TOWARDS RISK BASED DESIGN FOR NASA'S MISSIONS

Irem Y. Tumer
Francesca Barrientos
NASA Ames Research Center

Leila Meshkat
Jet Propulsion Laboratory

ABSTRACT

This paper describes the concept of Risk Based Design in the context of NASA's low volume, high cost missions. The concept of accounting for risk in the design lifecycle has been discussed and proposed under several research topics, including reliability, risk analysis, optimization, uncertainty, decision-based design, and robust design. This work aims to identify and develop methods to enable and automate a means to characterize and optimize risk, and use risk as a tradeable resource to make robust and reliable decisions, in the context of the uncertain and ambiguous stage of early conceptual design. This paper first presents a survey of the related topics explored in the design research community as they relate to risk based design. Then, a summary of the topics from the NASA-led Risk Colloquium is presented, followed by current efforts within NASA to account for risk in early design. Finally, a list of "risk elements", identified for early-phase conceptual design at NASA, is presented. The purpose is to lay the foundation and develop a roadmap for future work and collaborations for research to eliminate and mitigate these risk elements in early phase design.

INTRODUCTION

This paper describes the concept of Risk Based Design in the context of NASA's low volume, high cost missions. We define risk as anything that would prevent meeting mission requirements. Risk Based Design (RBD) is then a design process that formally identifies the risk elements from the onset, and continuously optimizes investments and decisions to mitigate those risks.

In most NASA efforts, risk is defined in terms of the likelihood and consequences of incidents that could result in hazards. Most RBD techniques at NASA are reliability analysis techniques applied to design. This approach, though of high value, is difficult to apply in the early design stages, where the models are vague, decisions are difficult to capture, probabilities are difficult to assign, especially in the case of low-volume, high-

cost NASA missions. Studies and design reviews have pointed to the early design stages as one of the best opportunities to catch potential failures and anomalies. Therefore, one of the aims of this work is to understand the current RBD attempts and identify the means to use RBD to avoid potential failures.

The concept of accounting for risk in the design lifecycle has been discussed and proposed under several research topics, including reliability, risk analysis, optimization, uncertainty, decision-based design, and robust design. A Risk Based Design Special Panel at the 2003 ASME International Design Theory and Methodology Conference put together experts in these fields, and put forward the challenge of applying design research techniques to start building a unified methodology for NASA's low volume and high risk mission design environment. An insightful outcome of this panel was an agreement that we need a unified effort to apply the research methods for effective use in early design. In this light, this work aims to identify and develop methods to enable and automate a means to characterize and optimize risk, and use risk as a tradeable resource to make robust and reliable decisions, in the context of the uncertain and ambiguous stage of early conceptual design, especially for NASA's low-volume, high-cost missions.

The end goal of this work is to enable risk informed design decision-making and trade studies throughout the process of design. To achieve this goal, one must: 1) understand the NASA design process, risk analysis, and the risk management efforts at NASA, 2) identify risks and failure modes related to design decisions, 3) enable making design decisions and choices based on the risk and failure information. To this end, the paper begins with a description of the early design process, followed by a description of the risk management efforts at NASA. The paper will then describe our current efforts to identify and account for risk and failures in early design. Specifically, we will first describe ongoing efforts to capture risks and decisions using a Risk Assessment Project (RAP) tool, followed by ongoing efforts to identify historical and potential failure modes at different stages in design, based on functional models. The utility and current state-of-the-art of visualization techniques will then be described to support these two efforts. The paper will conclude by presenting possible research areas to allow for making decisions based on risk and failure information, including optimization, decision-based design, ETC., and will set the path for future work in these areas.

UNDERSTANDING THE DESIGN PROCESS AND RISK MANAGEMENT AT NASA

Early Phase Design at NASA

Concurrent engineering teams greatly reduce the design time and costs. There are several real time concurrent design teams at the various NASA centers. One of these centers is the Advanced Project Design Center (TeamX) at the Jet Propulsion Laboratory. 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 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.

The engineers find a feasible conceptual design for a space mission to satisfy the customer requirements very rapidly. There are various modeling tools and techniques available to them for performing the necessary analyses. But ultimately many of the design decisions are based on expert opinions and there isn't sufficient time in the rapid design timescale for exploring the full option space. Rather, the team identifies a point design that satisfies the mission requirements. This is partially due to the fact that the existing high fidelity models are mostly at the subsystem level and the interrelationships between the different subsystems are not fully captured at the systems level.

Design decisions are made with consideration of risk, cost and performance. Nevertheless, from the final report, it is often unclear why certain design decisions were made, or what options were considered. Due to the lack of information about the rationale involved in making these decisions, it is not possible to verify the decisions or to make modifications to existing designs and reuse them for similar missions. Furthermore, the risk elements associated with the final design is (was) not adequately captured and described.

Due to the numerous dependencies that exist between the various subsystems in a spacecraft, and the speed with which the engineers make design decisions, it sometimes happens that the subsystem engineers are unaware of some important design choices of others. Since each design option correlates with particular types of risks, one way of keeping the engineers informed about the design options being considered is by informing them about the risks related to them dynamically.

