Proceedings of IDETC 2005
September 24-28, 2005, Long Beach, California, USA

DRAFT–DETC2005-85100

TOWARDS RISK BASED DESIGN (RBD) OF SPACE EXPLORATION MISSIONS: A REVIEW OF RBD PRACTICE AND RESEARCH TRENDS AT NASA

Irem Y. Tumer[1]
itumer@mail.arc.nasa.gov

Francesca A. Barrientos
francesca.a.barrientos@nasa.gov

Ali Farhang Mehr
amehr@email.arc.nasa.gov

Complex Systems Design Group
Intelligent Systems Division
NASA Ames Research Center
Moffett Field, CA 94035

ABSTRACT

This paper describes the concept of Risk Based Design in the context of NASA's low volume, high cost missions. The issue of accounting for risk in the design lifecycle has been heavily discussed in the literature under several research topics, including: reliability, risk and uncertainty analysis, optimization, decision-based design and robust design. Due to the risky nature of space missions, NASA centers have adopted a variety of techniques – developing tools, procedures, and guidelines to mitigate risk. Most of these techniques, however, require significant amounts of detailed and possibly quantitative information, making them inapplicable to early stages of design, where the requirements and models are vague, decisions are tentative and probabilities are unknown. This survey paper first presents a brief description of a design environment at NASA as well as current risk-based design practices and methods. Then, a summary of the topics from the NASA's Risk Management efforts is presented, followed by current research efforts within NASA to account for risk in the early stages of design. The purpose of this paper is provide a survey of NASA's capabilities (or lack thereof) in accounting for risk in the early design phase. This work lays the foundation for more effective collaborations between NASA researchers and academic research community.

INTRODUCTION

In most NASA efforts, risk is defined in terms of the likelihood and consequences of incidents that could prevent a mission or mission system from meeting its objectives. In this context, *Risk Based Design (RBD)* can be defined as a design process that formally identifies the risk elements during the mission design phase, and continuously optimizes investments and decisions to mitigate those risks. Since risk analysis tools cannot be used as the only basis for design decision-making, NASA often prefers the term *risk-informed* instead of risk-based design (Stamatelatos et al, 2002.) In this paper, these two terms are used interchangeably.

This paper is intended to lay the groundwork in understanding the challenges of incorporating RBD into NASA's low volume and high-risk mission design environment and to identify promising research directions, based on several findings:

- Most RBD techniques at NASA are reliability analysis techniques applied to design. This approach, although of high value, is difficult to apply in the early design stages, where the models are vague, decisions are difficult to capture and probabilities are difficult to assign. Studies and design reviews have pointed to the early design stages as one of the best opportunities to catch potential failures and anomalies (Mahadevan and Smith, 2003). Therefore, one of the aims of this work is to understand the limitations of current RBD practices applied during the conceptual design phase.
- There is a conspicuous need for more advanced risk-informed methods to characterize, balance and minimize risk in the uncertain and ambiguous stages of conceptual design. Such methods will treat risk as a tradable resource that can be used to make robust and reliable design decisions.
- To achieve this goal, one must: 1) understand the NASA design process, risk analysis practices and the risk management efforts at NASA; 2) identify risks and failure

[1] Corresponding Author. Phone: 650-604 2976.

modes related to design decisions; 3) enable making design decisions and choices based on the risk and failure information.

This paper does NOT aim to provide a comprehensive survey of all risk analysis and management methods in the literature (for review of such methods, see for instance, Schrader et al. 1993, Zang et al. 2000, Backman 2000, Choi 2001, Du and Chen 2002, Smith and Mahadevan 2003). Instead, we will focus on introducing those risk-based design methods that are currently used in various NASA centers. Further, we aim to outline the ongoing risk management research at NASA – setting the path for more effective collaboration between NASA researchers and the academic research community.

The paper begins with a description of a conceptual design team at NASA, followed by a description of the risk analysis and management efforts in the organization (Section 2). Section 2 also includes a brief overview of NASA-led Risk Management Colloquium that provides a platform for practitioners to collaborate and exchange ideas. Section 3 concludes the paper by presenting possible research areas that, in our opinion, have not yet been fully explored for potential application in mitigating risk of NASA's space exploration missions.

CURRENT DESIGN ENVIRONMENTS AND RISK MANAGEMENT PRACTICES AT NASA

The effectiveness of RBD requires a meshing of the design process with risk analysis and decision-making techniques. Further, accounting for risk in design occurs within the larger context of project risk management. Since we have identified early stage design as an important target of this research, we will describe one such design environment at NASA. Then we will briefly present the current state of risk analysis and risk management practices at NASA.

