Res Eng Design (2013) 24:259–275
DOI 10.1007/s00163-012-0142-0

ORIGINAL PAPER

A case for trading risk in complex conceptual design trade studies

Douglas L. Van Bossuyt · Irem Y. Tumer · Stephen D. Wall

Received: 15 June 2011 / Revised: 7 September 2012 / Accepted: 11 September 2012 / Published online: 22 September 2012

Abstract Complex conceptual system 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. A trade study example is presented based upon a simplified spacecraft model. Results from introducing the risk trading methodology into a simulated Collaborative Design Center are presented. The risk trading method offers an approach to more thoroughly consider risk during the creation of conceptual designs in trade studies.

D. L. Van Bossuyt (✉) · I. Y. Tumer
School of Mechanical, Industrial, and Manufacturing Engineering, Oregon State University, Corvallis, OR 97331, USA
e-mail: Douglas.VanBossuyt@gmail.com

I. Y. Tumer
e-mail: Irem.Tumer@oregonstate.edu

S. D. Wall
Jet Propulsion Laboratory, System Modeling and Analysis Program Office, California Institute of Technology, Pasadena, CA 91019, USA
e-mail: Stephen.D.Wall@jpl.nasa.gov

Keywords Trade study · Complex system design · Risk · Collaborative Design Center risk trading

1 Introduction

Risk has traditionally been an afterthought in the conceptual complex system design process. Risk is typically only formally assessed after a conceptual design has been created and does not explicitly play a role in the creation and selection of conceptual designs. Instead, implicit assumptions are often made about the "riskiness" of conceptual design models. Our hypothesis is that by moving risk into trade studies and giving it a place among more traditional system-level variables such as power and mass, 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.

In this paper, various risk metrics are placed in a vector denoted as $\overrightarrow{\text{Risk}}$. Risk in the engineering context is defined as the severity of a risk outcome multiplied by the probability that the event will occur (International Organization for Standardization 2009). The risk vector is traded in design trade studies. Based upon the desired level of $\overrightarrow{\text{Risk}}$ 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 Inc.'s ModelCenter (Phoenix Integration Inc. 2008) and demonstrated in a simulated Collaborative Design Center (CDC) environment using undergraduate and graduate participants

as subsystem engineers with direct control over subsystem decisions. In a previous conference paper (Van Bossuyt et al. 2010), the authors tested an earlier version of the method using an automated trade study.

The idea for this paper started after observing several Team X trade study sessions at the Jet Propulsion Laboratory (JPL). Through conversations with personnel currently and previously involved in Team X and similar groups, it became evident that the issue of accounting for risk in a meaningful way in trade studies needed to be addressed beyond what can be found in literature and practice. Development of the method presented in this paper followed. After positive feedback from a conference paper on the method (Van Bossuyt et al. 2010), the method was then tested on a simulated CDC environment using college students as subsystem engineers. In the future, the authors plan to test the method in an industrial CDC environment.

The following sections include background on trade studies; CDCs; trade study software; risk, reliability, robustness, and uncertainty methods; related work; and other necessary background information. The methodology to trade risk is developed and demonstrated in a trade study using a simplified spacecraft model adopted from Wertz and Larson (1999). Future work to expand the methodology is outlined.

The risk trading method presented in this paper allows for new design selection preferences to be created that otherwise would not be available to design engineers. Adding new design variables in the form of $\overrightarrow{Risk}$ enables engineers to find designs with higher utility as partially defined by risk metrics than if risk was ignored in design trade studies. This allows risk to be brought on par with other important system-level variables rather than being considered only after conceptual designs have been developed.

1.1 Design trade studies fundamentals

Design trade studies are used in conceptual complex system design to generate different design alternatives and compare among them. Trade studies can be performed either automatically using software packages or by teams of people. Whereas automated, computer-generated trade studies can create many thousands of design points quickly, manually conducted human-generated trade studies are often seen as having higher fidelity and are more likely to be accepted (Osburg and Mavris 2005). The demonstrative trade studies in this paper are all manual trade studies conducted with the assistance of computers.

Metrics such as cost, mass, power, volume, and other parameters are often traded in such trade studies. Each subsystem within a complex system is initially allocated specific amounts of the constraining 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 subsystem designers (NASA 1995; FAA 2006; Ross et al 2004). The resulting conceptual designs can then be ranked according to appropriate selection rules (Russell and Skibniewski 1988; Ji et al. 2007).

When there is a defined "measure of goodness," the basic mathematical concept behind trade studies is simple and straightforward. Trade-offs are made between design variables to achieve maximum design utility (Papalambros and Wilde 2000). 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 (Papalambros and Wilde 2000).

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 (NASA) JPL's Project Design Center (PDC) and the associated design team, commonly referred to as Team X. The group, formed in June 1994 (Shishko 2000), functions as a conceptual spacecraft mission design team.

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 (Deutsch and Nichols 2000). The design iteration portion of most Team X trade studies are completed in 2–3 days, compared to 3–9 months to complete a comparable trade study (Oberto et al. 2005). Team X has also reduced the cost of concept-level spacecraft mission design by a factor of five compared to conventional design processes (Oberto et al. 2005).

Within Team X and other CDC groups, there are often desired ranges 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 are desired. In the case of Team X, this is due to the desire to launch missions that are both cost-effective and challenging. Missions at NASA are selected for further development based on several factors including the mission risk profile. A risk target range has been defined that balances pushing the boundaries of engineering and science with a desired cost and level of mission success (Bennett and Roberts 2000).

1.3 Trade study software

Many formal trade studies are conducted using software packages. Commercially available and academic software packages exist that support both manual and automated trade studies. They include ICEMaker (Parkin et al. 2003), ATSV (Stump et al. 2009), and ModelCenter (Phoenix Integration Inc. 2008) among others (Meshkat et al. 2006).

This paper uses ModelCenter in the development of a risk trading methodology. Details of ModelCenter's use in CDC environments can be found in Van Bossuyt and Tumer (2010). However, the methods developed here are applicable in any other trade study software tool, whether for manual or automated trade studies.

1.4 Risk, reliability, robustness, and uncertainty

Trading any variable in a trade study requires agreed-upon definitions and values of the variables. 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, defining the value of "risk" is difficult and more abstract. This paper uses the strict engineering definition of risk where risk is defined as the probability of an event occurring multiplied by the impact of that event.

Risk is often defined in engineering as the probability of occurrence multiplied by the severity of impact (International Organization for Standardization 2009). 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 (IEEE 1990)." 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 (Du and Chen 2000). Uncertainty is a result of a lack of knowledge about system specifications, and errors resulting from imperfect models (Martin and Simpson 2006). Some researchers further break down uncertainty into multiple subcategories that often contain elements of risk, reliability, and robustness (Thunnissen 2003). This research uses the engineering definition of risk: probability of occurrence multiplied by severity of impact.

1.5 Risk analysis techniques

It is necessary for the methodology presented in this paper to be able to quantify risk, as defined by the probability of occurrence of a risk multiplied by the severity of the realization of the risk (International Organization for Standardization 2009), 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 (Department of Defense 1980; Stamanis 2003). FMEA provides probability and severity information for each identified and analyzed risk.

