AIAA SPACE 2010 Conference & Exposition
30 August - 2 September 2010, Anaheim, California

AIAA 2010-8741

Identification and Classification of Common Risks in Space Science Missions

Jairus M. Hihn*, Debarati Chattopadhyay, Robert A. Hanna
California Institute of Technology/Jet Propulsion Laboratory, Pasadena, CA, 91101

Daniel Port
University of Hawaii at Manoa, Honolulu, Hawaii, 96822

and

Sabrina Eggleston†
California Institute of Technology/Jet Propulsion Laboratory, Pasadena, CA, 91101

Abstract: Due to the highly constrained schedules and budgets that NASA missions must contend with, the identification and management of cost, schedule and risks in the earliest stages of the lifecycle is critical. At the Jet Propulsion Laboratory (JPL) it is the concurrent engineering teams that first address these items in a systematic manner. Foremost of these concurrent engineering teams is Team X. Started in 1995, Team X has carried out over 1000 studies, dramatically reducing the time and cost involved, and has been the model for other concurrent engineering teams both within NASA and throughout the larger aerospace community. The ability to do integrated risk identification and assessment was first introduced into Team X in 2001. Since that time the mission risks identified in each study have been kept in a database. In this paper we will describe how the Team X risk process is evolving highlighting the strengths and weaknesses of the different approaches. The paper will especially focus on the identification and classification of common risks that have arisen during Team X studies of space based science missions.

Nomenclature

ACS = Attitude Control Subsystem
EDL = Entry Descent and Landing
CDS = Command and Data Subsystem
RAP = Risk & Rationale Assessment Program
RHU = Radioisotope Heater Unit
RPS = Radioisotope Power System
TRL = Technology Readiness Level

I. Introduction

By its very nature, space exploration is a high-stakes, high-risk endeavor. Projects created to achieve the goals of space exploration are inherently risky because they are always going to new destinations in new ways. However, a history of devastating accidents such as the Apollo-1 fire and the space shuttles Challenger and Columbia disasters have at the same time created a risk adverse culture within much of NASA. As a result, when new projects are proposed in this environment, there is a tension between accepting the risks of pushing the boundaries of space exploration and the risk of project failure. Unfortunately, the techniques and processes for evaluating risk in the conceptual design and proposal stage of a project, when the definition of the project is just in its infancy, are not well-defined nor well understood. Despite the dramatic improvements of risk analysis techniques over the last 100 years, new techniques have provided little relief in this area. Decision Analysis, FMEA (Failure Modes and Effects Analysis) [1] and Probabilistic Risk Analysis [2, 3, 4] techniques have greatly improved the understanding of the risks in systems, designs and projects. However, these techniques are most effectively applied when there is a detailed understanding of the design or definition of a system. When project concepts are being evaluated for

* Team X Risk Lead, Mission Systems Concept Section, JPL, jhihn@jpl.nasa.gov and AIAA Member.
† Space Grant Summer Intern 2010

Copyright © 2010 by the American Institute of Aeronautics and Astronautics, Inc. The U.S. Government has a royalty-free license to exercise all rights under the copyright claimed herein for Go

selection for funding, there are a large number of unknowns in the definition of the project and detailed designs needed for risk analysis typically do not exist. In lieu of methods that depend on detailed information, expert knowledge must be used in order to identify risks of project failure, and those risks may affect the selection of a given project. One of the known limitations of expert knowledge is the non-uniform quality of risks identified based upon the individual expert involved in the process. Individual experts have biases from their personal experience that can cause them to overlook or underestimate particular risks of project failure. The Delphi method and other techniques were developed to eliminate biases derived from personal experience, but these techniques are often time consuming and thus difficult to utilize in a quick-turnaround feasibility study. Another recent attempt to address early lifecycle risk within NASA is DDP (Defect Detection and Prevention). DDP was first proposed ten years ago and has received a lot of attention because it does attempt to address the early life-cycle risk issues. However, DDP is difficult to apply in this context because of the time commitment required to implement the method [5,6].

So how can a project concept be quickly evaluated for risks of project failure in a short amount of time, when only limited detailed information is available? Part of the solution is to improve the quality of the expert knowledge in relevance and completeness by leveraging previously gathered expert input from similar proposals. Analyzing risk data provided by many experts in the past can provide guidance for risk evaluation in current proposal studies. Capturing and extracting meaningful data from individual projects is difficult because of the lack of consistent use of established or existing tools for capturing project data. However, it is very feasible in concurrent engineering teams, as they consistently use an established infrastructure and set of tools for design. The following is a description of the JPL Team X concurrent engineering environment, the shortcomings of the current risk assessment process in Team X, and the avenues being explored to raise the quality of the expert knowledge risk gathering process in the quick turnaround environment of the concurrent engineering process of Team X.

II. Background: Concurrent Engineering Teams at JPL

The Jet Propulsion Laboratory (JPL) extensively uses concurrent engineering teams in the conceptual design phase, or what is known as pre-Phase A and Phase A at NASA. A concurrent engineering team consists of diverse specialists working simultaneously in the same place, with shared data, to yield an integrated design or designs. Team X, started in 1995, has carried out over 1000 studies, dramatically reducing the time and cost involved compared to prior conceptual studies, and has been the model for other concurrent engineering teams both within NASA and throughout the larger aerospace community. Figure 1 shows a snapshot of the highly interactive environment of a Team X session. Team X has been so successful within JPL that it has expanded its capabilities from the original focus on mission point designs to perform instrument studies, high-level broad architecture trade studies, and technology assessments. A Team X mission design study generates one or two point designs over approximately three sessions, with additional supporting work often done outside of the sessions. In a typical Team X mission study there are 15 chairs, with a minimum of 8 for partial-mission studies. Not all chairs are required for every study – the subsystems included depend on the assessment needs of the study. Figure 2 below shows the list of the primary chairs and their configuration within the project design center. For a more detailed discussion of Team X and its tools, see [7] and [8].

