Towards Risk as a Tradeable Parameter in Complex System Design Trades

Conference Paper · August 2010

DOI: 10.1115/DETC2010-29016

3 authors, including:

Douglas Lee Van Bossuyt
Naval Postgraduate School
135 PUBLICATIONS **936** CITATIONS
SEE PROFILE

Irem Y. Tumer
Oregon State University
283 PUBLICATIONS **4,019** CITATIONS
SEE PROFILE

Proceedings of the ASME 2010 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference
IDETC/CIE 2010
August 15-18, 2010, Montreal, Canada

DETC2010-29016

TOWARDS RISK AS A TRADEABLE PARAMETER IN COMPLEX SYSTEM DESIGN TRADES

Douglas L. Van Bossuyt
Graduate Research Assistant
Complex Engineered Systems Design Laboratory
School of Mechanical, Industrial, and Manufacturing Engineering
Oregon State University
Corvallis, Oregon, 97331
Douglas.VanBossuyt@gmail.com

Stephen D. Wall
Integrated Modeling and Simulation Manager
System Modeling and Analysis Program Office
California Institute of Technology
Jet Propulsion Laboratory
Pasadena, California, 91019
Stephen.D.Wall@jpl.nasa.gov

Irem Y. Tumer*
Associate Professor
Complex Engineered Systems Design Laboratory
School of Mechanical, Industrial, and Manufacturing Engineering
Oregon State University
Corvallis, Oregon, 97331
Irem.Tumer@oregonstate.edu

ABSTRACT

Complex system conceptual design trade studies traditionally consider risk after a conceptual design has been created. Further, one person is often tasked with collecting risk information and managing it from each subsystem. This paper proposes a method to explicitly consider and trade risk on the same level as other important system-level variables during the creation of conceptual designs in trade studies. The proposed risk trading method advocates putting each subsystem engineer in control of risk for each subsystem. A risk vector is proposed that organizes many different risk metrics for communication between subsystems. A method of coupling risk models to dynamic subsystem models is presented. Several risk visualization techniques are discussed. An example is presented based upon a simplified spacecraft model. The risk trading method discussed offers an approach to more thoroughly consider risk during the creation of conceptual designs in trade studies.

Keywords: Trade Study, Complex System Design, Risk, Collaborative Design Center, Risk Trading

*Address all correspondence to this author.

1 INTRODUCTION

Risk has traditionally been an afterthought in the conceptual complex system design process. Risk is typically only assessed after a conceptual design has been created and does not explicitly play a role in the creation and selection of conceptual designs. Our hypothesis is that by moving risk into trade studies and giving it a place among other important more traditional system-level variables such as power, mass, etc., conceptual designs will be explicitly created and selected based on risk, reliability, robustness, and uncertainty metrics. Specifically, this research presents a method of explicitly trading and evaluating designs based upon risk in design trade studies among subsystems with the end goal of maximizing system utility and system integrity.

This paper presents one possible way to assess risk and make decisions based on risk in the complex conceptual design process. Risk is treated as a vector with multiple components defined by the requirements of the system. The risk vector is then traded in design trade studies. Based upon the desired level of risk for a system, specific point designs or portions of the design space can be identified for further study and development. The risk trading methodology presented in this paper is implemented in Phoenix Integration's ModelCenter [1].

The following sections include background on trade stud-

ies, Collaborative Design Centers (CDCs), related work, and other necessary background information. Methodology to trade risk is developed and demonstrated using a simplified spacecraft model adopted from Wertz and Larson [2]. Contributions of the methodology are discussed and future work to expand the methodology is outlined.

1.1 Design Trade Studies Fundamentals

Design trade studies are used in conceptual complex system design to generate different designs and compare amongst them. Trade studies can be performed either automatically using software packages or by teams of people. While computer generated trade studies can create many thousands of design points quickly, human generated trade studies are often seen as having higher fidelity and are more likely to be accepted.

Metrics such as cost, mass, power, volume, and other parameters are often traded in trade studies. Each subsystem within a complex system is initially allocated specific amounts of the constraint parameters. During the course of the design process, several subsystems are often found to be lacking in one or multiple constraint parameters but have additional quantities of other parameters available. These parameters can be traded between different subsystems and contain intrinsic value of varying degrees for different subsystems designers [3–5]. The resulting conceptual designs can then be ranked according to appropriate selection rules [6–9].

The basic mathematical concept behind trade studies is simple and straight-forward. Trade-offs are made between design variables to achieve maximum design utility [10]. This generally takes the form of $max\, f(\overrightarrow{U})$ where $\overrightarrow{U}$ represents relevant system utility metrics.

This simple equation provides the foundation for a wide range of analytic methods that all aim to find the optimal design given system constraints. Many different methods have been developed to computationally find the optimal solution. The difficulties, however, are in developing a series of equations that adequately model the system to then efficiently find the optimum solutions to those equations.

Trade studies provide fertile ground for the creation and ideation of new conceptual designs using equations that model the systems being studied. New design variables can easily be placed into the existing trade study framework. One such design variable is risk which is discussed in Section 3.1.3.

1.2 Conceptual Design Centers

Many companies and institutions have teams who perform trade studies as part of the early complex system design process. The first and most cited example is the National Aeronautics and Space Administration (NASA) Jet Propulsion Laboratory (JPL)'s Project Design Center (PDC) and the associated design team, commonly referred to as Team-X. The group functions as a conceptual spacecraft mission design team. It was formed in June 1994 [11].

The Team-X design team includes engineers and scientists from all major spacecraft mission subsystems co-located in the PDC, which is outfitted with the latest technology to aid in spacecraft mission development and concurrent design. This gives Team-X the ability to complete spacecraft architecture, mission, and instrument design trade studies very rapidly [12]. Most Team-X trade studies are completed in 2 to 3 days, compared to 3 to 9 months to complete a comparable trade study [13]. Team-X has also reduced the cost of concept-level spacecraft mission design by a factor of 5 compared to conventional design processes [13].

The success of Team-X spurred other NASA research centers to adopt the methods used by Team-X. These include the Langley Research Center (LaRC) [14], two other groups at JPL known as Team-Z [15] and Team-I [16], NASA Goddard [17], and the Johnson Space Center [11]. Similarly, the European Space Agency (ESA) has replicated the methods used by Team-X [18]. A collection of academic institutions including Stanford, CalTech, MIT, the Technical University of Munich, Georgia Tech, and others have also created Collaborative Design Centers (CDCs) to perform trade studies for simulated complex system design [11, 19–21]. Finally, several private companies have adopted the Team-X approach to Trade Studies. The first organization to follow the lead of Team-X was the Aerospace Corporation with the creation of a CDC named the Concept Development Center in 1999 [22]. Boeing's Military Aircraft division also houses a CDC, as do the successor companies of the TRW corporation [11].

1.3 Paper Focus and Contributions

Within Team-X and other CDC groups, there are often desired levels of system level risk. While it might appear that a design minimizing risk is always desired this is often not the case. Sometimes designs with a specific level of risk above the absolute potential minimum is desired. In the case of Team-X, this is due to the desire to launch challenging missions. NASA is in the business of developing new technologies and doing missions that no other organization has – both of which are risky, without taking unnecessary risks. Instead, missions are selected for further development based on several factors including the mission risk profile. A risk target window has been defined that balances pushing the boundaries of engineering and science with a desired level of mission success [23].

The method presented in this paper is developed to augment current methods and practices in use at JPL and other CDCs. The method provides a means for stakeholders to account for risk in conceptual designs, and for engineers to choose subsystem designs or components based upon risk. Managers selecting

specific risk-profiles can use this method to identify the most interesting designs. Customers of Team-X sessions can use this method to get a feel for the risk profile of the end design.

2 RELATED WORK

Some Collaborative Design Centers currently employ tools and methods to capture risk in the conceptual design process. However risk capture happens before or after conceptual designs have been generated, or as part of a process that happens in lieu of trade studies. Further, risk does not play a role in early conceptual design development. One such type of tool is Risk and Rationale Assessment Program (RAP) used by Team-X.

The RAP tool is a Probabilistic Risk Assessment (PRA)-based assessment software package that was developed internally at JPL. During a trade study session each subsystems chair has the ability to enter information into the tool as she sees fit. This data contains a Risk Priority Number (RPN) comprised of the likelihood of a specific risk occurring multiplied by the effects if the risk is realized. Mitigation information can also be entered in a free-form text box. In Team-X one person is dedicated to monitoring the RPN tool and compiling the data entered by the subsystems chairs to create an overall system-level risk assessment. This person is known as the risk chair [24].

While RAP does a decent job of identifying mission risks outside of normally accepted risks, it also can find surprise risks. However this only happens when the tool is actually used. Observations indicate that during Team-X sessions RAP is either used as an afterthought once most of the conceptual design work had finished or not used at all.

