhaustive effort to verify the design and analytical work. This testing program included numerous sub-scale tests, twenty-two full scale/short duration tests of specific components and six full scale/full duration motors. (ref. 1) With all of the testing and analyses completed previous to the first flight of the new RSRM in the fall of 1988, confidence was high that the optimum design had been achieved.

In preparation for and subsequent to the Space Shuttle return to flight, the effort to identify and communicate residual risk, assuring full and timely information bearing on flight safety, has been of utmost importance to Thiokol and NASA. "The Thiokol Vice President and RSRM Program Manager (PM) has overall responsibility for risk management. The PM, along with the Chief Component Program Managers and all Thiokol RSRM employees, utilize day-to-day processes and procedures to ensure risk is managed on the program. The NASA Certificate of Flight Readiness (CoFR) process is the key vehicle by which the PM certifies that the risk management process has been utilized to minimize flight risk. The Thiokol RSRM Flight Readiness Review (FRR) endorsements are a commitment from program, engineering, operations, and quality management levels that requirements have been followed to ensure safe mission performance. The RSRM Certification of Flight Readiness Plan, TWR-75759 is under MSFC control and is in compliance with NSTS 08117 requirements and

procedures for Certification of Flight Readiness." (ref. 2) The Flight Readiness Reviews with Thiokol and NASA Project and Program Managers as well as the independent Pre-Flight Assessment led by NASA's Safety and Mission Assurance office, communicate issues of potential risk prior to each flight. The review of potential risk issues assures that any change in risk or any new risk is understood and that appropriate controls have been employed to mitigate risk to an acceptable level prior to making a launch decision.

Baseline Analyses

The hazard analysis and fault tree effort for the RSRM is documented in the Flight Systems Hazard Reports for the Space Shuttle RSRM. These reports document 23 identified potential hazardous conditions, each noted in a separate hazard report. Within the 23 hazard reports there are 1085 identified hazard causes. There are zero unacceptable risk causes, 25 causes considered to be accepted risk and 1,060 considered to be controlled risk. (ref. 3) Approximately 10% of the hazard causes are unique to the hazard reports while the other 90% of the hazard causes reference the FMEA/CIL retention rationale for hazard controls. Controls and verifications to unique hazard causes (causes that are not also listed in the FMEA/CIL) provide evidence of how the appropriate hazard reduction methods control a hazard to an acceptable level.

The FMEA/CIL for the RSRM addresses potential failure modes, their causes and retention rationale that explain how each failure mode cause is being controlled. The CIL retention rationale includes testing and analysis information documenting how failure modes or hazards are controlled to an acceptable level. The retention rationale also identifies design features for specific RSRM components and lists the inspections and tests accomplished during the manufacturing process to assuring that the motor will meet design intent.

The qualification of the RSRM is documented in the Certificate of Qualification (COQ). The COQ provides certification and evidencing documentation that the design of the RSRM meets contract end item (CEI) specification requirements.

Continuous Improvement

Continuous improvement efforts begin with carefully weighing the effect of proposed changes. With various continuous improvement initiatives, twenty-one of the RSRM Hazard Report accepted risk causes have been identified as potential candidates for changes to reduce risk. (ref. 3) Since the original RSRM baseline was established and certified through analysis, test and demonstration, Thiokol and NASA have implemented a number of initiatives further improving the safety and Reliability of the RSRM. These initiatives have involved changes to RSRM design, tooling, and/or manufacturing processes. While there has been a desire to implement changes for performance improvements and a need to replace materials that have become obsolete, the robust design, completion of rigorous testing and flight success of the RSRM has resulted in a wise reluctance to make changes. Improvement initiatives and overcoming obsolescence roadblocks are weighed against the reluctance to change with careful comparison and evaluation. One of the primary inputs required to accompany each proposed change is a risk assessment by System Safety. Process Failure Modes and Effects Analyses (PFMEA), Risk Matrices, Fault Tree Analyses, Hazard Analyses, Certificate Of Qualification (COQ) and Critical Items List are System Safety tools used to weigh the effects of particular changes and to assure that the implementation of a change will not create a negative impact on the applicable component or associated system. System Safety assessment sheets, addressing potential impact to the FMEA/CIL, Hazard Report, and COQ are completed on all proposed RSRM process and design changes. A careful review of proposed changes, along with the System Safety assessments are then reviewed and assessed by Thiokol and NASA technical management. Only after thorough consideration are changes approved and implemented adding improvements to and reducing risk of the Space Shuttle RSRM.

