A HOLISTIC APPROACH FOR RISK MANAGEMENT DURING DESIGN

Leila Meshkat /Jet Propulsion Lab 4800 Oak Grove Drive, Pasadena, CA 91101

SUMMARY/ABSTRACT

In this paper, an approach for the identification, assessment, mitigation and continuous management of risks during the process of designing a space mission is presented. This approach has been developed by observing the risk patterns that occur at the Project Design Center of the Jet Propulsion Laboratory (TeamX) which develops conceptual, concurrent design of Space Missions. TeamX develops an end-to-end conceptual design of a Space Mission in a matter of one or two weeks. As the risk chair in TeamX, the author has had the opportunity to observe the risk patterns that occur during design over the course of many design sessions. This paper introduces an abstraction and generalization of those patterns. Risk is defined as anything that can go wrong, along with its approximate likelihood and consequence. The indicators, and causes, and effects of these risks are cross cutting across the multiple levels of people and processes involved in the design, and the actual design product itself.

Copyright © #### by ASME

INTRODUCTION

Effective Risk Management during the design phase of a space mission can result in the optimal use of available resources, and more robust and reliable space missions. Although the risk management process is seemingly straightforward to define and often involves keeping track of the identified risk elements and monitoring and mitigating them on a continuous basis, the successful implementation of this process is complex. The complexity arises due to the many dimensions of the design process, and the dependencies in between, and within each of these dimensions. Some of the dimensions involved include the design product, the design process, the institutions involved in the design process and their respective policies, the interactions between the institutions at various levels, including the management as well as the designer level, and the interactions between the designers and the managers within each institution.

In this paper, I propose an approach for risk management during design. This approach is developed based on my observations of the risk patterns at the Concurrent, Conceptual Design team of the Project Design Center of the Jet Propulsion Laboratory (TeamX), and my experience as the first "Risk chair" of that team. The next section provides a background about this team, and the process we currently use for risk management.

BACKGROUND

The Project Design Center (TeamX)

The Jet Propulsion Laboratory (JPL) employed the concept of concurrent engineering to create the Advanced Projects Design Team (Team X) in April 1995. This team produces conceptual designs of space missions for the purpose of analyzing the feasibility of mission ideas proposed by its customers. The customers often consist of principal investigators of design teams who aim to plan new mission proposals. The study takes one to two weeks (usually involving 3-hour collaborative sessions) and the design is then documented in a 30 to 80-page report that includes equipment lists, mass and power budgets, system and subsystem descriptions, and a projected mission cost estimate. The study is then reviewed and summarized and an abbreviated report is also produced. There have been over 100 to date. More detailed information about TeamX can be found in [1] and [2].

Risk Management in TeamX

The process used routinely for risk management in the TeamX allows for the identification, assessment and synthesis of the risk items perceived during the design process. The risk chair is responsible for identifying the relevant risk items and communicating them to the relevant experts using a distributed software tool, RAP [1]. Each of the experts, in turn, assesses the risks sent to them, and adds any additional risks they perceive in their design. Engineers deliberate on the risk items, and come to a consensus about their relative significance during the sessions. The risks are then synthesized into an overall risk report after deliberations in the team. Over the last year, we have conducted some experiments in building probabilistic risk assessment models in this team. Our experiments indicate that:

1. In order to build PRA models in real time, it's necessary to start with a reference PRA for a similar type of mission and refine as you go along.
2. TeamX can be used for verifying existing risk models using designer expert opinions.
3. Design and risk information generated during the TeamX session can be used for building PRA models after the design session.

More information about our experiments can be found in [17]. In the next sections, we will go through each of the steps involved in risk management, namely, risk identification, assessment, and mitigation, and explain the proposed approach for addressing them.

Copyright © #### by ASME

RISK IDENTIFICATION

In the first issue of the journal of *Risk Analysis,* Kaplan and Garrick formally defined risk to be a set of triplets:

$$R=\{<S_i, L_i, X_i>\}$$

where S_i is the ith "risk scenario", L_i is its corresponding likelihood, and X_i is a vector of possible adverse consequences[5]. S_i is determined by answering the question "What can go wrong". In a subsequent paper[7], they used an index,c,

$$R=\{<S_i, L_i, X_i>\}_c$$

to denote that this set must be complete, and include at least all the major scenarios, and they further introduced the idea of the "success" or "as planned" scenario (S_0), and defined risk scenarios to be deviations from it.

