Managing Safety Hazards In The Preliminary Design Phase of a Student-Lead Liquid Rocketry Program

Michael Johns[1]
University of Alabama in Huntsville, Huntsville, Alabama, 35805, USA

Tartarus is a student research and development liquid rocketry project, founded under the purview of the Space Hardware Club at University of Alabama in Huntsville. The aim of this project is to provide undergraduate students an experience with real hands-on liquid propulsion development and evaluation in order to build valuable industry-related skills. This paper will outline how Tartarus has been planning to mitigate potential risks, and outline how safety is approached on Tartarus. Due to the inherent risks associated with operating liquid rocketry test equipment, stringent safety planning and procedure is of utmost importance, and must be considered heavily in the preliminary design phase. Tartarus has implemented various methods of ensuring safe design and operation of equipment. A major challenge, and often a point of failure, is identifying well in advance risk conditions and where they can come from. Another important factor of managing safety is planning risk mitigation, and ensuring design and operational requirements conform to allotted safety parameters. Identifying where risks can come from before constructing or procuring hardware is a major challenge that Tartarus is working to mitigate. A major asset to management is the use of safety analysis tools, one of which is a risk analysis matrix. A risk analysis matrix numerically quantifies the severity and probability of a risk condition outcome, and can be used to determine to what extent mitigation is necessary. Tartarus uses this risk analysis matrix to drive selection of preliminary design requirements. Laying out risk conditions in this manner allows for an objective analysis of what measures must be taken in terms of design as early as possible in the design process. This approach helps reduce the probability and severity of risks.

I. Introduction

Tartarus is a student research and developed liquid rocketry project, with the aim of giving undergraduate students propulsion experience. The immediate scope of this project is to build a fully integrated and reusable mobile test stand system, and a low-power demonstration liquid oxygen / ethanol rocket engine. This paper is intended to outline the safety and mission assurance that is conducted in order to ensure that Tartarus is capable of meeting goals safely and efficiently. This project utilizes industry standard S&MA tools, such as risk analysis, in the preliminary design stage development. This approach allows for safety to be of the utmost importance, ingraining safety requirements into the most early stage of design. This means that from the ground up, safety is at the forefront of the mission. Liquid rocketry development entails a significant amount of risk, and because of this safety needs to be prioritized. A major tool that Tartarus has employed is the process of risk analysis. This process allows the team to identify all potential high-level risks the mission may encounter, and in turn use this information to create mitigation plans. By identifying what mitigation plans are necessary to reduce risks, this can be used as a basis to create preliminary design requirements.

[1] Undergraduate, Mechanical and Aerospace Engineering Dept, mjj0027@uah.edu, Student Member, 1424694.

II. Scope of The Tartarus Project

The goal of the Tartarus project is to give undergraduate students hands-on experience in liquid rocket propulsion development and testing. Tartarus was founded in 2016, with the initial goal of competing at Spaceport America Cup in the SRAD liquid division. The team had originally planned to build a fully integrated vehicle, with a 800 lb-f Nitrous Oxide / Ethane bipropellant engine, with the goal of a 30,000ft apogee. At the start of 2023, Tartarus attempted a final TRR (Test Readiness Review) prior to the team's first hotfire. This TRR identified major weaknesses in the design and firing regime of this engine, with many of these issues failing to be noticed in preliminary / critical design reviews. Because of this, we decided to have a full change of scope for the project.

The new scope of Tartarus conforms the team to resemble propulsion research and development, as opposed to competition. This new scope consists of three primary phases the project will operate in. Phase 1 is the first and current scope phase the project will operate in. This phase requires that the team is able to construct a safe and reusable mobile rocket engine test stand. Tartarus also conducts in-house rocket engine performance modeling, and the empirical validation of this model is another component of this phase. This phase intends to lay the foundation for continued engine development both in technical knowledge and in testing hardware. In order to meet these requirements, a fully integrated mobile test stand, named Hades, will be developed as a recursive testbed for a future multitude of different rocket engines. In addition to this test stand, a relatively simple and low thrust rocket engine, named Prometheus, will be developed as a demonstration engine that can validate our propulsion model as well as the MTS. Phase 1 will be concluded when the team has conducted a steady-state hotfire of this engine, collecting enough data to validate our propulsion model, and safely demonstrating the usability of our Mobile Test Stand.

Phase 2 is the second phase of the project, intended to be the constant operational phase of the project. After the completion of phase 1, the team will shift into phase 2 operations. Phase 2 is the constant development and testing of rocket engines. This phase has no planned offramp, continuing indefinitely with the goal of testing a multitude of different engines with various requirements and characteristics.

Phase 3 is intended to be an operational phase that works as a split branch from phase 2. Phase 3 is the section allotted for vehicle flight engine development. This phase is wholly dependent on the high power rocketry capability of the rest of the Space Hardware Club.