The Thiokol Risk Management Plan for the RSRM Project "identifies the activities and methods utilized by the Reusable Solid Rocket Motor in managing risk associated with safety, mission success, schedule, supportability, and cost of RSRM hardware, personnel, materials, and facilities." (ref. 2) The risk management philosophy within the Thiokol RSRM Program

includes: the Vice President and RSRM Program Manager who has overall responsibility for risk management and successful implementation of the risk management plan. Risk management is to pervade all decision-making processes within the RSRM Program and is designed to be auditable, measurable, and consistent with customer risk management philosophies. All RSRM work team members participate in the risk management process with communication of risks to the highest levels of management, where required, being an essential element of this process. (ref. 2)

Within the overall risk management effort, System Safety functions at Thiokol as well as at NASA are an integral part of the overall RSRM project. While being integral to the project, Thiokol System Safety and NASA Safety & Mission Assurance (S&MA) organizations are organizationally located to provide an independent voice to the project. Independent reviews and risk assessments are performed and provided by these organizations for all design and process changes.

The area of risk most significant to the efforts of the Thiokol System Safety department is of course safety/mission success. Specific System Safety efforts to fulfill risk management requirements are outlined in the Safety and the Reliability Plans for Space Shuttle RSRM Project and are aligned with NASA requirements in NSTS 5300.4 (1D-2), Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program. Further definition of specific risk management techniques of Fault Tree Analysis, Hazard Analysis, Risk Matrix, etc. are outlined in NSTS 22254, Methodology for Conduct of Space Shuttle Program Hazard Analyses, Requirements for Preparation and Approval of Failure Modes Effects Analysis (FMEA) and Critical Items List (CIL) outlined in NSTS 22206. The description and intended use of these efforts is to provide a comprehensive and systematic method for identifying, documenting, and communicating risk associated with operations of the RSRM. As risk is communicated through well defined, concise and specific lines of authority, the Thiokol RSRM Program Manager and MSFC RSRM Project Manager have the necessary information available to make optimal decisions. (ref. 2)

System Safety Risk Assessments: System Safety Assessment Sheets are required to accompany every formal change presented to the Thiokol and MSFC Configuration Control Boards. Each change to RSRM design or manufacturing processes whether they are a new design/process or a modification to an existing one is evaluated against the following risk criteria for baseline Hazard Reports and FMEA/CILs. Does the change: a) Introduce any new hazards/failure modes or hazard causes/failure causes? b) Eliminate, adversely affect, or invalidate any hazard controls, verification data, or CIL retention rationale? c) Reduce a margin of safety for any RSRM component? d) Change the criticality category assignment? e) Require an adverse (increase in severity or in probability) change to the NSTS 22254, risk matrix classification of a hazard cause? If any of these questions are answered "yes" a risk change Document Change Notice (DCN) to the baseline Hazard Report and/or FMEA/CIL may be required. Such a change also requires review and approval by Thiokol and MSFC Configuration Control Boards and presentation to the Level II System Safety Review Panel (SSRP), along with a Change Request (CR) to the Program Review Change Board (PRCB). The thoroughness with which Thiokol and NASA review changes ensures all RSRM related issues are properly "screened" against program risk criteria and that there is an awareness and understanding of any significant change in risk. (ref. 4) Documentation of these assessments and inclusion in change review presentations provides communication of any change in risk.

Hazard Reports: The RSRM Flight Systems Hazard Reports examine the flight article through all phases from manufacture through flight and the subsequent refurbishment and reuse of hardware. Each Hazard Report addresses a unique hazardous condition and lists all the causes that could result in the hazardous condition. Requirements, controls and verification of controls to mitigate risk are listed in each report. (ref. 5)

Included with each RSRM Hazard Report is a risk matrix giving a visual depiction of the estimation of relative risk with the hazardous condition in each report and the subsequent causes identified. The risk matrix defined by NASA in NSTS 22254 and used by all Space Shuttle element contractors is simple and

straightforward yet often generates vigorous and detailed discussion. The vigorous and detailed discussion of risk issues in the decision making process has been a significant aid in the conveyance of information concerning RSRM risk to top Thiokol and NASA management. Use of the 4 X 3 risk matrix, as shown in figure 1, is a risk management tool for every RSRM hazard report and is also often used in depicting the risk of major changes and in discussing the affects of unexpected conditions.