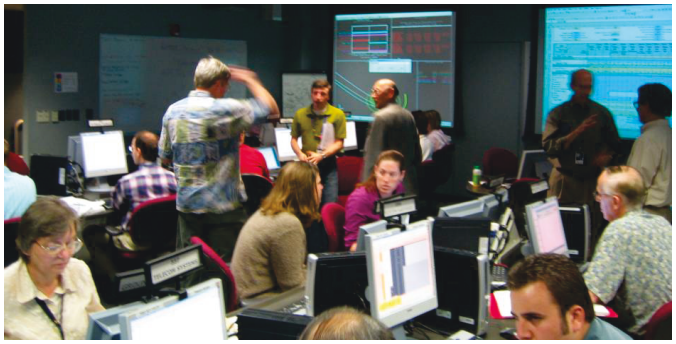

Figure 1: Team X Study in Action

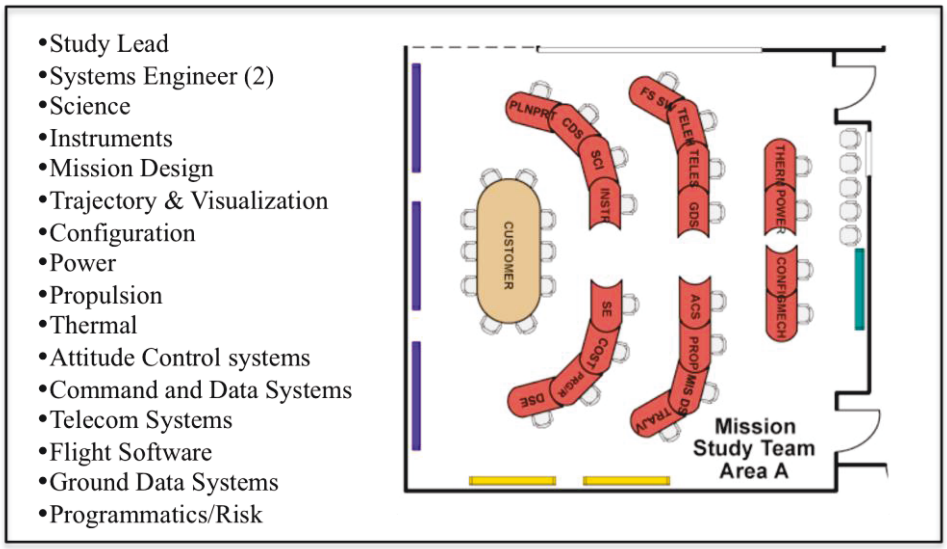

Figure 2: Team X Subsystems and Configuration

III. Risk in the Team X Environment

The Risk subsystem chair was introduced in 2001, and risk assessment is thus a relatively new capability in Team X. Incorporating risk assessment into the dynamic environment of a concurrent engineering team requires rapid response and adaptation. It is very important to understand that in an early-phase concurrent engineering study such as Team X, the focus is not on risk management but rather on risk identification and initial assessment. According to Conrow [9, Page 22],

> "Risk assessment is the process of identifying and analyzing program areas and critical technical process risks to increase the likelihood of meeting cost, performance and schedule objectives. Risk identification is the process of examining the program areas and each critical technical process to identify and document the associated risk."

In many cases, the identified 'risk' items are primarily issues that need to be addressed in a proposal or analyzed further in the early stages of a project. There is no analysis using fault/event trees or other formal methods. There is little quantitative data that is accessible during a study to provide a basis for risk estimates. Just generating consistent risk lists with inputs from all the relevant subsystems and presenting the results clearly to the stakeholders is difficult because of the speed with which decisions are made in the semi-organized chaotic environment of Team X. Often things are moving so fast that it is not possible to formally review the risks for each option as the study progresses, but only at the very end of the study. If a serious risk is identified during a session it is discussed with the customer, and the customer may make changes to the design requirements in order to avoid the risk. Potential mitigations are also recorded for later consideration, especially those associated with risks that appear significant.

The current risk tool used in Team X is the Risk & Rationale Assessment Program (RAP). The design and original use of the RAP tool is described in detail in [8]. The use of the RAP tool has changed over time but the core process for its use has been stable since the tool was introduced in Team X. The key features of the tool are

- All subsystem chairs can enter and score a risk (see Figure 3a)
- All risks are scored using the NASA 5x5 Matrix (see Figure 3b)
- All chairs notify all other chairs that may be affected by the risk so that they can also score the risk
- All affected chairs are notified if any change is made
- The Risk Chair determines the final wording and scoring of all mission level risks and presents the results to the customer and the team, usually near the end of the last design session
- All final scores and descriptions at the mission and subsystem levels are archived in a database