Early Conceptual Design Environments at NASA

Concurrent engineering teams greatly reduce the time and costs associated with the early design study of space exploration missions. There are several real time concurrent design teams at the various NASA centers. One of these centers is the Advanced Project Design Center at NASA's Jet Propulsion Laboratory, which houses a group of experts known as Team X. This team produces conceptual designs of space missions for the purpose of analyzing the feasibility and estimating the cost of mission ideas proposed by its customers. The customers often consist of principal investigators of design teams who plan to submit 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.

In the following, we summarize 3 major factors that make a straightforward application of most conventional risk-assessment techniques to Team X and other similar early concurrent design teams very difficult (if not infeasible):

1. In Team X, the engineers must rapidly find a feasible conceptual design for a space mission to satisfy the customer requirements. There are various modeling tools and techniques available to them for performing the necessary risk analyses (Rose 2000, Cornford 1998, Krasich 1995). But ultimately many of the design decisions are based on expert opinion. There is rarely sufficient time in the rapid design time scale for exploring the full option space and the corresponding risk elements. Rather, the team identifies a point design that satisfies the mission requirements. This is partially due to the fact that high fidelity models exist mostly at the subsystem level and the interrelationships among the different subsystems are not fully captured at the systems level.
2. 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 are not adequately captured and described due to a lack of standardized approach or taxonomy.
3. Due to the numerous dependencies that exist between the various subsystems in a spacecraft, and the speed with which the engineers make design decisions, the subsystem engineers are sometimes unaware of the important design choices of others. Since each design option correlates with particular types of risks, the only way to keep the engineers informed about the design options under consideration is by informing them about the risks related to them dynamically (i.e., live information feed).

This fast-paced concurrent engineering design environment is a special, but important, case of the overall NASA design process. We describe it here because of our focus on the conceptual design phase. In the next section we discuss risk analysis tools used by NASA in other phases of the design process. A description of NASA's design and development processes can be found in (Chao et al, 2004 and Chao et al, 2005.)

Risk Analysis during the NASA Design Process

NASA uses a wide variety of risk identification and analysis methods that fall in the general umbrella of risk-based design. Failure and risk analysis methods range from traditional reliability-based tools to more recent probabilistic risk

assessment (PRA) methods. Other tools are meant to help engineers consider risk while they design. These tools range from simple checklists to software knowledge bases. The concurrent engineering process has also driven innovation in risk analysis methods, forcing engineers to consider risk before a design reaches convergence.

Traditionally, NASA engineers and managers use reliability methods during the design process to locate critical subsystems or components in a design. Periodically a system is evaluated for failures as a whole, as it is during various design reviews. Analysis results identify how the likelihood of failure might be reduced through design changes. Examples of the most commonly used methods are, among others: Failure Modes Effects Analysis (FMEA), Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). These basic techniques continue to evolve and have spawned other techniques such as the Failure Modes and Critical Effects Analysis (FMECA), Event Sequence Diagrams (ESD), Reliability Block Diagrams (RBD) and the Master Logic Diagram (MLD).

These traditional reliability-based methods, and especially bottom-up methods, work hand-in-hand with the classical *safety factor* approach to design. In this approach, a design is fine-tuned by either reducing the safety factor—e.g., by incorporating newer materials—or restructuring the design. A major shortcoming to this approach is that the analysis methods do not guide the engineer in design decision-making. These decisions include selecting among alternative designs while trading-off risk with other objectives such as weight, cost and performance. This is a particular problem for NASA where cost and weight constraints are more severe than in other industries.

Another challenge for risk analysis methods is integrating with an evolving design process environment. Many require a fully converged design, so they integrate well into a system design process with major review stages, but these same methods cannot be applied during earlier phases when tenuous design decisions are made and withdrawn rapidly. Other methods cannot account for emerging classes of risk. For instance, FMECA does not analyze multiple failure interactions or human factors elements. Finally, some methods require that designers identify failure modes up front.

Probabilistic risk analysis (PRA) methods provide a framework to guide design decision-making during the design process. This approach to risk assessment that answers three questions: what can go wrong, how frequently will it happen and what are the consequences? (Stamatelatos et al, 2002). With PRA methods, decision-makers can use risk metrics to prioritize risk drivers, rank design alternatives and allocate resources appropriately.

NASA has funded many major PRA design methods program since the mid-1980's. Partial impetus to develop PRA arose 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. Early funded programs included the PSAM Project, the PFA Methods Program, probabilistic methods and the QRAS tools [Townsend and Smart, 1998]. Some of these tools, such as the finite-element program NESSUS produced by the PSAM project, combine a probability framework with design parameter sensitivity analysis. During the 1990's PRA was applied to designing upgrades to the space shuttle (Greenfield 2000), conceptual design of second-generation Reusable Launch Vehicles (RLV's) (Go et al 2003) and development of a testbed for manned space missions (Jones et al 2003). These more recent developments attempt to situate PRA methods into early mission design and the spiral design process.

