# Identifying, Assessing, and Mitigating Risk of Single-Point Inspections on the Space Shuttle Reusable Solid Rocket Motor

Phillip O. Greenhalgh, CSP; ATK Thiokol Inc.; Brigham City, Utah

Keywords: Space Shuttle, risk assessment, single-point inspection, risk prioritization, Reusable Solid Rocket Motor, RSRM

## Abstract

In the production of each Space Shuttle Reusable Solid Rocket Motor (RSRM), over 100,000 inspections are performed. ATK Thiokol Inc. reviewed these inspections to ensure a robust inspection system is maintained. The principal effort within this endeavor was the systematic identification and evaluation of inspections considered to be single-point. Single-point inspections are those accomplished on components, materials, and tooling by only one person, involving no other check. The purpose was to more accurately characterize risk and ultimately address and/or mitigate risk associated with single-point inspections. After the initial review of all inspections and identification/assessment of single-point inspections, review teams applied risk prioritization methodology similar to that used in a Process Failure Modes Effects Analysis to derive a Risk Prioritization Number for each single-point inspection. After the prioritization of risk, all single-point inspection points determined to have significant risk were provided either with risk-mitigating actions or rationale for acceptance. This effort gave confidence to the RSRM program that the correct inspections are being accomplished, that there is appropriate justification for those that remain as single-point inspections, and that risk mitigation was applied to further reduce risk of higher risk single-point inspections. This paper examines the process, results, and lessons learned in identifying, assessing, and mitigating risk associated with single-point inspections accomplished in the production of the Space Shuttle RSRM.

## Introduction

ATK Thiokol Inc. has produced the Space Shuttle Reusable Solid Rocket Motor (RSRM) developed for NASA since its inception in the mid-1970s. The RSRM is the largest human-rated solid propellant rocket motor ever flown and the only booster capable of recovery and reuse. During the initial 122 seconds of each Space Shuttle flight, two RSRMs, painted white and attached on each side of the orange external tank, expend over 2 million pounds of solid propellant in a plume of fire and smoke providing 80 percent of liftoff thrust. The RSRMs accelerate the Shuttle to a speed of 3,094 miles per hour before separating from the orbiter and external tank at an altitude of approximately 24 nautical miles. Nearly seven minutes after separation, the spent boosters parachute into the Atlantic Ocean approximately 140 nautical miles downrange from Kennedy Space Center (KSC), Florida. After each flight, the boosters are recovered, disassembled, and given a postflight inspection to assess performance. The inspection begins at KSC and continues as each motor segment is returned to the ATK Thiokol Inc., Component Refurbishment Work Center in northern Utah. After the postflight assessment is complete, the RSRM metal components are refurbished and prepared for reuse on future Shuttle flights (ref. 1).

In the production of each RSRM, over 100,000 inspections are performed. Approximately 70,000 of these inspections are accomplished at vendors and in Receiving Inspection on procured raw materials, hardware, and components. The RSRM production effort at ATK Inc. Thiokol takes place in five distinct work centers where another 39,000-plus inspections, including nondestructive evaluation (NDE), of each motor take place. ATK Thiokol Inc. initiated an endeavor to ensure that it maintains an inspection system that is robust, prevents defects from entering the final product, and ultimately represents a respected declaration of product quality in relation to RSRM systems. A primary project in support of this endeavor was to review the RSRM inspection system for single-point inspections. This effort to examine all single-point inspections was accomplished in two phases. The initial phase addressed the inspections in operations production planning for each work center and in NDE; the second phase was for inspections in procurement planning. Single-point inspection definitions and ground rules were defined as follows:

- Quality inspection of components, tooling, and materials with only one set of eyes and no re-verification are single-point inspections.

- Customer review or witness does not count as a second set of eyes.
- Processes reviewed by both Manufacturing Operations and Quality Assurance (QA) are considered redundant and not single-point inspections.
- Inspections completed in one work center with a single set of eyes that are re-inspected in another work center are not single-point inspections.
- Inspections performed by vendor and the ATK Thiokol Inc. QA representative at the vendor are not considered single-point inspections.
- Inspections completed by two separate inspectors with two separate buyoffs are not single-point inspections.
- Review of data obtained from supplier or testing is considered single-point inspection.

