Managing Safety Hazards for a Liquid Rocket Engine Test System

Vasilios J. Ekimogloy* , Lucian B. Stelk† and Luke Raque‡
University of Alabama in Huntsville, Huntsville, TN, 35899

Tartarus is a student research and development-focused liquid rocketry project, founded under the purview of the University of Alabama in Huntsville's Space Hardware Club. The goal of the project is to give undergraduate students hands-on experience with liquid propulsion and cryogenic fluid design to develop industry-related skills. In order to mitigate the risks associated with liquid propulsion systems (high pressurization, cryogenic temperatures, and oxidation hazards), a safety assurance system was modeled to track the condition of the test stand and its components. This process, after 2 years of development, utilizes a combination of component-level design failure modes and effects analysis (DFMEA) with a detailed risk analysis matrix to inform our design and processes. This information is then packaged into our Standard Operating Procedures, Test Safety Documents, and Test Incident Response Plan. A combination of all of these branches ensures the safety of members, furthering their liquid rocketry goals.

I. Nomenclature

$S_{Equipment}$	=	Equipment Severity Number
$S_{Severity}$	=	Severity Severity Number
$S_{Performance}$	=	Performance Severity Number

II. Introduction

The International Rocketry Engineering Competition has a total of 175 competitive teams for the 2026 competition cycle. One-hundred and sixty-three of those teams are using solid-based propulsion. Only twelve teams are using hybrids or liquids. Liquid propulsion, while offering higher specific impulse, greater reusability, and throttleable engine fires [1], is inherently more dangerous and significantly more complex for any student team daring enough to pursue it. Tartarus is a student-led liquid rocketry project part of the University of Alabama in Huntsville's Space Hardware Club. We are in our first phase, developing a reusable test stand, creating a command and control system, and testing our engine analysis using a liquid oxygen (LOx) and ethanol verification engine. During this crucial development phase, Tartarus has developed a full-scale safety and hazard analysis pipeline to ensure member safety and mitigate the hazards that come with the challenge of developing liquid propulsion. The tools we use include: Risk Assessment Matrix, Design Failure Modes and Effects Analysis, Hazard Identification Study, and Standard Operating Procedure. The combination of all of these tools serves as the basis for member safety and are separated into two categories: System and Process. These two are connected through our standard process, Fig. 1, which is the focus of this paper.

III. System Safety Analysis

A. Hazard Identification

In order to mitigate and understand the hazards that could be present in the system, we first had to identify all potential hazards within the system itself. Based upon [2] and [3] we identified 36 relevant potential hazards separated into 7 different categories: pressure, fire, cryogenic, explosion, chemical, personnel, physical/mechanical,environmental,

*Undergraduate, Mechanical and Aerospace Dept, vekimogl@uah.edu, AIAA University Student Member, 1823356.
†Undergraduate, Mechanical and Aerospace Dept, ljs0027@uah.edu, AIAA University Student Member, 1604671.
‡Undergraduate, Mechanical and Aerospace Dept, lrr0011@uah.edu, AIAA University Student Member, 1604908.

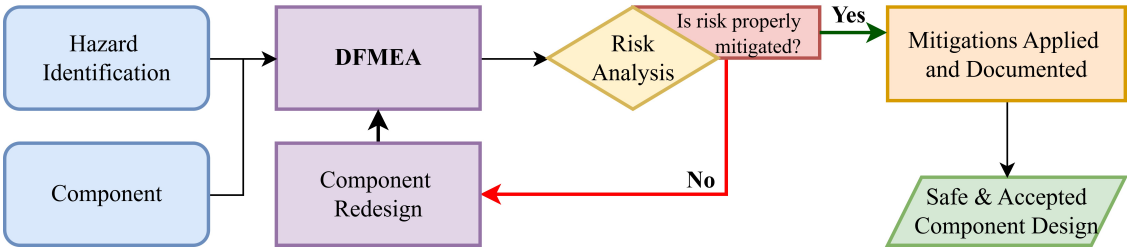


Fig. 1 Tartarus Safety Process Flowchart.

Table 2 Risk Priority Matrix.