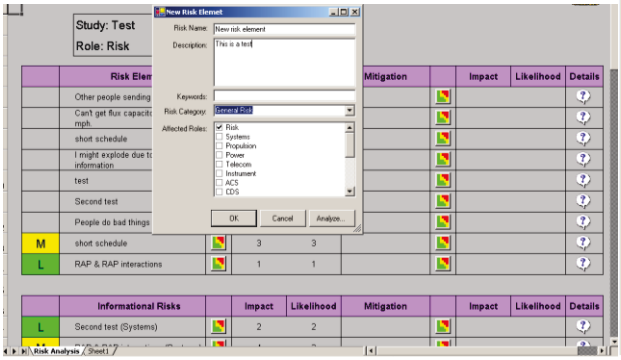

Figure 3a: RAP Risk Input Form

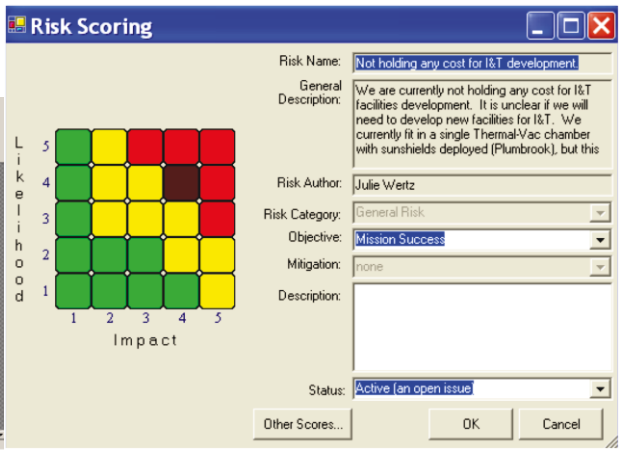

Figure 3b: RAP Risk Scoring Form

The guidance that was used in scoring risks until recently is shown Table 1. The boundary values appear to have been originally based on an analysis performed for NASA, in the context of manned missions [10].

Risk Table Level Definitions				
Levels	Mission Risk		Implementation Risk	
	Impact	Likelihood of Occurrence	Impact	Likelihood of Occurrence
5	Mission Failure	Very High, ~10%	Consequence or occurrence is not repairable without engineering (would require >100% of margin)	Very High, ~70%
4	Significant reduction in mission return (~10% of mission return still available)	High, ~5%	All engineering resources will be consumed (100% of margin consumed)	High, ~50%
3	Moderate reduction in mission return (~50% of mission return still available)	Moderate, ~1%	Significant consumption of engineering resources (~50% of margin consumed)	Moderate, ~30%
2	Small reduction in mission return (~90% of mission return still available)	Low, ~0.5%	Small consumption of engineering resources (~10% of margin consumed)	Low, ~10%
1	Minimal (or no) impact to mission (~99% of mission return still available)	Very Low, ~0.1%	Minimal consumption of engineering resources (~1% of margin consumed)	Very Low, ~1%

Figure 4: Impact and Likelihood Thresholds Used in Risk Scoring

IV. Issues in Team X Risk Assessment

Over the years, a number of key issues have arisen in Team X risk assessments related to inconsistency in both the identification and the scoring of risks, which is especially driven by the subjective nature of the activity. Generating consistent risk lists with inputs from all the relevant subsystems and presenting the results clearly to the stakeholders in a concurrent engineering environment is made especially difficult because of the speed with which decisions are made. The primary issue identified with the current process is that there has been limited consistency between studies with respect to which risks were identified, how they were described and how they were scored.

Additional issues that have been identified are listed below.

- In the early stages of the lifecycle it is difficult to distinguish between an issue, a lack of knowledge, and a formal risk. This is a characteristic of early conceptual design that has been discussed elsewhere in the literature (for example, see [11]).
- Engineers have great difficulty estimating likelihoods quantitatively.
    - In general, rather than identify and assess risks, engineers immediately change the design to mitigate or resolve them. They do not see the world as vectors of probabilities, but rather as problems to be solved.
    - Scoring is a fuzzy hybrid of qualitative and quantitative assessment. Cooper describes risk assessment in the early life-cycle as 'pre-quantitative risk' [12].
- Rather than thinking about risk quantitatively, engineers appear to have a better sense of three levels of risk. A representation of the thought process might be:
    - This is something to keep an eye on (green risk)
    - This is something that I am very worried about and it could cause total mission loss (red risk)
    - This is something to worry about and it might be even worse than I realize since there is limited information currently available (yellow risk)
- Risk identification is very dependent upon immediate experience. If a person is constantly involved in high-risk projects, their risk threshold may become higher than usual. If they were recently burned by a particular failure, they will overstate the existence of a related risk.
- There is a 'politics' of risk. A red risk cannot go out in a study report unless the risk analyst can make a very strong case for it, preferably with some form of supporting quantitative data. Most red risks are reduced by specifying a mitigation. While the mitigation is almost always reasonable, there is usually very little analysis of the mitigation identified in order to understand its feasibility and whether it introduces any new risks.
- Experienced subsystem chairs are able to score implementation risk (risks to budget or schedule) impact quantitatively, but only relative to their own subsystem costs and not from a mission perspective.
- Risk impact and likelihood values are dependent on the type of mission. The man-rated values shown in Figure 4 are not suitable for robotic missions, which often accept more risk. For example, the 'Very Low' likelihood threshold value many use is >0.1%, which is an appropriate level when assessing risk to human life, but for a robotic science mission such low likelihood risks can be accepted.A description of how the risk scoring guidance has been changed to better suit unmanned missions is provided in [13].

In order to improve the risk assessment process in Team X, a number of possible improvements to the current process were identified and are described in the following section.

