Management Science Letters 5 (2015) 669–678

Contents lists available at GrowingScience

Management Science Letters

homepage: www.GrowingScience.com/msl

Failure mode and effect analysis on safety critical components of space travel

Kouroush Jenab[a*] and Joseph Pineau[b]

[a]*Faculty of College of Aeronautics, Embry-Riddle Aeronautical University, 600 S. Clyde Morris Blvd. Daytona Beach, FL 32114-3900, USA*
[b]*Student of College of Aeronautics, Embry-Riddle Aeronautical University, 600 S. Clyde Morris Blvd. Daytona Beach, FL 32114-3900, USA*

C H R O N I C L E

Article history:
Received March 25, 2015
Received in revised format 28 March 2015
Accepted 12 May 2015
Available online
May 14 2015

Keywords:
Failure Mode
Space flight
Solid Rocket Booster
Criticality Analysis
FMEA
FMECA

A B S T R A C T

Sending men to space has never been an ordinary activity, it requires years of planning and preparation in order to have a chance of success. The payoffs of reliable and repeatable space flight are many, including both Commercial and Military opportunities. In order for reliable and repeatable space flight to become a reality, catastrophic failures need to be detected and mitigated before they occur. It can be shown that small pieces of a design which seem ordinary can create devastating impacts if not designed and tested properly. This paper will address the use of a Failure Mode, Effects, and Criticality Analysis (FMECA) with modified Risk Priority Number (RPN) and its application to safety critical design components of shuttle liftoff. An example will be presented here which specifically focuses on the Solid Rocket Boosters (SRBs) to illustrate the FMECA approach to reliable space travel.

1. Introduction

The Space Shuttle uses two solid rocket boosters (SRBs), which are attached to each side of an external tank containing liquid fuel, to propel the shuttle into space. The SRBs contribute 80% of the total thrust at liftoff. The SRB is made of 11 individual cylindrical sections. The sections are machined to find tolerances, and partly assembled into four casting segments at the factory. These segments are then sent to the launch side to be put together.

The solid rocket booster field joint is a joint which is made in the field to connect sections of steel together to form the housing for the rocket fuel. These joints are made in the field due to transportation logistics. When the individual sections of steel are assembled, they form a tube almost 116 feet long. The field joint is made of a tang and clevis which hold the assembly together and uses O-rings to prohibit leakage of propellant (see Fig. 1).

* Corresponding author. Tel: +1(416) 454 9767
E-mail address: kouroush.jenab@erau.edu (K. Jenab)