III. Defining Risk Analysis

A. Purpose of Conducting Risk Analysis

Risk analysis is a tool that is implemented in order to effectively define potential risks, what these risks come from, and how they can impact the project. Risk assessment is the specific process of quantifying these risks based on several defined metrics. This system can help identify risks

B. Defining A Risk

For the purposes of Tartarus, a risk is identified as an event that can cause deviation from expected mission requirements, or pose some form of safety hazard. There are a multitude of ways to generate and identify potential risks. Brainstorming is the process of researching and coming up with risk conditions based on what the goals of the mission are. Preliminary testing can also be used to identify potential risks, testing hardware before integration and reveal potential risks or failure modes that had been previously unseen. This is why consistently conducting risk analysis is critical to ensuring safety. The final method that can be used to identify risks is prior experience and lessons learned from previous attempts. This method is used heavily on Tartarus, this is because of the change of scope. Extensive documentation of the functionality and failures of a previous system has given the team a large repository of generational knowledge that can be used in identifying risks. [1]

C. Risk Assessment Matrix

A Risk Assessment Matrix is a tool used in risk analysis that can numerically quantify characteristics of different risks that may appear within the project. A risk matrix compares two major characteristics of a risk. These characteristics are the probability of the risk occurring, and the severity of the outcome of the risk. Probability is defined on a relative scale and in the preliminary phase is based on empirical history of probability, or a qualitative analysis. The severity is the metric based on the consequences on the outcome of the risk. These are split into multiple different categories, with each step of severity having a definition unique to the scope of this project.

Probability is defined as the likelihood of a risk condition generating consequences. [1] Due to Tartarus currently operating in the preliminary design phase of the project, the probability is a relative qualitative scale. This scale ranges from 1 to 5, going from lowest to highest probability. These probability characteristics are listed in order in Table 1.

Table 1 - Risk Probability Chart

Probability	
5	**Near Certain**
4	**Very Likely**
3	**Likely**
2	**Unlikely**
1	**Remote**

Severity is defined as the measurable impact of the consequences that follow a risk event [1]. The severity ranges from 1 to 5, going from least to most severe impact. This impact can happen in a number of different modes, affecting the mission performance, equipment, or personnel. The "designation" is the classification used to numerically quantify the level of severity.

In the preliminary design phase of Tartarus, the severity analysis of risks is still at the high qualitative level. The performance category deals with the mission timeline and requirements. A severity score in this category is referential of the magnitude of the deviation from a scheduled timeline, or inability to meet set requirements. The equipment category deals with physical loss, damage, or destruction of test hardware and equipment. A severity score in this category is referential to the severity of the damage / loss of physical equipment. The personnel category deals with any physical harm or damage dealt on human operators / observers. A severity score in this category is referential to the severity of harm dealt onto personnel. The specific severity case statement is shown in Table 2.

Table 2 - Risk Severity Chart

Severity				
Designation		**Performance**	**Equipment**	**Personnel**
5	Catastrophic	Severe loss of schedule, primary level requirements not able to be met	Major destruction or loss of system	Dismemberment of personnel or possible fatality
4	Critical	Major timeline slip, one or more second level requirements cannot be met	Major consequence, substantial damage to system	Severe personnel injury, onsite treatment not sufficient
3	Serious	Moderate setback, possible to not meet low level objectives	Moderate consequence, repairable damage to system	Possibility of personnel injury, on site first aid may be required
2	Minor	Minor setback, less than 1 week timeline shift	Minor consequence	Minor consequence

1	Negligible	Minimal Consequence	Minimal Consequence	Minimal Consequence

After being assigned a numerical value, risks are then evaluated using a risk assessment matrix. This model of a 5 x 5 probability / severity matrix is standard in industry risk analysis [1]. A risk assessment matrix assigns a single numerical value that the risk can be evaluated against. This "assessment score" is calculated with the product of severity and probability score:

$$Probability * Severity = Assessment\ Score \tag{1}$$

The computed number will fall somewhere on the risk assessment matrix. There are 3 main ranges that a risk can fall into, notated by color code in the matrix. The green range is the "accepted" range. Computed assessment scores under 5 fall into this category, meaning that the risk has a low enough probability or severity that no mitigation measures need to take place. The second, yellow, range is the "watch" category. Computed assessment scores greater than 4 and less than 10 fall into this range. A risk placed under "watch" means that the severity / probability of its consequences are still tolerable, however further research shall be conducted in an attempt to lower its score if possible and within reason. The final, red, range is the "mitigate" category. Computed assessment scores above 9 fall into this category. Any risk placed in this category is required to have a mitigation strategy bringing it into a more tolerable score. The risk matrix created by Tartarus is shown in Fig. 1

Fig. 1 - Risk Assessment Matrix

Risk Assessment Matrix					
Severity / Probability	5 (Catastrophic)	4 (Critical)	3 (Serious)	2 (Minor)	1 (Negligible)
(5) Near Certain	25	20	15	10	5
(4) Very Likely	20	16	12	8	4
(3) Likely	15	12	9	6	3
(2) Unlikely	10	8	6	4	2
(1) Remote	5	4	3	2	1

Mitigate Watch Accept

The main difference in the Tartarus risk assessment matrix is more stringent guidelines on what is a totally acceptable risk. Due to the potentially hazardous environments surrounding liquid rocketry test equipment, we decided to increase the stringency of our risk scores in order to ensure that proper mitigation plans are put into effect.