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 (Keeney and von Winterfeldt 1989). This is the case for both the severity and occurrence portions of risk. Expert judgment has found widespread use in various settings such as the aerospace industry, nuclear engineering, and other areas for many decades (Cooke 1991; Clemen and Winkler 1999). Several methods exist to elicit expert judgment and are covered in detail in the literature (Merkhofer 1987; Mosleh et al. 1987; Bonano et al. 1990; Keeney and von Winterfeldt 1989, 1991; Hora 1992; Otway and von Winterfeldt 1992). 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 (International Electrotechnical Commission 1990).

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) (Hardman and Ayton 1997), Event Tree Analysis (ETA) (McCormick 1981), Reliability Block Diagram (RBD) (International Organization for Standardization 1997), Probabilistic Risk Assessment (PRA) (Villemeur 2000), Functional Failure Identification location Propagation (FFIP) (Kurtoglu and Tumer 2008), Function Failure Design Method (FFDM) (Stone et al. 2005), Risk in Early Design (RED) (Grantham-Lough et al. 2007, 2008), and Risk and Uncertainty Based Integrated and Concurrent design methodology (RUBIC) (Mehr and Tumer 2006)

among others (Lough et al. 2009; Tumer and Stone 2003; Stone et al. 2006). This paper specifically uses FMEA, expert judgment, and FTA for illustration purposes; however, any risk method can be used.

2 Related work

Some CDCs such as Team X currently employ tools and methods to capture risk in the conceptual design process. However, establishment of mission risk posture usually happens before conceptual designs have been generated, and risk evaluation happens afterward, or risk evaluation is part of a process that happens in lieu of trade studies, or worse yet, risk does not play any role in early conceptual design development. But there is generally no accepted method to measure risk within each subsystem model as a parameter to be controlled and developed by individual subsystem chairs during conceptual design trade studies. This section will review several relevant tools and methods that are currently used in CDCs, have been proposed for such use, or could be adapted to the CDC environment.

2.1 Risk- and defect detection–based methods

The Risk and Rationale Assessment Program (RAP) tool is a PRA-based assessment software package that is employed during a trade study session (Meshkat 2007). Each subsystem chair has the ability to enter information into the tool as he/she sees fit. These data contain 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, the "risk chair," is dedicated to monitoring the RAP tool and compiling the data entered by the subsystem chairs to create an overall system-level risk assessment. Other groups outside of NASA have also used tools similar to RAP and with similar implementations yielding similar results and problems (McManus et al. 2004; McManus and Warmkessel 2004; Benjamin and Pate-Cornell 2004).

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 (Cornford et al. 2002). Literature on DDP does state that risk should be traded and provides a framework for trading, but trade studies are not suggested to be performed in CDCs. The literature does suggest that risk can be compared against performance metrics to find the optimum level of risk versus performance, but to examine risk, conceptual designs must be developed and solidified before the DDP method can be used to analyze risk (Cornford et al. 2006). In the authors' opinion, the DDP method suffers from the perception that it is 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. (2007) embeds the NASA Continuous Risk Management (CRM) process that is used in practice in many (NASA) groups into a broader decision framework that has not found use outside of academia. 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 still happens after conceptual designs have been created (Stamatelatos et al. 2006). Thus, the method does not place risk directly in the trade study process.

2.2 Uncertainty- and design margin–based methods

A normative method that attempts to balance cost, risk, and performance for decision-makers in preliminary spacecraft mission design is presented by Thunnissen (2004). 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-subcategories of model uncertainty (approximation errors, numerical errors, and programming errors), and four sub-subcategories of behavioral uncertainty (design, requirement, volitional, and human errors). To deal with the uncertainties, probabilistic methods and Bayesian techniques (Guikema and Pate-Cornell 2004) 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 design margins in trade studies and also attempts to trade risk in trade studies (Thunnissen and Tsuyuki 2004). However, trading risk is presented as 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.

Browning presents a method of modeling impacts of process architecture on cost and schedule risk in

product development (Browning et al. 2002; Browning and Eppinger 2000, 2002). The method examines how rework cascades throughout a process, and the resulting cost and schedule trade-offs. Risk, as partially defined by uncertainty of outcome, can be examined through a utility function in order to incorporate characteristics such as risk aversion into the method. The primary focus of Browning's method is the general process of product development rather than the creation of conceptual designs 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 Inc.'s ModelCenter software package (Charania et al. 2002). 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.

2.3 Robustness methods

Robust design methods have been used for more than 20 years in western engineering practices. Taguchi popularized the use of such robustness methods as factorial experiments and other statistical methods that are now widely used to improve the quality of industrial products (Taguchi 1993, 1986). While Taguchi originally advocated for his methods to be used during parameter design, the portion of the design process following conceptual design, others have since expanded his work into the conceptual portion of the design process (Andersson 1997). In order to improve the product, the methods that comprise robust design strive to make the product insensitive to environmental inputs. Several of the methods developed for the conceptual design process have the potential to be used in trade studies, but to the authors' knowledge, none have been implemented.

The Robust Concept Design Methodology (RCDM) proposed by Ford and Barkan (1995) loosely mirrors the trade study process. Stages 3 and 4 of the method develop a conceptual design, evaluate the design, and iterate as necessary. The main difference in this method as compared to trade studies is that robustness is treated as the only system-level parameter of merit. In trade studies, many different system-level variables can be considered at once.

Andersson presents a semi-analytic method based upon the error transmission formula with the goal of achieving conceptual robustness (Andersson 1996). The method aids engineers in making preliminary assessments of the levels of design variables to prepare for subsequent phases of design. A means of analyzing predetermined dependency relationships is also provided. In order to make these assessments, well-defined design functions are required which can be a hindrance during early-phase conceptual design where strong analytic functions are not always available.

Ziv Av and Reich (2005) develop the Subjective Objective System (SOS) method which generates optimized conceptual designs for diverse disciplines and a complementary procedure to develop robust conceptual designs (Reich and Ziv Av 2005). SOS has the ability to model design information at several different levels of resolution which resemble the House of Quality (Ullman 2003). The SOS method integrates market, technology, and organization information in order to produce design concepts matched to the market. The robust product concept generation method, an expansion of SOS, allows robustness to be traded with other aspects of a conceptual design as it is being generated. The method further allows a local sensitivity analysis of the resulting conceptual designs to determine how stable the concept is when customer parameters vary. While the methods developed by Ziv Av and Reich can model risk as a system goal, the methods are not explicitly developed for trade studies and do not place control subsystem risk models with subsystem engineers.

The robust decision-making concept developed by Ullman (2001) presents a 12-step method put forward as necessary to make robust decisions. Steps 5 through 7 extend Quality Function Deployment (QFD) to accept robustness product information. Step 8 develops multiple design alternatives with an allusion to performing trade studies, while Step 9 evaluates the design alternatives. The concept could conceivably be further extended to include risk, reliability, and uncertainty metrics as important system parameters and does advocate for appropriate decision-makers to be selected and queried. However, the concept does not produce a methodology focused on trading risk as a system-level parameter where all subsystem risk models are controlled by individual subsystem engineers as the method presented in this paper does.

2.4 Summary and contributions

In summary, some methods such as RAP and DDP have found use in some CDCs and elsewhere, while other methods such as those developed by Thunnissen, Charianian et. al., and others remain academic, and some such as SOS and RCDM have not been developed for CDC trade studies. 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, to the authors' knowledge, 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 fills the gap in existing methods.