Risk Analysis Efforts at NASA

There are various methods used at NASA that fall in the general category of risk-based design. NASA prefers the term *risk-informed* instead of *risk-based* because risk-based design augments rather than supplants classical design methods [PRA Guidelines]. *Risk Analysis* is used in design to evaluate alternative designs and relative risks of different subsystems. This identifies how risk might be reduced through design changes.

[Greenfield 2004] defines "risk" as something that would keep your team from meeting objectives. Analysis then includes determination of root causes, quantification of risk, its likelihood and consequences.

The traditional risk analysis tools include:

- FMEA – System and subsystem; bottom-up method
- FMECA – (Failure mode, effects and criticality analysis)
- FTA – Top-down assessment of risk and impacts rolled up from subsystem levels; system level

- ETA – Event Tree Analysis;
- RBD – Reliability block diagram
- MLD – Master Logic Diagram
- ESD – Event Sequence Diagram
- PRA – Probabilistic Risk Assessment
- Risk Elicitation – interviews
- Model-based –
- Checklists for identifying risks – based on collected wisdom

Expert elicitation is one of the primary means for predicting reliability and risk when developing new technologies. No hard data exists from previous designs. Essentially, one is forecasting risk. [Unal+2004] is an example of method for expert elicitation. This paper presents methodology for expert-judgment elicitation for launch vehicle conceptual design, addresses the problem of aggregating data from multiple opinions, and develops methods for calibrating and setting uncertainty distributions for the expert judgments.

Many traditional methods require a converged design. Many require that designers identity failure modes up front. FMECA does not analyze multiple failure interactions. Some, such as model-based PRA, are expensive to implement. Results, as in PRA, may be difficult to communicate. Some, such as FMECA, do not allow human factors to be considered. The classical approach to design is by using *safety factors*. The system broken down into design elements: systems > subsystems > components, and analyzed by discipline: thermal, fluids, controls. Design life is analyzed at component or cross-component level. In contrast, product reliability and safety are best analyzed at the *system* level, requiring integration across discipline boundaries. Requirements are driven by performance, cost, operations at system level. The design process requires a series of trades between conflicting requirements [Townsend+Smart1998]. A classical method for design is rule-based design, where a design is fine-tuned by reducing safety factor—e.g., by incorporating newer materials—or restructuring the design. By contrast, probabilistic methods fine-tune design by characterizing uncertainties in design and designing against those characteristics [Townsend+Smart1998].

By far the most common probabilistic trend is to use Probabilistic Risk Assessment (PRA) for risk analysis. Although appealing as a concept, the main shortcoming of PRA is that it uses low-probability and high-consequence events when not much statistical data exists. If events are possible but rare and the sample size is small, then they even may not appear in a statistical sample. PRA basically answers three questions: what can go wrong, how frequently will it happen and what are the consequences? [Stamatelatos 2002]. [Greenfield 2001] reports on application of PRA to designing upgrades to Shuttle and development and construction of ISS. Studies identify which element would produce biggest increase in safety if it were improved. [Stamatelatos2002] –also applies to conceptual design of 2nd gen RLV and Mars missions. [Jones+Dillon et al 2003] application to development of a testbed for manned space missions.
PRA as a concept is very different from classical methods so designers are often unsure about how to integrate it into design practice [Townsend+Smart]. The common complaints are difficulty to understand probability values especially when engineers and

managers lack formal training in probability and statistics, and, difficulty to deal with uncertainty. In order for PRA to be used in decision support, engineers and practitioners must have confidence in the PRA results, which can only result from a comprehensive set of scenarios and well-defined uncertainty distributions [NASA PRA Guidelines] [Stamatelatos 2002]. [Townsend+Smart1998] argue that probabilistic methods must be applied to component level before they are applied to system level. Component reliability data can predict system reliability, but system reliability data cannot as dependably define component reliability. They argue that that probabilistic methods are unproven and that system level methods are difficult to understand and have confidence in (in part because of so many assumptions) and that the best process for validating probabilistic methods is to start at the component level. Changing methods requires a change in *culture* as well as in methods.

There are various Risk Analysis tools in development for NASA applications, including Risk Analysis Tool and Risk Analysis Method: Risk analysis tool is an Integrated Logic Diagram [Bay-RMC], which is a kind of block diagram that integrates information from FTAs, FMEAs and other risk analyses. The tool also provides a cross-check on FMEAs. Color-coding of blocks visually highlights patterns in the types of risks present. Sorting is done by: how identified, who identified, what consequences are, how accepts risks, etc. Risk analysis method is an application of risk PRA to preliminary design of launch vehicles. It is a method for applying data from Shuttle risk assessment models to launch vehicle concepts. They use functional models to form analogs from shuttle to conceptual vehicles, then determine risk drivers, and use to evaluate alternative designs. [Fragola et al 2003]. This is a more generic framework for developing a database of heritage data with component failure rates or expert opinion is described in [Go+2003], integrating shuttle data, mission models, and component assemblies.