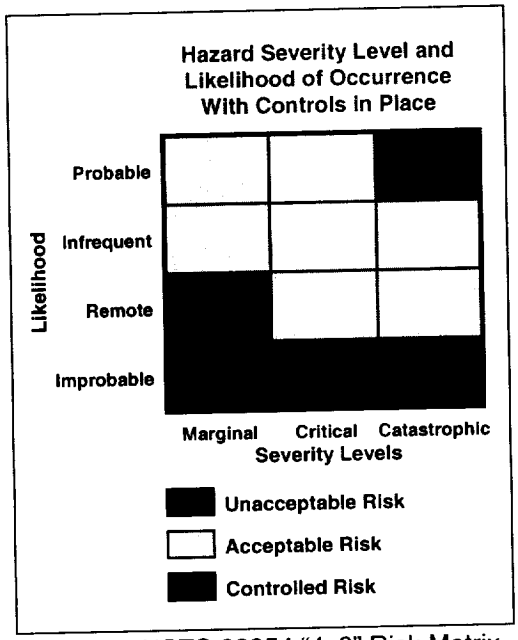

Figure 1 - NSTS 22254 "4x3" Risk Matrix

Each cause can be categorized in one of the following three risk classifications:

- Unacceptable Risk (upper right hand corner of the matrix) – Hazard for which corrective action must be taken prior to flight
- Accepted Risk (middle diagonal across the matrix) – Hazard that requires program evaluation and acceptance of control limitations and uncertainties
- Controlled Risk (lower left corner and lower part of matrix) – Hazard where appropriate controls have been implemented and comply with program requirements

Each cause is assessed for likelihood of occurrence by assessing the controls that are in place, for each cause, to determine if it is:

- Probable: Expected to happen in the life of the program
- Infrequent: Could happen in the life of the program. Controls have significant limitations or uncertainties
- Remote: Could happen in the life of the program, but not expected. Controls have minor limitations or uncertainties
- Improbable: Extremely remote possibility that it will happen in the life of the program. Strong controls in place

The severity level is an assessment of the most severe effects of a hazard, and is defined as follows:

- Catastrophic: Hazard could result in a mishap causing fatal injury to personnel and/or loss of one or more major elements of the flight vehicle or ground facility
- Critical: Hazard could result in serious injury to personnel and/or damage to flight or ground equipment, which would cause mission abort or a significant program delay
- Marginal: Hazard could result in a mishap of minor nature inflicting first-aid injury to personnel and/or damage to flight or ground equipment, which can be tolerated without abort or repaired without significant program delay (ref. 4)

Failure Modes And Effects Analysis / Critical Items List (FMEA/CIL): The FMEA has been used to identify all potential RSRM critical failures. The CIL provides the justification (termed as retention rationale) that explains how each particular failure mode is controlled to an acceptable level. RSRM hardware components are individually analyzed to determine possible failure modes and what occurrences such as process failures, material defects, etc. could cause the failure. The resulting worst-case effect of each failure mode is then assessed and documented. Based on the determined worst-case effects, all hardware items are classified according to an associated failure criticality. The

RSRM FMEA/CIL identifies three failure criticality levels with the following definitions:

Crit 1 - Single failure that could result in loss of life or vehicle

Crit 1R – Redundant hardware items(s), all of which, if failed, could cause loss of life or vehicle

Crit 3 – All others (ref. 6)

Note: Criticality 2 and 2R are for "loss of mission". Loss of mission without loss of life is not considers applicable as "worst case" for the RSRM.

The CIL is documented and maintained for all RSRM Crit 1 and 1R failure modes. CIL retention rationale documents how each component, material or hardware item is certified and what design safety margins are included. The CIL retention rationale also lists the inspections and tests performed during manufacturing and assembly processes that assure all failure causes are controlled and that the controls are verified. Each inspection or test listed in the CIL retention rationale is given a CIL code. These same inspections or tests with the corresponding CIL code are found in the manufacturing and inspection plans. CIL inspections and tests in manufacturing planning cannot be removed or changed without an assessment of risk, changing the CIL as applicable and the subsequent review and approval from Thiokol and NASA. Regular audits of manufacturing planning are conducted by a System Safety Engineer to verify that all the inspections listed in the CIL are properly called out in the planning. This process ensures that building the RSRM to design will be repeatable and that documented retention rationale will assure controls are in place so that failure modes will not occur. A summary of the FMEA/CIL benefits as listed in the RSRM Risk Management plan includes.