Although appealing as a concept, the main shortcoming of applying PRA in the NASA environment is that it must assess 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. NASA's low-volume production environment often does not generate statistically significant design data.

In order for PRA to be used in decision support, engineers and risk analysts must have confidence in the PRA results. A comprehensive set of scenarios and well-defined uncertainty distributions supports this confidence in analysts (Stamatelatos et al, 2002). However, PRA as a concept is very different from classical methods and therefore, designers are often unsure about how to integrate it into design practice (Townsend and Smart, 1998). PRA methods present engineers with characterizations of uncertainty, which does not translate directly into design decisions. Further, as a system level method, PRA results are difficult to understand and instill confidence in (partly because of so many assumptions). In fact, the best process for validating probabilistic methods is to start at the component level. Especially in the rapid pace of early design, designers do not have the resources to work through complicated risk analyses. PRA advocates suggest that risk analysts should continue to work shoulder-to-shoulder with design engineers to interpret the results of analyses.

A different direction in risk analysis is the use of knowledge-based methods for understanding risk. We consider knowledge-based methods to include everything from simple guidelines made up from the collective wisdom of expert designers to knowledge-based software incorporating expert systems. Indeed, PRA methods must rely on knowledge bases of quantitative data in order to derive their probabilities. Checklists are a lightweight method to identify risk and potential failures (Rose 2000.) NASA also expects its managers and engineers to use knowledge contained in the Lessons-Learned Information System (LLIS) [nasa7120.5b], and JPL has formalized a process for using their Center's lessons learned system (Clawson and Oberhettinger, 2001). Other databases for reporting anomalies, failures and problems exist

at NASA, which provide potential sources of information that can be used to inform knowledge-based software. Developing methods to mine this data is still an open research problem. Other tools attempt to present knowledge in a way that is immediately useful by the design engineer, such as the Risk Balancing Profile Tool (Greenfield 1999) and DDP (Cornford 1998.)

Finally, NASA personnel are the most important knowledge bases to tap. Expert elicitation is one of the primary means for predicting reliability and risk when developing new technologies, particularly when no hard data exists from previous designs. Unal et al (2004), for instance, present a detailed methodology for expert elicitation—addressing the problem of aggregating data from multiple opinions, and developing methods for calibrating and setting uncertainty distributions for the expert judgments. Another problem that needs to be solved is locating appropriate experts across the geographically distributed NASA centers and partner locations.

Once the risk is analyzed, it must be managed in order to mitigate the overall risk of a space mission. The following subsection reviews current risk management efforts at NASA.

Risk Management Efforts at NASA

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 (SMA) groups, work with the project managers during the conceptualization and development of projects to build risk management activities into the project plan.

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 NASA's risk study presentations and memos. 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.

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. Therefore, NASA holds *Risk Management Colloquiums* (RMC) to bring 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* (SMA). 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-informed" 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.

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 (held in 2000), 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). Integrated Logic Diagrams have also been recognized as an evolved version of FTA's, wherein block diagrams are used to summarize where mission-ending failures might exist – differentiating those that may lead to failure. Other RMC's 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 also 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. 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 the use of PRA in Shuttle upgrades, ISS development and Mars mission design.

RMC also features presentations on risk management activities beyond identification and analysis. Examples include: tracking, communicating, reporting, and archiving risks and decisions. As a simple example consider an electronic checklists or questionnaires that can be used 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 to integrate with project management software.

RISK BASED DESIGN RESEARCH EFFORTS

This section describes two ongoing risk-informed design projects at NASA: 1) *Risk & Rationale Assessment Program* (RAP) at Jet Propulsion Laboratory; and 2) *Function-Based Failure Identification Research* at NASA Ames Research Center. These two projects are examples of initial attempts by NASA to account for risk and uncertainty early in the design process.

Qualitative Risk Assessment Research

In an effort to qualitatively extract risk information from system designers during the Team-X early concurrent design process, a *Risk & Rationale Assessment Prototype* (RAP) was developed at NASA's Jet Propulsion Laboratory as an example of initial attempts by NASA to account for risk early in the design process.

The goal of the effort is to provide a systematic approach for the consideration of risk and design rationale throughout the lifecycle of a mission (for a detailed description of the application of this approach in JPL Team X environment, see Meshkat, Cornford et al. 2003; Meshkat, Feather et al. 2003; Meshkat and Oberto 2004). The approach consists of two main parts: a process and a tool: 1) The process includes a risk dictionary and a methodology for conducting risk assessment in the Team X design environment; 2) The tool is a distributed software system, designed and developed to enable communication of the risk items and their related attributes.