Another point of interest with RAP is how it is decoupled from the trade studies conducted by Team-X. Risk cannot be traded with RAP nor does it find its way into the trade studies. Instead risk assessment is conducted as an afterthought to the conceptual designs being created. It should also be noted that other groups outside of NASA have used tools similar to RAP and with similar implementations yielding similar results and problems [25–27].

In addition to RAP, JPL has also developed Defect Detection and Prevention (DDP), a tool that helps engineers determine what mitigation steps will provide the largest reduction in system-level risk [28]. The tool was originally conceived to be used in assurance planning [29], and has since been extended for use in conceptual complex system design [30]. To date no CDC has adopted DDP; however, some studies conducted outside of CDCs have been performed. While literature on DDP does state that risk should be traded and provides a framework for trading, trade studies are not suggested to be performed in CDCs. However, the method does suggest that trade studies can be used to determine how much risk should be mitigated in early conceptual design, and further, that risk can be compared against performance metrics to find the optimum level of risk versus performance [28]. But to examine risk, conceptual designs must be first created before the DDP method can be used to analyze risk [31]. The DDP method suffers from being perceived as an overly complicated tool and methodology.

While RAP and similar tools have been adopted in many CDCs and DDP has found some use outside of the CDC environment, several other methods have remained purely academic. For instance, a risk management method developed by Dezfuli et al. embeds the NASA Continuous Risk Management (CRM) process into a broader decision framework [32]. The method presents a risk management approach intended to be used throughout the product life-cycle. Performance measures and NASA's CRM process are relied on to assess risk. While the method does state that risk must be accounted for in the conceptual design phase, and further briefly mentions the trade study process, the actual analysis of risk happens after conceptual designs have been created [33]. Thus the method does not place risk directly in the creation of the conceptual designs in the trade study process.

A normative method that attempts to balance cost, risk, and performance for decision makers in preliminary spacecraft mission design is presented by Thunnissen [34]. The method focuses on uncertainty and classifies it into four different categories (ambiguity, epistemic, aleatory, and interaction), three subcategories of epistemic uncertainty (model, phenomenological, and behavioral), three sub-sub categories of model uncertainty (approximation errors, numerical errors, and programming errors), and four sub-sub categories of behavioral uncertainty (design, requirement, volitional, human errors). Thunnissen finds uncertainty in several areas of preliminary mission design. Launch vehicles have uncertainty due to the type and variant of launch vehicle with respect to availability both due to production schedules and political concerns, the reliability of the launch vehicle with regards to chance of mission loss, performance as measured by injecting the mission into the correct orbit, and cost of the launch. The launch date of a mission has uncertainty due to weather delays, range delays, launch vehicle delays, and spacecraft delays. Mission trajectory has uncertainty, as the total change in velocity (ΔV) a mission must achieve varies based upon unpredictable outside influences, and other miscellaneous uncertainties. To deal with these uncertainties probabilistic methods and Bayesian techniques [35] are employed. However, risk in the form of Thunnissen's uncertainty definitions is not considered during trade studies. Instead, it is analyzed for a specific subset of overall mission design during the very early stages of conceptual design prior or in lieu of trade studies.

Another method developed by Thunnissen formalizes margins in trade studies and also attempts to trade risk in trade studies [36]. However trading risk is an afterthought to the primary concern of design margins in the method. The risk model presented simply replaces an expected design constraint. Rather than setting a fixed minimum value for a design constraint, a

100% risk of failure is produced when the minimum value is crossed. The primary contribution of the work is the formalization of margins in trade studies – not implementing risk in trade studies.

Finally, Charania et al. present a collaborative design method that utilizes Probabilistic Data Assessment to trade risk in trade studies conducted using Phoenix Integration's ModelCenter software package [37]. However risk is treated as a separate "subsystem" in the trade studies. Risk is not explicitly incorporated into each subsystem model. Rather, like the RAP methods used by Team-X and others, one person or one "subsystem" model is in charge of risk.

In summary, some methods such as RAP and DDP have found use in CDCs and elsewhere while other methods such as those developed by Thunnissen, Charianian et. al., and others remain academic. Some of the methods analyze risk after conceptual designs have been created using trade studies. Others analyze risk prior to trade studies or bypass trade studies all together. One even analyzes risk within trade studies during the creation of conceptual designs as a separate subsystem. However, no method currently places risk within each subsystem model to be controlled and developed by individual subsystem chairs during the creation of conceptual designs in trade studies. This research asserts that a method is needed that gives the power to analyze subsystem risk and trade system-level risk to subsystems chairs during the creation of conceptual designs in trade studies. This will produce results that are more accurate and more trustworthy than currently available methods, resulting in a method that can be adopted in practice.

3 METHODS

In this section a methodology is presented to trade risk within trade studies during the creation of conceptual designs. Risk trading will happen between separate subsystems and be overseen by each subsystem. Risk will be tradeable as a system-level parameter. To facilitate risk trading, a risk vector is developed that encompasses risk, reliability, robustness, and uncertainty. Several topics are introduced next to facilitate the creation and population of the risk vector. Methods are presented to create a system-level risk vector from the constituent subsystem risk vectors. Ways of using the system-level vector in trade studies are then presented to demonstrate how to use the risk trading methodology. The steps involved are summarized in Table 1.

Table 1. Steps to Perform Trade Studies Using Risk as a Tradeable System-level Parameter

1. Construct subsystem-level risk vector
2. Implement risk vector into subsystems; populate subsystems models with risk methods
3. Combine subsystem vectors into system-level risk vector
4. Use appropriate means of visualizing system-level risk vectors
5. Perform trade study using risk vector as a tradeable system-level parameter

3.1 Relevant Methods and Concepts

Several relevant methods and concepts are used in this research. This section provides a brief review of software used to perform trade studies; a method of grouping risk, reliability, robustness, and uncertainty into one meta-category; and methods of quantitatively accounting for risk, reliability, robustness, and uncertainty. These methods and concepts are necessary for the development of the risk trading methodology presented here.

3.1.1 Trade Study Software Many formal trade studies are conducted using software packages. Several different commercial and academic packages exist on the market to enable both automated and manual trade studies. Automated trade studies are conducted by a computer and can create many different conceptual designs quickly. In such studies, humans set up automated trade studies and review the results but do not generate the concepts. Automated trade studies are used when large sets of conceptual designs are desired, often to map out the design space. Manual trade studies have humans in the loop and generate conceptual designs much more slowly. While automated studies can fill out a trade space quickly, manual trade studies are often viewed as having higher fidelity and being more true to life. Manual trade studies are used when expert judgment is more useful than pre-programmed formulas in creating a limited number of conceptual designs.

Commercially available and academic software packages exist that support both manual and automated trade studies. They include ICEMaker [38], Advanced Trade Space Visualization (ATSV) [39, 40], and ModelCenter [1] among others [41, 42]. Some such as ATSV are only capable of performing automated trade studies while others such as ModelCenter can be used to perform both manual and automated trade studies.

This research makes use of Phoenix Integration's ModelCenter software. ModelCenter integrates many of the functions of ATSV into a robust package that employs the concept of "wrappers" to the complex systems design process. Wrappers are used to interface design tools such as Microsoft Excel, EES, CATIA, etc. with an optimization and/or trade space exploration program. The wrappers can be linked together so that variables from one design tool can be interfaced with variables produced by another tool. The design tools can be controlled from multiple

computers across a network allowing large-scale collaboration on the order of a 30 person CDC environment.

ModelCenter automates the process of running trade space exploration and design optimization algorithms through the interconnected wrappers. The actual computations can be run either on a local machine or a remote cluster of servers. Very large data sets can be created quite quickly in this manner. Many visualization techniques and trade study tools are included in the ModelCenter software. These tools can allow a design team to quickly find weaknesses in a design, find optimal solution sets using multi-variable trade studies, and in general aid the design process.

ModelCenter also has the ability to be run in a manual mode with human-in-the-loop control over the process. In a CDC environment, this allows for complete control of the models and outputs of each subsystem. It is also possible to only have certain models and subsystems manually controlled while the rest of the subsystems in the trade study are automated [1].

This paper uses ModelCenter in the development of a risk trading methodology. However, the methods developed here are applicable in any other trade study software tool. They also work in both manual and automated trade studies.

3.1.2 Risk, Reliability, Robustness, and Uncertainty Trading any variable in a trade study can only occur when all of the models and all of the people agree on the definition and value of that variable. While it is easy to define a cost variable as the dollars it will take to build something or a mass variable as the mass of an object, it becomes increasingly difficult as the value being traded becomes more abstract. Risk is one such variable, and hence requires a clear definition.