doi: 10.5267/j.msl.2015.5.006

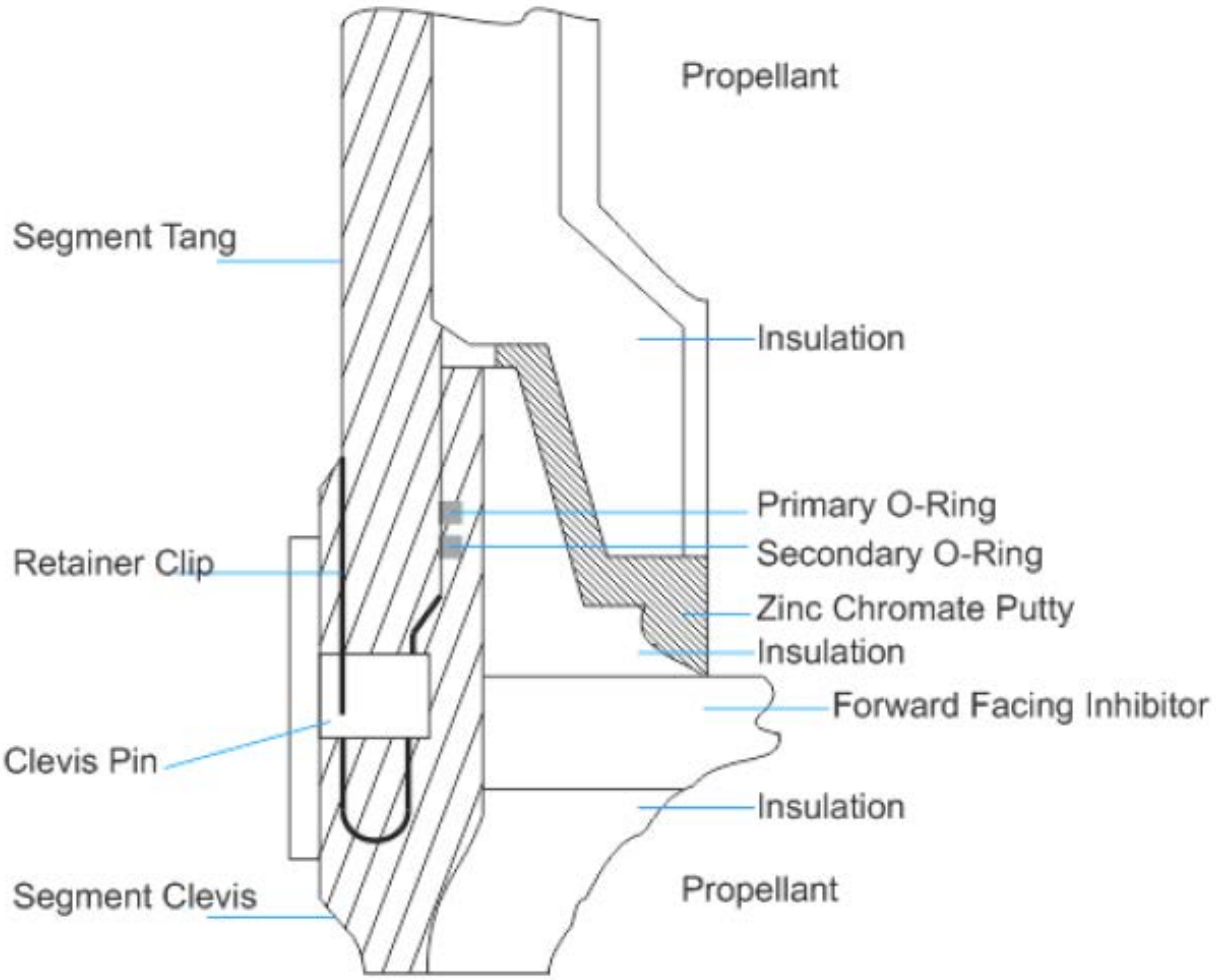

Fig. 1. Solid Rocket Motor Cross Section

The diameters of the two O-rings are 0.280 inches (+0.005, -0.003), these O-rings are installed when the four segments of steel are stacked together at the launch site. The O-ring static compression is dependent on the width of the gap between the tang and the inside leg of the clevis. This gap can vary depending on the size and shape of the segments as well as the loads on the segments. Due to the varying size of the gap, as well as to prevent direct contact of the O-ring with combustion gasses, Zinc chromate putty is applied to the insulation face prior to assembly. This putty not only prevents direct contact of combustion gasses with the O-rings, but also is used to pressure actuate the O-rings into the gap between the tang and clevis. The putty actuates the O-rings by combustion pressure displacing the putty into the space between the motor segments, and act as a piston which would compress the air ahead of the primary o-ring; forcing it into the gap between the tang and clevis.

“This pressure actuated sealing is required to occur very early during the Solid Rocket Motor ignition transient, because the gap between the tang and clevis increases as pressure loads are applied to the joint during ignition. Should pressure actuation be delayed to the extent that the gap has opened considerably, the possibility exists that the rocket’s combustion gases will blow by the O-ring and damage or destroy seals.” (Rogers et al., 1986)

From the *Report of the Presidential Commission on the Space Shuttle Challenger Accident*, it is clear that the field joint and its O-ring components are a Safety Critical item.