The purpose of the review and identification of these inspections was to accurately characterize risk in the system in relation to single-point inspections and ultimately address and/or mitigate risk associated with each single-point inspection (ref. 2).

The initial endeavor began several years ago as an ATK Thiokol Inc., Quality Assurance self-initiated effort motivated by a desire to identify and improve critical inspection points. In December of 2002 this initiative was expanded with the organization of multi-discipline teams to assess those inspections determined to be single-point. This initiative was believed to be in harmony with the Space Shuttle Independent Assessment Team Report to the Associate Administrator Office of Space Flight, October–December 1999 which expressed; "findings and observations that are systemic in nature and not confined to any one Shuttle subsystem or element" (ref. 3). Issue 6 of the report expresses the concern that "In the past, the Shuttle Program had a very extensive QA program. The reduction of the QA activity ("second set of eyes") and of the Safety & Mission Assurance function ("independent, selective third set of eyes") increases the risk of human single-point failures.... Human errors in judgment and in complying with reporting requirements (e.g., in or out-of-family) and procedures (e.g., identification of criticality level) can allow problems to go undetected, unreported or reported without sufficient accuracy and emphasis, with obvious attendant risk..." The recommendation provided to NASA states: "The Space Shuttle Program should systematically evaluate and eliminate all potential human single-point failures" (ref 3). The comprehensive review of inspections proved to be very useful in "scrubbing" the inspections that are heavily dependent on one human, to understand the inherent risk and provide risk mitigation where needed. Through this effort each team gained confidence that the correct inspections were being accomplished, that there was appropriate justification for inspections that are single point and that additional, revised or updated risk mitigating inspections were provided where needed to further reduce the risk associated with those single-point inspections deemed to have higher relative risk (ref. 2). While this effort began prior to the Columbia accident, those tragic events added an even greater sense of urgency to accomplishing a thorough review, assessment and mitigation of risk associated with single point inspections.

## Identification and Ranking of Single-Point Inspections in Work Center Planning

In order to perform the evaluation of each single-point inspection, teams within each of the five work centers as well as from NDE, were formed to review the inspection points (IP) and assign each a risk prioritization number (RPN; as explained below in Risk Prioritization Methodology). The individual teams assembled were multi-disciplined, cross-functional teams consisting of representatives from Quality Engineering, Quality Assurance, Design Engineering, Manufacturing Engineering, Manufacturing Operations, and System Safety/Reliability. Tasks were given to each team: 1) Prioritize the risk associated with each single-point inspection using the qualitative assessment for failure occurrence, severity, and detection as defined below; 2) Decide if changes to IPs are necessary to mitigate risk and, if so, what the mitigation efforts should be; and 3) Justify the decision to provide risk acceptance rationale or to recommend implementing additional risk mitigation actions. With the additional examination provided by the teams, if an IP did not meet the criteria of single-point inspection, the point was removed from the list.

An initial database of all inspections was obtained and scrubbed by a QA inspector familiar with the IPs in each work center. After the initial review, the inspection database applicable to each work center was narrowed to those identified as single-point inspections. Each work center team sorted their particular database in accordance with the part numbers or processes as they decided, assessed their respective IPs, and assigned an initial RPN to each buyoff. After the initial lists of all the inspections applicable to each work center were reviewed, assessed, and the single-point inspections identified, review teams used risk prioritization methodology, similar to that used in Process Failure Modes Effects Analysis (PFMEA) efforts, to rank the risk associated with each single-point inspection. Individual teams began their respective risk prioritization efforts using a qualitative assessment for occurrence, severity, and detection capability (defined in tables 1 through 3). The product of the numbers derived for occurrence, severity and detection capability

make up the RPNs. The RPNs show what inspections are the most significant in terms of risk to the product or to the process, with the highest number showing the greatest risk. This process of reviewing inspections and assessing risk through risk prioritization numbers is depicted in figure 1.