Risk is often defined in engineering as the probability of occurrence multiplied by the severity of impact. However many people including engineers think of risk more by its dictionary definition: the possibility of suffering harm or loss, or a danger. Other concepts such as reliability, robustness, and uncertainty are also often lumped in the same category as the engineering definition of risk. Reliability can be defined in engineering as "the ability of a system or component to perform its required functions under stated conditions for a specified period of time [43]." Robustness in the systems engineering context refers to a system that is resistant to failure due to inputs that are beyond the expected and designed for input range [44]. Uncertainty is a result of a lack of knowledge about system specifications, and errors resulting from imperfect models [45]. Some researchers further break down uncertainty into multiple subcategories that often contain elements of risk, reliability, and robustness [46].

3.1.3 Risk Analysis Techniques It is necessary for the methodology presented in this paper to be able to quantify risk in a repeatable and robust manner. Many risk evaluation tools exist that are commonly used in industry. For instance, Failure Modes and Effects Analysis (FMEA) and its extension, Failure Modes and Effects Criticality Analysis (FMECA), adding criticality analysis, find use across many industrial sectors. FMEA/FMECA analyses examine potential failure modes, their effects on a local and system-wide level, the severity of the effects, potential causes of the failure, the probability of occurrence of the failure, current detection methods for the failure, detectability of the failure, recommendations to mitigate failure effects or causes, and a Risk Priority Number (RPN) which is the product of severity, occurrence, and detectability that can be used when prioritizing which failure modes to address first. Severity refers to the severity of the impact of a failure. Occurrence is the likelihood of that failure occurring. Detectability is the ability to detect the failure in enough time to take corrective action to prevent the failure from occurring. Some FMEA/FMECA studies also include information on corrective action taken and other post-analysis information used for tracking progress of mitigating failure risks [47, 48].

In addition, in early conceptual design or when more rigorous risk analysis cannot be performed, expert judgment is often used. One or a group of experts is asked to rate the level of risk present in a component or subsystem. The resulting rating can take the form of "low, medium, high," a numeric scale, or many other options.

Another commonly used fault analysis tool is Fault Tree Analysis (FTA). FTA is employed when a top-down graphical approach to failure analysis is desired. Generally resembling business organization charts, FTA starts with a top-level failure and proceeds downward, analyzing all of the potential causes in turn. Boolean operators and logic gates are used to create the model. After appropriate reliability numbers have been assigned for each component, perhaps having been acquired from a failure database, a total fault probability can be garnered [49].

The risk methods presented in this section are only a small selection of the wide array of robust quantified methods available including Qualitative Risk Assessment (QRA) [50], Event Tree Analysis (ETA) [51], Reliability Block Diagram (RBD) [52], PRA [53], Functional Failure Identification Propagation (FFIP) [54], Function Failure Design Method (FFDM) [55–59], Risk in Early Design (RED) [60], Hierarchically Performed Hazard Origin and Propagation Studies (HiPHOPS) [61], and Risk and Uncertainty Based Integrated and Concurrent design methodology (RUBIC) [62] among others.

3.2 A Risk Trading Methodology: Main Steps

The risk trading method presented in this section trades risk as a system-level parameter in trade studies. Further, the method advocates that risk calculations and information for each subsystem be put under the control of each subsystem model and be the responsibility of each subsystem engineer. This section intro-

duces the concept of risk vectors, shows how to implement them in subsystem models, outlines methods of combining subsystem risk vectors into a system-level risk vector, and introduces various methods of using the risk vector to trade risk in trade studies. (See Table 1 for the steps of the proposed methodology.)

3.2.1 Creating Risk Vectors In industry and academia it is often the case that the definitions of risk, reliability, robustness, and uncertainty become blurred and mixed together. While it is important to tightly define these terms for the project at hand, one can think about this family of concepts under the meta-category of risk. Especially when talking with non-subject experts, grouping all of the related ideas into a risk meta-category can be very useful.

The concept of grouping risk, robustness, reliability, and uncertainty into one meta-category can be extended to create risk vectors. A risk vector, $\overrightarrow{Risk}$ is defined to include all components of risk, reliability, robustness, and uncertainty in a design. So long as $\overrightarrow{Risk}$ is defined properly for the design and everyone using $\overrightarrow{Risk}$ understands what the constituent components of the vector represent, representing the risk family in this manner is very useful. For example, Equation 1 shows one potential generic $\overrightarrow{Risk}$ configuration.

$$\overrightarrow{Risk} = \begin{Bmatrix} Risk metric\#1 \\ Risk metric\#2 \\ Robustness metric\#1 \\ Robustness metric\#2 \\ Reliability metric\#1 \\ Reliability metric\#2 \\ Uncertainty metric\#1 \\ Uncertainty metric\#2 \end{Bmatrix} \quad (1)$$

3.2.2 Populating the Risk Vector Populating the risk vector is simple and straightforward. The trade study facilitator and subsystems chairs must agree upon the risk metrics to be included and the construction of the vector. Depending upon the risk methods employed, the risk metrics that result either can be directly placed into the risk vector or will need to be transformed into a metric or suite of metrics that have meaning and value in a trade study setting. As long as the specific types of risks being analyzed are properly defined, $\overrightarrow{Risk}$ can be compared between different components, subsystems, and functions. This opens the door to trading $\overrightarrow{Risk}$ in trade studies. A robust method for properly defining risk in this context will be developed in future work.

Expert judgment, when conducted in a repeatable and quantifiable way, can be directly placed into risk vectors. FTA produces a top-level probability of failure that can be directly used in risk vectors [63]. Other methods that produce a top-level quantifiable metric can be directly integrated into risk vectors.

FMECA and other risk methods that have multiple metrics must be dealt with differently. The resulting Risk Priority Numbers (RPNs) from a FMECA are often prioritized from highest to lowest RPN in order to address the highest risks first and decide which risks must be addressed and which can be safely ignored under budgetary constraints. While using the highest RPN score from a FMECA can be effective in flagging a risky component or function, it does not tell the whole story. Another way of pulling meaningful information from a FMECA without looking at the entire list of RPNs is to sum the FMECA RPNs and divide by the total number of RPNs. This will produce an averaged RPN number. By looking at both the maximum RPN and the averaged RPN of a function or subsystem, a more complete picture of the FMECA can be obtained without having to review the entire FMECA.

A risk vector containing FTA, expert judgment, and FMECA data can take the form of Equation 2. Note that it is important to identify what each risk metric is analyzing. For instance, several different types of expert judgment or FTA analysis can be present and important in conceptual designs and trade studies.

$$\overrightarrow{Risk} = \begin{Bmatrix} MaxRPN \\ AverageRPN \\ FTA of Complete Mission Loss \\ FTA of Schedule Risks \\ Expert Judgment of Cost Overrun Risks \\ Expert Judgment of Risk of Mission Degradation \end{Bmatrix} \quad (2)$$

The risk vector developed in this section is not yet ready to be integrated into trade studies. Next, the risk methods that the risk vector represents must be implemented in the subsystems models. Risk metrics have been chosen and defined. At this stage, subsystems engineers must now develop their individual risk subsystem models. This is covered in the next section.

3.2.3 Developing Subsystem Risk Models Risk models found in the literature and in practice are typically static. They do not automatically change based upon new inputs. In fact, standard risk methods do not normally take new inputs. For effective risk trading, a dynamic approach to risk methods must be taken.

Three options are available to use risk methods in risk vectors implemented in trade studies. The first option is to use risk methods without any modification. Unlike the other options where dynamic inputs come from the subsystem models, this option uses risk methods and metrics that could otherwise standalone. This option is not especially useful or helpful unless the risks being accounted for in the risk vector do not change as the

rest of the subsystem design changes. Except in rare cases, this option will not accurately capture risk and further voids any ability to trade risk between subsystems.

The second option is to make the inputs to risk methods dynamic. This means that an FTA top level probability of failure, for instance, would change based on the probabilities attached to the sub-elements of the fault tree. The sub-element probabilities are no longer fixed static quantities as they would be in a standalone FTA. Instead, the sub-element probabilities are directly fed from dynamic inputs based upon other subsystem models and system-level parameters. This makes trading risk between subsystems easy as any change in input variables as a result of system-level parameter trading creates an immediate response in the risk vector. Thus, rather than having a static FTA or FMECA, a dynamic FMECA is available.

The third option requires the creation of several static risk models. The correct static risk model is then chosen either automatically or manually based upon the inputs to the subsystem. This can be especially useful if the subsystem model involves choosing between components or discrete functions.