The design failures of the O-rings are that the O-rings are sensitive to both pressure and temperature. While the rocket is sitting upright, the O-rings are compressed. During the initial transient of rocket

excitation, the gap between the tang and clevis increases from the force (see Fig. 2). The O-rings need to return to their uncompressed shape to allow for pressure actuation during this initial transient. If the initial static compression is too great, it could prohibit the O-ring from returning to its uncompressed shape during the transient. This mechanical issue is compounded by an environmental issue, cold weather.

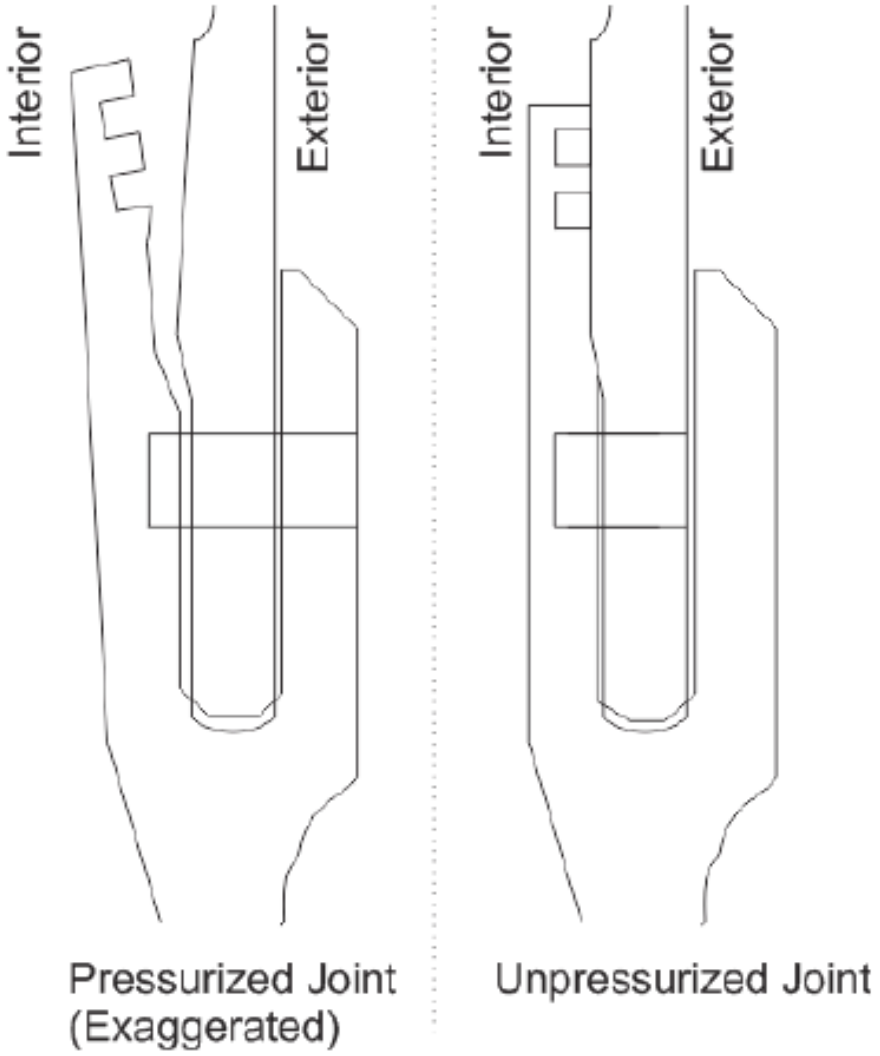

Fig. 2. Pressurized Joint Deflection

Cold weather would compound the issue of the O-ring not returning to its original shape and hence not sealing the gap sufficiently. Tests performed with different initial gap openings over a range of temperatures, "…indicate the sensitivity of the O-ring seals to temperature and O-ring squeeze in a joint with the gap opening characteristics of the Solid Rocket Motors." (Rogers et al.)