This paper makes five distinct contributions to the literature including the following. (1) A method 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. (2) The method provides a new means for stakeholders to account for risk in conceptual designs, and for engineers to choose subsystem designs or components based upon risk. (3) Managers selecting specific risk profiles can use this method to identify the most interesting designs. (4) Customers of Team X sessions can use this method to get a different feel for the risk profile of the end design than has been previously available. (5) 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 as a system-level parameter in 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 ($\overrightarrow{\text{Risk}}$) is developed that can be used to contain risk, reliability, robustness, and uncertainty metrics. In this paper, only risk as defined by the probability of an event multiplied by the consequences of its occurrence is used. However, other related concepts such as reliability, robustness, and uncertainty can be similarly traded. 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. Note that to maximize system utility, $\overrightarrow{\text{Risk}}$ does not necessarily need to be minimized. The four steps involved are summarized in the following list and mathematically demonstrated in Eq. 1.

1. Create risk vector schema and choose appropriate risk metrics
2. Implement risk vector into subsystems and populate subsystems models with risk methods
3. Combine subsystem vectors into system-level risk vector
4. Perform trade study using risk vector as a tradeable system-level parameter

$$\text{Max}(\text{Utility}) = [\text{Sys Metric 1}, \text{Sys Metric 2}, \ldots, \overrightarrow{\text{Risk}}] \tag{1}$$

3.1 A risk trading methodology: main steps

The following sections detail the four steps outlined earlier in Sect. 3 that are required to implement and make use of the risk trading methodology. Subsequent sections make use of the risk trading methodology implementation using an illustrative case study to show the utility of the risk trading methodology to practitioners.

3.1.1 Creating a risk vector schema

The first step in the risk trading methodology is to create a risk vector schema. It is often the case in industry and academia that the definitions of risk, reliability, robustness, and uncertainty become blurred and mixed together (Thunnissen 2003). 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 (Thunnissen 2003). 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, $\overrightarrow{\text{Risk}}$, is defined to include all components of risk, reliability, robustness, and uncertainty in a design. As an example, Eq. 2 shows one potential generic $\overrightarrow{\text{Risk}}$ configuration. In the remainder of this paper, only the engineering risk metric portion of $\overrightarrow{\text{Risk}}$ is examined. Engineering risk metrics can include FMEA RPN scores, FTA information, and other relevant risk-related metrics that are defined by the probability of an event multiplied by the consequences of that event.

$$\overrightarrow{\text{Risk}} = \left\{ \begin{array}{l} \text{Engineering risk metric } \#1 \\ \text{Engineering risk metric } \#2 \\ \text{Robustness metric } \#1 \\ \text{Robustness metric } \#2 \\ \text{Reliability metric } \#1 \\ \text{Reliability metric } \#2 \\ \text{Uncertainty metric } \#1 \\ \text{Uncertainty metric } \#2 \end{array} \right\} \tag{2}$$

3.1.2 Implementing and populating the risk vector

The second step in the risk trading methodology is to implement and populate the risk vector, $\overrightarrow{\text{Risk}}$. 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 resulting risk metrics can either 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. For instance, FTA data should be aggregated into several risk metrics, as discussed in Sect. 3.1.3. On the other hand, subsystem FTA data can be directly reported to the system-level risk vector. As long as the specific types of risks being analyzed are properly defined so that there is agreement between subsystems and between subsystem chairs, $\overrightarrow{\text{Risk}}$ can be compared between different components, subsystems, and functions. This opens the door to trading $\overrightarrow{\text{Risk}}$ 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 (International Electrotechnical Commission 1990). 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 Risk Priority Numbers (RPNs) resulting from a FMECA are often prioritized from highest to lowest RPN in order to address the highest risks first. 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. One informative way of using FMECA is by summing the RPNs and dividing by the total number of risk elements, producing 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 engineering risk metrics including FMECA and FTA data can take the form of Eq. 3.

$$\overrightarrow{\text{Risk}} = \left\{ \begin{array}{c} \text{Max FMECA RPN} \\ \text{Average FMECA RPN} \\ \text{FTA\% Chance of Loss} \end{array} \right\} \tag{3}$$

Risk models found in the literature and in practice are typically static and 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 have been identified by the authors to implement risk methods to derive the risk vector for trade studies. The first option is to use risk methods without any modification. Only one static risk model represents a subsystem, irrespective of any change in input variables. This option is only valid if 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 subelements of the fault tree. The subelement probabilities are no longer fixed static quantities as they would be in a stand-alone FTA. Instead, the subelement probabilities are directly fed from input variables that can vary between each iteration of a trade study model 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 version is available.

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

For any of the risk model trade study options, the risk models must be integrated into the existing subsystem models. Further, the risk models must be created, managed, and be accessible by the individual subsystem chairs.

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 subsystem risk models cannot be managed by one person. The implicit risk knowledge present in each subsystem chair would no longer be captured in the subsystem risk models.

At the end of this step, the appropriate risk models have been created and integrated into the subsystem models. The risk vectors are populated with the risk metrics produced by the individual subsystem risk models. Next, the subsystems are unified into trade studies where risk can be traded like any other system-level parameter.

3.1.3 Creating a system-level risk vector

The third step in the risk trading methodology creates the 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. The system-level risk vector is analogous to any other system-level parameter such as cost or mass. However, unlike other system-level parameters, the subsystem risk vectors cannot always be directly 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

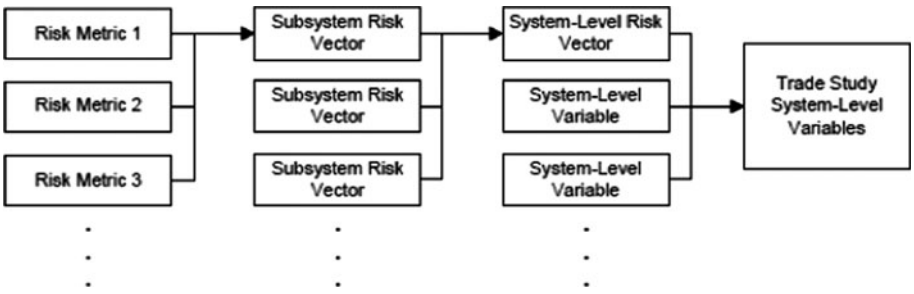

Fig. 1 Formation of risk vectors and their use in trade studies

represent that metric's system-level risk. Figure 1 graphically demonstrates how subsystem risk metrics are combined into subsystem risk vectors which are then developed into a system-level risk vector and finally are used in a trade study with other system-level variables.

Note that the method presented in this paper does not provide guidance for subsystem or component interaction effects or dependencies. All risks are assumed to be independent of one another. Various methods (Stone et al. 2005; Grantham-Lough et al. 2007; Krus and Grantham-Lough 2007; Clarkson et al. 2004; Jensen et al. 2009; Kurtoglu and Tumer 2008; Kurtoglu et al. 2010) are available to extend this method in order to consider dependencies and interaction effects as is deemed necessary by the practitioner.