Whatever risk model trade study option is chosen, the risk models must be integrated into the existing subsystems models. Further, the risk models must be created, managed, and be accessible by the individual subsystems chairs. If using subsystems models written in Microsoft Excel or similar programs, it is relatively easy to add basic risk models by creating a new tab in the Excel workbook for risk models. In the case of more advanced models or where proprietary source code is used, a second model encapsulating the risk models can be used. However, the separate risk models must still be part of the overall subsystem model.

To create a practically useful risk trading method, each subsystem chair must be in control not only of their normal subsystem models but also of the risk models for their subsystems. The full set of subsystems risk models cannot be managed by one person. The implicit risk knowledge present in each subsystems chair would no longer be captured in the subsystems risk models.

The appropriate risk models have now been created and integrated into the subsystems models. The risk vectors are now populated with the risk metrics produced by the individual subsystems risk models. Now the subsystems are ready to be unified into trade study where risk can be traded like any other system-level parameter.

3.2.4 Creating a System-Level Risk Vector Bringing subsystem risk vectors together to create an overall system-level risk vector is necessary to be able to conduct trade studies. Unlike other system-level parameters such as mass or cost, the subsystem risk vectors cannot always be summed together. Each constituent risk metric and the risk method behind it must be examined and a determination must be made about how to best represent that metric's system-level risk.

In the case of FTA all that must be done is to create a system-level fault tree that only includes the subsystems. A dynamic FTA risk model is then easy to create. The top level probability of failure is then reported to the system-level risk vector.

Expert judgment must be handled on a case-by-case basis. The type of judgment being made will affect how the expert judgment metrics from each subsystem will be combined to create a meta expert judgment for the entire system. For instance, if experts are asked to estimate the probability of failure of their individual subsystems, it is appropriate to create a system-level FTA using the expert judgments as the subsystem probabilities. If subsystems experts are asked to rate individual subsystem risk either high or low it is useful to display the total number of high-rated subsystems versus low-rated subsystems.

FMECA and the RPNs it generates are handled in two different ways. In Section 3.2.3, the risk trading methods developed suggest that both the maximum subsystem RPN and the average subsystem RPN be included in the subsystem risk vector. At the system level, the maximum RPN of the entire system should be reported in the system-level risk vector. Likewise at the system level, the average RPN of the entire system should be included in the system-level risk vector.

Each risk method requires careful analysis to determine the best method to combine subsystem-level risk metrics into system-level risk metrics. FTA, expert opinion, and FMECA all have their own ways of combining subsystem-level risk metrics to the system-level. Other risk methods must be adapted in a similar fashion to report useful and meaningful information to the system-level risk vector. With the system-level risk vector now prepared, the trade study is ready to be performed.

3.2.5 Trading Risk To be able to use risk as a tradeable parameter in trade studies, four steps must be taken. First, appropriate subsystems risk models must be created. Then, those risk models must be integrated into the individual subsystems models. Next, risk vectors must be created and populated. Finally, the individual subsystem risk vectors must be combined to create an overall system-level risk vector. Once these preparations have been made risk can now be traded in trade studies.

Trading risk follows exactly the same procedures as trading any other system-level variable. In automated trade studies the risk vector can be treated as either a design variable or a response variable. As a design variable the risk vector is able to be manipulated with the full gamut of design of experiments methods. As a response variable the risk vector acts as a bounding constraint. Further, the risk vector is able to be used in objective functions to drive the population of the trade space. In other words, it works exactly the same as any other system-level design variable.

In manual trade studies, the risk vector is used in the same manner as any other system-level variable. However, there are several ways to visualize the data that the vector contains. The

most straightforward method is to display each of the individual system-level risk metrics encapsulated within the risk vector. This method only requires that the risk vector be displayed in a numerical form on a spreadsheet projected onto the wall of a CDC or in some other way displayed for the subsystems chairs to see.

Another way to display the system-level risk vector is to use a multi-dimensional visualization method such as one of the many included in ATSV as part of ModelCenter. For instance, a parallel axis graph can be setup with high and low axis numbers pulled from the maximum and minimum subsystems risk metric values. A parallel axis graph setup in this fashion quickly displays both the system-level risk metrics and where they are located with relation to subsystem-level risk metrics. Figure 7 in the results section is an example of a parallel axis graph displaying risk vector information.

The third method of displaying a risk vector is useful to get an overall picture of system-level risk. To achieve this goal, each risk metric is combined into an overall risk number for the system. A careful analysis of how to transform disparate risk metrics and methods into one risk number must be performed for each individual trade study risk vector configuration. This system-level risk vector display method can be extended to a graphical color scale where one color such as red means high risk while another such as green means low risk. It then becomes very easy to glance at the risk color to see the overall system-level risk. However, this method is not useful except for a very broad overview of the level of risk in a system. Simplifying all the nuances of risk to a single value can obscure important risk information. This method of risk visualization requires more research and development before it will be a practical choice.

With appropriate visualization tools in place, the trade study can now be conducted. The system-level risk vector and its constituent parts are traded back and forth between subsystems for other system-level parameters. Risk can now be traded for mass, power, cost, or any number of important system-level variables.

4 CASE STUDY

To demonstrate the proposed risk trading methodology developed in this paper, a simplified spacecraft model is adopted from Wertz and Larson [2]. This simplified spacecraft model was originally created as an academic demonstration of trade studies in a complex system design course at Oregon State University and is implemented here using ModelCenter.

The model is of a simple circular earth-orbiting imaging satellite. The model includes attitude, computer, payload, power, structures subsystems, and orbital models. The computer subsystem model is further broken into mass and power, and cost models. The payload subsystem model includes formulas relating to a camera package. Rather than selecting between individual components, all of the models are function-based. The variables being traded between the subsystems are mass, power consumption, and cost. Other important subsystem-specific variables include data rate, several payload parameters, and mission life.

This section will first conduct a trade study using the simplified spacecraft model as-is, without any risk information. A basic risk vector will then be created, subsystems risk models will be developed and integrated into the subsystems models, a system-level risk vector will be created by appropriate integration of subsystem risk vectors. Finally, a trade study will be conducted using the simplified spacecraft model augmented with risk information. Methods for both automated and manual trade studies using risk trading methods will be demonstrated.

4.1 Simplified Spacecraft Model Without Risk

Simplified spacecraft models were first run without consideration of risk. The simplified spacecraft subsystems models were developed using Microsoft Excel. Formulas from Wertz and Larson [2] were used in their original forms or in simplified forms. The resulting models are a good approximation of a complete spacecraft model that have balanced the nuances of the models presented by Wertz and Larson with simplicity for computational and understanding ease [2].

After the subsystems models were developed, they were brought into ModelCenter using the Excel Wrapper plugin. The system-level variables were mapped and linked between subsystem models using the link tool. A summation function was added to the system model to sum the individual subsystems costs. The subsystems power variables were summed in the power subsystem model. The subsystems mass variables were summed in the structure model. Two converging functions were used to converge the power and mass requirements of the attitude control subsystem with the power and mass requirements of the other subsystems via the power and structure subsystems. Figure 1 shows a graphical view of the subsystems in ModelCenter.

Next, an automated trade study was created in ModelCenter for the simplified spacecraft model. Each input variable was bounded with maximum and minimum values, and initial values were assigned. Using a Latin-Hypercube design of experiment 200 input variable combinations were created. The system-level mass, cost, and power variables were set as output variables. After the initial 200 design concepts were created, the system model was driven to find designs that were low-cost, had a long mission life, and returned high scientific value as defined by a payload subsystem variable. An additional 100 conceptual designs were created in this manner. The results are discussed in Section 5.