> "The results indicate that with a 0.020-inch maximum initial gap, sealing can be achieved in most instances at temperatures as low as 25 degrees Fahrenheit, while with the 0.004-inch initial gap, sealing is not achieved at 25 degrees Fahrenheit and is marginal even in the 40 and 50 degree Fahrenheit temperature range. For the 0.004-inch initial gap condition, sealing without any gas blow-by, did not occur consistently until the temperature was raised to 55 degrees Fahrenheit." (Rogers et al.)

The ambient air temperature at launch was 36 degrees Fahrenheit, up from the overnight temperature in the low 20s Fahrenheit. Approximately seven inches of rain fell while the rocket was on the Launchpad for 38 days, and ice was present on the Launchpad on the day of the launch. It is possible

that ice had also formed within the field joint. The ice had been shown in tests to have the potential to unseat the secondary O-ring.

The mechanical and environmental issues with the O-ring suggest that the selection of the particular O-ring was a poor design decision; or if the O-ring was the only available option, care was not taken to restrict operation of the SRB under temperature and static/dynamic compression conditions.

2. Literature Review

Quality, safety, and reliability have always been a concern of designers. Failure Mode and Effects Analysis (FMEA) has become an important tool in ensuring quality, safety, and reliability by systematically determining the potential causes of failures and their effects on a system. FMEA was created in the 1960s as part of the U.S. Minuteman rocket program in order to find and mitigate unanticipated design problems (Goble, 2012).

Since the origin of FMEA, an additional element of Criticality has been added making the definition: Failure Mode, Effects and Criticality Analysis (FMECA). McKinney (1991) postulated that in order for FMECA to be effective, it must be implemented early in development so that design may be altered to mitigate or eliminate the catastrophic, critical, and safety related failure possibilities. Bowles (1998) brought FMECA in line with modern design practices by creating a new standard. This new standard would incorporate three major changes; FMECA would be classified as a process which should be used throughout the development cycle, grouping together of failure modes which have equivalent effects in order to reduce duplicative work, and assigning Criticality based on the probability and severity of the failure mode using a Pareto ranking procedure.

Stålhane and Wedde (1998) applied three different process together in order to analyze safety critical systems; Fault Tree Analysis (FTA), FMECA, and code analysis. They concluded that, FMECA should not be used for safety analysis of a complete system, because each failure mode would need to be traced up to the top level, which is an analysis logically close to that of a FTA. Jianfeng et al. (1999) used a combination of FTA and FMECA to analyze the reliability of modern control systems. They believe that since FTA is a top down approach, and FMECA is a bottom up approach; the knowledge base gained from each approach will apply to the other and once enough information is present in a database, the subtrees of the system's typical components can be constructed with the aid of a computer in order to complete the entire fault tree.

Buzzatto (1999) studied the application of FMECA applied to the Reusable Launch Vehicle (RLV). He found that the FMECA process has been used for many years, but never seems to be complete early enough to be used as originally intended by the programs in accordance with MIL STD 1629A. His paper explores broadening the traditional FMECA approach by combining the Critical Components List (CCL) and FMECA together to meet mission needs and comply with Federal Aviation Administration (FAA) regulations for commercial space travel.

Franceschini and Galetto (2001) emphasized deficiencies with the current method of determining the Risk Priority Number (RPN) in the FMEA process. They developed another method to calculate the RPN which is just as easy to calculate, but does not require any arbitrary and artificial scaling of collected information. De Miguel et al. (2005) studied software development of safety critical systems for the direct application of safety analysis on software architectures. The method involved classification of components based on type and configuration with specific attributes; these attributes and types are then used in the safety analysis for the generation of FMECA models. Jenab and Dhillon (2005) developed a group based FMEA which tried to resolve conflict among experts. Chao and Ishii (2007) presented an example and case study using a modified FMEA design process. It decomposed the design process into six potential problem areas and used a question-based FMEA approach.