- Provides visibility of RSRM risks, affording special attention to critical hardware in program-critical decisions
- Provides an assessment for designers of the potential failure modes and effects of the design
- Identifies actions required and taken to develop and control retention rationale for criticality categories 1 and 1R failure modes
- Informs Thiokol Quality Engineering via the CIL Inspection Index of those operations/processes having control requirements that cannot be changed without prior approval
- Informs launch site operations of those operations/processes having control requirements
- Provides a reliability analysis for NASA that identifies all possible RSRM failure modes, failure mode effects, failure mode criticalities, and the retention rationale for all criticality 1 and 1R categories
- Provides data for the System Safety hazard analysis (ref. 2)

Certificate of Qualification (COQ): System Safety utilizes the Certificate of Qualification (COQ) for the RSRM to assess risk. The COQ provides certification and evidencing documentation that the design of the RSRM meets contract end item (CEI) specification requirements. "This assessment takes place at the initiation of the proposed change and receives Thiokol and NASA approvals prior to each launch. Like the Hazard Reports and FMEA/CILs, a detailed assessment sheet and disciplined change control system provides the necessary risk mitigation and confidence that all proposed changes are meeting the required verification method of validation or re-certification." (ref. 7) System Safety assessment criteria for COQ re-certification consists of answering yes to any of the following:

- Design or manufacturing process changes have been made that affect form, fit, or function, and/or adversely affect safety and/or reliability of the RSRM and/or its components
- Manufacturing source or location is changed that affect form, fit, or function, and/or adversely affect safety and/or reliability of the RSRM and/or its components
- Previously certified design and performance requirements are no longer met, previous certification baseline is challenged, and/or manufacturing processes produce hardware that is out of family (ref. 2)

Other Independent Assessments/System Safety Tools: While Hazard Reports, FMEA/CIL and COQ are the major contract documents required by NASA to identify risk and document evidence that such risks are controlled to an acceptable level; additional risk mitigation tools are also used in evaluating changes.

System Safety provides each noted flight hardware discrepancy that occurs during the manufacturing or assembly processes with a discrepancy report risk assessment. Providing the hardware criticality that is assigned by the FMEA/CIL and the discrepancy criticality specific to the discrepant condition provides a quick look at risk. For example: a discrepancy that has noted criticalities of 1/3 would show that the affected hardware has a documented criticality of 1 in the FMEA/CIL and that the noted discrepancy (3) is of a nature that it constitutes an insignificant change in risk from baseline, a discrepancy that has noted criticalities of 1/1 shows a documented hardware criticality of 1 in the FMEA/CIL and that the noted discrepancy (1) constitutes an increase in risk from baseline. Discrepancies that may constitute an increase in risk include such issues as those that may be outside of history, a worst-case condition, a first time repair or a new analytical technique, etc. Discrepancies that are of greater significance, including all assigned criticalities of 1/1, go on to be reviewed and assessed by the Senior Material Review Board (SrMRB). For each discrepant condition that goes to SrMRB a System Safety assessment sheet describing the discrepancy and providing rationale of why the risk would be acceptable is provided. Thiokol and NASA Project and Program Managers as well as Thiokol and NASA Safety and Mission Assurance Representatives, discuss SrMRB discrepancies again in the Flight Readiness Reviews and Pre-Flight Assessment meetings. The review of SrMRB discrepancies assures that any change in risk or any new risk is understood and that appropriate mitigation efforts have been employed to control risk to an acceptable level. (ref. 8)

One of the many process verification methods utilized on the RSRM is the Process Failure Modes Effects Analysis (PFMEA). Use of the PFMEA as a tool to assess modification of systems or equipment and to provide recommendations to increase safety, quality, reliability, and efficiency has been recognized and employed by NASA and Thiokol. A PFMEA is an analytical tool used to assess how a process can fail to make a good product, similar to the way that the FMEA is used to assess potential failures of a product. A team of engineers, operators and others who are familiar with a particular process typically accomplish the PFMEA efforts. The PFMEA answers questions such as: "How can this process fail? What effect will these process failures have on the end product (or user)? How can these potential failures be eliminated or controlled?" The PFMEA also requires the team to discuss and give a numerical rating known as a risk prioritization number to the severity, probability and ability to detect process failures. PFMEAs are accomplished on new processes and are used to evaluate and improve well-established processes. Obviously, to maximize potential benefits, a PFMEA should be performed as early in the manufacturing development cycle as possible. The value of the consistent effort to identify and analyze processes with PFMEA methodology is difficult to quantify, however, Thiokol data has shown a reduction of special issues as manufacturing processes are reviewed and assessed with PFMEA approach. All PFMEAs completed to support the RSRM project (at Thiokol or KSC) are tracked with a closed - loop tracking system for implementation of recommended risk reduction actions. (ref. 2 and 9)