Severity → Probability ↓	Low (1)	Medium (2)	High (3)
Low (1)	1	2	3
Medium (2)	2	4	6
High (3)	3	6	9

and electrical. This list is dynamic and has both hazards and their definitions which changes as new potential hazards are found either by advisement, industry, or other student teams. The hazards go on to form the basis for failure mode identification and their effects on the overall system.

B. Risk Priority Number

The most ambiguous portion of risk analysis is the determination of how to convert the qualitative aspects of a system's state, risks, and hazards into a quantifiable metric for the safety of a system. To accomplish this, Tartarus utilizes a variation on the Revised RPN. Our variation is dependent on two factors, the Probability and Severity, each ranging from 1 to 3. They make up the risk priority matrix shown in Table 2 leading to RPN values of 1-9. The calculation of the RPN is found from multiplying the highest severity of a failure by its probability, shown in Eq. 1. Acceptable RPNs are 1-2. RPNs of 3-4 require mitigation and a high RPN rationale, which will be defined later, and RPNs of 6 or greater are not permitted and must be mitigated further before declaring the part safe. This is notably different from the traditional calculation of RPN [4], which has 3 parameters and which scale from 1-10, giving a final RPN range of 1-1000. The reason for the reduction is threefold: limited failure rate data, limited personnel, and high turnover rate.

$$RPN = \max(S_{Performance}, S_{Eqipment}, S_{Personnel}) \cdot P_{Probability} \tag{1}$$

The ability of a student team, given the lack of failure rate information, to determine accurate probabilities regarding the potential of failure for a component is limited. In order to avoid the effects of imprecise probabilities from perpetuating through the design of the test stand, the probability is defined qualitatively. A 1 is defined as something having a low likelihood of failure. This is generally only applied to COTS components within the system, particularly when they do not have any human factors relating to their failure. A 2 is given to any component that has a human factor with a given process or design mitigation. This component may not be a COTS component; however, it must be coupled with analysis or testing for a layer of verification. A 3 is applied to any component that is both manufactured in-house and does not currently have any testing to verify its analysis. The severity is separated into three categories: Performance, Equipment, and Personnel. Their descriptions are outlined in Tables 3, 4, and 5.

C. Design Failure Modes and Effects Analysis

As a student team, we have a limited number of members able to contribute to the safety analysis of the system. We find it therefore necessary to apply tools which allow for focus on the component level failures of the system. While designing a system for 2-fault or even single-fault tolerance is not logical [5], we decided that a focus on the design was critical in order to develop greater understandings of the failure modes of the system. In order to do this, we

Table 3 Performance Risk Severity Definitions.

Description	Severity Score
Event may result in virtually no impact or major change in schedule or mission goals. Parts may be replaced quickly by components on hand, or require minimal personnel interaction to repair.	1
Event may result in noticeable delay or shift of schedule, and difficulty in meeting testing goals. Event causes overall testing goals to be reassessed however still may be completed after adjustment.	2
Event may result in significant delays possible cancellation of the current test. This will result in a new test date being selected and new pre-test process to occur.	3

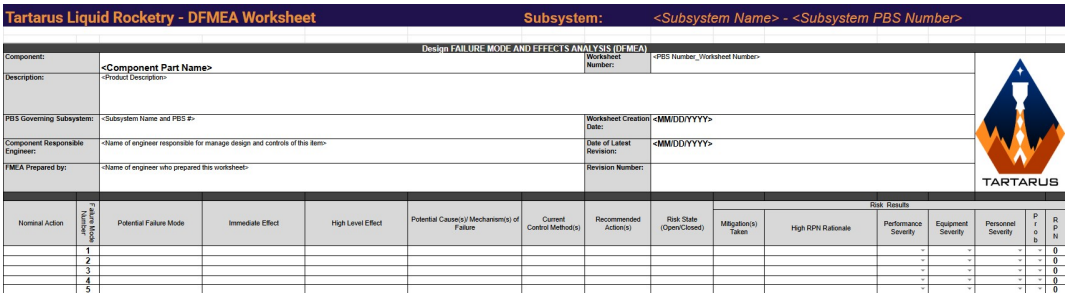
Table 4 Equipment Risk Severity Definitions.