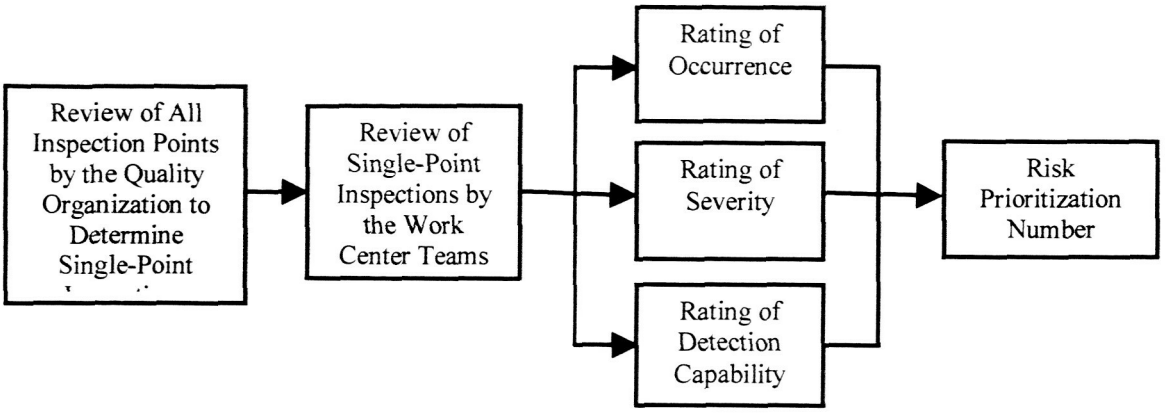


Figure 1 – Inspection Review and Risk Ranking Process

Occurrence Rating: The occurrence rating is the estimated probability of there being a discrepant condition on the hardware related to the inspection being assessed. The occurrence is assessed independent of severity and detection. Each team subjectively estimated the probability of occurrence on a 1 to 10 scale as defined in table 1.

**Table 1 – Occurrence Rating Criteria**

| Probability of Occurrence | Criteria<br>Evaluating the likelihood of discrepant hardware in relation to the inspection being evaluated | Rating |
|---|---|---|
| Very Low | Hardware rarely, if ever, experiences a discrepancy | 1 |
| Low | Hardware has experienced relatively few discrepancies | 2-3 |
| Moderate | Hardware periodically experiences discrepancies, but not in major proportions | 4-5-6 |
| High | Hardware relatively often experiences discrepancies | 7-8 |
| Very High | Hardware typically experiences discrepancies | 9-10 |

Severity Rating: Severity is the factor that represents the seriousness or impact of hardware failure. The severity rating is a subjective evaluation using worst-case effects a failure could have on the hardware assuming it has a discrepancy for which the inspection being assessed is intended to detect. Severity is assessed independent of occurrence and detection. Each team subjectively estimated severity on a 1 to 10 scale as defined in table 2.

**Table 2 – Severity Rating Criteria**

| Severity of Occurrence | Criteria<br>Evaluates worst-case effects of hardware assumed to have discrepancy for which inspection is assessing. Severity is considered as though no controls are in place; is independent of occurrence and detection. | Rating |
|---|---|---|
| Low | Hardware discrepancy that has very little effect on further processing or product performance | 1 |
| Minor | Hardware discrepancy that has minor effect on further processing or product performance | 2-3 |
| Moderate | A hardware discrepancy that causes customer concern or program impact but will not cause a Criticality 1 failure of the end item or an equivalent process failure | 4-5-6 |
| High | Hardware discrepancy that causes severe impact to component or process and may contribute to a Criticality 1 failure of the end item or an equivalent process failure | 7-8-9 |
| Very High | Hardware discrepancy that contributes to a known or highly probable Criticality 1 failure of the end item or an equivalent process failure involving loss of life or a major loss of manufacturing facilities | 10 |

Detection Rating: The detection rating is a subjective evaluation of the likelihood of detecting discrepant conditions on hardware for which the assessed inspection is intended to detect. Inspection strengths and downstream inspections that would catch the particular discrepancy are considered. The detection rating is assessed independent of occurrence and severity rating. Each team subjectively estimated severity on a 1 to 10 scale as defined in table 3.