Risk Management Efforts at NASA

NASA's Risk Management Colloquium (RMC) brings together leaders from every management and technical areas who support and implement NASA's Risk Management Program. The colloquium, first held in 2000, was launched at a time when NASA was moving from a "rule-based" to a "risk-based" approach to safety and mission assurance. Under the rule-based policy, fixed design requirement drove project managers and engineers to spare no expense in developing missions and hardware to meet those requirements. Safety professionals employed reliability methods and qualitative risk assessment tools to uncover potential hazards, and then used all available resources to mitigate those hazards. In the mid-1990s the need to control costs while improving safety propelled NASA to adopt "risk-based" methods. The problem of meeting strict design requirements was recast into the problem of identifying and evaluating risks and then making informed decisions about the mitigation or acceptance of those risks. In other words, risk would be treated as a resource to be traded among project elements such as cost, schedule or technical performance. Under this new paradigm, risk management is folded into program management so that at each stage of project planning and deployment risk management plans are integrated into the project plan as a whole.

NASA's risk management program is based on a process known as *Continuous Risk Management* (CRM). Activities in the process occur in sequential stages that are repeated throughout the lifecycle of a project. CRM activities are formally defined in NASA guidelines as: *identify* risk issues and concerns; *analyze* risk through evaluation, classification and prioritization; *plan* risk mitigations and acceptances; *track* risk mitigation status using appropriate metrics; and *control* the process through reevaluating plans and using informed decision making. The aim of the program is to assure that all risks are assessed in a systematic fashion, that their mitigations or acceptances are documented, that planned mitigations are carried through, and that all risk information is documented and communicated to all levels of the program. The actual implementation of this process involves tailoring for each project. Risk managers, usually from the Safety and Mission Assurance community work with the project managers during the conceptualization and development of projects to build risk management activities into the project plan.

Because of advances in the field of risk management, the deployment of the formal risk management program continues to be a work in progress. Program managers and other organizational leaders improve their procedures, policies and organizational structures as they learn about new risk management methods and tools. The Risk Management Colloquium (RMC) provides a forum for attendees to share information on the progress of risk management implementations on different projects, views from different disciplines on risk, information about available processes, methods and tools, levels of personnel training and current issues in risk management deployment. In addition, NASA invites practitioners from outside NASA and its contractors, including representatives from the US Navy, and NASA partners such as the European Space Agency (ESA) and the National Space Development Agency of Japan (NASDA) to share their knowledge about risk management.

Safety is a high priority at NASA and a continually re-emerging theme in risk management. NASA's Office of Safety and Mission Assurance oversees the implementation of the risk management program, and Safety and Mission Assurance (SMA) personnel are responsible for supporting CRM planning and processes for each project. So, the people who developed the risk management policies and guidelines are the same people who are most concerned with system safety. The risk management program is also driven by findings from mishap, anomaly and mission failure reports, such as the 2000 Mars mission failure reports and the 2003 Columbia accident report. Findings from these reports are usually highlighted at RMC presentations and opening remarks. A major theme in these reports is the need for improvements in understanding and controlling risk as a means to ensure safety and mission success. So, although part of the aim of a structured risk management program is to optimize the use of resources in controlling risk, NASA expects the risk-based decision-making to provide equivalent or better safety than the displaced rule-based approach.

The technical disciplines represented at the RMC encompass various disciplines from systems engineering and hardware design to program management and information

technology security. The focus of the colloquium remains on risk management procedures applied to system safety and technical performance. This focus reflects the interests of the original RMC sponsors and of the core attendees, representatives from the SMA community. Over the years, the colloquium has seen increasing participation from practitioners from other disciplines, including reliability, acquisition, cost, schedule, organizational management, software design, human factors and information technology security.

Innovations in risk management tools are an important topic at each RMC. Most of the tools are aimed at the problem of risk identification and analysis. At the first RMC, a survey of available tools reviewed the well-established technical risk identification tools used by the systems engineering discipline: Failure Modes Effects and Analysis (FMEA) and Fault Tree Analysis (FTA). An evolution of FTAs is the Integrated Logic Diagram, which provides a method to summarize where mission-ending failures might exist and differentiates among the types of causes leading to failure. Other RMCs have reviewed the use of corporate knowledge tools, such as the Lessons-Learned Information System, a database containing 40 years worth of past failure and mishap data. More recently, these qualitative analytical tools and knowledge systems have been integrated into quantitative methods such as Probabilistic Risk Assessment.

Advances in Probabilistic Risk Assessment (PRA) methods are regularly presented at the RMC. An introduction to PRA methods was offered at the first RMC in 2000, the same year that NASA began its thrust toward developing a world-class in-house PRA capability. By this time other industries, especially the nuclear power industry, had established PRA as a principle technique for safety assessments, and had been improving its use over the previous two decades. NASA's impetus to investigate PRA methods came from the 1986 Challenger accident report asserting the need to estimate probabilities of failures on Shuttle elements and the 1988 "Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management" recommending immediate application of PRA methods to Shuttle risk management. During the 1990's, NASA conducted pilot studies of the use of PRA on Shuttle and International Space Station (ISS) development. Successful results from these studies eventually lead to NASA policies requiring use of PRA in Shuttle upgrades, ISS development and Mars mission design.

NASA's PRA activities include the implementation PRAs in risk management programs, continuing pilot studies, and research into new application areas. The RMC has seen presentations on the implementation of PRAs to risk management in ISS program development and ISS software design. The first PRA application to payload design was presented in 2002. NASA is still investigating risk-based design methods for payloads where, unlike the Shuttle or ISS, safety policy mandates the use of rule-based safety certification. Investigation of PRA into new areas continues, including areas such as trend analysis, acquisition, cost and scheduling. NASA also improves its own PRA processes by exchanging information with other government agencies and international partners.