The RAP software tool is a distributed system that enables the communication between various designers using a Microsoft Excel interface The tool relies on the user to fill in the information about the risk and identifies the affected subsystems. In order to assess the risk, the user clicks on a fever chart button that appears next to the risk element title on the table. 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 selecting the roles of interest, the user can see the risk elements associated with those roles on the fever charts. Finally, the tool has the capability of generating automated "Risk reports" based on information available on the spreadsheets. 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.

Function-Based Failure Identification Research

In an effort to introduce consideration of risk due to potential operational failures early in the design process, a *Function-Failure Design Tool* is under development at NASA's Ames Research Center. The goal of this work is to enable the gathering and assessment of potential failures modes for a given functionality of the desired component, subsystem or system, during the early stages of conceptual design, and to enable making tradeoffs in functionality and concept selection to avoid potential failures (Tumer and Stone, 2003; Stone et al, 2005; Stock et al, 2005.) The method results in risk elements in the form of "potential failures" for each functional description. The failure modes are gathered from historical databases and knowledge of potential failures. A broadly applicable step-by-step process can be followed to develop detailed function-failure information such that it can be used at a more abstract level for assessing failure potential during the conceptual design of subsystems.

To enable the use of this approach, the NASA team is currently working with a design repository tool, developed at the University of Missouri-Rolla in collaboration with NIST, and adapting it for the function-failure design method (Bohm and Stone, 2004.) In the course of looking through various anomaly databases and gathering potential failures modes from FMEAs, etc., a detailed list of elemental failure modes has been generated for mechanical and electrical failures. This list is currently being mapped to higher-level problem descriptions to better match the team-X design phase. The goal is to map the higher-level failure mode and failure effect descriptions to the risk elements generated from a qualitative risk elicitation approach (e.g., the RAP tool.)

POTENTIAL AREAS OF RBD RESEARCH

Knowing the scope of current risk-based design efforts at NASA, one may raise the question of which other areas of risk-related research have not yet been effectively tackled for space exploration missions. As mentioned earlier in this paper, the literature is fairly rich in this area of research; however, NASA is far from implementing a comprehensive risk-informed design tool that can be used practically in all phases of conceptual design for low-volume high-cost space missions. As such, one of the purposes of this paper is to identify relevant research areas that can be leveraged to develop a risk based design framework for NASA. In this section, we highlight a few research areas, which although seem promising, have not yet been thoroughly investigated for possible application to NASA's conceptual design environment. Needless to say, this is by no means a complete list. There are other areas of risk-related research that may be potentially applicable to space missions but are not included in this paper, and will be explored in fuure work.

Risk Visualization

This is a fledging area of research at NASA. Visualization methods are useful when a designer is presented with a vast amount of information that must be used to make a decision. In the context of risk management, for instance, designers will need to explore the design space in order to find suitable performance and failure trades to minimize 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 and Faltings, 2003; Balling 1999). Visualization, therefore, supports designers by graphically presenting the space of possible designs and providing tools to examine the structure of the design space. This will allow them to quickly find patterns and aberrations in complex data sets. 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, however, interactivity is required to find these patterns in the first place. Information visualization researchers have shown that adding interactivity to static graphics substantially increases its effectiveness in data analysis tasks (Dix and Ellis, 1998). The DDP tool (Feather 2002; Feather et al. 2002), 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 2002) techniques are needed to find the information buried in NASA's vast risk knowledge bases. Developing appropriate visualizations will require substantial research into understanding the needs of risk-based design system users.

Multi-Objective Optimization of Space Missions (with risk as an objective)

A space mission design problem, like any other real-world engineering design problem, can be posed as a multi-objective optimization problem with several conflicting objectives and constraints. For instance, the pressure vessel designer wants to maximize the engine fuel capacity, the control engineer wants to maximize the effectiveness (and therefore the weight and volume) of the control modules, the structural engineer wants to maximize the stiffness, the risk analyst wants to maximize the safety, and the project manager wants to minimize the overall weight of the entire system. Obviously, many of these objectives are at least partially conflicting – resulting in tradeoffs between multiple design criteria. There has been a growing attention to this area of research in the literature in recent years (For comprehensive survey, see among others: Steuer 1986, Deb 2001, Collette and Starry 2003). In the presence of multiple objectives, there is no unique solution to the design problem. Instead, a set of optimal solutions known as Pareto set represents all possible best solutions to such tradeoff problems. Researchers in many areas have embraced the concept of formulating risk as an additional objective, which can be traded for other objectives in a multi-objective Pareto set (see for instance Steuer et al. 2004 for application of multi-objective optimization in the context of risk-return tradeoff in portfolio theory). There have been, however, relatively few attempts to formulate multi-objective design optimization problems for aerospace systems (e.g., among others, Martin and Crossley 2002, Hassan and Crossley 2002, Tapetta 2000). NASA, therefore, still lacks a formalized and universal design tool that can quantitatively formulate an aerospace system design problem as a multiobjective optimization process, and tradeoff risk in a multi-objective sense. Indeed, Sobieksi and Haftka (1997) state that despite the multiobjective nature of aerospace systems, there are very few papers that take a multiobjective design optimization approach to address them. A current effort at NASA Ames is looking into risk and uncertainty based quantification of functional failures and the associated reallocation of resources to mitigate the risks due to these failures (Mehr and Tumer, 2005b.)