Carmignani (2009) proposed a modified approach to FMECA named priority-cost FMECA (PC-FMECA). PC-FMECA seeks to correlate potential failure to economic aspects in order to better define the RPN.

Dale & Anderson (2009) wrote a book which defines safety critical systems and the processes which can be used to solve issues related to safety. The book contains case studies related to safety critical systems, as well as safety standards. Bozzano and Villafiorita (2010) also contributed to the safety assessment of critical systems with a book focused on techniques and methods for dependability, reliability, and safety assessment. Illiashenko and Babeshko (2012) declared that there is no universally valid approach for determining which technique to use for reliability analysis. Their study had two main goals; reduce the risk of incorrect safety assessment, and examine FMECA-based techniques to determine how and when to use them for particular tasks. They go on to conclude that use of only one analysis technique is insufficient, and suggest combined usage of methods is important in safety analysis of critical systems. Haider and Nadeem (2013) detailed the informal and formal techniques which are available for the safety analysis of critical systems. Their study found that a combination of formal and informal techniques can reap the benefits of each method; that using the input of informal techniques into a formal technique can narrow the scope of the minimal critical set.

A common problem with FMECA is the long amount of time and laborious paperwork involved. The amount of time FMECA takes can result in the analysis being complete after the design is completed, negating the purpose of FMECA in the first place. Therefore, this study aimed at developing a process which uses two types of analysis. Fault Tree Analysis performed by NASA systems engineers as an input to a formal Failure Mode and Effect Analysis performed on safety critical components in order to limit the scope of the FMECA to ensure completion and use in the design process. The top-down FMEA performed by NASA links up to the bottom-up Criticality Analysis performed by the contractors, allows for communication and oversight of the entire design development. This paper will use this process on the case study of the Challenger explosion due to field joint O-ring failure of the Solid Rocket Booster.

3. Precision Failure Mode, Effects and Criticality Analysis Using a Modified Risk Priority Number

A Failure Mode, Effects and Criticality Analysis (FMECA) is most useful when used in conjunction with a second Quality Assurance Technique. FMECA and Fault Tree Analysis (FTA) are similar processes, where FMECA is a bottom up process, and FTA is a top down process. When a FTA is used as input to a FMECA it reduces the scope of the FMECA to be performed, which allows the FMECA analysis to be completed earlier in development in order for it to be used to modify the design in order to mitigate risks which the analysis has identified. Once the Safety Critical components have been identified (Severity Class of I, or II), then a FMECA can be performed on the sub-components to determine the critical fault paths. An example of a Failure Mode and Effects Analysis worksheet is provided below.

Table 1
Failure Mode and Effects Analysis

ID Number	Nomenclature	Function	Failure Modes and Causes	Mission Phase/Operational Mode	Failure Effects			Failure Detection Method	Compensating Provisions	Severity Class	Remarks
					Local Effects	Next Higher Level	End Effects				

The Failure Mode and Effects Analysis can be populated with the results of the FTA. A second table can then be filled in with the sub-components to determine the Failure Modes which would lead to the Severity Class of Catastrophic (I) or Critical (II). This second table would include the Modified Risk Priority Number for each Failure Mode.

Table 2
Criticality Analysis

ID Number	Nomenclature	Function	Failure Modes and Causes	Mission/Phase	Severity	Occurrence	Detection	RPN	Remarks

The Table below shows the qualitative relationship between Severity (S), Occurrence (O), and Detection (D) and the Level (L) assignment and relative Importance (I).

Table 3
Correspondence Map

Level (L)	Severity (S) Index	Occurrence (O) Index	Detection (D) Index	Importance (I) (S, O, D)
L_1	No	Almost Never	Almost Certain	None
L_2	Very Slight	Remote	Very High	Very Low
L_3	Slight	Very Slight	High	Low
L_4	Minor	Slight	Moderate High	Minor
L_5	Moderate	Low	Medium	Moderate
L_6	Significant	Medium	Low	Significant
L_7	Major	Moderately High	Slight	Major
L_8	Extreme	High	Very Slight	High
L_9	Serious	Very High	Remote	Very High
L_{10}	Hazardous	Almost Certain	Almost Impossible	Absolute

Each Index (Severity, Occurrence, Detection) can be assigned Importance Values which are used to assign weights to their importance. This flexible weight scale can be shifted based on program specific assessment of the relative importance of each Index.