Clearly, the first step in any risk management activity is to identify the risk elements. The risk elements observed in the TeamX environment fall into two main categories: mission risk drivers, and surprises observed during the design process. While there's insufficient evidence to conclude that the elements described below permeate a complete set of possible adverse scenarios, their relevance has been observed time, and time again.

Mission Risk Drivers

Often the key risk drivers for a mission are predictable from early in the design process. Some of the factors that immediately call for attention can be classified as follow:

1. New Technology, New Engineering, or New Development

Anytime we use a technology that has little heritage, or an innovative approach that hasn't been used before, it's important to pay attention and make sure that we are considering all the different aspects of this technology and approach. Note that new technology or innovative approaches do not necessarily lead to higher risk, but there's more potential epistemic uncertainty about them.

2. Environmental Factors

Extreme environments, such as the high radiation environment of Jupiter, or the extremely hot environment of Venus, clearly pose risks that need to be considered during the design process. Sometimes environmental phenomena such as solar flares, micrometeoroids, or dust storms on the surface of Mars are difficult to model due to the lack of sufficient knowledge about their behavior, and time of occurrence, therefore there's some extent of epistemic uncertainty associated with them.

3. Design Challenges

The limited resources available for any spacecraft design, and the unique requirements of each spacecraft sometimes cause the design of a particular element of the spacecraft to be especially challenging. These challenges might lead to design decision making without consideration of the risks involved. Therefore, areas of design that are particularly challenging might lead to risky design decisions.

4. Reliability Issues

The required lifetime of the spacecraft, and the degradation due to the thermal cycling, or the environmental conditions is another element to take into consideration in the risk identification process. For instance, the mechanisms may wear out in time, and the electronics can be subject to single event upsets caused by the environment.

5. Major Events during the mission

The key events that occur during a space mission, such as the launch of the spacecraft, the orbit insertion, rendezvous between several units, separation events, etc. are all elements that could lead to an increased chance of failure.

6. Multi-institute collaboration issues

When multiple institutions are involved in the development of a spacecraft or management of a space mission, there can be additional risks due to the different conventions used by each of the organizations, and the communication and collaboration issues involved.

Copyright © #### by ASME

Surprises during the Design Process

Following are some of the surprises that occur during the design process, which often indicate that the system is out of balance, and are red flags that need to be taken into consideration by the risk manager:

1. Significant deviation from expected mass, cost or performance for any element of the spacecraft.

Often, we have an expectation for the mass, cost and performance measures of each of the spacecraft elements based on our design experience. While significant deviation is not necessarily an indication of increased risk, it is a cause for further investigation and a red flag.

2. Significant deviation from the expected challenge associated with any subsystem design.

The approximate amount of effort required for the design of any part of the spacecraft is predictable. If it turns out that this amount of time deviates significantly from what we expect it to be, there might be a cause for concern, and it's important to explore the causes of this deviation in more detail.

3. Human issues: Interaction between designers.

Since the various subsystems in a space craft are all inter-related, each of the expert designers spend a considerable amount of time understanding the relationship between their associated subsystem, and other subsystems. In a concurrent engineering design team, designers collaborate by real time communication. Therefore, the amount of communication between them is an indicator of how much they are interacting with each other. Here are some of the related surprises and their possible causes.

a. Too much or too little interaction between a designer and the rest of the team.
    i. Too much interaction:
        Possible Cause: Is it a complex issue, or is the designer missing an important piece of information?
    ii. Too little interaction
        Possible Cause: Is the subsystem in question keeping up to date with the rest of the design?
b. Too much or too little management (team lead and systems engineer).
    i. Too much
        Possible Cause: Is there some disagreement between domain expert and management?
    ii. Too little
        Possible Causes: Is there a critical issue that management is unwilling to address?
        Is something going unnoticed?
c. Too much or too little effort (man/hours) needed
    i. Too much
        Possible Cause: Are we over-designing?
    ii. Too little
        Possible Cause: Are we doing our best?

Measuring Surprises

Following are some suggestions for measuring the surprises observed during the design process.