4.2 Creating the Risk Vector

Next, risk was integrated into the trade study. The first step is to create a basic risk vector that will be used in the subsystem and system-level models. In this model, it was decided that

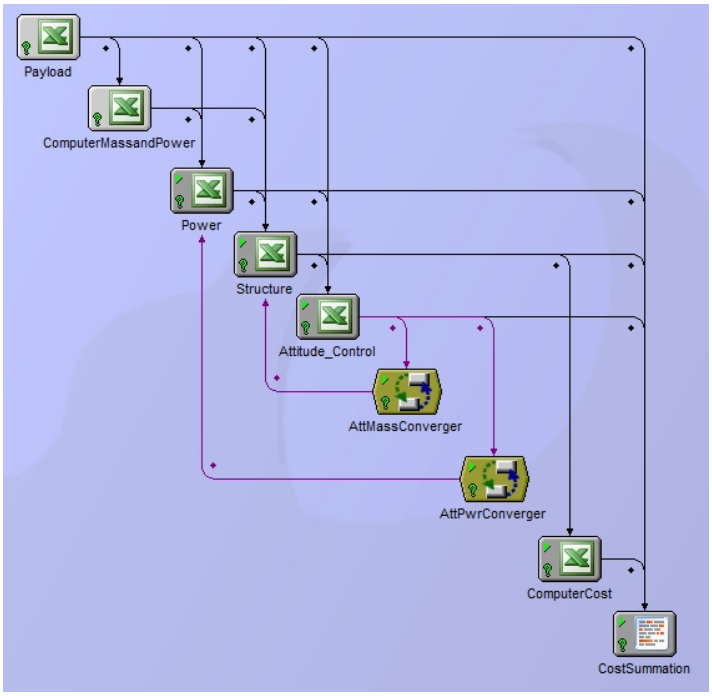

Figure 1. Simplified Spacecraft Model.

cost uncertainty as described by a simulated expert judgment, schedule uncertainty derived from expert judgment, and risk of mission loss provided by dynamic FMECA should constitute the risk vector, as seen in Equation 3. These four risk metrics were selected for this example because they are representative of some of the largest concerns of stakeholders in spacecraft design.

$$\overrightarrow{Risk} = \begin{Bmatrix} MissionLoss : MaxRPN \\ MissionLoss : AverageRPN \\ ExpertJudgment : CostOverrunUncertainty \\ ExpertJudgment : ScheduleUncertainty \end{Bmatrix} \quad (3)$$

4.3 Developing Subsystem Risk Models

With the risk vector created, the next step is to create and integrate risk models for each subsystem. As outlined in Section 3.2.3, the dynamic FMECA models were created with a minimum of two and a maximum of 10 events that could cause mission loss. Different quantities of failure events were populated in each subsystem to demonstrate the need of more than one RPN metric to display the underlying risks. The two metrics derived from the FMECA and populated into the risk vector are Max RPN and Average RPN. Figure 2 shows the power subsystem dynamic FMECA which is typical of the FMECAs implemented for each subsystem in the simplified spacecraft example. The gray boxes indicate which inputs are being dynamically driven by the rest of the power subsystem model. That is, the dynamically driven values of the FMECA are being automatically updated throughout the trade study by inputs from the rest of the subsystem model. The other boxes in the FMECA are static values that do not change in response to inputs. It should be noted that all numeric data in Figure 2 are hypothetical and only useful in this the context of this research.

The expert judgment of cost overrun uncertainty was simulated using simple formulas driven by inputs from other portions of the subsystem models. For instance, the power subsystem calculated the expert judgment of cost overrun uncertainty by multiplying the power subsystem cost by a percentage that the cost overrun was expected to achieve. Simulation was used rather than subsystems chairs in order to create a large number of conceptual designs quickly. For the purposes of this case study, using a formula rather than a human does not affect the results. However, were this trade study to be used in the real world, subsystems chairs would have to determine this risk metric. The units on this risk metric are US dollars.

The expert judgment of schedule uncertainty is derived from formulas using subsystem variables as inputs and from expert judgment. Different subsystems relied upon different formulas to determine the schedule uncertainty. For instance, the power subsystem used mission life as the model-driven input. The expert judgment input was entered by the subsystems chairs at the beginning of the trade study session. The two inputs were multiplied and divided by a standard correction factor. Subsystems engineers are free to change the expert judgment variable that they directly control. In this case study, the human-controlled input variable was set only once.

4.4 Integrating Subsystem Risk Vectors into the System-Level Risk Vector

After risk has been integrated into the subsystem models, the subsystem risk vectors are merged together to create the system-level risk vector. In the case of the two expert judgment variables, the subsystems expert judgment metrics are simply summed to produce a worst-case picture of the risk and uncertainty these two variables present. The FMECA RPN metrics are dealt with in the same manner as was outlined in Section 3.2.4.

4.5 Trading Risk

With risk integrated in the simplified spacecraft model, a trade study is performed. Next, the model is once again created in ModelCenter but with the risk-specific components added. New summing functions and a simple Microsoft Excel spreadsheet are added to calculate the system-level risk vector. The resulting model is shown in Figure 3. The three boxes highlighted in the lower right corner of the figure contain the system-level risk vector and are not present in the simplified spacecraft model that does not contain risk (Figure 1).

Function	Failure Mode	Effects	Severity	Cause(s)	Occurrence	Detection	Criticality	RPN
Power Delivered	Power Subsystem Failure	Mission Loss	10	Aliens	7.4	10	3	740
Power Delivered	Power Cable to Camera Failure	Camera Functionality Loss	10	Vibrations	1	3	10	30
Power Delivered	Partial Solar Panel Loss	Mission Science Diminished	5	Micrometeor	3.7	10	5	185

Figure 2. The power subsystem dynamic FMECA. It is typical of the dynamic FMECA models implemented in each subsystem of the simplified spacecraft model. The gray boxes indicate inputs being dynamically driven by the power subsystems model. It should be noted that all data presented in this graphic is hypothetical and only useful in the context of this research.

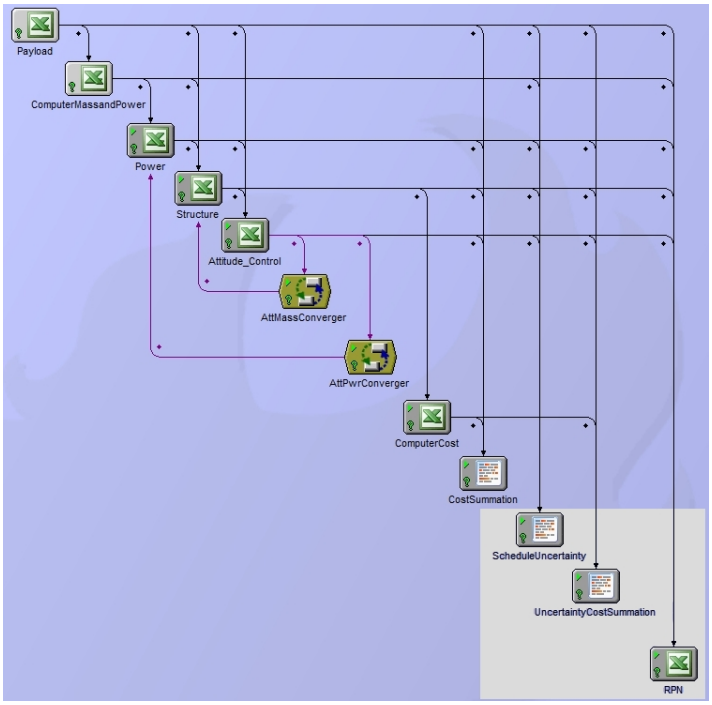

Figure 3. Simplified spacecraft model with risk. The three highlighted boxes in the lower right corner contain the system-level risk vector and are not present in Figure 1.

A Latin-Hypercube was run to create 200 designs. Design and variables were the same as in Section 4.1 with the addition of the risk vector components as response variables. After the initial 200 conceptual designs were created the system model was driven to find designs with long mission life and low cost, as was done in Section 4.1. The system model was also simultaneously driven to find designs with a minimized risk vector. The only difference between the trade studies performed with a risk vector and without a risk vector is the addition of the risk vector and its associated preference. Everything else is identical between the two models and trade studies. The results are discussed in Section 5.

5 RESULTS

The results of the simplified spacecraft model without risk and the simplified spacecraft model with risk are presented in this section. The most preferential designs are shown to be different between the two sets of results. Adding $\overrightarrow{Risk}$ and subsequently giving preference to designs with low $\overrightarrow{Risk}$ changes the most preferred designs. Furthermore, three methods of $\overrightarrow{Risk}$ visualization are demonstrated with data from the simplified spacecraft example. The three methods are compared for usefulness and appropriateness. Direction is provided on which of the $\overrightarrow{Risk}$ visualization techniques is most appropriate for various audiences.

5.1 Simplified Spacecraft Model Without Risk

The results of the simplified spacecraft model trade study are presented in Figure 4. Equal preference was given to designs with high science value, low cost, and long mission life. Other variables were given no preference. The size of the box and the shade of the box indicates preference of the design. The best design is the largest box with the darkest shading. The most preferential designs are clustered together within the oval drawn on the graphic.

5.2 Simplified Spacecraft Model With Risk

The results of the simplified spacecraft with risk trade study can be seen in Figure 5. Preference is indicated by the size and shading of the point with the larger and darker shaded points indicating higher preference designs. The most preferential designs are spread across the Mission Life axis and at the upper end of the Science Return axis. They have been highlighted with arrows for clarity.

As can be seen in Figure 5, the most preferential design points, indicated with arrows, are scattered across the upper left side of the trade space. This is directly as a result of the design preferences that were set to prefer long mission life, low cost, high science return, and low $\overrightarrow{Risk}$. Had preference not been placed on low $\overrightarrow{Risk}$, the preferred designs would have been identical to those found in the simplified spacecraft model without risk where the preferred designs are clustered together in the extreme upper left.

