Risk Informed Design Modeling Process & Design Team – Analyst Interaction

Chris Mattenberger, Valador, Inc.

Key Words: risk informed design, probabilistic risk assessment, Altair lunar lander, risk management

SUMMARY & CONCLUSIONS

As demand for highly reliable complex systems increases, engineers are being forced to consider the risk implications of design decisions earlier in the conceptual phase of projects and with greater accuracy. Standard probabilistic risk assessments (PRA) usually employed to verify that a product meets requirements are too resource intensive and too slow to keep up with the speed at which the design is maturing; while classical qualitative methods do not provide the level of detail and granularity required by the designers to make high-quality risk informed decisions. The Altair design team was able to overcome these challenges by employing a process of Risk Informed Design utilizing the Valador Reliability Tool [1] (VRT). This tool is able to quickly and accurately produce estimates of the risk of Loss of Mission (LOM) and Loss of Crew (LOC) per mission and provide insight to the designers as to how their decisions will impact overall mission success. The VRT employs a method or risk assessment that is unlike traditional PRA as it effectively engages the designers in the model building process and as a result of this increased Designer – Analyst interaction both the quality of the design and the quality of the PRA model is increased.

This method of PRA seeks to create a baseline model by first capturing a complete set of initiating failure events which can lead to LOM/LOC based upon the Master Equipment List (MEL), dynamic mission events and identified hazards. Next, the event trees of these failures are generated automatically by correctly identifying the response of the system to an initiating failure and the risk exposure times of each failure mode through the use of schematics, designer interviews, and a priori knowledge. Once a baseline configuration has been captured in the reliability model, the tool facilitates the isolation of specific subsets of risk for directed trade studies. Now, the flexibility and speed of the tool can be leveraged to rapidly produce a large number of design options guided by the initial LOM/LOC scoring of the subset of components. The VRT gives the analyst the capability to model, score and analyze options in real-time with the designer. This provides immediate feedback and allows for a rapid iterative process which gives the team more freedom to effectively search the risk design space and find the "differences that make a difference."

Ultimately, a scatter plot of LOM/LOC vs. Delta-Mass can be used to compare the relative implications of each option to one another by highlighting the cost and benefit of each option and the overall trend of the curve. Furthermore, the design team is able to compare options across trade study boundary lines, enabling a global risk perspective. The insight into the risk reduction efficiency of each option aides the design team in determining the best ways to spend mass to increase reliability across the vehicle given a constrained mass budget. Moreover, the VRT serves as an excellent method for vehicle integration to capture cross system dependencies, to find errors in the MEL and schematics, and to identify synergistic relationships that may not be immediately apparent due to the 'stove piping' of the design into specific subsystems.

1 INTRODUCTION

As part of NASA's Constellation Program, the Altair lunar lander will serve as the vehicle to return man to the moon. The spacecraft is analogous to the Lunar Module (LM) of the Apollo program, except the performance requirements have been increased considerably. Unlike the LM, Altair will be capable of transporting four astronauts to any place on the moon for a period of seven days instead of only transporting two astronauts to select locations on the moon for about a day. These performance requirements increase the necessary complexity of the system and the effect is compounded by the constraint on mass that has been determined by the selection of the Ares V as the launch vehicle. To meet these ambitious performance requirements while staying within the control mass, the Lunar Lander Program Office (LLPO) has adopted a risk based design approach during the conceptual phase of the project. Using this approach, the team first designed a minimally functional lander which could complete the mission under the mass budget, but with an unacceptable risk of LOM or LOC. Then, this approach sought to improve vehicle reliability by focusing design efforts on the LOC risk drivers of the design, using the available unallocated mass to buy-down risk. To perform the risk analysis necessary to implement risk based design during the conceptual phase of the project, the LLPO has utilized the VRT. Through interaction between risk analyst and designer, the VRT uses a component based method to identify all initiating events which may lead to a LOM/LOC event. For each component, the tool takes in a predicted failure rate, expected duty cycle, and applicable system responses to a loss of component

978-1-4244-5103-6/10/$26.00 ©2010 IEEE

functionality. The deterministic tool is able to quickly produce results at the component, system, and vehicle level while easily adapting to the rapidly changing design space.

Most recently, the team completed a design analysis cycle which focused on minimizing the risk of LOM occurring during a nominal mission. This paper will explore this analysis cycle from the perspective the risk analyst and describe the process, challenges, and lessons learned from this experience.