Description	Severity Score
Event may result in no damage to any test stand equipment.	1
Event may result in the damage of minor test stand equipment which is able to be fixed within time frame of test.	2
Event may result in damage which is unable to be repaired within the time frame of the test or results in damage to a critical component.$250.	3

Table 5 Personnel Risk Severity Definition.

Description	Severity Score
Event may result in no harm or distress to any operators. Any required actions taken will not put operators in undocumented and mitigated hazards.	1
Event may result cause distress to operators, and require action not explicitly covered by the test packet.	2
Event may result in injury of any kind to operators.	3

created a modified DFMEA which aligns itself with our definitions of risk and our RPN calculations. Figure 2 depicts the DMFEA template, which is split into the following sections: Nominal Action, Failure Mode Number, Potential Failure Mode, Immediate Effect, High Level Effect, Potential Causes/Mechanism of Failure, Current Control Methods, Recommended Actions, Risk State, Mitigations Taken, High RPN Rationale, Performance Severity, Equipment Severity, Personnel Severity, Probability, and RPN.



Tartarus Liquid Rocketry - DFMEA Worksheet				Subsystem:	<Subsystem Name> - <Subsystem PBS Number>											
Design FAILURE MODE AND EFFECTS ANALYSIS (DFMEA)																
Component:	<Component Part Name>				Worksheet Number:	<PBS Number_Worksheet Number>										
Description:	<Product Description>															
PBS Governing Subsystem:	<Subsystem Name and PBS #>				Worksheet Creation Date:	<MM/DD/YYYY>										
Component Responsible Engineer:	<Name of engineer responsible for manage design and controls of this item>				Date of Latest Revision:	<MM/DD/YYYY>										
FMEA Prepared by:	<Name of engineer who prepared this worksheet>				Revision Number:											
												Risk Results				
Nominal Action	Failure Mode Number	Potential Failure Mode	Immediate Effect	High Level Effect	Potential Cause(s)/ Mechanism(s) of Failure	Current Control Method(s)	Recommended Action(s)	Risk State (Open/Closed)	Mitigation(s) Taken	High RPN Rationale	Performance Severity	Equipment Severity	Personnel Severity	Prob	RPN
	1										-	-	-	-	0
	2										-	-	-	-	0
	3										-	-	-	-	0
	4										-	-	-	-	0
	5										-	-	-	-	0

Fig. 2 Tartarus DFMEA Template.

Our process of DFMEA begins with a nominal action, which is what the part or system being analyzed is supposed to do. Then, a potential failure mode, as in any possible failure state of the component, is listed along with its immediate effect on the system, which is the physical result as an effect of the failure within the current subsystem. After this, the ultimate outcome of the possible failure, referred to as the high level effect, is examined, along with any reason the failure could have occurred. With this, the current control method for such an error is documented, along with any risk mitigation measures to be taken if needed. The design mitigations built into the system to help prevent or lessen a failure, which is known as the current control methods, are listed alongside the recommended actions. The severity of the effect on performance, personnel, and equipment is given a number from one to three, with one being the least and three being the greatest, along with the probability of such a case occurring. The case is assigned a RPN, obtained from the Risk Priority Matrix in Table. 2. As stated previously, if the RPN is 6 or higher, the risk event is too high and the component must go through component or subsystem redesign until it has reach an appropriate an acceptable RPN. Once the DFMEA is completed, the responsible engineering for the subsystem reviews the DFMEA and any high failure modes to ensure any needed mitigation steps are taken. Once fully reviewed, the risk state, whether or not the component has been deemed safe or has necessary mitigation steps taken, is closed and the DFMEA is fully finished.

Any and all components which are unable to mitigated below and RPN of 3 or 4, must be given a high RPN rationale. A high RPN rationale is a description and acknowledgment that a part is unable to be specifically further mitigated, however, is necessary in the current system. This rationale must be confirmed by the Chief Engineer for the project, the Responsible Engineer for the subsystem, the member compiling the DFMEA, and the current Range Safety Officer for testing. This component then gets permanently added to the Critical Items List (CIL) as an important potential hazard for all future tests. Through this method, the team has a list of the critical items within the system during testing.