In the case of FTA, a system-level fault tree can be created that is inclusive of the subsystem fault trees. 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 subsystem 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. In the example, the expert judgment of system-level schedule uncertainty is simply the sum of each subsystem schedule uncertainty metric. Similarly, the system-level expert judgment of cost uncertainty is a summation of the individual subsystem cost uncertainty metrics.

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 prepared, the next step is to perform the trade study.

3.1.4 Trading risk

Trading risk follows exactly the same procedures as trading any other system-level variable. The risk vector can be treated as either a set of design variables or as response variables. As a design variable, the risk vector is able to be manipulated with the full gamut of design of experiments methods. The authors assert that 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 order for engineers to easily understand the risk vector, there are several ways to visualize the data that the vector contains. These methods allow for the risk vector to play an integral role in developing conceptual designs during manually conducted trade studies. Risk vector visualization information can be found in Van Bossuyt et al. (2010).

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 Implementation in a CDC environment

To demonstrate and test the risk trading methodology described in this paper, simplified spacecraft models and risk models detailed in the following section were implemented in a simulated CDC environment at the Complex Engineering Systems Design Laboratory at Oregon State University. Study participants traded risk both without and with the risk trading methodology. The results of the manually conducted trade studies demonstrate the usefulness of the risk trading to a CDC in creating and choosing conceptual designs.

4.1 An illustrative example of trading risk

In order to illustrate the risk trading methodology, a simplified spacecraft model based upon Wertz and Larson (1999) and a manually conducted trade study are introduced in this section and further details are provided in Appendix 1. The model was initially created without any risk methods or data. Four representative subsystems were chosen to represent the spacecraft including Communication, Data Handling, Attitude Control, and Power. Each subsystem model was programmed to have two user inputs and three function or component-driven outputs. The inputs were specific to each subsystem. They consisted of either a drop-down menu where several component options could be chosen or an input box where bounded numeric values could be input to drive function-based models.

Three outputs were chosen to represent spacecraft output data from the subsystems to replicate real-world CDC trade studies: Subsystem Power Requirements, Subsystem Mass, and Subsystem Cost. All values and variables including user-selectable inputs, internal variables, and outputs had their units intentionally removed. Additionally, all formulas and other numeric information were altered to only generally correspond to real-world spacecraft systems. This is exemplified by the subsystem cost parameter that generally ranged between a unitless value of 1 and 30. The models and results presented in this section are for demonstrative purposes only and should not be misconstrued as viable spacecraft models or conceptual designs.

4.2 Subsystem risk models

For the illustrative example used in this paper, a dynamic FMEA was developed for each of the four user-operable subsystems. Each subsystem FMEA contained ten identified failure modes. The three component-based subsystem FMEAs were stepwise risk models. Individual failure modes were activated or deactivated based on what inputs had been selected. The function-based subsystem FMEA was a dynamic risk model. Failure mode RPN values dynamically varied based upon the user inputs. The subsystem FMEA Maximum RPN and Average RPN values changed as a result of changing the user input variables. The Power Subsystem FMEA, shown in Fig. 2, is representative of the four user-operable subsystems.

A dynamic FTA was created at the system level that represents the four user-operable subsystems and representative sub-subsystems or components, as shown in Fig. 3. The FTA uses OR gates at all levels of the tree. Sub-subsystem percentages are derived from subsystem input parameters. The percentages represent the chance of total system failure during the course of the system life.

4.3 Study population

Two distinct populations participated in the research study: One group of graduate mechanical engineering students, and two groups of undergraduate junior- and senior-level mechanical engineering students at Oregon State University participated. Each graduate and undergraduate group consisted of four people. The graduate mechanical engineering student group consisted of four people specializing in areas related to complex design, conceptual design, and collaborative design including trade studies. All had experience with CDC environments and were familiar with the general concepts of trade studies. All four participants have taken graduate-level coursework at Oregon State University in state-of-the-art risk- and model-based design methods. Two of the participants had previously interned with NASA and hence also possessed general knowledge of conceptual satellite design. This group of participants can be viewed as an experienced user group. An analogous group of people in an established CDC would be people with some experience within the CDC.

Two groups of undergraduate mechanical engineering students participated in the experiment. Each group of four

Function	Failure Mode	Effects	S	Cause(s)	O	Current Controls	D	RPN	Power Source	Energy Storage
power provided	Power surge	end of mission	10	EMI	1	shielding	3	30	all	all
power provided	Failure of primary battery	end of mission	10	Radiation	2	shielding	5	0	all	primary battery only
power provided	Failure of secondary battery	degraded performance	10	Radiation	1	shielding	8	0	photovoltaic	primary and secondary
power provided	Failure of power cable	degraded performance	7	Micro meteor	3	redundant cable	5	0	simple	all
power provided	Loss of solar panel	degraded performance	10	Meteor	1		5	0	photovoltaic	all
power provided	Short circuit	degraded performance	4	Johnny 5	2	Nova Laboratories	4	32	all	all
power provided	Failed-open breaker	degraded performance	10	EMI	3		10	300	static, dynamic	all
power provided	Faded out solar array	degraded performance	3	Space dust on panels	3		6	0	photovoltaic	all
power provided	Premature fuel exhaustion	end of mission	10	Micro meteor	1	shielding	4	40	dynamic	all
power provided	Cooling loop failure	end of mission	10	Micro meteor	1	shielding	5	0	static	all

Total RPNS	MAX RPN
4	300

Average RPN
100.5

Fig. 2 Power subsystem FMEA

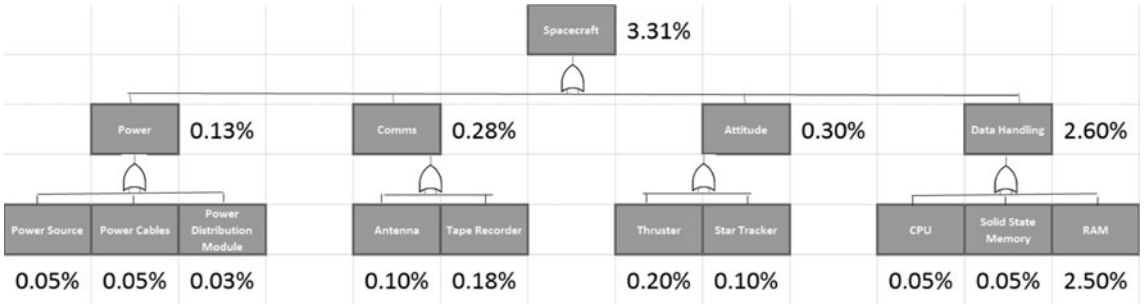

Fig. 3 System-Level FTA

was a mix of junior-level and senior-level students who had satisfactorily completed junior-level design courses that contained material on the mechanical design process and had a collaborative design project. The undergraduate mechanical engineers did not have prior knowledge of trade studies. This group of participants can be considered a general user group. A similar group in a CDC might be engineers and scientists who are just being introduced to the CDC.

All study participants were recruited through classroom and professional society e-mail lists. Students were compensated $40 for their participation. Informed consent was obtained from all participants. Each experimental run lasted approximately three hours including preparticipation screening, obtaining informed consent, acquainting participants with the software and hardware configuration, and performing the experiments.

4.4 Mission scenarios

Two mission scenarios were used for the three phases of the experiment including a weather satellite and a navigation satellite. The missions were both earth-orbiting satellites that consisted of a series of design constraints and requirements. All constraints, requirements, and mission data were based upon information from Wertz and Larson (1999) but were intentionally modified so that information used in this experiment did not closely resemble real-world or proposed conceptual satellite design information.