2 LUNAR DESIGN ANALYSIS CYCLE

Implementation of a risk informed design began during the first Lunar Design Analysis Cycle (LDAC1) when the design team created a minimally functional lunar lander with an amount of unallocated mass. Next, during LDAC2, the team focused on using a portion of the unallocated mass to decrease the probability of LOC. Now, over a period of four months, the LLPO chose to focus LDAC3 on decreasing the risk of LOM. To complete this schedule, Valador used a team of four analysts to work in concert with the designers to produce a set of potential design options for each trade study. During LDAC3, over 300 design options were created, modeled, and scored for more than 20 different trade studies. One analyst was assigned to each trade study and followed the same overall process to create the final risk models. At the end of the cycle, these models were then integrated to form an overall vehicle level risk model. During the process, issues with tool capability, data resources, information flow-down, and other challenges were encountered. Ultimately, LDAC3 proved to be a success and the challenges of the design cycle led to many improvements in the VRT as well as the method.

2.1 Process

The first step in the process for a single trade study is isolating the subset of components that will be treated. This was often performed by the Vehicle Engineering & Integration (VE&I) team consisting of program management and the chief engineer; however, sometimes the trade study definition was broad and left the specifics of the components to the subsystem lead to decide. For the purposes of the trade study, the subset of components is treated in isolation, assuming that all external components are working properly.

Once the scope has been defined, the next step is to obtain a MEL and Powered Equipment List (PEL) of those components considered as well as a schematic of the components from the subsystem design lead. These documents allow the analyst to setup a rough baseline model or to cross check against the previously existing model from LDAC2. In addition, this procedure allows the analyst to develop an understanding of the subsystem and to identify areas of uncertainty. To resolve this uncertainty the analyst must extract the insight of the designer to complete and verify the model.

Each component requires three pieces of data: failure rate association, response to failure, and duty cycle. The duty cycle can often be easily obtained from the PEL while the schematic and insights of the designer can provide the response of the system to a failure of a component. In some cases, the design is too immature for the duty cycle to be established and an estimate must be made by the designer. Determining the response of a system to an initial failure and all applicable failure modes for a particular component can be challenging and the use of additional standard reliability practices, such as creating reliability block diagrams or performing a preliminary failure mode and effects analysis, can be very informative. The failure rate association is an exponential failure distribution based failure rate from a similar piece of hardware found in an approved data source. Currently, data is from the Space Shuttle PRA, International Space Station Modeling and Analysis Data Set and actual flight data, Ares I-X PRA, Orion PRA and expert judgment. Once the designer and analyst agree the model accurately represents the baseline design, the analyst is then able to utilize the tool to create a stacked bar chart of the components in the trade study as shown in Figure 1.

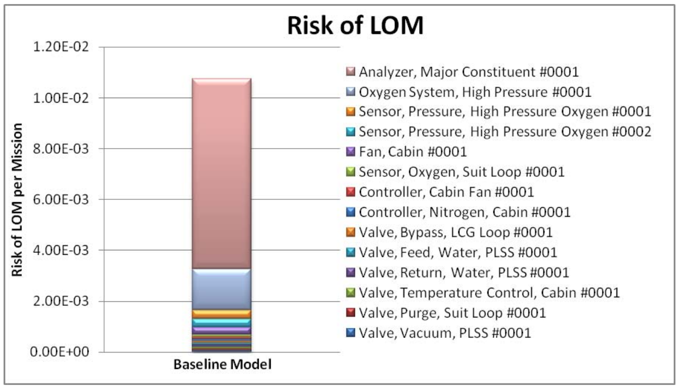

Figure 1 – Trade Study Risk Drivers Chart

This chart identifies the risk drivers and informs the intuition of the designer about the relative impact on the LOM/LOC scoring of each component. Moreover, this chart serves as a road map for how to effectively improve reliability.

Another method of examining the LOM/LOC scoring breakdown is to examine the risk roll up in the VRT itself. Rather than graphically viewing the risk by component, this function of the tool automatically computes the risk of assemblies based upon the component risk scores. The risk roll up displays the aggregate risk scores according to the work breakdown structure and informs the designer of how the risk is distributed and balanced across assemblies in a subsystem trade study.

Now, armed with the chart in Figure 1, the engineering expertise of the designer and the reliability insight of the analyst, an array of trade study options can be created with redundancy ideas and configuration alternatives being put forth by both the designer and the analyst. Each of these options is then modeled using the tool to come up with a LOM/LOC score while the designer computes the delta-mass above the baseline mass needed to implement the new trade study option. Here, the process leverages the speed and agility of the VRT to iteratively search the design space in real-time, guided by the system knowledge of the designer and the reliability knowledge of the analyst. The risk drivers chart can be utilized to compare various design options against one another and the impact of the design differences upon the reliability can easily be elucidated. With this information, the designer and analyst are able to focus their efforts upon the 'differences that make a difference' and produce a set of design options that effectively increases the reliability of the system using varying levels of unallocated mass. Information from each design option is then used to create a LOM/LOC vs. Delta-Mass chart, as shown in Figure 2.