V. Proposed Improvements to the Risk Assessment Process

The focus for improvements to the risk assessment process in Team X is to facilitate the generation of more consistent and complete risk assessments. The following steps are proposed to address the issues related to risk identification and scoring described in Section IV, in order to improve the Team X risk assessment process. In this paper we primarily address developing checklists and verifying them on the basis of past design studies (items a and b).

a. Develop checklists of risks for each subsystem, based on previous design studies, that can be used in the Team X environment to improve consistency of risk identification between studies
b. Create a set of risk scoring guidelines, based on previously recorded risks in the risk database, to improve consistency of the scores
c. Change the threshold values for the risk likelihoods and impacts to values that are more reflective of the types of mission risks that arise at this early stage of conceptual design, which will provide better scoring guidance to subsystems (see [12]).

d. Engage in a research task to capture the risk mental models that would enable the extraction of more accurate and consistent risk information from team members, by providing information and querying members in a way that best addresses their mental models.

VI. Developing Risk Checklists

One of the very first steps taken to improve risk identification in Team X was to develop an initial set of checklists for each chair. These were constructed by :

- Reviewing the risks reported in selected studies completed over the previous six months to generate a basic list of commonly identified risks for each subsystem;
- Asking each subsystem lead to review and to revise these checklists to help create lists that could be used during Team X sessions;
- Piloting the checklists over approximately 6 Team X studies.

An example of a checklist used during the pilot is shown in Figure 5. The results of the pilot in Team X indicated that the subsystem chairs did not use the checklists often, because the leads felt that they did not need a checklist to identify risks, and the associate staff found the checklists too long to use during the sessions. On the other hand, the risk chair was able to effectively use the checklist to add risks into the RAP tool to extract responses from the subsystems. While this test provided valuable experience, the feedback from the team was that the process could be improved by providing subsystems with risk templates specifically tailored to each study's characteristics.

Propulsion	*Implementation*	*Mission*
Organizational		
Outside development of mission parts/contractor relations		
Multiple collaborating implementing organizations		
Technology Development and Heritage		
Low TRL /New Technology		
Lack of experience with technology at JPL		
Scaling of existing technology (significant increase in size, power, mass)		
Technology inheritance from future missions		
Optimistic heritage assumptions		
Reliance on availability of residual hardware (such as Galileo heat shield, or SEP from DAWN)		
Availability of commercial parts		
Redundancy/Critical Failure		
Lack of Redundancy		
Dependencies on other flight systems within the mission		
Inability to test certain components in a relevant environment		
Very long mission (impact on component reliability)		
Environmental		
Harsh environment		
Unknown environment		
Environmental contaminants		
Subsystem Specific		
Restricted configuration to avoid contamination of other subsystems		
Meeting deorbit maneuver fuel requirements		
Unbalanced Thrusters		

Figure 5: Example Risk Item Checklist for Propulsion Chair

VII. Risk Frequency in the RAP Database

The RAP tool database has been maintained since the tool was first introduced in Team X in 2004. The database contains entries for each risk recorded in the approximately 200 studies that have utilized the RAP tool. Each entry in the database contains identifying information about the study, including the study name and identification number, the name and description of the original risk submitted in the tool, the name of the subsystem that the risk scorer represents, and scores for impact and likelihood of the risk. If the risk was sent to other subsystems for comment and scoring through the tool interface, those responses are recorded as independent entries in the database, with the same risk name and description. Risks that are identified during the study, but are not included in the final risk tally (often because they were replaced with differently worded risks, or if the design has been changed such that the risk no longer applies) remain in the database, but can be distinguished from the final risks using a combination of column entries.

As there has been no consistent policy or guidance regarding the capture of risks in Team X, a wide variance in the quality of the risk reporting between studies and over time was anticipated. A glance at the past data in the database confirms that the lack of a rigorous risk identification process leads to inconsistent risk identification and scoring for similar risks in similar studies. A more rigorous risk identification and scoring method in Team X will help reduce variable risk reporting and allow comparison between mission studies on a consistent basis of risk. More consistency in risk reporting will also facilitate the leveraging of risk information from previous studies by enabling easier data mining of the risk database.

In order to address the issues that were identified in the pilot of the initial risk checklists, the RAP database was analyzed to identify the most commonly reported risks for each subsystem. In looking at a database of nearly 10,000 risk entries, it was evident that prior to any analysis some preparation of the data would be required to remove deleted risks, risk mitigation entries, and other extraneous database elements. The mitigation entries and deleted risks were removed from the data, resulting in a final data set of 170 different studies, with 3361 unique risks - on average, approximately 20 risks per study.

In the Team X environment, 'risks' are captured in a dynamic environment when issues of concern arise during the design process, and as a result there is limited organization or consistency in the risk names and descriptions. In such a varied dataset of risk descriptions, it was necessary to bin similar risks into categories that would allow us to understand the different types of risks identified. Manipulating numbers is second nature to engineers, but finding commonality in the language of text descriptions of risk was a challenging task, due to the large diversity of words and turns of phrase that could potentially describe the same fundamental risk. Text mining, a process of extracting information through parsing of text, was employed in order to organize the risk data into relevant groupings.

An initial cut at binning the data was performed using text mining algorithms trained using the initial checklists, after which final binning was performed manually. Text mining identifies patterns extracted from natural language. For comparison, the better known technique of data mining extracts patterns from structured databases of facts. Text mining is far less mature than data mining as an analysis technique.