IV. Process Safety Analysis

A. Testing Packet

Once a component has been mitigate as far as possible through system analysis means, there is often a list of procedural mitigations that were considered for the assignment of a components RPN. These process mitigations are complied together to serve as the basis for the creation of our testing packet. Our testing packets serve as the comprehensive guide for any given test using the equipment on the test stand. Testing packets include a Testing Requirements Document, a testing Safety and Hazard Report, an Operator Assignment and Description, SOP, Post-Test Procedure, and Appendix.

The Testing Requirements Document is the outline of all requirements, expectations, and desired outcomes for a given test. All requirements and the source of derivation of those requirements must be included with appropriate citations if referencing existing standards, for example the "ASME B31.3 Process Piping Guide" as a reference for hydrostatic testing. This document also must include the success and failure criteria for the test. This is done to help eliminate possible ambiguity during the testing procedure creation or application. The second section of the test packet

is the Safety and Hazard Report. This section covers the hazards associated with the test with their descriptions, as well as mitigations taken to bring the hazard into acceptable bounds. The safety procedure requirements are also in this section including required PPE for all operators. Additionally, the color delineated hazard levels for the test are explained and described. General color assignments are green for all clear, yellow for operators only, blue for cryogenic hazard, and red for no personnel. These are subject to change from test to test and are paired with descriptions and rationale for the test's color system.

B. Operator Assessment

Every test has different roles required to complete that test, and their responsibilities may not transfer exactly from one test to another. The Operator Assignment and Description describes potential roles for all personnel who may be present at a test. All tests are required to have a Test Coordinator, Test Lead, and Range Safety Officer (RSO) of record. Their responsibilities are the same from test to test as they are jointly in charge of test procedure. All other operator roles are described with reference to the specific test, including the number of potential operators, requirements including necessary certifications, and duties. Operator assignments must be made a minimum of 1 week prior to a test itself and alternate operators must be listed as well. If operators are to be changed all listed operators must be updated wit the date of assignment. All personnel at a test unless otherwise specified is considered to be an observer. Whether or not observers are permitted to attend a test is dependent on the test article itself and is up to the discretion of the Test Coordinator, Test Lead, and RSO. As their are some hazards which are unavoidable, all operators have a specified hazard level which is specified in their role description. For full-scales tests, operators are required to pass a Testing Hazard Exam written the by RSO and Chief Engineer for the project which covers the hazards present in the test, and their operator role's relation to that hazard. Operators will only be exposed to hazards given the appropriate PPE, prior knowledge regarding the occurrence, familiarity with the system, and the approval of the RSO.

C. Standard Operating Procedure

The SOP is the incremental procedure guide for the actionable items within a test. It describes all actions taken by operators separated into the following sections: Testing Diagram, Procedure Overview, Pre-Test Preparation, and Test Procedure. The testing diagram is the diagram of the system or subsystem which houses the test article. If applicable, it should be either a P&ID or photograph of the test article to serve as a reference for operators during testing. Additionally, it provides information regarding which components of the test article present possible hazards visually using the test color system established in the Safety and Hazard Report. The Procedure Overview is a short description of the testing procedure and reiterates the Testing Requirements Document for operators. The Pre-Test Preparation outlines all required actions required for testing to begin. This includes final environmental checklists, required PPE verification, calibration and commissioning, setting safety radii, and any other process required to mitigate the hazards of the system prior to beginning official testing. The Test Procedure is an ordered list of all the required steps and who completes them to get from the beginning to the end of the test. It is a color coordinated list with plain test actions and a verification section which must be checked off RSO which also contains the safety level of the test article. The sample shown in Fig. 3 shows the main test procedure for our second igniter test.

D. Post-Test Documents

After a test, it important to make sure all traces of the test are gone, both to avoid any potential environmental impact as well as to prevent leaving anything behind at a test site. That is why at the end of the packet there is a the Post-Test Procedure which outlines all required items which must be accounted for at departure and instructions on how to efficiently pack these items. There is also a Discrepancy Report which gives the Test Lead the opportunity to comment on the proceedings of the test and mention any issues with test procedure which need to be discussed or improved for future tests. The end of the packet also has the Emergency Contact Sheet which has the contact information for local and university authorities in the case of an incident. This includes the emergency and non-emergency numbers for local authorities, the contact of the faculty advisor, the Project Lead, the head of the Office of Environmental Health and Safety, and the nearest Hospital to the testing location. In the event something does happen, the Test Coordinator, Test Lead, and RSO are required to fill out the internal Incident Report document outlining information regarding the incident, causes of the incident, effects of the incident and preventative measures which need to be applied for future tests. The Appendix consists of the CIL, the P&ID for the test stand, overview schematic for the command, control, and instrumentation system, and relevant DFMEAs for the test.