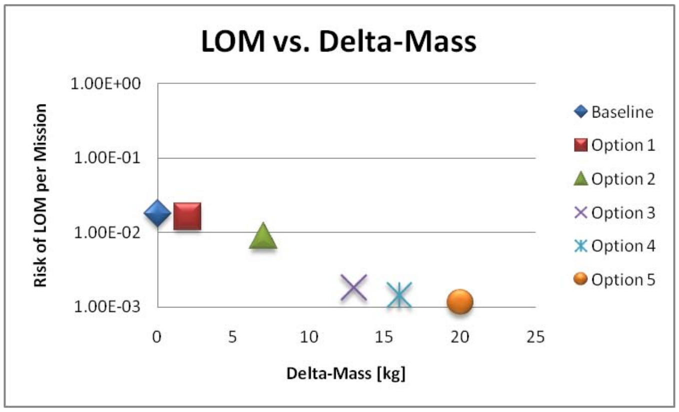

Figure 2 – Trade Study LOM vs. Delta Mass Scatter Plot

This chart is useful to view the overall trend of the reliability of the trade study options and to identify the 'knee in the curve' at which the risk benefit begins to level off as more mass is used. Moreover, by considering each option within a trade study by LOM/LOC and Delta-Mass, it enables comparisons to be made across trade study boundaries. This allows the VE&I team, which is responsible for the final decision on which trade study option to accept, to more easily understand risk implication when making integrated decisions and to identify options which reduce the greatest amount of risk per unit mass spent.

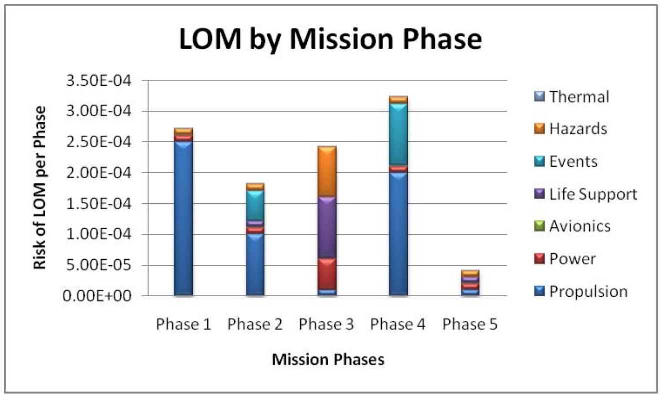

Figure 3 – Vehicle Level LOM by Mission Phase Chart

Another useful analysis of the LOM/LOC scoring is by mission phase. Breaking up the LOM/LOC scoring into conglomerated mission phases yields greater understanding of where the risk is coming from and can lead to better insight on how to mitigate it. This can be done at the trade study, subsystem, or vehicle level. An example of this at the vehicle level is shown in Figure 3.

Moreover, integrated LOM results are very useful for examining overall design cycle progress as well as identifying risk drivers remaining in the system, as seen in Figure 4. This chart can be used to speak to the progress and success of the design cycle and can be helpful in planning future design cycles.

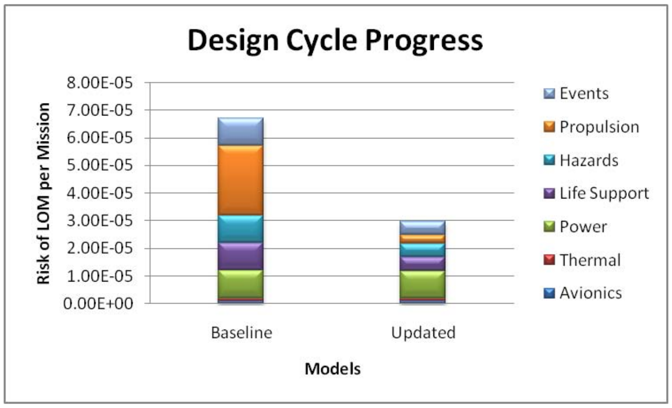

Figure 4 – Vehicle Level LOM Score Comparison Chart

2.2 Challenges

Most of the trade studies performed during LDAC3 were able to follow this standard approach without any appreciable challenges; however, in some trade studies situations arose which required additional work beyond the process outlined here. One of the greatest challenges was finding appropriate failure rate associations that accurately represent the component of interest. In situations where the data sets did not contain a component that was sufficiently similar, adjustments of existing failure rates were made by using expert modification factors. In some situations, the data sets contained a component that itself was sufficiently similar, but the operating environment was not close enough and thus modifications were made by using expert environmental modification factors.