The objective of text mining the database was to help organize the thousands of risks collected by the RAP tool into meaningful risk categories such as "Attitude Control Errors". Manually this would have been a tedious, time-intensive, and error-prone undertaking. Furthermore, manual categorization might also introduce biases and misinterpretations from a given individual. The basic approach in the text mining method used was to define a distance measure for the textual risk descriptions (in "semantic space") then use this measure to define neighborhoods (or "clusters") based on the k-nearest neighbors (or k-NN algorithm). Latent Semantic Analysis (LSA) [14] was used to determine the choice of particular text-mining techniques (e.g. use of Porter stemming, "cosine" as distance measure, tf-idf weighting, etc.). The text mining literature suggests LSA is a practical method for the statistical characterization of natural language that allows us to approximate human judgments of overall meaning similarity. The text mining was implemented entirely within the Rapidminer‡ system.

‡ The Rapidminer text mining tool is open source. The documentation and source code can be found at www.rapidminer.com

Use of unsupervised clustering (e.g. without given categories and a training data for them) either placed the majority of risks into a single cluster or the clusters had no discernable meanings. The risk identification checklists (Figure 5) provide a meaningful scheme of risk classification, which is referred to as a 'taxonomy' in text mining literature, The risk examples in the checklists are ideal for classification (i.e. the supervised analog of clustering). The flattened taxonomy items were used as initial classifications and their examples as their training data e.g., Propulsion → Organizational would be the classification "Propulsion Organizational" with "Outside development …" and "Multiple collaborating …" as training data (see Figure 5).

A number of different approaches were tested to create classification models. Performance of the text miner (as measured by percentage of misclassifications) when applying the entire taxonomy (combining the risk categories for all of the subsystems into a master list) to the risk database resulted in an unreasonable number of misclassifications. Furthermore, as a particular risk can belong to multiple categories, the text miner results were especially difficult to interpret at this stage. The performance of the text miner greatly improved when the risk data was subdivided into subsystem data sets, including only those risks that were scored by the subsystem and performing classification only on the taxonomy for that subsystem. Additional refinements were made such as including the taxonomy name in the training set, as some of the taxonomy items had few or no examples. The resulting classified subsystems data sets were manually checked and risks were reclassified in cases where the text miner was inaccurate. The text mining and subsequent manual checking process lead to important refinements of the risk taxonomy and a deeper understanding of the quality of risk reporting. At the end of the checking process, despite the initial cleaning of the data and improvements to the text miner, there were still 12-35% data errors including poorly worded risks that could not be interpreted, and risks that belonged in other subsystems. Excluding the data errors, the text miner correctly binned risks 37-75% of the time. The text miner greatly reduced the effort that would have been required to manually categorize nearly 10,000 risks. Given the customizations that were made in the text mining process during this study, the tool can be used to analyze the risk database more effectively in the future.

VIII. Results

The several top categories of risks for each subsystem are shown in Tables 1a – 1c. Each column also includes a discussion of the risk categories and the rationale for their relative importance to each subsystem.

Science		Instrument		Mission Design		ACS	
TOTAL	464	TOTAL	453	TOTAL	276	TOTAL	343
Environmental	15%	Technology Development and Heritage	24%	Maneuver	28%	Failure of critical components	8%
Measurement Risk	12%	Environmental	16%	Trajectory	20%	Low TRL hardware/algorithms	7%
Entry, Descent and Landing	11%	Entry, Descent and Landing	11%	Launch	11%	Attitude Control Inability to meet pointing accuracy requirement	6%
Technology Development and Heritage	9%	Redundancy/Critical Failure	8%	Environmental	7%	Attitude Control Inability to meet pointing stability or jitter requirement	6%
				Entry, Descent and Landing	5%	Entry, Descent and Landing	6%
						Redundancy Lack of redundancy	6%
- Main risk categories involve risks that could reduced science return (mission risk), while new development of instruments poses a risk to implementation		- There is rarely a mission that plans to fly the a copy of an already flown instrument to the same target environment, so the Risk of new development for instruments is a primary concern for many missions		- Mission design is primarily concerned with the potential for error in large maneuvers, such as the orbit insertion sequence. Uncertainties in delta V exist in the design in this early stage, because a full trajectory analysis is not possible in the limited time of a Team X study		- Top risk categories in ACS are lower percentages of the total, as the initial checklist is very detailed, so the risk categorization had more resolution compared to other subsystems. The higher level categories did not provide the level of information required to understand the driving risk categories, so the subcategories were compared instead.	
- Harsh or unknown environments pose a risk to science return due to reduced performance of instruments or failures due to the environment		- Harsh environments, such as high radiation environments, are a significant concern for reduced instrument performance; the performance of an instrument in an unknown environment is uncharacterized and may not be as anticipated		- Trajectory uncertainties include cases where the target body ephemeris may not be known with sufficient accuracy for probe or lander EDL, or when the target an unexplored body. Until further analysis of the trajectory can be completed, there is a risk of unintentional collisions with planetary bodies.		- Loss of critical components in the ACS subsystem may lead to loss of control of the spacecraft and end of mission. Inability to meet attitude control requirements such as pointing stability to pointing accuracy may reduce science return significantly.	
- If there is a risk leading to insufficiently accurate or numerous measurements, the science objectives may not be achieved		- Landing on a planetary surface may damage instruments, or terrain may block instrument FOV		- While launch is always a high risk event for any mission, the launch category of risks in the Team X database is not the largest category, simply because it is generally an accepted risk, and not always recorded. However, use of an unproven launch vehicle is a risk that would be identified during a study.		- Low TRL components or complex control algorithms may require new development; Entry, descent and landing risks include precision landing related risks and hazard avoidance issues	