Both missions contained payload power, mass, and cost output variable data. Constraints placed upon subsystem design decisions were also provided. Table 1 details the payload requirements and design constraints of each mission.

In addition to payload output variables and subsystem design constraints, each mission also demanded that cost and mass be minimized while also assuring that a positive power balance was achieved. Additional general information about the function of a particular payload was provided to several groups who requested more details on the purpose of the mission and its scientific goals. The problem statements given to the participants can be seen in Appendix 2.

Table 1 Mission constraints

	Weather	Navigation
Energy storage	Primary and secondary battery	N/A
Power source	N/A	Photovoltaic
Spacecraft bus	2 unit	N/A
Stability method	N/A	N/A
Required processing	105	140
Maximum mass	27	45
Maximum cost	15	15

4.5 Questionnaires, work products, discussions

To gather information on participants' opinions of and interactions with the risk trading method, four methods of data collection were used during the experiments. One method that was invisible to the participants was subsystem and system-level passively collected data from ModelCenter. The other three methods including work products, questionnaires, and group discussions required user input and interaction. At the end of each trade study session, the participants were asked to fill out a "System Design Report" document. The document asked the participants to write down all design decisions they made, the rationale behind those design decisions, and any comments that they had about the session. Participants were instructed to concentrate on their own individual subsystems but also record pertinent information on decisions and rationale of other subsystems with which they interacted. Following the completion of the System Design Report, a questionnaire was administered to the participants and a group discussion was held. Questionnaire questions are available in Appendix 3. Group discussion questions are available in Appendix 4. The work product template is available in Appendix 5.

5 CDC implementation results

While the number of participants does not lend itself to statistically significant results, several anecdotal insights

can be drawn from the experiments. Both the graduate and undergraduate research populations generally preferred conducting trade studies using the risk trading methodology. For instance, one participant stated "I liked the risk trading method," while another stated "the resulting design is more complete when using the risk trading method." In addition, six participants stated that the results of trade studies that included risk as a system-level parameter made them more confident that the end result of the trade study was of the highest possible utility. For instance, one participant stated "I am more confident in conceptual designs created using the risk trading method." Rather than implicit assumptions and no real conversation taking place about the risk of various subsystem choices, both participant populations openly discussed the risks in the design and negotiated to determine the optimum trade-off point between mass, power, cost, and risk. Appendixes 6 and 7 provide additional relevant participant questionnaire and group discussion responses, respectively.

Four participants indicated that they would be more comfortable showing the result of a trade study with risk as a system-level variable to their boss or a client than showing a trade study result that had not considered risk. For instance, three participants stated "I would be more comfortable to show my boss the conceptual design created using the risk trading method." One participant reported that including the risk models gave him more confidence that the subsystem models were more complete and that the resulting designs would be more in line with the desired risk propensity of the organization or individual that had commissioned the study.

The results were presented in various forms. Numeric and dynamic FTA displays of system-level risk information were found to be the most preferred representations of risk for both groups of participants. Glyph plots and parallel axis plots were identified as less useful. The participants believed that with more training, glyph plots and parallel axis plots could be an interesting addition to help understand risk and other multi-dimensional data. However, especially among the undergraduate participants, glyph and parallel axis plots were found to be difficult to understand. Further information about the various display techniques can be found in Van Bossuyt et al. (2010).

As compared to the risk-less portion of the study, the participants took 10 minutes or about 30% longer to complete the trade study with risk trading. The graduate student participants identified trading risk variables as a factor in the extra time required to finish the study. However, the graduate students also pointed toward risk trading as the motivator and inspiration for their creative solution to the over-constrained problem. The undergraduates felt the need to understand how each piece of risk data was derived and how it affected the overall risk profile of the system and subsystems. There was much questioning of how risk model numbers were derived and whether they were realistic or not. In an effort to understand the risk models more fully, the undergraduate participants left their individual stations, a rare occurrence in previous sessions, and investigated how all of the subsystem models worked to gain a better overall understanding of the way the models interacted with one another. Had the undergraduates not required such a detailed understanding of the models, the trade study would have concluded more quickly. However, the undergraduate participants felt that the time spent understanding the risk models was well spent and helped them to produce a result that was more confidence-inspiring. Likewise, in spite of the extra time required to complete the trade study and extra mental effort needed to understand the methodology, the graduate student participants had a strong preference for conducting trade studies using risk as a tradeable system-level parameter.

One of the goals of this method was to create conceptual designs that are of higher utility as partially defined by risk metrics than when not using the risk trading methodology. This goal was met when the final spacecraft models selected by the experiment participants using the risk trading method as having the highest utility were different and of higher utility than the highest utility models generated without using the risk trading method. This mirrors the results found in Van Bossuyt et al. (2010). When the risk trading methodology is used, designs with higher utility as partially defined by risk metrics can be found.

The other central goal of the method is to explicitly trade risk at the subsystem level and give the power to analyze subsystem risk to the subsystem chairs during the creation of conceptual designs in trade studies. The trade study experiments clearly demonstrated that subsystem chairs do explicitly trade based upon risk metrics in order to maximize system utility. From anecdotally observing the trade study sessions, the authors additionally feel that in this limited test case, a balance was struck between the risk metrics and other important system-level parameters such as cost, mass, and power.

6 Discussion and specific contributions

This paper contributes to the literature a risk trading method that allows for new design selection preferences to be created that otherwise would not be available to design engineers, thus satisfying contribution #1 listed in Sect. 2.4. Using $\overrightarrow{\text{Risk}}$ as a tradeable design variable enables engineers to find designs with higher utility as partially defined by risk metrics than if risk was ignored, thus satisfying contribution #2. This elevates risk to the same level

as other important system-level variables rather than having risk considered as an afterthought to creating conceptual designs. Further, it allows engineers and decision-makers to explore interesting designs that were previously difficult to identify or justify, thus satisfying contribution #3. It is therefore desirable to include $\overrightarrow{\text{Risk}}$ in trade studies.

Risk methods such as FMECA, FTA, and expert judgment can be used with the risk trading method. When developing FMECA, FTA, or similar numeric models for use with the risk trading method, 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. Further, CDC customers are able to better understand how changes in the conceptual design impact the risk profile of the final design, thus satisfying contribution #4 discussed in Sect. 2.4.

Participants in trade studies generally indicated their preference of using the risk trading methodology over not considering risk during the trade study process. They found that the risk trading methodology inspired greater confidence in the end product of the trade study. Additionally, several stated that they would be more comfortable with showing superiors results produced using the risk trading methodology. Several participants went so far as to state that the extra time and extra mental effort imposed by the learning curve in implementing the risk trading methodology was outweighed by the benefits of the methodology. This satisfies contribution #5 listed in Sect. 2.4.

7 Limitations

Several limitations to the method and its current validation exist. While the risk trading method presented in this paper was tested on teams of undergraduate and graduate students in a simulated CDC environment, it has not yet been tested in a production-level CDC. In order to test new trade study methods in well-respected CDCs that are open to being used as test cases, the time of the CDC must be purchased. In the case of Team X, this amounts to many tens of thousands of dollars for a single trade study. This is an ongoing challenge for researchers developing new methods for CDCs.