The reusable nature of the RSRM provides a unique opportunity for retrieval, disassembly, inspection and assessment of post-flight hardware. System Safety participates in and is part of the post-fire disassembly and evaluation effort for each flight to verify that RSRM hardware functioned safely and reliably. Observations made during the post-fire inspection are evaluated against established limits. When there is a variation from the limits an assessment is made to evaluate the risk. With each post-flight assessment the limits are continuously re-evaluated based on increased technical knowledge, flight experience, and implemented hardware changes. With hardware improvements and increasing experience, the number of items that exceed limits and require in depth evaluation after flight continues to decline. (ref. 2)

Conclusion

The effort to put rockets into space has and always will have significant inherent risks. Knowing, understanding and controlling those risk is of utmost importance to Thiokol and to NASA. RSRM risks have been analyzed providing current baseline documentation of what the risks have been and what they presently

are. While the intent is to stay as close to the current baseline as possible, changes to the RSRM are accomplished to provide performance improvements as well as to replace materials that have become obsolete. All changes, including improvement initiatives and the replacements for obsolescent materials, are evaluated carefully through the perspective of various disciplines. The system safety discipline provides input to the change process with the use of various analytical tools to document and communicate the assessment of risk. The review and re-review of potential risk issues for each flight assures that any change in risk or any new risk is understood and that appropriate mitigation efforts have been employed to control risk to an acceptable level.

References

1. Morton Thiokol Pamphlet, Thirty –Two Months to Discovery. Morton Thiokol Inc., Aerospace Group, Space Operations, Brigham City, Utah, 1988.
2. Kerry G. Sanofsky, Risk Management Plan for the Reusable Solid Rocket Motor (RSRM) Project, TWR-77231. Thiokol Propulsion, Brigham City, Utah, October 15, 2000.
3. Kerry G. Sanofsky, RSRM Accepted Risk Status Report, TWR-77350, Thiokol Propulsion, Brigham City, Utah, October 23, 2000.
4. NSTS 22254, Methodology for Conduct of Space Shuttle Program Hazard Analyses. National Aeronautics and Space Administration, Lyndon B. Johnson Space Center, Huston, Texas, February, 2000.
5. Flight Systems Hazard Reports for the Space Shuttle Reusable Solid Rocket Motor. Thiokol Propulsion, Brigham City, Utah, October 15, 1999.
6. NSTS 22206, Instructions for Preparation of Failure Modes Effects Analysis (FMEA and Critical Items List (CIL). National Aeronautics and Space Administration, Lyndon B. Johnson Space Center, Huston, Texas, December 10 1993.
7. RSRM Certificate of Qualification Data Report, TWR-18764. Thiokol Propulsion, Brigham City, Utah, 13 June 2001.
8. Safety Plan for the Space Shuttle Reusable Solid Rocket Motor, TWR-15902. Thiokol Propulsion, Brigham City, Utah, January 7, 1998.
9. PFMEA Guideline for Performing, TWR-63794. Thiokol Propulsion, Brigham City, Utah, March 23, 1999.

Biography

Phillip O. Greenhalgh, CSP
437 West 200 South
Brigham City, UT 84302

(435) 734-2291 (Home)
(435) 863-5438 (Business) (435) 863-2884 (Fax)
E-mail: Phillip.Greenhalgh@Thiokol.com

Phil Greenhalgh is a Principal Engineer/Scientist in System Safety and Reliability working on the Space Shuttle Solid Rocket Motor program for ATK, Thiokol Propulsion. After completing a Masters Degree in Safety at Central Missouri State University he began his career at Thiokol in 1985. In his sixteen years at Thiokol, he has been involved in the Space Shuttle Challenger Accident Investigation and the subsequent redesign of the Solid Rocket Motor. His experience includes preparing Hazard Analyses, FMEA/CILs, PFMEAs, Problem Assessment Reports, fault tree analyses, risk assessments, conducting audits, and presenting System Safety briefings to Thiokol and NASA Management. Phil has also served, as a contractor member of the NASA System Safety Review Panel. He is presently the System Safety Project Engineer in the Thiokol Mix/Cast Work Center working with solid rocket propellant. Phil joined the System Safety Society in 1987. In 1996 he became a Certified Safety Professional (CSP).