Table 3 – Detection Rating

| Probability of Detection | Criteria<br>Evaluates likelihood of detecting discrepancy considering inspection strengths and downstream overlapping/complementary inspections. | Rating |
|---|---|---|
| Very High | Improbable that discrepant hardware leaves the work center containing the defect | 1 |
| High | Low probability that discrepant hardware leaves the work center containing the defect | 2-3 |
| Moderate | Discrepant hardware likely to leave work center. However, improbable that discrepant hardware will be flown. Hardware defect is detectable by subsequent processing in other work centers that have inspections/ processes that overlap the inadequate inspection | 4-5-6-7 |
| Low | High probability that hardware defect is not identified prior to flight. There are no overlapping inspections that would detect defect | 8-9 |
| Improbable | Very high probability that hardware defect is not identified prior to flight. There are no overlapping inspections or processes that would detect defect. Detection would require special inspection techniques | 10 |

Risk Prioritization Number: The RPN is the product of the occurrence, severity, and detection ratings for each inspection assessed, the highest RPNs being considered the most critical. The RPN for each inspection is based on the judgment of the individual team that made the assessment. Recommended actions provided by the individual teams are suggestions to further reduce the risk to RSRM flight hardware associated with the specific inspections (ref. 4).

While the overall team approach was the same, a significant variation of RPNs existed from one team to another. With this difference in the initial RPNs, an attempt was made to understand the variation. Each team reevaluated the assigned RPNs, placing less emphasis on history (occurrence) and giving more to the severity and detection capability ratings in order to determine if the numbers should be more consistent across work centers. Even with less emphasis on history, it was determined that each team was unique and that the RPNs had relevance only within each work center and not necessarily from one to another. With this, each work center team determined their own threshold RPN at which specific risk mitigation, acceptance, or justification was provided to each of the assessed buyoffs. Inspections points with RPNs below the work-center-specific thresholds were determined to need no further mitigation or written justification.

Determining Risk Threshold and Providing Risk Mitigation, Acceptance, or Justification

The effort to prioritize risk with use of PFMEA methodology is dependent on the subjective assigning of numbers in the rating of occurrence, severity and detection capability of discrepancies associated with each inspection point. The RPNs naturally varied from team to team due to the parts, materials and processes each team reviewed and the experiences of the individual team members. While it was not possible to determine absolute risk, the use of risk prioritization relative to each work center provided the opportunity to prioritize risk. After determining the RPNs for the inspections reviewed, each work center team decided on their own threshold RPN, independent of the other teams, based on the significance of risk relative to their assessments. The unique threshold RPN determined by each team signified a point at which additional effort was needed. Numbers below the threshold were considered to indicate very minor risk associated with the inspection. Low threshold numbers were determined to be acceptable with no further explanation than that given by rating occurrence, severity, and detectability in the determination of the RPN. Numbers above the threshold were considered to indicate that there was a more significant risk of the inspection not adequately accomplishing the intended assessment. Inspections judged to have such limitations or uncertainties as indicated by RPNs above the threshold were determined to be in need of risk acceptance justification or mitigating actions. Risk acceptance justification was provided for the inspections that had RPNs above the threshold but had solid rationale explaining why the inspection is sufficient as is. Rationale for acceptance of risk is based on experience and may include ease of inspection, different tests, inspections, or evaluations that provide verifying data, reliability, accessibility, etc. Risk mitigating actions are given as recommendations to improve those inspections that are judged to be in need of remediation. Changing inspection methods, techniques, or instruments or adding a redundant inspection to the already existing IP are examples of ways to accomplish mitigation of risk associated with IPs that were found to be in need of remediation (ref. 2).

In the work centers and in NDE, QA representatives initially reviewed 39,118 IPs. Of these IPs, 2,784 were determined to be single-point inspections. After careful review of each of the single-point inspections and determining a risk prioritization using the RPNs, the teams found a total of 2,304 of the 2,784 inspections that were judged to have very low risk, thus requiring no further explanation or mitigation. The remaining 480 single-points

inspections were judged according to the teams to constitute a risk above the unique threshold given by each team. The IPs with RPNs above the thresholds were determined to need either 1) a written justification listing solid rationale of why the associated risk was acceptable or 2) a plan of recommended mitigating action to reduce risk. It was determined by the individual teams that 458 of the single-point inspections should be addressed with justification listing rationale as to why the risk was acceptable without change to the inspection. Mitigating action to reduce risk was recommended for 22 of the single-point inspections (ref. 2).