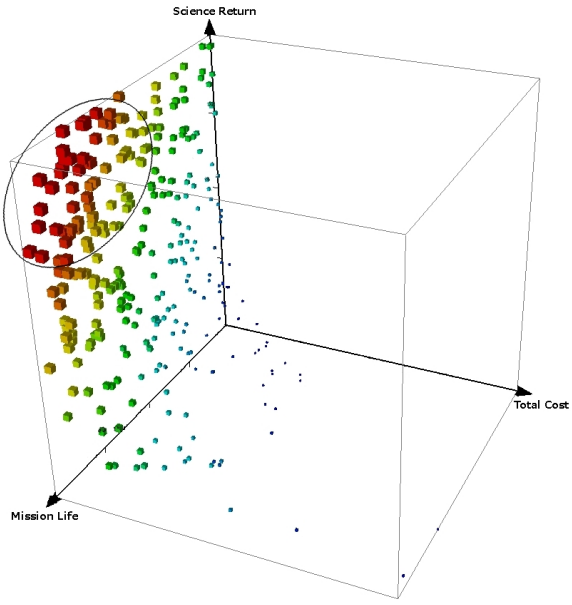

Figure 4. Simplified spacecraft model without risk trade study containing 300 designs. Preference is indicated by size and shading of point. The larger and darker the point, the more preferable the conceptual design. The most preferred designs are clustered within the oval.

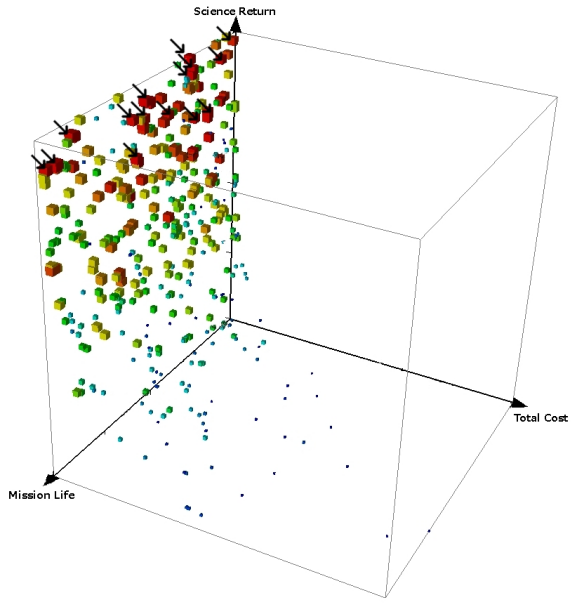

Figure 5. Simplified spacecraft model with risk trade study containing 300 designs. Preference is indicated by size and shading of point. The larger and darker the point, the better the conceptual design. The most preferential designs are indicated by arrows.

Schedule Uncertainty (Years)	0.284961714
Total Uncertainty Cost (Dollars)	1.20882E+11
Average System RPN	128.8512227
Max System RPN	318.3333333

Figure 6. A numeric representation of the risk vector. Note that the numeric values are hypothetical and only useful in the context of this research.

5.3 Visualization of the Risk Vector

There are several ways to visualize the risk vector for use in human-generated trade studies: displaying numeric values for the risk vector shown in Figure 6, multi-dimensional visualization techniques such as a parallel axis graph shown in Figure 7, and an overall risk number that is color-coded. It should be noted that all numeric values are hypothetical and only useful in the context of this research.

Figure 6, Figure 7, and the color coding are all drawn from the simplified spacecraft example. The numeric representation of $\overrightarrow{Risk}$ in Figure 6 is most useful for engineers and others who want to see quantified details for each component of the system-level risk vector. However, numerically displaying all of the components of $\overrightarrow{Risk}$ can become overwhelming when a great number of risk metrics is included.

Displaying $\overrightarrow{Risk}$ on a parallel axis graph as in Figure 7 is useful for engineers. However, caution must be employed when using a parallel axis graph as it is possible for people who are not well-versed in risk to become unnecessarily concerned. A better choice for people overly concerned about risk is a color coded indicator. It is useful to quickly assess overall risk and to hide data that might be unnecessary and a cause for unwarranted concern in some trade study participants. However, a color coded indicator is not particularly useful for subsystems chairs who need detailed risk information.

While it is possible to use all three of these methods of visualization at the same time and display all three visualizations on the same screen, doing so can result in information overload. Unwarranted concern can also be generated by showing too much and too detailed of risk information to people who are not trained in risk methods. It is therefore desirable to display only the method of visualization that is most understandable and useful for the person or people viewing the information. In a CDC setting, this is implemented by displaying the color indication of overall risk level to all trade study participants and observers via a central large display. Individual subsystem workstations display either parallel axis graph $\overrightarrow{Risk}$ visualizations or numeric $\overrightarrow{Risk}$ visualizations depending upon the preference of each subsystems chair. Segregating $\overrightarrow{Risk}$ visualizations in this manner minimizes information overload and helps to keep concerns over $\overrightarrow{Risk}$ at a

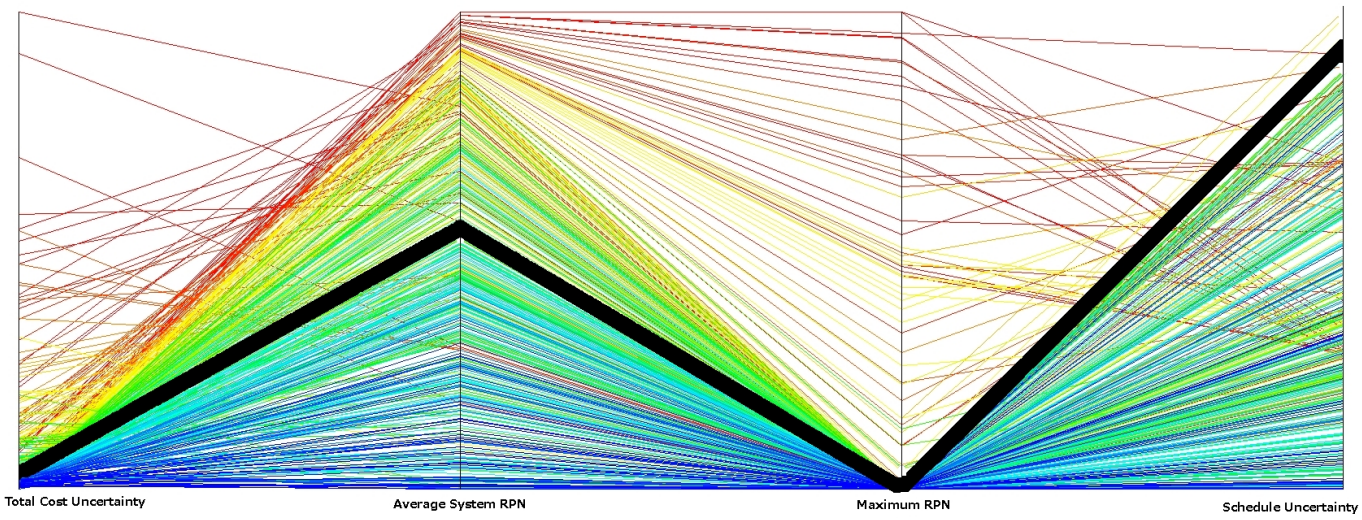

Figure 7. A parallel axis graph visual representation of the risk vector. The heavy line indicates the current conceptual design under review. The other lines indicate the full spread of the design space.

reasonable level.

5.4 Comparison of the Risk and Risk-less Results

As can be seen in Figures 4 and 5, the most preferential designs in the simplified spacecraft model with risk are found in a different area of the design space than the most preferential designs in the simplified spacecraft model without risk. The most preferential designs are clustered in the upper left corner of the design space in the simplified spacecraft model without risk, as shown in Figure 4. The most preferential designs in the simplified spacecraft model with risk are scattered across the entire length of the upper portion of the design space along the mission life axis as shown in Figure 5. This is directly as a result of adding $\overrightarrow{Risk}$ as a design parameter and adjusting preferences to find designs with a minimum level of risk. When the preferences are expanded to include $\overrightarrow{Risk}$, different designs in a different portion of the design space are found to be the most preferred.

The differences between the risk and risk-less results are a direct result of the subsystem risk models. In the subsystem risk models, low cost, long mission life, and high science return are generally not correlated with low risk. Because of this, designs that are the most preferred under the risk-less trade study become less preferred in the trade study containing risk models.

6 DISCUSSION AND SPECIFIC CONTRIBUTIONS

Adding risk vectors to trade studies allows for new preferences to be created that otherwise would not have been available to the designers. Adding new design variables in the form of $\overrightarrow{Risk}$ enables the engineers to find designs with higher utility than if risk was ignored. It is therefore desirable to include $\overrightarrow{Risk}$ in trade studies.