In order to get more precise risk analysis scores that can help better develop a mitigation strategy, each identified risk is given 3 assessment scores. These assessment scores correspond to each severity category identified, with each category getting its own score based on qualitative assessment. The organization of these scores is noted in Table 3.

Table 3 - Categorical Assessment Scores

Performance	Equipment	Personnel
Prob. x Severity Assessment	Prob. x Severity Assessment	Prob. x Severity Assessment

D. Risk Mitigation

The purpose of the risk assessment matrix is to assign a quantitatively determined, yet still numerically defined value, that can be used to identify and form a proper mitigation plan. The goal of risk mitigation is to either reduce the probability of a risk condition, or reduce the severity of the consequences. Mitigations are actions or design decisions made that can reduce the assessment score. Risks are analyzed before and after mitigation in order to record the effectiveness of a planned mitigation, and determine if more mitigation actions are required to be implemented. For the purposes of Tartarus, proper mitigations are determined during the preliminary design phase. This means that planned mitigations are used as defining design requirements. This method allows for risk management to be a foundational requirement for all system design.

E. Risk Analysis Conclusion

After applying the risk assessment method to all identified high level preliminary design risks, a finalized overview of all risks can be generated. Assessment scores are evaluated again after mitigation requirements have been set, and from here a "Total Risk Rating" (labeled "Rating" in Table 4) can be given to each risk. This number is a relative value, used to rank the importance of a risk compared to other identified risks. We were able to identify 11 high level risks we could expect to see in our Mobile Test Stand and Prometheus engine operating environments. These risks were identified in the PDR and have been used to set design requirements for their respective subsystems. The overview of these risks can be seen in Table 4.

Table 4 - PDR Risk Analysis Overview

Risk Analysis Overview			
Risk	**Rating**	**Primary Mitigation Method**	**Conclusion**
Frozen Components	14	Reduce Probability and severity	Accepted
Engine Hard Start	13	Reduce Probability	Accepted
Oxide Fire	12	Reduce Probability	Accepted
Fuel Fire	12	Reduce Probability	Accepted
Loss of Test Data	12	Reduce Probability	Under Watch
Test Stand Structural Failure	11	Reduce Probability	Accepted
BLEVE Event	10	Reduce Probability and severity	Accepted
Overpressure Event	10	Reduce Probability and Severity	Accepted
LOx/LN2 Spill	9	Reduce Probability and Severity	Accepted
Control System Failure	9	Reduce Severity	Accepted
Failure to Start Engine	9	Reduce Probability	Under Watch

IV. Example Case

Tartarus has employed this modified version of industry standard risk analysis during the preliminary design phase of the project. We had conducted this risk analysis for a Preliminary Design Review, as well as a way to set system design requirements. This section will detail an example case taken from our PDR to illustrate our method.

A. Identification of A Risk - BLEVE Event

A potential risk identified was a BLEVE (Boiling liquid expanding vapor explosion) event, a risk common in cryogenic equipment. In order to properly identify a risk, a set of conditions and outcomes must be defined. For this risk, we determined that accidental trapped and unvented volumes of cryogenic fluid, as well as the absence of proper system ventilation, were the main conditions that could cause this risk to have consequences. The outcomes of this risk were identified to be: explosion of the MTS fluid system, damage to the MTS, engine, or control system, and injury of test personnel during cryogenic loading operations.

B. Pre-mitigation risk assessment

Once risk conditions and outcomes have been identified, the risk can be assessed according to each severity category. Table 5 shows the calculated assessment scores of this risk before mitigation

Table 5 - BLEVE Risk Pre-Mitigation Assessment Scores

Before Mitigation		
Performance	Equipment	Personnel
4x5 20	5x5 25	3x5 15

These pre-mitigation assessment scores all fall into the red “Mitigate” zone of the risk assessment matrix, meaning that a mitigation plan is required in order to guide a design that is within acceptable risk.