Multi-Level Hierarchical Risk Minimization

NASA's complex systems can be often better understood in a hierarchical abstraction, where the entire system is decomposed into subsystems and then into components in a systematic and top-down architecture. Objectives, variables, and constraints can be defined at both system and subsystem levels. In one of the first attempts to develop a formal method for optimization of NASA's aerospace systems, researchers at NASA Langley and their affiliates have developed a Bi-Level Integrated System Synthesis (BLISS) that optimizes such complex systems in a bi-level fashion (e.g., Sobieski et al. 2000). However, in the context of multi-level risk management,

NASA has yet to devise a formal method to systematically track, correlate, and minimize risk at all levels, i.e., from component-level failure to subsystem-level and system-level risks and uncertainties. A current effort at NASA Ames Research Center aims at rearranging current models of Integrated Vehicle Health Management (IVHM) systems in a hierarchical architecture that can then be used to minimize risk in a bi-level optimization fashion (Mehr and Tumer, 2005a). This is an area of potential research contribution that, although of paramount interest to space mission designers, has been scarcely addressed by researchers within or outside NASA.

Human Guided Design Steering (Optimization)

When using design 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 and Mayne, 1979) while more recent advances from the multi-disciplinary optimization field include (Messac and Chen, 2000) and (Winer and Bloebaum, 2002a and 2002b). Interaction features can include the ability to move the starting point of the search algorithm, as in Eddy and Lewis (2002). In the field of intelligent user interfaces, Anderson et al (2000) have studied this same interaction feature in what they call the human-guided simple search paradigm. Pu and Lalanne (2002) 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. As methods for incorporating risk into the design optimization process improve, advanced multidimensional visualization of tradeoffs (Pareto set) will be needed to assist the engineers in making design decisions. Finally, the combination of human-guided search with automated search may prove to be more powerful than automated optimization alone.

Risk Management in the Context of Decision-Based Design

Decision-Based Design (DBD) is an interpretation of the design process as a sequence of decisions (See for instance, Shupe and Mistree et al. 1990, for comprehensive review of DBD methodology). In DBD, the major role of a designer is to make decisions in the ambiguous, uncertain, and risky phases of design (Henk et al, 2003). There is a striking similarity between risk management and DBD in that they are both based on the concept of objective and structured decision making processes. In fact, many researchers have suggested various decision-theoretic interpretations of risk and uncertainty management in the context of design. These interpretations vary from probabilistic approaches (e.g., Reddy and Mistree 1992, Zhou et al. 1992), to Fuzzy (Allen 1996) and Bayesian methodologies. These papers and many others conclude that a decision-theoretic approach to the design process can be easily modified to account for uncertainty and risk. Therefore, one may expect that such novel decision-theoretic approaches (whether fuzzy, probabilistic, or Bayesian), if applied to the ambiguous design environment of NASA's concurrent design teams, can greatly help reduce the risk and uncertainty in a systematic and logical manner. As one example of a preliminary step in this direction, NASA Ames Research Center and its contractors is currently working to develop a Bayesian decision-aid tool, referred to as X-Change, for managing risk and uncertainty during the conceptual phase of JPL's TeamX rapid design environment.

FINAL WORD

In this paper, we argued that despite intensive research efforts by NASA and its affiliates to incorporate risk factors into the concurrent conceptual phase of designing space missions, there are many potentially-helpful research areas (developed by academic community or other research labs) that have been either ignored or under-investigated for NASA applications. The Special Panel on Risk Based Design at ASME's International Design Theory and Methodology Conference (2003 and 2004) is the first step towards providing an open forum for all researchers to communicate and collaborate more effectively – leading to a more coherent and scientifically-rigorous platform, on which designers at NASA can operate to develop safer space exploration missions. The efforts described in this paper are intended to lay the foundation to initiate research in the area of Risk Based Design applied to the challenging NASA problem of low-volume and high-risk designs. In this light, the authors would like the readers to contemplate the following: What would be the most important contributions for the specific problems NASA is facing? How can we leverage ongoing academic work? What combination of efforts would best benefit the current RBD situation at NASA? The future goal of our efforts is to combine the ongoing and proposed research areas into a comprehensive early design risk and failure assessment framework.