Test Procedure				
	1	Stand Operator	Set hydrostat pump to fluid setting	
	2	Stand Operator	Wait until water begins to flow out of all openings in the tubing assmebly	
	3	Stand Operator	Begin attaching end caps onto tubes in assembly until all tubing in the system is closed off from atmosphere	
	4	Stand Operator	Set hydrostat pump to compressor setting and pump to 1500 psi, and record final pressure	
	5	Stand Operator	Turn compressor pump off	
	6	Stand Operator	Check the assembly for any leaks in the system (for leaks check fail procedure)	

Fig. 3 Section of Testing Procedure for Second Igniter Test.

V. Conclusion

Over the course of developing our safety analysis system and methodology, Tartarus has identified 36 potential end effect hazards, completed 131 component level DFMEAs and completed secondary verification on 66, wrote and utilized three testing packets, and induced 13 design changes to mitigate testing hazards. Going forward, the team hopes to solidify the RPN formulation to more accurately define what it means to a student team, continue writing testing packets for our upcoming test stand verification, wet-dress, and hot-fires tests, and complete secondary verification on all 192 components in the system. Despite the present dangers inherent in liquid rocketry at the collegiate level, Tartarus will continue its commitment to making it more accessible and safe for all.

Acknowledgments

The authors would first and foremost like to thank Dr. Gang Wang and Dr. Richard Tantaris for their mentorship to The University of Alabama in Huntsville's Space Hardware Club. We would also like to thank Mr. Lorenzo Coley for representing AIAA at The University of Alabama in Huntsville. We are also very grateful to the MAE department at UAH and Mr. Jon Buckley in particular for the use of their machine shop, and mentoring in manufacturing techniques. The Alabama Space Grant Consortium and the University of Alabama in Huntsville have graciously given us the resources necessary to fund this project through the Space Hardware Club. Thank you especially to AVCO for giving insightful technical feedback and providing cryogenic valves for the Modular Fluids System. Thank you to Swagelok for their generous donation and as well to MiTiGen for their in-kind contribution and support. Finally, we would like to thank all members of Tartarus for their continued support and dedication to the project.

References

[1] Sutton, O., George P.and Biblarz, *Rocket Propulsion Elements*, John Wiley and Sons, Inc., 2013.

[2] Carter, G. T. and Others, "Liquid propellants safety handbook," Tech. Rep. NASA-TM-X-56611, NASA John F. Kennedy Space Center, Cocoa Beach, FL, 1965. URL https://ntrs.nasa.gov/api/citations/19650018358/downloads/19650018358.

[3] The JANNAF Hazards Working Group, "Chemical Rocket/Propelland Hazards Volume 1 general safety engineering design criteria," Tech. rep., Joint Army Navy NASA Air Force (JANNAF) Interagency Propulsion Committee, Silver Spring, Maryland, 1971. URL https://apps.dtic.mil/sti/tr/pdf/AD0889763.

[4] Kim, K. O., and Zuo, M. J., "General model for the risk priority number in failure mode and effects analysis," *Reliability*

Engineering and System Safety, Vol. 169, 2018, pp. 321–329. https://doi.org/https://doi.org/10.1016/j.ress.2017.09.010, URL https://www.sciencedirect.com/science/article/pii/S0951832017302235.

[5] Air Force Research Lab Edwards AFB CA Propulsion Directorate, "Test and Evaluation Guideline for Liquid Rocket Engines," Tech. rep., Joint Army Navy NASA Air Force (JANNAF) Interagency Propulsion Committee, Huntsville, AL, 2010. URL https://apps.dtic.mil/sti/tr/pdf/ADA554916, work in progress; draft for submittal to the propulsion community.