Other tools that have been presented are aimed at supporting risk management activities beyond identification and analysis. These activities include tracking, communicating,

reporting, and archiving risks and decisions. The simplest of these tools are electronic checklists or questionnaires for use by project managers or independent reviewers. These checklists, based on databases or statistical analyses of previous mishaps, stimulate program managers or independent reviewers to systematically assess and track risks to particular projects. More sophisticated tools incorporate features for communicating risks to management or design team members. The most comprehensive tools are full-fledged commercial enterprise software systems designed to support operationalization of an organization's risk management program and integrate with project management software.

Research In DESIGN Risk AND FAILURE IDENTIFICATION AT NASA

Risk Assessment and Decision Capture Research

The goal of the effort described in this section has been to provide a systematic approach for the consideration of risk and design rationale throughout the lifecycle of a mission. The approach and corresponding process implemented in the team for this purpose is described in detail in [ref1, ref2, ref3]. A summary of this approach is presented here.

Approach

Our approach consists of two main parts: the tool and the process. On one hand, we designed, developed and implemented a distributed software tool to enable communication of the risk items and their related attributes. On the other hand, we defined a common risk dictionary for use by the team and developed a process for conducting risk assessment in the team. An overview of our approach is shown in Table 2. Initially, we defined the risk dictionary and iterated on it with the team. The team also helped us identify the software requirements; they included the ease of use and the interoperability with the Excel spreadsheets on which the whole software infrastructure is built. It was necessary for our process to be as minimally obtrusive as possible, due to the fact that the design sessions are intense and there is very limited time for additional work. The next step involved the design of the architecture for building the tool and the initiation of the process of "risk training" within the team. We iterated on the risk-related definitions and terms with the team members. Furthermore, the risk expert discusses the risk items implied by the design decisions with the individual engineers to facilitate the communication between them during the design sessions.

STEP ONE:	STEP TWO	STEP THREE	FUTURE STEPS
•Define Risk Terminology; •Define software requirements	•Design Architecture for Software tool •Initiate Process of "risk training" within team	•Develop prototype tool. •Train team members to use tool and refine tool using team feedback. •Determine role of risk chair/ approach for risk communication within team.	•Use tool concurrently during design. •Build standard risk item libraries to make consistent assessments across missions. •Refine tool •Add additional features; •Towards Probabilistic Risk Assessment in Conceptual Design

Table 1: Overview of approach for establishing risk assessment process in TeamX.

In the following section, we discuss the software tool and some of the experimental results obtained from it's use within the team

Risk & Rationale Assessment Program (RAP)

The RAP software tool is a distributed system that enables the communication between various designers using a Microsoft Excel interface. Figure 1 shows a screenshot of the RAP user interface. Once the RAP tool is installed on the computer, it can be initiated by pressing the button "New RAP sheet" that appears on the Excel toolbar. Then the user is given a menu of "studies", "roles" and "user-names". Once the user picks from that menu, the screen shown in figure 1 appears. In this screen, the study name is "Test" and the role "Risk". The user defies new risk elements by pressing on the "New Risk" button on the toolbar. This initiates the "New Risk Element" box shown in figure 1. The user then fills in the information about the risk and identifies the affected subsystems. In order to assess the risk, the user clicks on the fever chart button that appears next to the risk element title on the table. This is shown in figure 2.