REFERENCES

Afimiwala, K. A. and R. W. Mayne (1979). "Interactive Computer Methods for Design Optimization." CAD Journal 11(4): 201-208.

Allen, J.K., (1996). "The Decision to Introduce New Technology: The Fuzzy Preliminary Selection Decision

Support Problem," *Engineering Optimization,* Vol. 26, No. 1, 61-77, 1996.

Anderson, D., E. Anderson, et al. (2000). Human-Guided Simple Search. National Conference on Artificial Intelligence (AAAI).

Backman, B., (2000). "Design Innovation and Risk Management: A Structural Designer's Voyage into Uncertainty," ICASE Series on Risk-based Design, November 2000.

Balling, R. (1999). Design by shopping: a new paradigm? Proceedings of the Third World Congress of Structural and Multidisciplinary Optimization, Buffalo, New York, USA.

Bohm, M., and Stone, R., (2004) "Product Design Support: Exploring a Design Repository System", *ASME International Mechanical Engineering Congress IMECE* 2004-61746.

Chao, L.P., Tumer, I.Y., Ishii, K., (2004), "Design process error proofing: Engineering peer review lessons from NASA." ASME Design for Manufacturing Conference/IDETC 2004. Salt Lake City, UT. September 2004.

Chao, L.P., Tumer, I.Y., Ishii, K. (2005), "Design process error proofing: Benchmarking of the NASA development cycle." IEEE Aerospace Conference. Big Sky, MN. March 2005.

Choi, K., (2001), "Advances in Reliability-Based Design Optimization and Probability Analysis - PART II", ICASE Series on Risk-based Design, December 2001.

Clawson, J. F. and Oberhettinger, D., (2001), "The lessons learns process: an effective countermeasure against avoidable risk." Annual Reliability and Maintainability Symposium, Philadelphia, PA. 2001.

Cornford, S., (1998), "Managing Risk as a Resource using the Defect Detection and Prevention Process", International Conference on Probabilistic Safety Assessment and Management.

Deb K., (2001), Multi-Objective Optimization using Evolutionary Algorithms, John Wiley & Sons, 2001.

Dix, A. and G. Ellis (1998). Starting Simple: adding value to static visualization through simple interaction. Proceedings of the working conference on Advanced visual interfaces AVI98. T. Catarci, M. F. Costabile, G. Santucci and L. Tarantino. L'Aquila, Italy, ACM Press: 124-134.

Du, X. and Chen, W., (2002). "Efficient Uncertainty Analysis Methods for Multidisciplinary Robust Design", AIAA Journal, 40(3), 545-552, 2002.

Eddy, J. and K. E. Lewis (2002). Visulization of Multi-Dimensional Design and Optimization Data Using Cloud Visualization. ASME Design Technical Conferences, Design Automation Conference, Montreal, Canada.

Feather, M. S. and S. L. Cornford (2003). "Quantitative Risk-based Requirements Reasoning." Requirements Engineering Journal (Springer) 8(4): 248-265.

Feather, M., (2002), 'A quantitative risk-based model for reasoning over critical system properties'. Proc. Int. Workshop on Requirements for High Assurance Systems, Essen, Germany, September 2002, pp. 11-18

Feather, M., Conford, S., Dunphy, J., and Hicks, K., (2002), 'A quantitative risk model for early lifecycle decision making'. Presented at Society for Design and Process Science Conf. on Integrated Design and Process Technology (IDPT), 2002

Flippen, A. A., A. M. Larsen, et al. (2002). The Application of Probabilistic Risk Assessment to Habitable Payloads: Utilization of Risk-Based and Trditional Rule-Based Methodologies. Proceedings of IMECE '02, November 17-22, 2002. New Orleans, Louisiana.

Fragola, J. R., B. F. Putney, et al. (2003). A risk evaluation approach for safety in aerospace preliminary design. IEEE Annual Reliability and Maintainability Symposium, Tampa, FL

Gershon, N., S. G. Eick, et al. (1998). "Information visualization." ACM interactions 5(2): 9-15.

Go, S., D. Mathias, et al. (2003). A top-down risk assessment tool for a reusable launch vehicle development program. 41st AIAA Aerospace Sciences Meeting & Exhibit, Reno, NV, Reston, VA: American Institute of Aeronautics and Astronautics, Inc.

Greenfield, M. A. (1999). Risk balancing profile tool. 50th IAF Intrnational Astonautical Conference, Amsterdam, Netherlands, 1999.