- Expected mass, cost, performance for each subsystem of each type of mission.

These expected values can be obtained from historical data, and adjusted for the space mission in question.

- Expected challenge associated with a subsystem design.

We can define indices for the complexity of each subsystem based on the degree of interdependency between that subsystem and other elements of the spacecraft, and determine the challenge associated with the subsystem design based on the complexity index.

- Expected interactions between designers, and management.

Copyright © #### by ASME

The number of times, and number of issues brought up at formal reviews of design teams (such as Monthly Management Reviews) can be counted, and compared to the average number of communications for similar types of missions.

RISK ASSESSMENT

> To the extent that risk assessment is precise, it is not real.
> To the extent that risk assessment is real, it is not precise.
>
> Yacov Haimes, *Risk Modeling, Assessment & Management*, 2004[8]

Once the risky area has been identified, we zoom into the area and ask as many questions as necessary to either determine that the surprise was a false alarm, or determine the approximate likelihood and impact of the risk identified. Well defined quantitative risk assessment techniques such as "Probabilistic Risk Assessment[7]", as well as any other applicable technique, such as fuzzy logic, can be used for assessing the identified risks. It's important to note that while assessment is an integral part of any risk management activity, the quantitative results should be explored in the context of the design problem, the underlying assumptions of the model, and the level of fidelity of available data.

RISK MITIGATION

Determination of the most appropriate method for mitigating a risk is done by brainstorming with all the subsystem designers whose subsystems are in one wary or another effected by the risk. It's also important to note that even though a subsystem may not be affected by a risk element, it might be affected by the suggested mitigation. So once a mitigation decision is made, it's important to make sure that all the affected subsystem engineers are aware of the new mitigation strategy.

CONTINUOUS RISK MANAGEMENT

We define the "System Balance" to be a vector V, where

$$V=\{[E(\text{mass}), E(\text{cost}), E(\text{performance}), E(\text{interaction between combinations of key project personnel}), ..]\}_t$$

The index t signifies the fact that this vector is a function of time. The value of the "System Balance" vector can be measured at significant points of time in the lifecycle of a project. Tracking its fluctuations help us to keep track of the risk levels of the system, and continuously manage them. The risk management process, is of course an iteration of the risk identification, assessment, and mitigation processes.

CONCLUSIONS & FUTURE DIRECTIONS

While my observations in TeamX have led me develop a general approach for risk management during design, I have not yet elaborated on the intricacies of this approach. I think it's imperative to study the risk management problem during design from multiple perspectives and my observations are one of those perspectives.

In the future, I plan on elaborating on this approach and formally implement it on a sample design project.

ACKNOWLEDGMENTS

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.

Copyright © #### by ASME

REFERENCES

[1] L.Meshkat, R.E. Oberto, " Towards a Systems Approach for Risk Considerations during Concurrent Design", *United Nations Space Conference, Beijing, China*, May 2004.

[2] Mark, G. (2002). Extreme collaboration. *Communications of the ACM. Vol. 45(6), pp.89-93*

[3] *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, version 1.1, prepared for the Office of Safety and Mission Assurance, NASA HQ, Washington, DC, August 2002.

[4] L. Meshkat & A. Shapiro, "Probabilistic Risk Assessment for Concurrent, Conceptual Design of Space Missions", Proceedings of the AIAA Space Conference, Fall 2005.

[5] S. Kaplan, & B. Garrick, "On the quantitative definition of risk", *Risk Analysis* 1(1) 11-27, 1981

[6] S. Kaplan, Y. Y. Haimes, and B.J. Garrick, 2001, Fitting hierarchical holographic modeling (HHM) into the theory of scenario structuring and a refinement to the quantitative definition of risk, *Risk Analysis* 21(5): 807-819.

[7] S. Kaplan, "The general theory of quantitative risk assessment – It's role in the regulation of agricultural pest"s, *Proceedings of the APHIS/NAPPO International Workshop on the Identification, Assessment, and management of Risks due to Exotic Agricultural Pests* 11(1), 123-126.

[8] Y. Haimes, "Risk Modeling, Assessment, and Management" Second Edition, John Wiley & Sons, Wiley Series in Systems Engineering and Management.

Copyright © #### by ASME