Adding a risk vector comprised of multiple risk metrics to trade study subsystem models that are then traded to create conceptual designs allows for risk to be brought on par with other important system-level variables. Rather than being an afterthought as it is in existing methods, risk is able to be considered during the creation of conceptual designs. Both computational methods such as FTA and FMECA, and expert judgment can be captured and used with this method.

When developing FMECA, FTA, or similar numeric models to be used with the risk trading method developed in this paper, one can base risk calculations on variables. This is used on most of the risk models embedded in the simplified spacecraft example used in this research. When accurate, dynamic risk models can be very beneficial to help shape conversations in CDC environments during trade study sessions.

The risk trading methodology presented here addresses the shortcomings of previously developed methods. The RAP tool [24], the methodology built on top of NASA CRM [32], and Tunnissen's normative method [34] do not consider risk as part of the conceptual design creation process during trade studies. Instead these methods consider risk either after designs have been created or before trade studies have been conducted. Charanian et. al. [37] address this shortcoming by introducing trading risk in trade studies. However, they maintain risk as an isolated "subsystem" as RAP does. DDP [28] suffers from being perceived as an overly complicated tool. These deficiencies have been addressed in the risk trading methodology introduced in this paper. Risk has been integrated into each subsystem model and aggre-

gated at the system level via a risk vector. This enables subsystem chairs to control risk in each subsystem and trade risk with other system-level parameters to maximize overall system utility.

One major drawback to this method is the level of training and coordination required for subsystems engineers to generate useful risk data. All of the people involved in generating risk data to be used in a trade study must speak the same risk language. If one person is producing data under a different set of assumptions, different definitions, or using different methods, $\overrightarrow{Risk}$ becomes an invalid parameter for multi-attribute decision making when setting design preferences and for trading parameters during the design process. However, bringing an entire CDC team up to speed and teaching everyone how to speak the same risk language is far from a bad thing. An alternative approach could take the form of a system to translate the risk language that one person speaks into terms and quantities that another person can understand.

One potential solution to address differences in the understanding of risk between different people is to introduce a normalized risk vector. This could take several forms including but not limited to the following. The risk vector can be normalized by normalizing the risk metrics that comprise the risk vector to present all components of the risk vector on the same scale. Risk data being produced and consumed by individual subsystems engineers can be normalized to each person's individual risk profile. Doing this will allow people to produce and consume risk information naturally and without having to conform to risk concepts that might not hold significant meaning to some individuals.

Another issue with this method is the lack of subsystems interaction effects in risk models. No way of effectively capturing risks of emergent behaviors is provided. This is an area that must be developed further in the future for this method to more comprehensively capture risk in the early stages of conceptual design. One potential method of addressing subsystem interaction effects is to use geometric proximity models to model spurious energy, mass, and signal propagation between disconnected subsystems.

In spite of the deficiencies of this method in its current state, the ability to bring risk into the early conceptual design process as an equal partner to other system-level parameters is a valuable contribution to the processes that currently exist in practice and the literature. The risk trading method introduced in this paper provides an excellent way of capturing and quantifying expert risk knowledge.

7 CONCLUSION AND FUTURE WORK

In typical complex system design trade studies, risk does not explicitly play a role in the creation and selection of conceptual designs. It is only assessed after a conceptual design has been created. This research presents a method of explicitly trading, and evaluating designs based upon risk in design trade studies among subsystems with the goal of maximizing system utility and system integrity.

The method presented in this paper details a novel way to assess risk and make decisions based on risk in the complex conceptual design process. Risk is treated as a vector with multiple components defined by the requirements of the system. The risk vector is traded in design trade studies. Based upon the desired level of risk for a system, specific point designs or portions of the design space can be identified for further study and development. Risk has traditionally been treated as an afterthought or completely ignored in the conceptual complex system design process. By moving risk into trade studies and giving it a place among other important more traditional system-level variables such as power, mass, etc., conceptual designs will be explicitly created and selected based on risk metrics.

For the risk trading method to be adopted, additional examples using expanded risk methods must be developed. Trade studies must also be conducted by real-world practitioners to verify and enhance the method with their feedback. Further a method of accounting for subsystem interaction risks must also be developed.

Trading risk in early conceptual complex system design holds great promise. This paper aims to start a larger effort to set risk in line with system-level design parameters. No longer can risk be a mere afterthought in conceptual design. It must share equal weighting with other important design metrics.

ACKNOWLEDGMENT

This research was carried out in part at JPL, Caltech, under contract with NASA. Special thanks goes to Scott Ragon, Taurik Elgabrowny, and others at Phoenix Integration for providing software donations and technical support, and Steve Cornford at JPL for providing valuable feedback and inspiration. Any opinions or findings of this work are the responsibility of the authors, and do not necessarily reflect the views of the sponsors or collaborators.

REFERENCES

[1] Phoenix Integration Inc., 2008. Phx model center, Nov. `http://www.phoenix-int.com/software/phx_modelcenter.php`.

[2] Wertz, J. R., and Larson, W. J., 1999. *Space Mission Analysis and Design*. Springer.

[3] NASA, 1995. *NASA Systems Engineering Handbook*. NASA.

[4] FAA, 2006. *National Airspace System System Engineering Manual*, 3.1 ed. Federal Aviation Administration ATO Operations Planning.

[5] Ross, A. M., Hastings, D. E., Warmkessel, J. M., and Diller, N. P., 2004. "Multi-attribute tradespace exploration as front

end for effective space system design". *Journal of Spacecraft and Rockets,* ***41***(1), pp. 20–29.

[6] Ravi, B., and Srinivasan, M. N., 1990. "Decision criteria for computer-aided parting surface design". *Journal of Computer Aided Design,* ***22***.

[7] Russell, J. S., and Skibniewski, M. J., 1988. "Decision criteria in contractor prequalification". *Journal of Management in Engineering,* ***4***(2), pp. 148–164.

[8] Bacon, C. J., 1992. "The use of decision criteria in selecting information systems/technology investments". *MIS Quarterly,* ***16***(3), pp. 335–353.

[9] Ji, H., Yang, M. C., and Honda, T., 2007. "A probabalistic approach for extracting design preferences from design team discussion". In Proceedings of the ASME Design Engineering Technical Conferences; Computers and Information in Engineering Conference, IDETC/CIE.

[10] Papalambros, P. Y., and Wilde, D. J., 2000. *Principles of Optimal Design: Modeling and Computation*. Cambridge University Press.

[11] Shishko, R., 2000. "The proliferation of pdc-type environments in industry and universities". In Proceedings of the 2nd European Systems Engineering Conference, EuSEC.

[12] Deutsch, M.-J., and Nichols, J. S., 2000. "Advanced approach to concept and design studies for space missions". *Astrophysics and Space Science,* ***273***, pp. 201–206.

[13] Oberto, R. E., Nilsen, E., Cohen, R., Wheeler, R., DeFlorio, P., and Borden, C., 2005. "The nasa exploration design team: Blueprint for a new design paradigm". In Proceedings of the 2005 Aerospace Conference, no. 8957662 in IEEE Conferences, IEEE, pp. 4398–4405.

[14] Gough, K. M., Allen, B. D., and Amundsen, R. M., 2005. "Collaborative mission design at nasa langley research center". In Space Systems Engineering Conference.

[15] Edelson, R. E., 2000. "Team z, a rapid reaction approach to mission operations system design and costing". In The Proceedings of SpaceOps, AIAA.

[16] Oxnevad, K. I., 1998. "A concurrent design approach for designing space telescopes and instruments". In Space Telescopes and Instruments.

[17] Karpati, G., Martin., J., and Steiner, M., 2003. "The integrated mission design center (imdc) at nasa goddard space flight center". In Aerospace Conference.

[18] Bandecchi, M., Melton, B., and Ongaro, F., 1999. "Concurrent engineering applied to space mission assessment and design". *ESA Bulletin,* ***99***.

[19] Osburg, J., and Mavris, D., 2005. "A collaborative design environment to support multidisciplinary conceptual systems design". *SAE Transactions,* ***114***, pp. 1508–1516.

[20] Finkel, S., Wilke, M., Metzger, H., and Wahnfried, M., 2002. "Design centers - transfering experience from astronautics to aeronautics". In Proceedings of the 12th Annual Symposium of the International Council on Systems Engineering, INCOSE.

[21] Masher, T. J., and Kwong, J., 2004. "The space systems analysis laboratory: Utah state universitys new concurrent engineering facility". In Aerospace Conference.

[22] Aguilar, J. A., Dawdy, A. B., and Law, G. W., 1998. "The aerospace corporations concept design center". In Proceedings of the 8th Annual International Symposium of the International Council on Systems Engineering.