C. Mitigated Risk Assessment

After identifying that the risk needs to be mitigated, a list of requirements are generated that guide design and operation of the system to an acceptable risk level. Table 6 shows the assessment scores after mitigation

Table 6 - BLEVE Risk Post-Mitigation Assessment Scores

After Mitigation		
Performance	Equipment	Personnel
2x2 4	1x3 3	1x3 3

After mitigation, all assessment scores fall into the green “Acceptable” zone of the risk assessment matrix, meaning that the mitigation plan will likely ensure that the risk is acceptable under the guide of generated requirements. After research and internal analysis, a basic list of design requirements were generated as a mitigation plan for this risk. These design requirements include: use of vented cryogenic valves, passive overpressure prevention (burst disks), automated software aborts, and the conceptual requirement of removing the possibility of accidental trapped volumes. These requirements primarily reduce the likelihood of a BLEVE event occurring, and partially reduce the severity of the outcome.

V. Tartarus Safety Plans

Liquid rocketry research and development has a host of inherent risks and dangers associated with even nominal operation of testing equipment. Because of this, safety is always the number one consideration for this project. Because of this, Tartarus has conducted a significant amount of safety planning just in the preliminary design stage of Phase 1. In order to ensure that safety is properly considered throughout the project, Tartarus employs internal Safety and Mission Assurance guidelines. These guidelines set design requirements, test operating environments, and safety analysis.

A. Safety and Mission Assurance

Safety and mission assurance ensures that The organization of team safety and mission assurance goals falls under the purview of the project’s Chief Engineer. The Chief Engineer is responsible for ensuring that the team is

always operating under proper safety guidelines. In order to ensure this, the employment of industry standard tools are used to manage this. These tools include Risk Analysis, Standard Operating Procedures, and Failure Mode & Effects Analysis. The Chief Engineer is responsible for consistently conducting internal design audits to ensure that these designs meet the design requirements set by these safety analysis tools.

B. Safety During Testing

A large portion of Tartarus' development lies in conducting a multitude of tests. The purpose of conducting these tests is to subject components to hotfire conditions while being isolated from the full system, and testing one characteristic at a time. This allows for empirical validation of the safe operation of subsystems prior to a final hotfire. To manage risks during pre-hotfire testing, tests are broken down into two main categories: low-level and high-level tests.

Low-level tests are defined by tests that operate in a relatively low-risk environment with minimal complexity. The formal definitions are: test conducted at ≤100 PSIG (standard component muscle pressure), no hazardous materials involved, no extreme temperature / cryogenic conditions, relatively low complexity. In order to ensure that these tests serve a meaningful purpose, and are still organized and operate safely, low level tests have required documents that must be made for the test. These documents include: basic written up test procedure, defined test goal and requirements list, and expected results.

High-level tests are defined as tests that operate in a high-risk environment and have a high complexity. The formal definition of high-level test conditions are: ≥100 PSIG inside the system, hazardous, flammable, or cryogenic materials, and high complexity. In order to ensure that high-level tests are conducted safely and successfully, there are significantly more stringent requirements for these tests. In addition to all the requirements needed for a low-level test, a high-level test must also have: fully detailed standard operating procedure, component failure modes and effects analysis chart, and have to conduct a TRR (Test Readiness Review) with the approval of the Space Hardware Club officer board and University Faculty Advisor.

VI. Conclusion

Liquid rocket research and development is a field of work that poses a multitude of inherent risks and failure potentials. Because of this, safety is an incredibly important factor that must be incorporated into design and procedure as early as possible in the project life cycle. Tartarus is currently in the preliminary to critical design stage of project development. This stage is critical for defining and implementing adequate safety measures, and requires tools to ensure that it can be done accurately. One of the main tools Tartarus has used to define design requirements is Risk analysis. This process identifies potential risks, what causes them, and their impact, which means that a mitigation plan can be developed which will drive design requirements. Tartarus uses Safety and Mission Assurance strategies to ensure that all stages of the project are operating safely and within requirements. The adaptation of industry standard tools to a collegiate amateur rocketry environment has proven to be beneficial in organizing and planning ahead for the safety of the team.

Acknowledgments

The author thanks the Alabama Space Grant Consortium for continual support of the Tartarus team and Space Hardware Club. The support from ASGC has allowed for this team to operate and continue the mission of hands-on student learning. The author would like to thank Blue Origin for sponsoring the team in 2024 allowing continued development of the project. The author thanks the University of Alabama in Huntsville's Faculty Advisor, Dr. Gang Wang for mentorship, as well as various industry professionals who have provided support and feedback, including Mr. Jim Turner, Mr. Pravin Aggarwal, Dr. David Lineberry, Mr. Scott Claflin, and Mr. Preston Jones.

References

[1] Costello, Kenneth "S3001: Guidelines for Risk Management" ,[NASA], URL: **https://www.nasa.gov/wp-content/uploads/2015/10/s3001_guidelines_for_risk_management_-_ver_g_-_10-25-2017.pdf** [retrieved 24 Feb. 2024]