To determine the Modified RPN for each failure mode, the equation below is used.

$$RPN(a_i) = Min\ [\ Max\ \{\ Neg\ (I(\ g_i\ )),\ g_j(\ a_i\ )\ \}\ ], \tag{1}$$

where

$RPN(a_i)$	is the Modified Risk Priority Number for the failure mode a_i
$I(g_j)$	is the importance associated with each criterion g_j
$Neg(I(g_j)$	is the negation of the importance's assigned to each decision-making criterion

The negation of the importance's is found by using the equation below.

$$Neg(L_i) = L_{10} - i + 1, \tag{2}$$

where L_i is the ith level of the scale.

This method of being able to assign weights to the RPN allows for more information to be obtained on which failure mode should be addressed over another, than simply multiplying the Severity, Occurrence, and Detection together as is done with the standard method of determining the RPN.

4. Illustrative Example

Considering NASA's Space Transportation System (STS) solid rocket booster (SRB) malfunction which caused the explosion of the Challenger, it was known by engineers at Morton Thiokol Inc. that cold weather could adversely impact the functionality of the Field Joint O-Rings; but this information was not communicated well and safety precautions were not enacted to prevent the realization of the safety critical issue.

Using the combination of methods of a top-down FTA, performed by NASA systems engineers; and a bottom-up FMECA, performed by Morton Thiokol Inc. engineers would have bridged the communication gap and design flaws which lead to Challenger explosion.

First, NASA systems engineers would perform a FTA to determine the possible failures in a top-down manner. The top-down process starts with an unwanted effect and works down to determine possible causes. The effects which are determined to be safety critical items are gathered and put into a FMEA. This paper will observe only the FMEA related to the Field Joint of the SRB. An example of the FMEA for the Field Joint is shown in the table below.

Table 4
NASA FMEA of Field Joint Example

ID Number	Nomenclature	Function	Failure Modes and Causes	Mission Phase/Operational Mode	Failure Effects			Failure Detection Method	Compensating Provisions	Severity Class	Remarks
					Local Effects	Next Higher Level	End Effects				
C-123	Field Joint	Hold together SRB body	Field Joint Seal can leak/break due to improper installation, O-Ring failure, tang-and-clevis failure	Launch	Field Joint does not contain SRB gasses	Loss of structural integrity of the SRB body	Loss of entire STS	None	Robust design and testing. Detailed maintenance procedures. Addition items on launch checklist detailing out of normal conditions	Cat I	Morton Thiokol Inc. responsible contractor for SRB

The FMEA documents would then be sent to the responsible contractor to perform a Criticality Analysis of the sub-components of the items in the FMEA. Traceability of the FMEA with the Criticality Analysis can be maintained this way and allow for NASA system engineers to oversee the design development. NASA could use the Modified RPN method, described in Section 3 of this paper to adjust the weights for the RPN to different levels for each contactor or sub-system as desired. The weights assigned to the importance of the three Indexes (Severity, Occurrence, Detection) will be 10, 8, 6, respectively. An example of the Criticality Analysis with using a modified RPN is shown in Table 5.

The RPN number in the table is the modified RPN number, which is determined by using Equation 1 in section 3. The first example of the failure mode of the Primary O-Ring Static/Dynamic compression failure mode is worked out below.

$RPN(a_i) = Min [Max \{ Neg (I(g_i)), g_j(a_i) \}]$

$RPN = Min \{ Max [Neg(L_{10}),L_{10})], Max [Neg(L_8),L_5)], Max [Neg(L_6),(L_{10})]\}$

The Negation of a Level is found by using Equation 2 in section 3.