[23] Bennett, R., and Roberts, B., 2000. "Risk management for the nasa/jpl genesis mission: A case study". In Proceedings of the 2000 International Council on Systems Engineering Conference, INCOSE.

[24] Meshkat, L., 2007. "A holistic approach for risk management during design". In IEEE Aerospace Conference.

[25] McManus, H. L., Hastings, D. E., and Warmkessel, J. M., 2004. "New methods for rapid architecture selection and conceptual design". *Journal of Spacecraft and Rockets,* ***41***(1), January-February, pp. 10–19.

[26] McManus, H. L., and Warmkessel, J. M., 2004. "Creating advanced architectures for space systems: Emergent lessons from new processes". *Journal of Spacecraft and Rockets,* ***41***, pp. 69–75.

[27] Benjamin, J. L., and Pate-Cornell, M. E., 2004. "Risk chair for concurrent design engineeering: Satellite swarm illustration". *Journal of Spacecraft and Rockets,* ***41***(1), pp. 51–59.

[28] Cornford, S. L., Dunphy, J., and Feather, M. S., 2002. "Optimizing the design of spacecraft systems using risk as currency". In IEEE Aerospace Conference.

[29] Cornford, S. L., 1998. "Managing risk as a resource using the defect detection and prevention process". In 4th International Conference on Probabilistic Safety Assessment and Management.

[30] Meshkat, L., Voss, L., Cornford, S. L., and Feather, M. S., 2005. "An integrated approach to risk assessment for concurrent design". In *IEEE Aerospace Conference*. IEEE.

[31] Cornford, S. L., Feather, M. S., and Jenkins, J. S., 2006. "Intertwining risk insights and design decisions". In Eigth International Conference on Probabilistic Safety Assessment and Management.

[32] Dezfuli, H., Youngblood, R., and Reinert, J., 2007. "Managing risk within a decision analysis framework". In Second International Association for the Advancement of Space Safety Conference, IAASS.

[33] Stamatelatos, M., Dezfuli, H., and Apostolakis, G., 2006. "A proposed risk-informed decision-making framework for nasa". In Eigth International Conference on Probabilistic Safety Assessment and Management.

[34] Thunnissen, D. P., 2004. "Balancing cost, risk, and performance under uncertainty in preliminary mission design". In AIAA Space Conference.

[35] Guikema, S. D., and Pate-Cornell, M. E., 2004. "Bayesian

analysis of launch vehicle success rates". *Journal of Spacecraft and Rockets,* ***41***(1), pp. 93–102.

[36] Thunnissen, D. P., and Tsuyuki, G. T., 2004. "Margin determination in the design and development of a thermal control system". In 34th International Conference on Environmental Systems (ICES).

[37] Charania, A. C., ohn E. Bradford, J., Olds, J. R., and Graham, M., 2002. "System level uncertainty assessment for collaborative rlv design". In Second Modeling and Simulation Subcommittee Joint Meeting.

[38] Parkin, K. L., Sercel, J. C., Liu, M. J., and Thunnissen, D. P., 2003. "Icemaker: An excel-based environment for collaborative design". In Aerospace Conference.

[39] Stump, G. M., Yukish, M., Simpson, T. W., and O'Hara, J. J., 2004. "Trade space exploration of satellite datasets using a design by shopping paradigm". In Aerospace Conference.

[40] Simpson, T. W., Carlsen, D. E., Congdon, C. D., Stump, G., and Yukish, M. A., 2008. "Trade space exploration of a wing design problem using visual steering and multidimensional data visualization". In 4th AIAA Multidisciplinary Design Optimization Specialist Conference.

[41] Volk, S. K., Wheeler, R., Wilkinson, B., Jones, M., and Birgel, S., 2000. "Concurrent real time engineering via the fredrik work environment: Helping engineers produce their products by structuring their access to relevant information". In Proceedings of the International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, WETICE.

[42] Meshkat, L., Weiss, K. A., Luna, M., and Leveson, N., 2006. "Supporting concurrent engineering in jpls advanced project design team using a systems engineering development environment". In Proceedings of Virtual Concept.

[43] IEEE, 1990. *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. IEEE, New York, NY.

[44] Du, X., and Chen, W., 2000. "Towards a better understanding of modeling feasibility robustness in engineering design". *ASME Journal of Mechanical Design,* ***122***(4), pp. 385–394.

[45] Martin, J. D., and Simpson, T. W., 2006. "A methodology to manage system-level uncertainty during conceptual design". *ASME Journal of Mechanical Design,* ***128***, pp. 959–968.

[46] Thunnissen, D. P., 2003. "Uncertainty classification for the design and development of complex systems". In 3rd Annual Predictive Methods Conference.

[47] of Defense, D., 1980. Procedures for performing failure mode, effects, and criticality analsysis. MIL-STD-1629A.

[48] AIAG, 1993. *Potential Failure Mode and Effects Analysis (FMEA) Reference Manual*. Automotive Industry Action Group.

[49] Commission, I. E., 1990. International standard iec 61025 fault tree analysis.

[50] Hardman, D. K., and Ayton, P., 1997. "Arguments for qualitative risk assessment: the star risk adviser". *Expert Systems,* ***14***, pp. 24–36.

[51] McCormick, N. J., 1981. *Reliability and Risk Analysis (Methods and Nuclear Power Applications)*. Academic Press.

[52] , 1997. Iso 10628: Flow diagrams for process plants - general rules.

[53] Villemeur, A., 2000. *Reliability, Availability, Maintainability, and Safety Assessment*. John Willey and Sons.

[54] Kurtoglu, T., and Tumer, I. Y., 2008. "A graph-based fault identification and propagation framework for functional design of complex systems". *Journal of Mechanical Design,* ***30***(5).

[55] Stone, R. B., Tumer, I. Y., and Wie, M. V., 2005. "The function-failure design method". *Journal of Mechanical Design,* ***127***(3), May, pp. 397–407.

[56] Mehr, A. F., and Tumer, I. Y., 2006. "Risk-based decision-making for managing resources during the design of complex space exploration systems". *Journal of Mechanical Design,* ***128***, July, pp. 1014–1022.

[57] Jensen, D., Tumer, I. Y., and Kurtoglu, T., 2009. "Flow state logic (fsl) for analysis of failure propagation in early design". In ASME International Design Theory and Methodology Conference, IDETC/CIE2009.

[58] Tumer, I. Y., Stone, R. B., and Roberts, R. A., 2003. "Analysis of jpl's problem and failure reporting database". In ASME International Design Engineering Technical Conferences / Design Engineering Technology Conference, IDETC/DTM.

[59] Uder, S. J., Stone, R. B., and Tumer, I. Y., 2004. "Failure analysis in subsystem design for space missions". In ASME International Design Engineering Technical Conferences / Design Engineering Technology Conference, IDETC/DTM.

[60] Grantham-Lough, K., Stone, R., and Tumer, I. Y., 2007. "The risk in early design method". *Journal of Engineering Design,* ***20***, Apr., pp. 155–173.

[61] Grunske, L., Kaiser, B., and Papadopoulos, Y., 2005. "Model-driven safety evaluation with state-event-based component failure annotations". In Component-Based Software Engineering.

[62] Hoyle, C., Mehr, A. F., Tumer, I. Y., and Chen, W., 2009. "Health management allocation for conceptual system design". *ASME Journal of Computing & Information Sciences in Engineering,* ***9***.

[63] Vesley, W. E., Goldberg, F. F., Roberts, N. H., and Haasi, D. F., 1981. The fault tree handbook. Tech. rep., US Nuclear Regulatory Commission.

Nomenclature

ATSV Advanced Trade Space Visualization
CATIA Computer Aided Tridimensional Interactive Application
CDC Collaborative Design Center
EES Engineering Equation Solver
ESA European Space Agency
ETA Event Tree Analysis
FFDM Function Failure Design Method
FFIP Functional Failure Identification Propagation
FMEA Failure Modes and Effects Analysis
FMECA Failure Modes and Effects Criticality Analysis
FTA Fault Tree Analysis
HiPHOPS Hierarchically Performed Hazard Origin and Propagation Studies
JPL Jet Propulsion Laboratory
LaRC Langley Research Center
NASA National Aeronautics and Space Administration
PRA Probabilistic Risk Assessment
QRA Qualitative Risk Assessment
RBD Reliability Block Diagram
RED Risk in Early Design
RUBIC Risk and Uncertainty Based Integrated and Concurrent design methodology
RPN Risk Priority Number
RAP Risk and Rationale Assessment Program
DDP Defect Detection and Prevention
CRM Continuous Risk Management
PDC Project Design Center