Greenfield, M. A. (2000). NASA's Use of Quantitative Risk Assessment for Safety Upgrades. Proceedings of the IAA Symposium, Rio de Janeiro, Brazil, Univelt, Inc.

Hassan, R. A. and Crossley, W. A., (2002), "Multiobjective Conceptual Design of a Geostationary Communication Satellite," paper no. AIAA-2002-1323, 43rd AIAA/ASME/ ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference, Denver, CO, Apr. 2002.

Henk, W. Chen, W., Cheng, J., Sudjianto, A., (2003), "Demand Analysis for Decision-Based Design of Automotive Engine", 2003 SAE World Congress, Paper 04M-133.

Jones, H. W., R. L. Dillon-Merill, et al. (2003). Reducing the Risk of Human Space Missions with INTEGRITY. 33nd International Conference on Environmental Systems, Vancouver, British Columbia; Canada.

Keim, D. A. (2002). "Information Visualization and Visual Data Mining." IEEE Transactions on Visualization and Computer Graphics 8(1): 1-8.

Krasich, M., (1995), “Reliability Achievement through the Technical Risk Assessment”, Proceedings of the 41st Technical Meeting of the Institute of Environmental Sciences, pp. 80-85.

Mahadevan, S., Smith, L., (2003), “System Risk Assessment and Allocation in Conceptual Design”, NASA/CR, May 2003.

Martin, E. T. and Crossley, W. A., “Multiobjective Aircraft Design to Investigate Potential Geometric Morphing Features,” 2nd AIAA Aircraft Technology, Integration, and Operations (ATIO) 2002 Forum, Los Angeles, CA, Oct. 2002.

Mehr, A. F., Tumer, I., (2005a) “Optimal Design of Integrated Health Management (IHM) Systems for improving safety in NASA Orbital Space Planes: A Two-Level Multidisciplinary Design Approach”, Submitted to the 6th World Congress on Structural and Multidisciplinary Optimization, Rio de Janeiro, Brazil 2005.

Mehr A. F. and Tumer I.Y., (2005b), “A new approach to probabilistic risk analysis in concurrent and distributed design of aerospace systems.” Submitted to the ASME IDETC 2005/Design Automation Conference. 2005.

Meshkat, L., S. Cornford, et al. (2003). Risk Based Decision Tool for Space Exploration Missions. Proceedings of the AIAA Space Conference.

Meshkat, L., M. S. Feather, et al. (2003). Traceability and Decision Capture in Semi-structured Contexts. to appear in Proceedings of the 2003 Workshop on Software Engineering Decision Support (SEDECS'2003), San Francisco, California, U.S.A.

Meshkat, L. and R. E. Oberto (2004). Towards a Systems Approach for Risk Considerations during Concurrent Design. United Nations Space Conference, Beijing, China.

Messac, A. and X. Chen (2000). "Visualizing the optimization process in real-time using physical programming." Engineering Optimization Journal 32(5).

Mistree, F., Smith, W.F., Bras, B.A., Allen, J.K., and Muster, D. (1990), "Decision-Based Design: A Contemporary Paradigm for Ship Design," *Transactions of the Society of Naval Architects and Marine Engineers,* Vol. 98, 565-597, 1990.

NASA7120 NPR 7120.5b NASA Program and Project Management Processes and Requirements, NASA Procedural Requirements.

NASA8000.4 NASA NPR8000.4 Risk Management Procedures and Guidelines w/Change 1 (4/13/04), NASA Office of Safety and Mission Assurance.

Pu, P., B. Faltings, et al. (2003). User-Involved tradeoff analysis in Configuration tasks. Third International Workshop on User-Interaction in Constraint Satisfaction.

Pu, P. and D. Lalanne (2002). Design visual thinking tools for mixed initiative systems. Intelligent User Interfaces IUI'02, San Francisco, California, USA, ACM.

Reddy, R., and Mistree, F., (1992), "Modeling Uncertainty in Selection Using Exact Interval Arithmetic" in *Design Theory and Methodology 92,* (L.A. Stauffer and D.E. Taylor, Editors), ASME, 193-201, 1992.

Rose, J., (2000), “Risk Management for Jet Propulsion Laboratory Project”, ASME/SERAD International Mechanical Engineering Congress and Exposition, Orlando, Florida.

Schrader, Stephan, William M. Riggs and Robert P. Smith, (1993), "Choice over Uncertainty and Ambiguity in Technical Problem Solving," Journal of Engineering and Technology Management, Vol. 10, pp. 73-99, 1993.

Shupe, J.A.,(1988). *Decision-Based Design: Taxonomy and Implementation,* Ph.D. Dissertation, Department of Mechanical Engineering, University of Houston, Houston, Texas, 1988.