$RPN = Min \{ Max [L_1,L_{10}], Max [L_3,L_5], Max [L_5,L_{10}]\}$

$RPN = Min \{L_{10}, L_5, L_{10}\}$

$RPN = L_5$

The other modified RPN numbers are found in the same manor, which allows the most severe risks to be identified. Once the risks have been identified in the Criticality Analysis, work on mitigating the most severe can begin immediately. The Criticality Analysis is linked to the FMEA which gives NASA systems engineers the needed oversight into and communication with contractors and sub-contractors. The oversight also can be used to create and modify the pre-flight checklist to include a temperature restriction for launch if a different O-Ring which performs better in cold weather is not found.

Table 5
Contractor Criticality Analysis of Sub-Components with Modified RPN

ID Number	Nomenclature	Function	Failure Modes and Causes	Mission/Phase	Severity	Occurrence	Detection	RPN	Remarks
C-123-1	Primary O-Ring	Seal SRB Junction	Static/Dynamic Compression causes O-Ring to fail to return to uncompressed state which inhibits proper sealing	Launch	10	5	10	L_5	Detail Gap tolerance for installation of Field Joints. Require Inspection to ensure tolerances are met
			Cold weather causes O-Ring to fail to return to uncompressed state which inhibits proper sealing	Launch	10	7	8	L_7	Re-design with O-Ring which performs better at Cold Temperature/ Limit launch GO to acceptable temperature for O-Ring functional range
			Ice unseats the Primary O-Ring which inhibits proper sealing	Launch	10	2	7	L_3	Re-design with O-Ring which performs better at Cold Temperature/ Limit launch GO to acceptable temperature for O-Ring functional range
C-123-2	Secondary O-Ring	Seal SRB Junction	Static/Dynamic Compression causes O-Ring to fail to return to uncompressed state which inhibits proper sealing	Launch	10	5	10	L_5	Detail Gap tolerance for installation of Field Joints. Require Inspection to ensure tolerances are met
			Cold weather causes O-Ring to fail to return to uncompressed state which inhibits proper sealing	Launch	10	7	8	L_7	Re-design with O-Ring which performs better at Cold Temperature/ Limit launch GO to acceptable temperature for O-Ring functional range
			Ice unseats the Primary O-Ring which inhibits proper sealing	Launch	10	4	7	L_4	Re-design with O-Ring which performs better at Cold Temperature/ Limit launch GO to acceptable temperature for O-Ring functional range
C-123-3	Tang-and-Clevis	Join SRB	Tang-and-Clevis connection break causing Field Joint to come apart	Launch	10	1	9	L_3	Write detailed Maintenance/Installation Manuals for SRB Body. Require Inspection of Tang-and-Clevis joints while being installed.
C-123-4	Zinc Chromate Putty	Isolate O-Rings from hot gases and enhance Seal of SRB	Zinc Chromate Putty causes O-Ring to fail to return to uncompressed state which inhibits proper sealing	Launch	10	2	10	L_3	Perform testing with Putty do determine effects on O-Rings at different temperatures. Require Inspection of application of Putty during installation.

5. Conclusion

System Quality Assurance and the tools which are available remain an important aspect of design. Each tool has its advantages and disadvantages. For Safety Critical components of Space Craft, using more than one tool allows to employ the strengths and mitigate the weaknesses. The top-down approach of a Fault Tree Analysis performed by NASA systems engineers, finds the Safety Critical components. These identified Safety Critical components and failure modes are then used to populate a FMEA. The FMEA is then distributed to contractors to perform a Criticality Analysis of the sub-

components. In this way, a FMECA is limited in scope by only being performed on the Safety Critical items. This top-down and bottom-up approach which meets together at the component level, also allows systems engineers the needed oversight and communication in order to ensure the design is acceptable and mitigation of risks is accomplished. Using the modified RPN number in assigning a Criticality, rather than the standard RPN number which only multiplies the three indexes together, also improves the information inherent in the RPN number. A hazardous failure mode which has a low likelihood to occur and easily detected will no longer appear to be a low risk by simple multiplication of the three indexes which uses a combined scale of 1 – 1000. The implication and limitation of this method are rooted in the use of RPN which does not satisfy the requirements of measurement. For future work, one may consider the use of type II fuzzy FMEA for safety critical components.