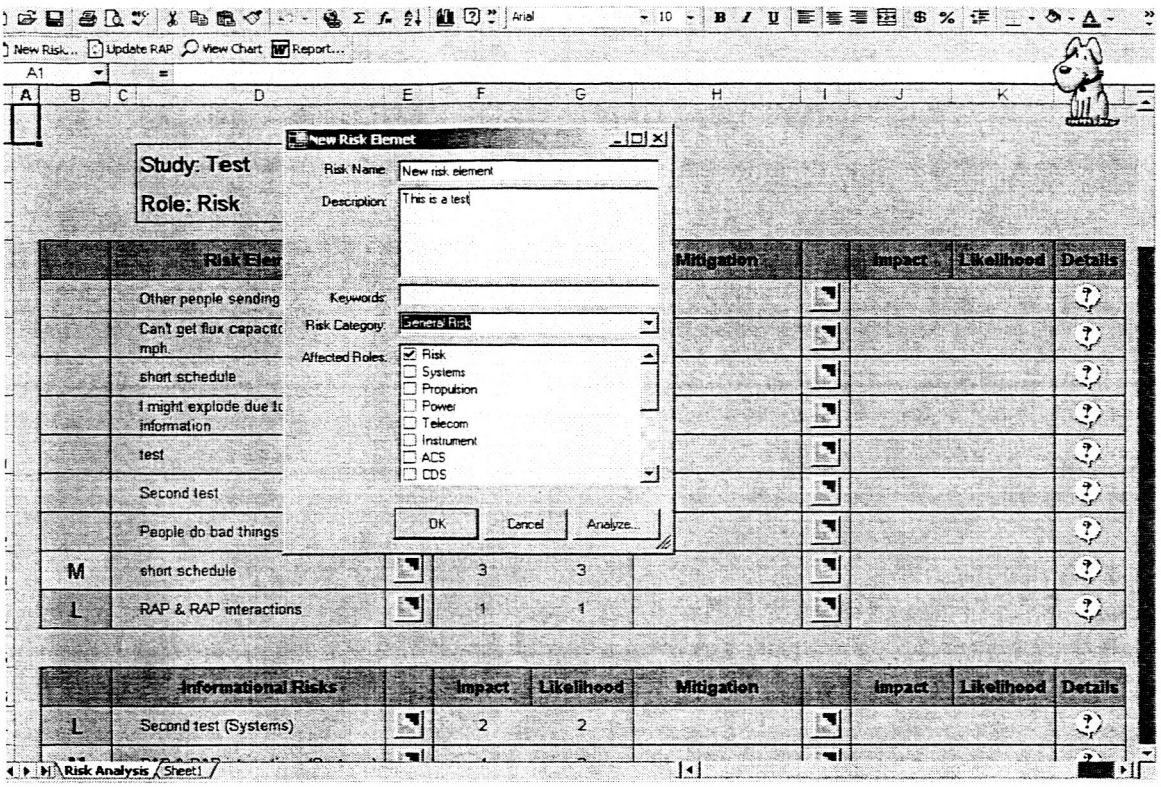

Figure 1: RAP screenshot showing the "New Risk Element" initiation process.

The second table shown on the user interface includes the attributes of the "Informational Risks". These are the same risks that the user in question initiated and sent to other subsystems by indicating their roles as being affected by them. The user can view the assessment of these risks by those subsystem experts and any information that they've included in their assessments by looking into the various attributes

The second fever chart button next to the "Mitigation" column collects information about possible mitigations and an assessment of the risk item in question after the mitigation has been applied. The users can indicate a mitigation to be "applied" or "suggested". In cases where mitigation is suggested, but not applied, it doesn't affect the residual risk of the item. Pressing on the "details" button on the right hand side column can capture other kinds of descriptions and/or explanations about the item. The information is communicated through a centralized database. The users click on the "Update Interface" button on the toolbar to send or receive information from the database.

The tool also provides the users with the capability to view the global risk profile for the mission at any point during the design process. By clicking on the "view chart" button on the toolbar, the user's can access the fever chart shown in figure 3. By selecting the roles of interest, the user can see the risk elements associated with those roles on the fever charts. Clicking on the subsystem acronyms on the chart then provides the user with the detailed information about the risk items associated with the subsystem.

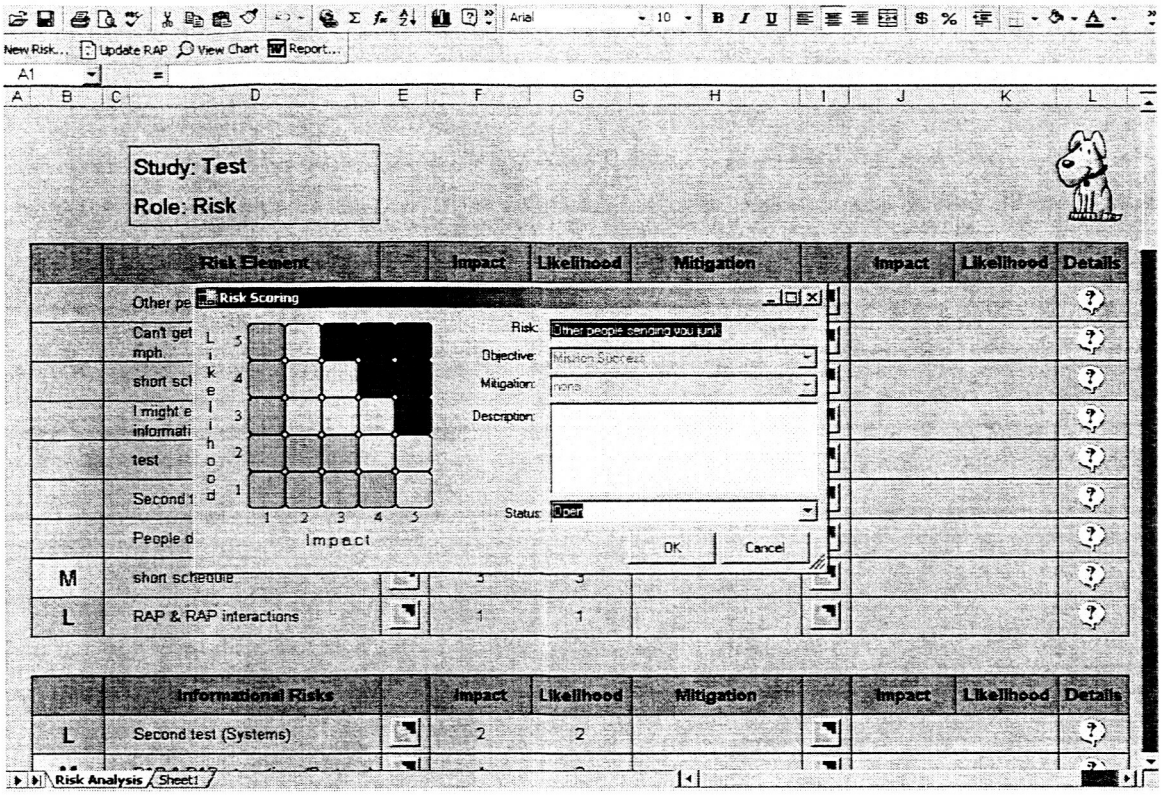

Figure 2: RAP screenshot showing the "Risk Scoring" process.