Following are examples (tables 4 through 6) of several inspection points from three of the work centers noting the occurrence, severity, detection (O-S-D) ratings and resultant RPN, and whether or not changes/additions should be made to the inspection point along with appropriate justification/comments from several teams (ref. 2).

**Table 4 – Mix/Cast (Propellant) Work Center Example**

| Inspection Point | Change – Yes/No | Justification (O-S-D) (RPN) |
|---|---|---|
| **Assemble/Cast Aft 1U77504-11 (901)** | | |
| QA inspect Slit Plate for Contamination Prior to Bell-to-Bowl Connection | No | Manufacturing inspects and cleans all bell-to-bowl tooling (including slit plate) and buys off the planning prior to inspections (2-5-2) (20) |
| QA Inspect Slit Plate Using a Long Mirror for Contamination | Yes | Add manufacturing buy off. (2-5-2) (20) |
| **Liner/Aft 1U77504-12** | | |
| Required or Not Required for Class 1 or Limited-Use Conditions | No | This single-point inspection requires QA to contact Quality Engineering to verify processes will not further degrade limited defect on which limited condition is based. Limited condition is re-measured at last processing sequence prior to mate. Therefore, verification of this single-point inspection is sufficient as determined by team because of detection rate. (3-4-1) (12) |

**Table 5 – Nozzle Work Center Example**

| Inspection Point | Change – Yes/No | Justification (O-S-D) (RPN) |
|---|---|---|
| **Machine/Bond** | | |
| Tag End Testing | Yes | QA verifies lab work request acceptability – does not review data, approves or rejects lab data. *Recommendation*: Short Term – Change to have QA look at the acceptability of data. Long Term – Have the lab incorporate Electronic Shop Instructions (planning) with range data. (3-6-4) (72) |
| Laser Hardening Material Evaluation Laboratory | Yes | Lab work request received from Wright-Patterson AFB with data, and Program Office reviews data with Marshall Space Flight Center before releasing memo to bond part. *Recommendation*: Establish engineering requirements. (2-5-4) (40) |
| Tape Wrap – All inspections in this group have O-S-D <3 | N/A | N/A |
| **Nose-Throat Assembly** | | |
| Verify Plug Head is Flush to Spot Face per STW7-9199, Para 5.3.1.D | No | This inspection is robust and easy to perform. Measured with depth micrometer (standard measuring instrument). (1-4-2) (8) |
| Verify Leak Check Port O-ring Has Not Been Damaged or Violated Prior to Use | Yes | Prepacked O-ring inspected at vendor, QA verifies no damage at package opening prior to greasing. *Recommendation*: Manufacturing buyoff to ensure integrity of the seal. (1-9-8) (72) |

Table 6 – Nondestructive Evaluation Example

| Inspection Point | Change – Yes/No | Justification [Team Comment] (O-S-D) (RPN) |
|---|---|---|
| **X-ray Igniters Unloaded** | | |
| Verify Subsurface Defects Do Not Exceed Specification | Yes | High RPN [Add double buyoff in planning to verify NDE report data are correct and reported accurately (worked by two people, one more buy-off needed)]. (2-8-3) (48) |
| Verify Component Temperature and Exposure to Ambient Environment During In-Plant Transportation, STW9-3828 | No | Temperature recorder records the temperatures and is downloaded by another work center as a double check. [Keep as is]. (3-6-2) (36) |
| Prefired Igniter Insulation Thickness Matrix | Yes | High RPN [Add double buyoff in planning to verify NDE report data are correct and reported correctly (worked by two people, one more buy-off needed)]. (2-7-3) (42) |
| **X-ray Igniters Loaded** | | |
| Verify Cracks Conform to Engineering Specification | Yes | High RPN [Add double buyoff in planning to verify NDE report data are correct and reported correctly (worked by two people, one more buy-off needed)]. (1-7-8) (56) |
| Verify Bond Separations Conform to Engineering Specifications | Yes | High RPN [Add double buyoff in planning to verify NDE report data are correct and reported correctly (worked by two people, one more buy-off needed)]. (1-7-8) (56) |
| Verify Voids Conform to Engineering Requirements | Yes | Worked by two people, one more buy-off needed to be technically redundant [Add double buyoff in planning to verify NDE report data are correct and reported correctly]. (2-6-3) (36) |
| Verify Void Area Meets Process Control Limits (PCL) | No | Process Control Limits are below engineering limits, which are also checked. [Keep as is]. (3-4-3) (36) |