One major drawback to this method is the level of training and coordination required for subsystem 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 produces data under a different set of assumptions, different definitions, or using different methods, $\overrightarrow{\text{Risk}}$ 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 can add great value.

Another potential drawback of this method is the lack of subsystem 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 (Kurtoglu and Tumer 2008).

8 Future work

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. Normalization of the risk vector can occur 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 subsystem 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.

9 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 and mass, conceptual designs will be explicitly created and selected based on risk metrics.

Future work includes developing methods to efficiently and effectively generate subsystem risk models. The models must be matched between subsystems in order to ensure a fair comparison of risk vectors across subsystems. An effective method of normalizing and harmonizing individual subsystem chair interpretations of risk is also needed.

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. Specifically, a method to include risk in trade studies was developed and implemented in a mock CDC using a simple example to show the utility of the method in practice.

Acknowledgments 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 Inc. for donating software and providing technical support, and Steve Cornford at JPL for providing valuable feedback and inspiration. The study protocol was reviewed and approved by the Institutional Review Board, Study 4611, at Oregon State University. The opinions and findings of this work are the responsibility of the authors and do not necessarily reflect the views of the sponsors or collaborators.

Appendix 1: Subsystem development

To represent the spacecraft, four representative subsystems including Communication, Data Handling, Attitude Control, and Power were chosen. The *Communication Subsystem* is a function-based model that accepts user input for the Antenna Size and Frequency Downlink variables. Function-based subsystem models are function-driven over a range of numeric inputs, while component-based subsystems have a predefined, limited selection of potential subsystem components. Antenna size can range from 1 to 4, and Frequency Downlink can range from 1 to 18, including decimal values. Both of the user input fields have corresponding instructions for the user to maintain input values between the allowable ranges. The Communication Subsystem *Power* requirements, *Mass*, and *Cost* output variables were computed using the formulas shown in Eqs. 4, 5, and 6, respectively.

$$\text{Power} = -\text{Antenna Size} + 0.6 \times \text{Frequency Downlink} + 3 \tag{4}$$

$$\text{Mass} = \text{Antenna Size} \times 2.5 + 2 \tag{5}$$

$$\text{Cost} = \text{Antenna Size} \times 0.75 + \text{Frequency Downlink} \times 0.1 \tag{6}$$

Table 2 Data handling subsystem input and output variables

Input variables		Output variables		
System complex.	Bus config.	Power	Mass	Cost
Simple	One unit	7.5	4.8	0.9
Typical	One unit	11.25	6.6	1.35
Complex	One unit	15	12	1.8
Simple	Two unit	11.25	3.6	1.575
Typical	Two unit	16.875	4.95	2.3625
Complex	Two unit	22.5	9	3.15
Simple	Integrated	6	2.8	1.35
Typical	Integrated	9	3.85	2.025
Complex	Integrated	12	7	2.7

The *Data Handling Subsystem* is a component-based model that contains two user inputs in the form of drop-down selection boxes. The first user input, System Complexity, has the options of "simple," "typical," and "complex." The other user input is Spacecraft Bus Configuration which allows the user to select either "one unit," "two unit," or "integrated" which refer to the spacecraft having one or two primary computing units and distributed subsystem computers, or an integrated unit that handles all command and data handling functionality. The resulting Data Handling subsystem outputs are shown in Table 2.

The *Attitude Control Subsystem* is a component-based model that gives the user control over two inputs via drop-down selection boxes. The inputs are "Stability Method" and "Pointing Method." Table 3 displays the full range of user-selectable components and the corresponding output variable values.

The *Power Subsystem* is driven by a component-based model that has two inputs, namely "Power Source" and "Energy Source," which are controllable via drop-down selection boxes. Table 4 presents the range of possible user-selectable input variable combinations and their corresponding output variables. Unlike the other three subsystems, the Power output variable for the Power Subsystem indicates how much power is available to the entire spacecraft system from the power produced within the Power Subsystem.

In addition to the four participant-controlled subsystems, a *Payload Subsystem* was also developed from Wertz and Larson (Wertz and Larson 1999). It is used only to set the mission objectives and requirements. The two possible payloads consist of a weather and navigation package. Only one payload package is selectable at any given time. The Payload Subsystem outputs power, mass, and cost variables. It also produces data on system constraints due to the payload. Table 5 presents the two payload choices and corresponding output data.

Table 3 Attitude control subsystem input and output variables

Input variables		Output variables		
Spin method	Pointing method	Power	Mass	Cost
Gravity grad.	Nadir pointing	4.5	1.05	0.99
Gravity grad.	Scanning	6	2.55	1.485
Gravity grad.	Off-Nadir point	3	1.05	1.188
Spin	Nadir pointing	9	4.2	3.3
Spin	Scanning	12	10.2	4.95
Spin	Off-Nadir point	6	4.2	3.96
3-Axis	Nadir pointing	13.5	2.8	2.53
3-Axis	Scanning	18	6.8	3.795
3-Axis	Off-Nadir Point	9	2.8	3.036

Table 4 Power subsystem input and output variables

Input variables		Output variables		
Power source	Battery	Power	Mass	Cost
Photovoltaic	Primary only	41.25	3.8	1.9
Photovoltaic	Prim. and second	70.125	7.6	3.8
Static	Prim. only	27.5	6.65	20
Static	Prim. and second	46.75	13.3	40
Dynamic	Prim. only	82.5	13.3	1.4
Dynamic	Prim. and second	140.25	26.6	2.8

Table 5 Payload subsystem input and output variables

	Navigation	Weather
Power	50	30
Mass	2	3
Cost	6	7

Appendix 2: Problem statements

The riskless trade study session used a simple navigation satellite problem. The problem statement is as follows:

This satellite is designed as a navigation satellite to add to the GPS network allowing GPS units to acquire more accurate data on Earth. It carries equipment on board to support its mission. Because of this, the following constraints are given for the mission:

POWER SUBSYSTEM Power Source: photovoltaic
COMMUNICATIONS SUBSYSTEM: Frequency downlink: 18
DATA HANDLING SUBSYSTEM: Required processing: 110
TOTAL SPACECRAFT: Maximum mass: 30 Maximum cost: 18

The trade study session conducted using the risk trading methodology used a simple weather satellite problem. The problem statement is as follows:

This satellite is designed as a weather satellite to monitor the climate on Earth and carries equipment on board to support its mission. Because of this, the following constraints are given for this mission:

POWER SUBSYSTEM Energy Storage: primary and secondary battery
DATA HANDLING SUBSYSTEM: Spacecraft bus: 2 units Required processing: 105
TOTAL SPACECRAFT: Maximum mass: 27 Maximum cost: 17

Appendix 3: Questionnaire questions

Following each trade study session, participants were asked to fill out a questionnaire individually. The following questions were common to both trade studies.