Table 1 a: Risk Categories by Subsystem

Propulsion		Power		Telecom		Ground	
TOTAL	319	TOTAL	328	TOTAL	264	TOTAL	124
Critical component leaks or failures	29%	Technology Development and Heritage	17%	Redundancy/Critical Failure	30%	Availability of Stations and Tracks	23%
Technology Development and Heritage	16%	Redundancy/Critical Failure	14%	Technology Development and Heritage	18%	Downlink/Uplink	21%
Redundancy/Critical Failure	11%	Solar Arrays	13%	Environmental	14%	Trajectory/Ephemeris Timing of critical events when communications are blocked	9%
Thruster issues	9%	Environmental	12%	Insufficient communication during mission critical events	8%		
Potential contamination caused by Propulsion subsystem	8%	Constrained power availability	7%				
Environmental	6%	RPS	5%				
- Critical component failures in the Propulsion subsystem may lead to loss of the mission		- As Team X does many studies for missions that are far in the future, and power availability is one of the largest drivers in a mission, sometimes assumptions are made about technology availability in the future. Low TRL is the biggest single concern - RPS development, new battery technology development, high efficiency solar cell		- Critical failures include gimbal mechanism for antenna or failure of the HGA for a planetary mission, as well as failure of a relay asset when the data link depends on a relay, e.g. for a surface lander		- Availability of stations may be uncertain due to expected capabilities that may not exist at the time of the mission	
- Some missions may require unusual trajectories to outer planets, resulting in a need for new high thrust engines. Tanks are very often custom made in order to minimize the launch mass.		- Power availability on planetary missions is often limited, due to distance from the sun and the desire to reduce mass. Also, power modes at this phase of conceptual design are estimates, so there is some uncertainty. Components may need to be cycled in order to meet power constraints. .		- DSN capability or higher power transponders that are expected to be available in the future, when included in the design, lead to technology development risk		- There are risks to the data downlink if there are only limited opportunities available for downlink (e.g., in the case of an atmospheric probe) or if the data return strategy has little margin	
- There is a conflict between the requirement to put thrusters in a particular location with respect to the center of gravity of spacecraft and avoiding contamination of the solar panels, instruments, etc.		- Solar panel deployment problems, dust adherence on solar panels, and harsh environments have a potentially large impact on power availability, especially in cases where there is little margin		- High radiation environments or unknown environments could affect the data link			

Table 1 b: Risk Categories by Subsystem

CDS		Software		Thermal		Structures	
TOTAL	203	TOTAL	151	TOTAL	238	TOTAL	244
Technology Development and Heritage	24%	Software inheritance from future missions	31%	Redundancy/Critical Failure	24%	Critical Separations	12%
Redundancy/Critical Failure	20%	Technology Development and Heritage other	24%	Environmental	13%	Entry, Descent and Landing	12%
Entry, Descent and Landing	10%	Redundancy/Critical Failure	9%	RHU/RPS use	11%	Mass Volume Uncertainty	12%
Insufficient design margins	8%	Optimistic software reuse	6%	Technology Development and Heritage	9%	Technology Development and Heritage	11%
Environmental	5%			Thermal isolation of payload	7%	Environmental	10%
				Thermal stability	5%	Critical Deployments	10%
- The need for new custom-made CDS boards and the assumption of inheritance of product line hardware from future missions result in technology development being the leading category		- The assumption that product line software currently under development for a future mission will be available for the mission under consideration is the most significant risk for the software subsystem, as it has a considerable impact on the cost assumptions		- A primary driver for the redundancy/critical failure category is a very long mission duration, where there may be lack of reliability of thermal subsystem components or degradation caused by many thermal cycles over time		- Largest categories involve landings, separations and deployment - these are usually essential to a mission (e.g. deployment of solar panels, release of a probe, etc). Landing is usually a complex series of events including multiple critical deployments, and thus is a large portion of the risks.	
- Long mission durations and single string designs are a major concern for failures		- The inability to update flight software during a mission or the use of a single on board processor leads to the risk of a critical failure		- High variation in the temperatures during the mission and extreme temperatures (e.g., may cause freezing of components)		- Structures mass estimates at this early stage of design and in the limited time available for the study are usually obtained from scaling of subsystem masses or scaling from previous missions, and as such have a fair amount of uncertainty. Configuration at this level is a feasibility study to make sure that the large structures can be configured and fit on the vehicle and within the launch vehicle.	
- Insufficient on board storage may lead to loss of science data; High radiation environments are a significant risk for CDS systems				- Use of radioisotope heater units or radioisotope power systems in the mission lead to a number of risks including uncertainty in launch approval due to on board nuclear materials, as well as complicated integration issues (as radioisotope components must be integrated at the launch pad) and uncertain radioisotope fuel supply.			