Sobieski, S. J. and Haftka, R. T., (1997), “Multidisciplinary aerospace design optimization: survey of recent developments,” Structural Optimization, Vol. 14, 1997, pp. 1-23.

Sobieski, J. S., Emiley, M.S., Agte, J., S., Sandusky, R. R., (2000), “Advancement of Bi-level Integrated System Synthesis (BLISS)”, Proceedings of the 38th AIAA Aerospace Sciences Meeting and Exhibit, January 2000.

Smith, N., and S. Mahadevan, (2003), "Probabilistic Methods for Aerospace System Conceptual Design," Journal of Spacecraft and Rockets, AIAA, Vol. 40, No. 3, pp. 411-418, 2003.

Stamatelatos, M., G. Apostolakis, et al. (2002). Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners v1.1, NASA Office of Safety and Mission Assurance: 310.

Steuer R. E. (1986), Multiple Criteria Optimization: Theory, Computation, and Applications , John Wiley & Sons, Inc., 1986

Steuer, R. E., Y. Qi and M. Hirschberger, (2004) "Suitable-Portfolio Investors, Nondominated Frontier Sensitivity, and the Effect of Multiple Objectives on Portfolio Selection," Working Paper, Department of Banking and Finance, University of Georgia, January 2004.

Stone, R.B., Tumer, I.Y., VanWie, M. (2005) “The function-failure design method.” Journal of Mechanical Design. 2005.

Stock, M.E., Stone, R.B., Tumer, I. Y., (2005), “Linking product function to historical failures to improve failure analysis in design” Research in Engineering Design. In Print. 2005.

Stump, G., T. W. Simpson, et al. (2002). Multidimensional visualization and its application to a design by shopping paradigm. 9th AIAA/ISSMO Symposium on Multidisciplinary Analysis and Optimization, Atlanta, Georgia, USA.

Stump, G. M., M. Yukish, et al. (2003). Design space visualization and its application to a design by shopping paradigm. ASME 2003 Design Engineering Technical

Conferences and Computers and Information in Engineering Conference, Chicago, Illinois, USA.

Tapetta, R.,(2000) “Interactive Multiobjective Optimization of Engineering Systems”, Ph.D. Dissertation, Aerospace and Mechanical Engineering Dept., University of Notre Dam, January, 2000

Townsend, J. S. and C. Smart (1998). Reliability/risk analysis methods and design tools for application in space programs. AIAA Defense and Civil Space Programs Conference and Exhibit, Huntsville, AL.

Tumer, I. Y., Stone, R.B., (2003), “Mapping Function to Failure During High-Risk Component Development” Journal of Research in Engineering Design, Vol. 14, pp.25-33. 2003.

Tweedie, L., B. Spence, et al. (1995). The influence explorer (video). CHI 95 Conference Companion, Vancouver, British Columbia, Canada, ACM Press New York, NY, USA.

Unal, R., C. Keating, et al. (2004). Development of an expert judgement elicitation and calibration methodology for risk analysis in conceptual vehicle design. Norfolk VA, Aerospace Systems, Concepts and Analysis Competency, NASA Langley Research Center.

Yann, Collette and Patrick Starry, (2003). Multiobjective Optimization. Principles and Case Studies, Springer, August 2003.

Ward, M. O. (1994). XmdvTool: Integrating Multiple Methods for Visualizagin Multivariate Data. IEEE Visualization '94, Washington DC, USA.

Winer, E. H. and C. L. Bloebaum (2002a). "Development of visual design steering as an aid in large-scale multidisciiplinary design optimization. Part I: method development." Structural and Multidisciplinary Optimization 23(6): 412-424.

Winer, E. H. and C. L. Bloebaum (2002b). "Development of visual design steering as an aid in large-scale multidisciiplinary design optimization. Part II: method validation." Structural and Multidisciplinary Optimization 23(6): 425-435.

Wittenbrink, C. M., A. T. Pang, et al. (1996). "Glyphs for visualizing uncertainty in vector fields." IEEE Transactions on Visualization and Computer Graphics 2(3): 266-279.

Zang, T.A., Michael J. Hemsch, Mark W. Hilburger, Sean P. Kenny, James M. Luckring, Peiman Maghami, Sharon L. Padula, W. Jefferson Stroud, (2002), “Needs and Opportunities for Risk-Based Multidisciplinary Design Technologies for Vehicles”, NASA TM, July 2002.

Zhou, Q-J., Allen, J.K. and Mistree, F., (1992), "Decisions Under Uncertainty: The Fuzzy Compromise Decision Support Problem," *Engineering Optimization,* Vol. 20, 21-43, 1992.