Finally, the tool has the capability of generating automated "Risk reports" based on information available on the spreadsheets. By clicking on the "Report" button on the toolbar, a report is generated in Microsoft Word. This report includes the fever chart, a table with all the risks as assessed by various subsystem engineers and an appendix including all the details about each of the risk items.

Experimental Results

The risk assessment process & tool explained earlier is currently being used in the team. It has been used for the risk assessment of numerous studies. These studies include "red team reviews" which are the most rapid type of study conducted in TeamX. Their time span is usually one full day and during this time the team reviews a preliminary design provided by the customer. The process helps the designers to communicate their risk items and keep on top of the design decisions made by other designers. It also helps develop better risk profiles for the missions.

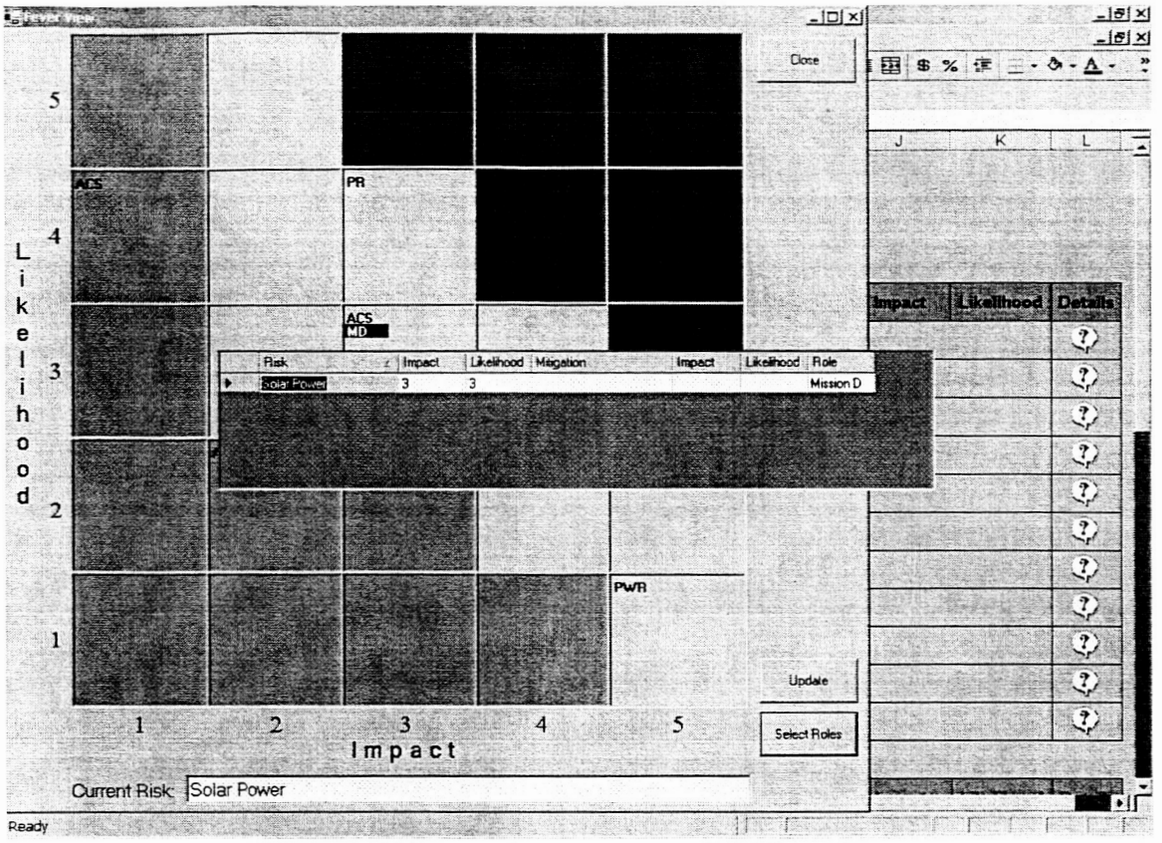

Figure 3: RAP screenshot showing the global fever chart.

Sample, Generalized Risk Elements from Team X

General Missions:

- Short schedule
- New Developments
- New Engineering
- New Technology (low TRL for the technology)
- Inability to fully test some new technologies (such as solar sails) on earth before space mission.
- COTS components
- Performance
- Integration (especially risky when different parts are provided by various vendors.)
- Interface issues
- Single point failures
- Complexities introduced by extra redundancy
- Assuming the success of ongoing missions and building on their heritage which may not be available at the time of mission deployment.
- Life issues for long missions.
- Radiation issues (especially for missions to high radiation environments such as Jupiter.)
- Custom designed components may have unexpected failure modes.

- Complex trajectories.
- Not achieving final orbit due to complex orbit.
- Loss of data.
- High error rate in data.
- Loss of communication.
- Loss of antenna.
- Distributed software development
- Touch and go Systems:
  - sample gathering.
  - Damage to the solar arrays.
- Rocket launches.
- Insufficient battery power
- Plume & pingment issues.
- Contamination issues (e.g. dust contamination.)
  - Damage to the solar arrays.