- Rank the ease of use of each subsystem model on an Easy (1) to Hard (5) scale:

  Attitude control
  Data handling
  Power
  Communications

- Indicate the ease of use of the two types of subsystem models on an Easy (1) to Hard (5) scale:

  Component-based
  Function-based

Additional questionnaire questions were tailored to the risk trading session including:

- Describe any difficulties you encountered while understanding and using the subsystem risk models
- How did you find the transition from conducting trade studies without risk models to trade studies with risk models on an Easy (1) to Hard (5) scale?
- Indicate which set of models produced results in which you feel more confident on a Confident in no-risk model results (1) to confident in models with risk results (5) scale
- Indicate the ease of understanding risk data for each risk visualization technique on an Easy (1) to Hard (5) scale:

  Fever charts
  Glyph plots
  Parallel axis
  Numeric data
  Dynamic fault tree

- Is there anything that should have been done differently when transitioning from trade study models not containing risk information to trade study models with components?
- Do you have any additional comments about the study or anything else you wish to convey to the researchers?

Appendix 4: Group discussion questions

Group discussion followed completion of the System Design Report and the questionnaire in both trade study sessions. The following questions were repeated at the end of both sessions:

- Were any of the subsystem models hard to understand and use? Were any particularly easy?
- Did you prefer component-based or function-based subsystem models?

The following questions were used in the group discussion only for the second trade study:

- Did you encounter any difficulties using subsystem models with risk data?
- Were you able to understand the graphical representations of risk? Which did you prefer? (Glyph plot, fever chart, parallel axis plot, dynamic fault tree)
- Is there anything that should have been done differently when transitioning from trade study models not containing risk information to trade study models with risk components?
- Do you have any additional comments about the study or anything else you wish to convey to the researchers?

Appendix 5: Work product template

At the end of both trade study sessions, participants completed brief reports about the work that they had just completed. The following free entry form was provided to the participants:

- Subsystem
- Design Decisions
- Rationale
- Comments

Most participants wrote a paragraph or more for each of the last three questions.

Appendix 6: Questionnaire results

Relevant questionnaire responses are aggregated in this appendix. Identifying information has been removed, and data have been anonymized.

Describe any difficulties you encountered while understanding and using subsystem risk models

- The risk models were extremely helpful and intuitive.
- The risk models were easy to understand but mitigating design problems was difficult.
- The only challenge was to observe how design changes propagated through the subsystem and system models.

How did you find the transition from conducting trade studies without risk models to trade studies with risk models

- Risk is just one more thing to analyze. Engineers should already be doing this.
- Trading risk was straight forward.
- The risk trading method provided more perspective and helps me to feel confident in the final design.
- Risk adds another variable for consideration that can make it more difficult to find a satisfactory solution.
- The risk method is more all-encompassing.
- Risk adds another parameter and is not hard to deal with.

Indicate which set of models produced results in which you feel more confident

- Knowing that design decisions are backed by the science of risk methods such as (FMEA) makes me very confident in our design choices.

Is there anything that should have been done differently when transitioning from trade study models not containing risk information to trade study models with risk components?

- No.
- The brief training was straightforward.
- The transition was straightforward.
- A better understanding of the trade-offs between risk metrics and other system variables would be useful.

Do you have any additional comments about the study or anything else you wish to convey to the researchers?

- The risk trading method and dynamic (FMEA) model are big improvements over existing methods. The method provides for another layer of reliability in the design.

Appendix 7: Group discussion results

Relevant group discussion responses are aggregated in this appendix. Identifying information has been removed ,and data have been anonymized.

- Using the risk trading method was not harder than not using the method.

- I liked the risk trading method. It validates that there is more to the model.
- The resulting design is more complete when using the risk trading method. The resulting design is safer.
- The risk trading method was as easy to use as standard trade study methods. It was more complex but not more difficult.
- I would be more comfortable to show my boss the conceptual design created using the risk trading method. (three participants stated this)
- Using the risk trading method helped me to make design decisions more comfortably.
- It makes sense from an engineering perspective that there is a trade-off between traditional variables such as power, mass, and cost, and engineering risk metrics.
- I am more confident in conceptual designs created using the risk trading method.
- I prefer using the risk trading method over not using the method.

References

Andersson P (1996) A semi-analytic approach to robust design in the conceptual design phase. Res Eng Design 8:229–239

Andersson P (1997) On robust design in the conceptual design phase: a qualitative approach. J Eng Design 8(1):75–90

Benjamin JL, Pate-Cornell ME (2004) Risk chair for concurrent design engineering: satellite swarm illustration. J Spacecr Rockets 41(1):51–59

Bennett R, 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

Bonano EJ, Hora SC, Keeney RL, von Winterfeldt D (1990) Elicitation and use of expert judgment in performance assessment for high-level radioactive waste repositories. Tech. Rep. NUREG/CR-5411, Nuclear Regulatory Commission, Washington

Browning TR, Eppinger SD (2000) Modeling the impact of process architecture on cost and schedule risk in product development. Sloan Manag Rev WPN 4050

Browning TR, Eppinger SD (2002) Modeling impacts of process architecture on cost and schedule risk in product development. IEEE Trans Eng Manag 49(4):428–442

Browning TR, Deyst JJ, Eppinger SD, Whitney DE (2002) Adding value in product development by creating information and reducing risk. IEEE Trans Eng Manag 49:443–458

Charania AC, ohn E Bradford J, Olds JR, Graham M (2002) System level uncertainty assessment for collaborative rlv design. In: Second modeling and simulation subcommittee joint meeting

Clarkson P, Simons C, Eckert C (2004) Predicting change propagation in complex design. J Mech Des 126:788

Clemen RT, Winkler RL (1999) Combining probability distributions from experts in risk analysis. Risk Anal 19(2):187–204

Cooke RM (1991) Experts in uncertainty: opinions and subjective probability in science. Oxford University Press, New York

Cornford SL, Dunphy J, Feather MS (2002) Optimizing the design of spacecraft systems using risk as currency. In: IEEE aerospace conference, ddptool.jpl.nasa.gov

Cornford SL, Feather MS, Jenkins JS (2006) Intertwining risk insights and design decisions. In: Eigth international conference on probabilistic safety assessment and management

Department of Defense (1980) Procedures for performing failure mode, effects, and criticality analysis. MIL-STD-1629A.

Deutsch MJ, Nichols JS (2000) Advanced approach to concept and design studies for space missions. Astrophys Space Sci 273:201–206

Dezfuli H, Youngblood R, Reinert J (2007) Managing risk within a decision analysis framework. In: Second international association for the advancement of space safety conference, IAASS

Du X, Chen W (2000) Towards a better understanding of modeling feasibility robustness in engineering design. ASME J Mech Des 122(4):385–394

FAA (2006) National airspace system engineering manual, 3rd edn. Federal Aviation Administration ATO Operations Planning

Ford RB, Barkan P (1995) Beyond parameter design—a methodology addressing product robustness at the concept formation stage. In: Proceedings of the national design engineering conference

Grantham-Lough K, Stone R, Tumer IY (2007) The risk in early design method. J Eng Des 20:155–173

Guikema SD, Pate-Cornell ME (2004) Bayesian analysis of launch vehicle success rates. J Spacecr Rockets 41(1):93–102

Hardman DK, Ayton P (1997) Arguments for qualitative risk assessment: the star risk adviser. Expert Syst 14:24–36

Hora SC (1992) Acquisition of expert judgment: Examples from risk assessment. J Energy Eng 118:136–148

IEEE (1990) IEEE standard computer dictionary: a compilation of IEEE standard computer glossaries. IEEE, New York