Table 1 c: Risk Categories by Subsystem

Science	Instrument	Mission Design	ACS	Propulsion	Power	Telecom	Ground	CDS	Software	Thermal	Structures
Environmental	Technology Development and Heritage	Maneuver	Failure of critical components	Critical component leaks or failures	Technology Development and Heritage	Redundancy/Critical Failure	Availability of Stations and Tracks¶	Technology Development and Heritage	Software inheritance from future missions	Redundancy/Critical Failure	Critical Separations
Measurement Risk	Environmental	Trajectory	Low TRL hardware/algorithms	Technology Development and Heritage	Redundancy/Critical Failure	Technology Development and Heritage§	Downlink/Uplink	Redundancy/Critical Failure	Technology Development and Heritage	Environmental	Entry, Descent and Landing
Entry, Descent and Landing	Entry, Descent and Landing	Launch*	Attitude control Inability to requirement	Redundancy/Critical	Solar Arrays	Environmental	Trajectory/Ephemeris Timing of critical events when communications are blocked	Entry, Descent and Landing	Redundancy/Critical Failure	RHU/RPS use	Mass Volume Uncertainty
Technology Development and Heritage	Redundancy/Critical Failure	Environmental	Attitude Control Inability to meet pointing stability or jitter requirement	Thruster issues	Environmental	Insufficient communication during mission critical events		Insufficient deisgn margins	Optimistic software reuse	Technology Development and Heritage	Technology Development and Heritage
		Entry, Descent and Landing	Redundacy Lack of redundancy	Potential contamination caused by Propulsion subsystem	Constrained power availability			Environmental		Thermal isolation of payload	Environmental
				Environmental	RPS					Thermal stability	Critical Deployments
		* includes *Use of Unproven Launch Vehicle*				§ includes *Needed hardware capability not currently available*	¶ includes *Needed capability not currently in operation*				
			Risks related to technology development and optimistic heritage assumptions are clearly a risk driver in most subsystems. It is comparatively more important in some subsystems than others.								
			Environmental risks (related to harsh or unknown environments, or environmental contamination) are seen as a primary concern in many of the subsystems. Exceptions are ACS and Ground Systems.								

Table 2: Comparing Risk Categories Across All Subsystems

A comparison of the main risk categories identified for each subsystem brings several differences to light. The nature of the initial checklist used for categorization has a significant effect on the data analysis, and accounts for several of the differences noted between the subsystems. For example, the Attitude Control Subsystem (ACS) checklist generated with the help of the Team X ACS chair was very detailed, including many risk categories. As a result of the fine resolution of risk categories, the percentage of risks per category in the frequency tally for the top categories was much lower than found in other subsystems, as is seen in Table 1a. However, it is still the rank ordering of the risk categories that provides valuable insight into the primary risk drivers for each subsystem.

While looking at the frequency results within a subsystem leads to conclusions about the risk drivers within a subsystem, comparison across the twelve subsystems allows the analyst to draw inferences from the similarities and differences between the subsystems. It is of note that as the initial checklists were developed with the help of the subsystem chairs, the naming of the categories reflect the preferences and mental models of the subsystem chairs, which is why the same type of risk – e.g., Low TRL/new technology – is found under different category headings in Telecom, Mission Design and Ground Systems.

Technology development appears as a major risk category in all of the subsystems. Team X often analyzes missions that are very early in the conceptual design phase, intended for launch decades in the future, and JPL robotic missions are constantly attempting to push the technological and scientific boundaries to explore distant planetary bodies. As a result of the nature of missions that are studied in Team X, the high frequency of risks associated with new developments and low TRL components was not unexpected at the beginning of this study. Technology development and optimistic heritage assumptions that lead to more development than anticipated are clearly a risk driver for all of the subsystems, as is shown in Table 2. However, this category appears to be of relatively higher importance in certain subsystems than others. In the case of the Instruments subsystem, the importance of this risk category may be due to the fact that though high heritage from previously flown instruments is often claimed, the exact same instrument is never really flown twice. Even if the proposed instrument is identical to a flown instrument, it may be on a mission to an entirely new environment, for which is it not proven and where its capabilities are uncertain. In this case there is a Instrument subsystem risk that the assumption of heritage is optimistic, and that some new development and additional costs may still be required to ensure the instrument provides the needed capability in the new environment. This philosophy provides an explanation for the clear dominance of the Technology Development and Heritage category in the Instruments risk list. However, in the case of Mission Design, as launch is a known high-risk event for any mission, it is generally preferred to use a reliable existing launch vehicle. Only in cases of missions far in the future are new launch vehicles considered, as it can be assumed that launch vehicles currently in development will have been tested prior to the slated launch date. This is reflected in the risk categories in the Mission Design list – clearly, new development (as in 'Use of unproven launch vehicles', which is one subcategory of the Launch category) is not the main risk consideration for the Mission Design subsystem in Team X.

A second inference can be drawn using the Environmental risks category - which includes risks related to operating a mission in a harsh environment or a currently unknown environment, as well as other environmental effects – and also appears in the top risk categories for most of the subsystems. The Environmental category is notably absent in the ACS and Ground Systems lists. In the case of Ground Systems, Environmental types of risks were included within other categories such as Downlink/Uplink or Availability of Stations and Tracks (as Unavailability of ground stations due to weather effects, or loss of link due to mission environment). In the case of ACS, this is because the specification of the checklist was such that the risks were categorized and worded with more of a focus on the impacts (such as failure of sensor) rather than the cause of the risk (high radiation environment). The differences among the subsystems illustrate that the original checklist affects the outcome of the categorization process, as mentioned earlier. However, as the checklists were created in collaboration with the subsystem chairs, they can be assumed to be representative of how the subsystem chairs think about risk during a design session. As the goal of this research is to identify ways to assist the team members in identifying and assessing risks, recognizing the differences in their perspectives on risk is a key aspect of risk process improvement and will inform the risk mental model research currently underway.