The effort to identify, assess and prioritize the risk of single-point inspections as well as to provide risk acceptance justification rationale or mitigating action, where necessary, was also completed in the Insulation/Component, Final Assembly, and Component Refurbishment Work Centers as well as with approximately 70,000 procurement inspections. QA management accepted and approved the risk methodology of identifying, assessing, and mitigating risk of single-point inspections on the Space Shuttle RSRM. Assignments of persons responsible to complete the actions for the enhancement of certain inspections were made and tasks/accomplishments are being tracked to completion by a closed-loop QA system to ensure implementation.

## Conclusion

Launching rockets has, and always will have, significant inherent risks. Prudent risk management ensures that the shuttle is safe to fly. Because the Space Shuttle is a human-rated system, risk management requires an even more keen understanding of the inherent risk and a continual vigilance of risk mitigating controls. The continuous endeavor to know, understand, and control risk is of utmost importance to ATK Thiokol Inc. and to NASA. The risk assessment effort is unrelenting and diligence in examining and reexamining systems is required. The process of identifying, assessing, and mitigating the risk associated with single-point inspections was a significant effort to enhance the overall risk management of the Space Shuttle RSRM.

ATK Thiokol completed this comprehensive review of inspections including an identification, characterization, and risk justification/mitigation exercise in relation to single-point inspections. Identification of single-point inspections and ranking the inherent risk proved to be very beneficial in "scrubbing" the inspections to understand risk as well as providing risk mitigation where needed. While this effort was exhaustive and time consuming, each team gained confidence that their particular work center "maintains an inspection system that is robust, prevents defects from entering the final product, and ultimately represents a respected declaration of product quality in relation to RSRM systems" (ref. 2). Assurance of the appropriateness of each inspection came through application of RPNs, acceptance rationale/justification, and risk-mitigating actions to further reduce risk. With knowledge gained through this endeavor it became apparent that the overall inspection system could be strengthened by a continuous single point inspection evaluation. Ongoing evaluation of single point inspections will provide future opportunities to identify risk and to

provide additional mitigation. Future Quality Assurance risk management plans include a follow-on project to develop methodology and procedures for continuous evaluation/ improvement of single-point inspections to control/reduce risk.

## References


1. P. O. Greenhalgh, B. Q. McCann "Multiple Changes to Reusable Solid Rocket Motors, Identifying Hidden Risks." Conference Proceedings, 21st International System Safety Conference, 2003 – Broader Perspectives, Focused Solutions, p 787.

2. P. O. Greenhalgh, Single Point Inspection Risk Prioritization and Mitigation Assessment, TR014536, ATK Thiokol, Brigham City, Utah, September 30, 2003, pp 1 - 41.

3. Space Shuttle Independent Assessment Team, Report to the Associate Administrator, Office of Space Flight, October – December 1999, Report Issue No. 6.

4. Instructions for Preparation of Process Failure Modes Effects Analysis (PFMEA), TWR-63794, ATK Thiokol, Brigham City, Utah, September 30, 2003, p 1.


## Biography


Phillip O. Greenhalgh, principal engineer/scientist, System Safety and Reliability, ATK Thiokol Inc., P.O. Box 707, Brigham City, UT 84302, USA, telephone – (435) 863-5438, facsimile – (435) 863-2884, e-mail – phillip.greenhalgh@atk.com


Mr. Greenhalgh enjoys a career at ATK Thiokol Inc. in Northern Utah, working on the Space Shuttle RSRM Program. After completing a master's degree in Aviation Safety at Central Missouri State University, Phil began his career at Thiokol in 1985. In his nineteen years at Thiokol, he has been involved in the Space Shuttle Challenger Accident Investigation, the subsequent redesign of the Solid Rocket Motor, and the maintenance of flight system safety and reliability. He has served as a contractor member of the NASA System Safety Review Panel. Mr. Greenhalgh joined the System Safety Society in 1987. In 1996, he became a Certified Safety Professional.