Comet Missions:

- Uncertainty about the environment.
  - Possibility of micrometeoroids.
  - Dust contamination of sensors, solar arrays and science instruments.
  - Uncertainty about the comet surface
- Landing and anchoring on the comet.
- Landing on a comet and taking off safely; this has been demonstrated on an asteroid, but not on a comet.

Planetary Missions:

- Environmental effects (for instance sulphuric acids on Venus)
- Failure during Entry, Descent, Landing
- Maneuver failure and missing the planet in case of fly-by's.
- Hitting the planet with RTG's.
- Planetary protection issues.

Missions Involving Landers:

- Poor aeromaneuvering.
- Hovering safely before landing.
- Failure of hazard avoidance technique
- Landing Unsafely
- Obstacle avoidance mechanism failure
- Uncertainty about collecting samples in unknown environments.
- Keeping the samples within the appropriate temperature range.
- Sample transfer chain
- Rendezvous with orbiter (if applicable.)
- Uncertainty of terrains.
- Nonexistence of desired science data on selected landing sites.
- Science Instruments inappropriate for conducting science mission.
- Science Instrument (e.g. Drill) failure.

Function-Based Failure Identification Research

Risk elements from function model-based failure modes from historical databases and knowledge of potential failures. EFDM/UMR work. Early design and later stages of design. Standard function and failure mode vocabulary with synonyms, etc. Tools for concept selection based on functional modeling. High level and detailed functional models and their correlation with failure modes.

Approach

Summarize the work so far...

Functional Basis and Models for Spacecraft Subsystems

give examples of functional models of star tracker high-level and low-level, and give examples

Failure Modes for Spacecraft Subsystems

(Irem)

List of FM from UMR collaboration so far.
Refer to papers.

Risk Visualization Research

Visualizations are useful when a designer is presented with a vast amount of information to be used in making decisions about a design. Visualization allows humans to quickly find patterns and aberrations in complex data sets [Card+Mackinlay+Schneiderman]. In risked based design, the two types of data sets of interest are the risk data and the design space data. Risk data is analyzed in order to find risk drivers in designs or to compare risk among competing designs. As methods for incorporating risk into design optimization improve, visualizations of the design trade space will be needed to help engineers make decisions about how to trade among design elements. Finally, the combination of human visual search with automated search may prove to be more powerful than automated optimization alone.

The data associated with risk has a multitude of facets, such as type of consequence, relation to mission objectives, which subsystem it belongs to, which phase of the mission it impacts, how it was identified, which technologies mitigate it and to what degree, etc. It is important to be able to classify the risk in different ways so that various risk and discipline experts can find relevant risk information [Bay]. The Integrated Logic Diagram [Bay] attempts to differentiate among risks in a tree-type visualization by coloring nodes according to risk. Traditionally risk analysts use static graphics such as scatter plots, stacked bar charts and risk plots to show patterns in the data. For large data sets interactivity is required to find these patterns in the first place. Information visualization researchers have shown how adding interactivity to static graphics substantially increases its effectiveness in data analysis tasks [Dix+Ellis]. The DDP tool [cornford ref?], a risk analysis tool developed at JPL, follows this route and adds interaction to bar charts and risk plots to analyze complex risk data. This is merely a first step. Additional visual data mining [keim] techniques are needed to find the information buried in NASA's vast risk knowledge bases. Developing appropriate visualizations will require research into understanding the needs of risk-based design system users.

Designers will need to explore the design space in order to find suitable performance trades to optimize risk. Some researchers assert that during the early stages of design, designers are best served by being able to see and critique examples of possible designs [Pu+][Balling]. Visualization supports designers by graphically presenting the space of possible designs and providing tools for the designer to interactively examine the structure of the design space. Many multi-dimensional visualization techniques have been developed, and most visualization packages implement several of these techniques into an integrated data analysis application. High-dimensional visualization techniques include glyph plots, scatter matrices, parallel coordinates, child windows, brushing, interactive histograms and linked displays. Examples of such applications include XmdvTool [Ward] , Influence Explorer [tweedie+spence+et-al96] and [witenbring+Pang+Lodha1996???] . An important structure to find in the design space is the Pareto Frontier. In the tool described in [Stump et al 2002/2003], users can color designs with respect to their relationship to the Pareto Frontier. [Pu+Lalanne] describes a novel visualization for balancing among a number preferences instead of showing the Pareto Frontier explicitly.

When using optimization, constraint satisfaction or other design space search tools, real-time visualization allows the designer to watch the running search algorithm and intervene in the search process. This interleaving of automated and manual search takes advantage of the computer's ability to search rapidly and the human's ability to search using knowledge that is not easily formulated into a numeric objective measure. In the design literature, such techniques are called *computational steering* or sometimes *design steering*. An early attempt at interactive optimization is described in [Afimiwala+Mayne] while more recent advances from the multi-disciplinary optimization field include [Messac+Chen] and [winer+bloebaum????]. Interaction features can include the ability to move the starting point of the search algorithm, as in [eddy+lewisAIAA2003] [eddy+lewis-detc2002]. In the field of intelligent user interfaces, [Anderson et al AAAI2000] have studied this same interaction feature in what they call the *human-guided simple search* paradigm. [Pu+Lalanne] have developed intelligent interfaces to allow designers to select from a set of search algorithms, monitor running algorithms and re-order constraints in a configuration design application.