The data also supports correlations between the role of each subsystem in the concurrent design environment and the risks identified by them. For example, 'leading' subsystems, which are the subsystems that make decisions with the greatest impact to the science requirements, e.g. Science, Instrument, Mission Design – are much less concerned

with critical failure of parts, and more concerned with uncertainties in capability in a given environment. This is seen in Table 3 in the relatively higher ranked Measurement Risk and Environmental categories in Science, or Technology Development and Heritage and Environmental in Instrument, and Mission Design Maneuver and Trajectory (which describe uncertainties in target ephemeris, or uncertain design assumptions during the study). Risks for other subsystems, such as ACS, Propulsion, Power, Telecom, CDS and Thermal, are dominated by redundancy/critical failure concerns, which is indicative of their design role to reliably fulfill mission requirements set by the leading subsystems. Risks noted for software are almost exclusively related to the potential reuse or inheritance of product line software. The Structures subsystem has both critical failure (i.e., Failure of critical separation, deployment) and uncertainty in assumptions (both Mass Volume Uncertainty and Uncertain design assumptions). As the Structures subsystem is tasked with estimating the mass and configuration of the spacecraft, the subsystem design is wholly dependent on the decisions made by other subsystems, and thus a primary concern is failures of major components/events. The early phase of the design also leads to considerable uncertainty in the mass of the spacecraft, leading to many risks related to being able to fit within a mass envelope.

The results presented here represent only a selection of the findings from the risk database study. There are many other valuable conclusions that can be obtained from the data, and will be used to improve the subsystem risk checklists in the future.

IX. Conclusion

There is significant variability in risk reporting in early conceptual design. While some of this variability is due to the inherently vague and uncertain state of the design in this phase, especially in a chaotic concurrent engineering team environment, it is also in part due to the lack of an organized risk identification and scoring process that would improve the level of consistency in risk reporting. Generating risk checklists that can be used for risk identification guidance during Team X studies will enable more consistent risk reporting. However, as this guidance may bias the resulting risk assessment, it is important to have a verified list of categories that span the major risk drivers for each subsystem. Analysis of the historical risk data from previous studies provides valuable insight into the relative importance of various risk categories to each subsystem, and may allow us to streamline the checklists and tailor them to each study and subsystem, thus enabling more efficient risk assessment. Access to the past risks also enables the leveraging of past mission information in subsequent studies. In addition, it is hoped that this initial cut at identifying common risks for science based space missions is of assistance to others who work in this part of the aerospace industry.

X. Future Work

The research presented here is only one step in improving the risk identification and assessment in Team X. The checklists will be updated based on the information results of the categorization of the risks presented in this paper. In the future, the risk categories in the checklists may be associated with specific study characteristics that would allow the risk analyst to provide tailored checklists for use during a study. The association of risk types with study characteristics would allow one to easily identify the potential key risk categories for each study quickly and easily. Analysis of the scoring of risks in the database is a future step that may help provide a basis for scoring guidance and consistency in risk scoring in Team X. A research effort into studying the risk mental models of concurrent engineers is also being undertaken to enable the effective use of the checklists and scoring guidance to the design team in the limited time available in a study.

XI. Acknowledgments

The authors thank the following Team X members who provided valuable input to this study: William Smythe, Alfred Nash, Mark Wallace, Robert Kinsey, Peter Meakin, Frank Picha, Ronald Hall, Michael Pugh, Greg Welz, Joseph Smith, Dwight Geer, Karen Lum, Jay Brown, Robert Miyake, Christopher Landry, Laura Newlin, Jared Lang, Joan Ervin, Robert Shishko. This task would have been much more difficult if not impossible without their assistance.

This research was conducted at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

References

[1] J. Jones, Supportability Engineering Handbook, McGraw Hill, 2007

[2] T. Bedford and R. Cook, Probabilistic Risk Analysis: Foundations and Methods, Cambridge University Press, 2001

[3] Stamatelatos, M., Rutledge, P., "Probabilistic Risk Assessment at NASA and Plans for the Future," Joint ESA-NASA Space-Flight Safety Conference, 2002, pp, 21-24.

[4] Stamatelatos, M., OCA, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC, 2002, pp. 1, 6-9.

[5] S. Cornford: "Managing Risk as a Resource using the Defect Detection and Prevention process", Proceedings, 4th International Conference on Probabilistic Safety Assessment and Management, 13-18 September 1998, New York City, NY.

[6] M. Feather, S. Cornford, J. Dunphy, K. Hicks, A Quantitative Risk Model For Early Lifecycle Decision Making, Integrated Design and Process Technology, IDPT-2002, June 2002.

[7] Warfield, K. and Hihn J., "Spreadsheets in Team X: Preserving Order in an Inherently Chaotic Environment", Proceedings of the 42nd Hawaiian International Conference on System Sciences (HICSS 42), Waikoloa, HI, January 5-8, 2009

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

[9] Conrow, E., Effective Risk Management 2nd Edition, AIAA, 2003.

[10] Malone, M. and Moses, K.. Development of Risk Assessment Matrix for NASA Engineering and Safety Center (NESC), Project Management Challenge 2005.

[11] Risk Management: Concepts and Guidance, Defense Systems Management College, FT. Belvoir, 1989.

[12] L. Cooper, How Project Teams Concieve of and Manage Pre-Quantitative Risk, Doctoral Dissertation, USC, 2008

[13] Hihn, J., Chattopadhyay, D., Shishko, R., "Risk Identification and Visualization in a Concurrent Engineering Team Environment,"Proceedings of the ISPA/SCEA 2010 Joint International Conference, 2010.

[14] Landauer, T. K., Foltz, P. W., & Laham, D.. Introduction to Latent Semantic Analysis. Discourse Processes, Vol 25, 1998.