Additionally, while working with the subsystem designers it became clear that the VRT would not be able to handle particularly complicated or unique subsets of components. These situations were handled by either improving the capabilities of the tool or creating reliability models outside of the standard VRT framework. Increasing the capability of the tool to handle a unique situation in one trade study allowed for additional flexibility in other trade studies; however, introducing additional capabilities to certain trade study models added additional complexity when all the trade study models were integrated into a vehicle model. Employing side models to capture unique situations proved to be a simpler method, though not as straight-forward for an outside observer to understand.

2.3 Lessons Learned

In retrospect, there are many lessons that can be learned from LDAC3 and taken forward into other design cycles. For example, initially the risk analysts were involved only at the trade study team level. This led to constraints on information flow down from the VE&I team as design decisions affecting the risk modeling would not flow down to the analysts. As the design cycle progressed, it became apparent that the risk analysis is an integrated issue and must be involved from the top levels of the vehicle. Though, due to the separation between VE&I and the risk analysts, the risk analysts were able to provide a great check on the accuracy of the MEL, PEL, and other integrated vehicle issues such as synergy or conflict across subsystem boundaries.

Furthermore, in order to improve the cohesion of an integrated model as well as improve the comparability across subsystem trade study boundaries, it is very important to have a complete and consistent set of approved failure rates. This is no easy task as there exists no such data set for space applications and thus the creation of such a data book would be great future work.

Additionally, when integrating the trade study models into a vehicle model, it became obvious which portions of the vehicle had been treated during LDAC3 and which had not been updated since LDAC2. In future design cycles it will be important to cover all areas of the vehicle in order to update the entire model to the most recent understanding, methodology, and data sets.

Moreover, in situations where an estimate of a components duty cycle must be used, it is imperative to document the methodology for creating an estimate so that the estimate can be updated as the design matures without much additional work.

Also, it was extremely useful to verify the model by ensuring that the risk drivers chart and the designer's intuition matched. If they did not match, it was an indication that either the model was not correct or that the designer did not have a good understanding of the risk in the subsystem. In either case, such a difference indicated that additional work is required to improve the model or improve the intuition of the designer.

3 CONCLUSION

Risk informed design helps to make the design team a 'smart buyer' by aiding in the efficient and effective allocation of resources. By including the designer in the risk modeling, the designer will understand the reliability implications of a system better and by including the analyst in the design team, the analyst will understand the system better. Moreover, having the ability for the designer and risk analyst to interact with the model to produce results in real time yields a deeper understanding of how design decisions immediately impact reliability. Using a risk drivers chart as a guide helps focus the efforts of trade studies and validate the model fidelity against the intuition of the designer. The LOM vs. Delta Mass charts allow for easy comparison of trade study options against one another as well as easy comparison of options across trade study boundaries. The integrated LOM/LOC scoring charts allow managers to track design cycle progress, identify areas of importance for future design iterations, and effectively communicate the current reliability of the system. And what's more, this process can be applied to a wide range of design projects outside the scope of manned space exploration.

As the political realities which have forced NASA to make crew safety and mission reliability a design driving requirement begin to spread to other industries, the demands upon complex systems to operate reliably and to continue operating in light of a failure will continue to increase. These demands will further require reliability analysis to evolve and mature tools which can effectively, rapidly, and accurately add value to design projects earlier and earlier in the conceptual design phase.

4 ACKNOLEDGEMENTS

The author would gratefully like to acknowledge the support and leadership of the Lunar Lander Program Office at Johnson Space Center. The author would also like to thank all of the fellow analyst at Valador and colleagues at the Jet Propulsion Laboratory, Marshall Space Flight Center, and Glenn Research Center for all of their hard work and efforts put into this design project.

REFERENCES

1. B.F. Putney, E. Tavernetti, J.R. Fragola, E. Gold. "Reliability Tool for a Preliminary Quantified Functional Risk and Hazard Analysis." Reliability and Maintainability Symposium, 2009.

BIOGRAPHIES

Chris Mattenberger
1860 Embarcadero Road
Suite 155
Palo Alto, CA 94303 USA

e-mail: chris.mattenberger@valador.com

Mr. Mattenberger is a Systems Engineer in the Modeling & Simulation division of Valador, Inc. His work with Valador has focused on supporting risk informed design throughout the Constellation Program since joining the company in 2008. Previously, Mr. Mattenberger attended the Massachusetts Institute of Technology and received a Bachelor of Science in Aerospace Engineering with Information Technology in 2006 and he continued on to attend Stanford University and received a Master of Science in Aeronautics and Astronautics in 2008.