FUTURE WORK: MAKING DESIGN DECISIONS BASED ON RISK AND FAILURE INFORMATION

Decision based design and Robust decisions work

(Irem)
(http://dbd.eng.buffalo.edu/position.html)
http://www.eng.nsf.gov/dmii/Message/EDS/ED/ed.htm
Robust Decisions http://www.robustdecisions.com/

Optimization In Engineering Design

(Irem)

Uncertainty in design

(Irem & Francesca)

Optimization, decision based design, etc.; combination of efforts to make them work for the NASA problem. What would be the most important contributions for the specific problems NASA is facing? How can we leverage ongoing academic work?

References:

Risk Colloquium summary, risk management (see Zang at LaRC)
Goddard...IMDC? Carmel Conaty?

Cornford and Meshkat papers at JPL (see AIAA paper refs): Team-X, DDP
Risk management at NASA (Risk colloquium summary).
Include JPL (Cornford, Leila, etc., PDC, Team-X), LaRc (Zang?), Goddard (IMDC), in the survey.

Uncertainty/Probabilistic design/reliability:
The following fall in this category of applying reliability based design; however, these do not work at the early stages of design, work with detailed models. (see Vanderbilt report)
Zang at Langley: mostly probabilistic design, uncertainty propagation, for aircraft, airframe, CFD, etc. Monte Carlo, etc.
Needs and opportunities for risk based multidisciplinary design technologies for aerospace vehicles. NASA TM, 2002? Hemsch, Hilburger, ..., Sharon Padula, etc.
System risk assessment and allocation in conceptual design
Mahadevan and Smith, Vanderbilt
NASA/CR-2003-212162
Fragola
Zang
Townsend & Smart

Decision based design:
Mistree, Linda Schmidt, Kemper Lewis, Wei Chen, Bill Wood, George Hazelrigg, etc.

Optimization:
??? Same as decision-based design in most cases
BALAZS, M.E., PARKS, G.T. and CLARKSON, P.J. (2000) 'Survey on the status of design optimisation research and practice', Cambridge University Engineering Department, Technical Report CUED/C-EDC/TR99
SMITH, J. and CLARKSON, P.J. (2000) 'A method for the improved robustness of mechanical design' in Engineering Design Conference (EDC 2000), Brunel University, Uxbridge, 555-562
BALAZS, M.E., PARKS, G.T. and CLARKSON, P.J. (2002) 'Optimisation in industry - what does industry really need?' in Optimisation in Industry, 1, 15-24
SMITH, J.S. and CLARKSON, P.J. (2001) 'Improving reliability during conceptual design' in 13th International Conference on Engineering Design (ICED 01), Glasgow, Scotland, UK, Design Methods for Performance and Sustainability, 83-90
LIU, J-S., PARKS, G.T. and CLARKSON, P.J. (2002) 'Optimisation of turbine disk profiles by metamorphic development' in ASME Journal of Mechanical Design, 124 (2), 192-200
Judy Vance

Robust Design:
Dave Ullman, Dave Kazmer, etc.
Padhke's textbook
Uncertainty in design:
Erik Antonsson, Maria Yang, Chris Paredis, etc.

Fitch, P., J.S. Cooper, "A method for understanding uncertainty in Design for Environment," Submitted to Research in Engineering Design (2003).

From Francesca's risk notes:

NASA Documents
{recheck how current this list is!}

NPG 7120.5 – NASA Program and Project Management Processes and Requirements
"The program or project manager shall apply risk management principles as a decision-making tool which enables programmatic and technical success"

NPG 8715.3 – NASA Safety Manual
"Purpose of risk assessment is to identify and evaluate risks to support decision making regarding actions to ensure safety and mission assurance"

NPG 8705.x- {double check} PRA Application Procedures and Guidelines

NPG 8000.4 – {double check} Risk Management Procedures and Guidelines

NSTS 222-6 [Space Shuttle]

SSP 30235 [ISS]

Tools

Databases used to track risks in project development [Pereira 2003] in ISS.

Databases to track lessons-learned [Clawson+Oberhettinger2001] Lessons-learned drawn from significant events from which lessons can be learned that can be applied to future projects. {Also reference from RMC} These can arise from problems and failures, but [Clawson+] emphasizes the importance off successes that should be repeated.

DDP [refs??] tool for organizing, managing, and optimizing risk tradeoffs. Organizes very large projects. Need to find risk drivers. Compare different designs. Find holes during risk elicitation and aggregation.

Future

NESC

Unused

[Rose- Risk Management at the Total Project Level] [Rose – risk management fro JPL Flight projects]Description of risk management at JPL.

[Adams] – reviews literature on organizational culture and safety. Survey done for LaRC.

[Baron+Pate-Cornell] Discusses a decision support framework for tradeoffs between safety and productivity over product lifecycle. Uses probabilistic mode.

[Markeset+Kumar] Trying to improve life-cycle cost analysis by incorporating methods from risk analysis.

[Kaye+Sobota] sort of the Air Force Faster/Better/Cheaper program

[Dean et al] Method for estimating cost risk.