International Electrotechnical Commission (1990) International standard IEC 61025 fault tree analysis

International Organization for Standardization (1997) ISO 10628: Flow diagrams for process plants—general rules

International organization for standardization (2009) ISO 31000:2009 risk management—principles and guidelines

Jensen D, Tumer IY, Kurtoglu T (2009) Flow state logic (fsl) for analysis of failure propagation in early design. In: Proceedings of the ASME design engineering technical conferences, international design theory and methodology conference, IDETC/CIE2009, San Diego

Ji H, Yang MC, Honda T (2007) A probabilistic approach for extracting design preferences from design team discussion. In: Proceedings of the ASME 2007 international design engineering technology conferences and computers in information and engineering conference (IDETC/CIE2007), IDETC/CIE, Las Vegas, NV

Keeney RL, von Winterfeldt D (1989) On the uses of expert judgment on complex technical problems. IEEE Trans Eng Manag 36(2):219–229

Keeney RL, von Winterfeldt D (1991) Eliciting probabilities from experts in complex technical problems. IEEE Trans Eng Manag 38:191–201

Krus D, Grantham-Lough K (2007) Applying function-based failure propagation in conceptual design. In: The Proceedings of the ASME design engineering technical conferences, international design theory and methodology conference, Las Vegas, NV

Kurtoglu T, Tumer IY (2008) A graph-based fault identification and propagation framework for functional design of complex systems. J Mech Des 30(5)

Kurtoglu T, Tumer IY, Jensen D (2010) A function failure reasoning methodology for evaluation of conceptual system architectures. Res Eng Des 21(4):209

Lough KG, Stone RB, Tumer IY (2008) Implementation procedures for the risk in early design (red) method. J Ind Syst Eng 2(2):126–143

Lough KG, Van Wie M, Stone R, Tumer I (2009) Promoting risk communication in early design through linguistic analyses. Res Eng Des 20(1):29–40

Martin JD, Simpson TW (2006) A methodology to manage system-level uncertainty during conceptual design. ASME J Mech Des 128:959–968

McCormick NJ (1981) Reliability and risk analysis (methods and nuclear power applications). Academic Press, London

McManus HL, Warmkessel JM (2004) Creating advanced architectures for space systems: emergent lessons from new processes. J Spacecr Rockets 41:69–75

McManus HL, Hastings DE, Warmkessel JM (2004) New methods for rapid architecture selection and conceptual design. J Spacecr Rockets 41(1):10–19

Mehr AF, Tumer IY (2006) Risk-based decision-making for managing resources during the design of complex space exploration systems. J Mech Des 128:1014–1022

Merkhofer MW (1987) Quantifying judgmental uncertainty: methodology, experience, and insights. IEEE Trans Syst Man Cybern 17:741–752

Meshkat L (2007) A holistic approach for risk management during design. In: IEEE aerospace conference

Meshkat L, Weiss KA, Luna M, Leveson N (2006) Supporting concurrent engineering in JPL's advanced project design team using a systems engineering development environment. In: In the proceedings of virtual concept

Mosleh A, Beier VM, Apostolakis G (1987) A critique of current practice for the use of expert opinions in probabilistic risk assessment. Reliab Eng Syst Saf 20:63–85

NASA (1995) NASA systems engineering handbook. NASA

Oberto RE, Nilsen E, Cohen R, Wheeler R, DeFlorio P, Borden C (2005) The NASA exploration design team: blueprint for a new design paradigm. In: Proceedings of the 2005 Aerospace Conference, IEEE, no. 8957662 in IEEE Conferences, pp 4398–4405

Osburg J, Mavris D (2005) A collaborative design environment to support multidisciplinary conceptual systems design. SAE Trans 114:1508–1516

Otway H, von Winterfeldt D (1992) Expert judgment in risk analysis and management: process, context, and pitfalls. Risk Anal 12:83–93

Papalambros PY, Wilde DJ (2000) Principles of optimal design: modeling and computation. Cambridge University Press, Cambridge

Parkin KL, Sercel JC, Liu MJ, Thunnissen DP (2003) Icemaker: an excel-based environment for collaborative design. In: In the Proceedings of IEEE Aerospace Conference

Phoenix Integration Inc (2008) PHX Model Center. http://www.phoenix-int.com/software/phx_modelcenter.php

Reich Y, Ziv Av A (2005) Robust product concept generation. In: International conference on engineering design ICED05

Ross AM, Hastings DE, Warmkessel JM, Diller NP (2004) Multi-attribute tradespace exploration as front end for effective space system design. J Spacecr Rockets 41(1):20–29

Russell JS, Skibniewski MJ (1988) Decision criteria in contractor prequalification. J Manag Eng 4(2):148–164

Shishko R (2000) The proliferation of pdc-type environments in industry and universities. In: Proceedings of the 2nd European systems engineering conference, EuSEC

Stamanis DH (2003) Failure modes and effects analysis: FMEA from theory to execution, 2nd edn. ASQ Quality Press, Milwaukee

Stamatelatos M, Dezfuli H, Apostolakis G (2006) A proposed risk-informed decision-making framework for nasa. In: 8th international conference on probabilistic safety assessment and management

Stone RB, Tumer IY, Wie MV (2005) The function-failure design method. J Mech Des 127(3):397–407

Stone RB, Tumer IY, Stock ME (2006) Linking product functionality to historical failures to improve failure analysis in design. Res Eng Des 16(2):96–108

Stump GM, Lego S, Yukish M, Simpson TW, Donndelinger JA (2009) Visual steering commands for trade space exploration: user-guided sampling with example. J Comp Inform Sci Eng 9(4):044,501:1–10

Taguchi G (1986) Introduction to quality engineering. Quality Resources, White Plains

Taguchi G (1993) Taguchi on Robust Technology Development. ASME, New York

Thunnissen DP (2003) Uncertainty classification for the design and development of complex systems. In: 3rd annual predictive methods conference

Thunnissen DP (2004) Balancing cost, risk, and performance under uncertainty in preliminary mission design. In: AIAA space conference

Thunnissen DP, Tsuyuki GT (2004) Margin determination in the design and development of a thermal control system. In: 34th international conference on environmental systems (ICES)

Tumer IY, Stone RB (2003) Mapping function to failure mode during component development. Res Eng Des 4(1):25–33

Ullman DG (2001) Robust decision-making for engineering design. J Eng Des 12(1):3–13

Ullman DG (2003) The mechanical design process, 3rd edn. McGraw-Hill, New York

Van Bossuyt DL, Tumer IY (2010) Toward understanding collaborative design center trade study software upgrade and migration risks. In: Proceedings of the ASME 2010 international mechanical engineering congress and exposition IMECE2010, ASME, Vancouver

Van Bossuyt DL, Wall S, Tumer I (2010) Towards risk as a tradeable parameters in complex systems design trades. In: Proceedings of the ASME 2010 International design engineering technology conferences and computers in information and engineering conference (IDETC/CIE2010), ASME, Montreal, pp DETC2010–29,016

Villemeur A (2000) Reliability, availability, maintainability, and safety assessment. Willey, New Jersey

Wertz JR, Larson WJ (1999) Space mission analysis and design. Springer, Berlin

Ziv Av A, Reich Y (2005) Sos-subjective objective system for generating optimal product concepts. Des Stud 26(5):509–533