Acknowledgement

The authors would like to thank the anonymous referees for constructive comments on earlier version of this paper.

References

Bowles, J. B. (1998, January). The new SAE FMECA standard. In *Reliability and Maintainability Symposium, 1998. Proceedings., Annual* (pp. 48-53). IEEE.

Bozzano, M., & Villafiorita, A. (2010). *Design and safety assessment of critical systems*. CRC Press.

Buzzatto, J. L. (1999). Failure mode, effects and criticality analysis (FMECA) use in the Federal Aviation Administration (FAA) reusable launch vehicle (RLV) licensing process. In *Digital Avionics Systems Conference, 1999. Proceedings. 18th* (Vol. 2, pp. 7-A). IEEE.

Carmignani, G. (2009). An integrated structural framework to cost-based FMECA: The priority-cost FMECA. *Reliability Engineering & System Safety*, *94*(4), 861-871.

Chao, L. P., & Ishii, K. (2007). Design process error proofing: failure modes and effects analysis of the design process. *Journal of Mechanical Design*, *129*(5), 491-501.

Dahiru, A. T. (2014). A simplified methods of fast tracking FMECA using smart software tool: A case study. *International Journal of Current Research and Review*, *6*(13), 70-77.

Dale, C., & Anderson, T. (2009). *Safety-Critical Systems: Problems, Process and Practice: Proceedings of the Seventeenth Safety-Critical Systems Symposium Brighton, UK, 3-5 February 2009*. Springer Science & Business Media.

de Miguel, M. A., Fernandez, J., Pauly, B., & Person, T. (2005, February). Model-Based integration of safety analysis and reliable software development. In *Object-Oriented Real-Time Dependable Systems, 2005. WORDS 2005. 10th IEEE International Workshop on* (pp. 312-319). IEEE.

Franceschini, F., & Galetto, M. (2001). A new approach for evaluation of risk priorities of failure modes in FMEA. *International Journal of Production Research*, *39*(13), 2991-3002.

Goble, W. (2012). The FMEA method. *INTECH*, *59*(2), 14-16,18,20. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1008351257?accountid=27203

Haider, A. A., & Nadeem, A. (2013). A survey of safety analysis techniques for safety critical systems. *International Journal of Future Computer and Communication, 2*(2), 134-137. doi:10.7763/IJFCC.2013.V2.137

Illiashenko, O., & Babeshko, E. (2012). Choosing FMECA-based techniques and tools for safety analysis of critical systems. *Information & Security, 28*(2), 275-285. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1368133256?accountid=27203

Jenab, K., & Dhillon, B.S. (2005). Group-based failure effects analysis (GFEA). *International Journal of Reliability, Quality and Safety Engineering*, 12(4), 291-307.

Jianfeng, T., Shaoping, W., Yiping, Y., & Peiqiong, L. (1999, November). Reliability analysis on combination of FMECA and FTA for redundant actuator system. In *Digital Avionics Systems Conference, 1999. Proceedings. 18th* (Vol. 1, pp. 3-B). IEEE.

McKinney, B. T. (1991, January). FMECA, the right way. In *Reliability and Maintainability Symposium, 1991. Proceedings., Annual* (pp. 253-259). IEEE.

Rogers et al. (1986). Presidential Commission on the Space Shuttle Challenger Accident. Retrieved from http://history.nasa.gov/rogersrep/genindex.htm

Stålhane, T., & Wedde, K. J. (1998). Modification of safety critical systems: an assessment of three approaches. *Microprocessors and Microsystems*, *21*(10), 611-619.