Risk Evaluation in the Pre-Phase A Conceptual Design of Spacecraft

Leo L. Fabisinski, III[1] and Charlotte Dauphne Maples.[2]
Jacobs Engineering, Science, and Technical Services Group
in support of NASA Marshall Space Flight Center in the Advanced Concepts Office
Huntsville, Alabama, 35806

Typically, the most important decisions in the design of a spacecraft are made in the earliest stages of its conceptual design – the Pre-Phase A stages. It is in these stages that the greatest number of design alternatives is considered, and the greatest number of alternatives is rejected. The focus of Pre-Phase A conceptual development is on the evaluation and comparison of whole concepts and the larger-scale systems comprising those concepts. This comparison typically uses general Figures of Merit (FOMs) to quantify the comparative benefits of designs and alternative design features. Along with mass, performance, and cost, risk should be one of the major FOMs in evaluating design decisions during the conceptual design phases. However, risk is often given inadequate consideration in conceptual design practice. The reasons frequently given for this lack of attention to risk include: inadequate mission definition, lack of rigorous design requirements in early concept phases, lack of fidelity in risk assessment methods, and undervaluation of risk as a viable FOM for design evaluation.

In this paper, the role of risk evaluation in early conceptual design is discussed. The various requirements of a viable risk evaluation tool at the Pre-Phase A level are considered in light of the needs of a typical spacecraft design study. A technique for risk identification and evaluation is presented. The application of the risk identification and evaluation approach to the conceptual design process is discussed. Finally, a computational tool for risk profiling is presented and applied to assess the risk for an existing Pre-Phase A proposal. The resulting profile is compared to the risks identified for the proposal by other means.

Nomenclature

Pr_1	= likelihood of risk 1
Pr_2	= likelihood of risk 2
Pr_n	= likelihood of risk n
n	= the number of risks
Π_i	= product operator
Pr_i	= probability of risk i
Vr_1	= the total risk value of risk 1
Vr_2	= the total risk value of risk 2
Vr_n	= the total risk value of risk n
Σ_i	= summation operator
Vr_i	= risk value of risk i

I. Introduction.

NASA (the environment in which the authors of this paper work), uses NPR 7120.5, the NASA Systems Engineering Handbook, to define the initial level of conceptual design as Pre-Phase A. This phase includes design activities that define fundamental characteristics of space architectures and concepts. Pre-Phase A design is the activity in which the major choices of configuration, mission design, and high-level component selection are made. At the architecture level, it is the phase in which competing concepts are down-selected. Because of this, much of the focus of Pre-Phase A conceptual development is on the objective evaluation and comparison of whole concepts

[1] Senior Engineer, International Space Systems, Inc., 555 Sparkman Drive, Suite 440, Huntsville AL 35816, AIAA Senior Member.
[2] Systems Engineer, Qualis Corporation, 5000 Bradford Drive, Suite B, Huntsville AL 35805, AIAA Member.

and the major systems, subsystems, and components comprising them. Individual components and subsystems are compared in design trades. Competing concepts are compared to decide which best meet the requirements of a given set of mission objectives.

To make objective comparisons, Figures of Merit (FOMs) are devised. A FOM is an objective measure that allows comparisons to be made. There are typically a number of FOMs explicitly or implicitly weighted in accordance with their importance in the comparison process. As an example, Cost and Injected Mass are FOMs normally used to compare launch vehicle concepts. Lower cost and greater injected mass are considered superior. The weighting of these FOMs (along with all the others) will often depend on the individual mission, customer requirements, and other considerations.

FOM characteristics needed for a FOM to be useful in making design decisions are listed below:

1) Objective – A FOM value should be largely independent of the evaluator and all factors unrelated to the design.
2) Comparable – A FOM value should accurately measure a desired quality to the extent that a 'better' value for the FOM reflects a 'better' design choice for that quality.
3) Easily Evaluated – A FOM value should compute with a fairly simple and straightforward analysis. Pre-Phase A studies are usually performed in a matter of weeks. Each individual analysis must be completed quickly to be of value.

This paper discusses Risk as a FOM in Pre-Phase A design. This paper proposes a specific method of Risk Analysis uniquely suited to early conceptual design and presents an analysis tool to identify and score risk as a viable FOM.

II. Overview of Risk Management

A. Risk Management as Defined in this Paper

For the purposes of this paper, a risk is any possible future event whose occurrence is uncertain and that may result in failure to meet a mission requirement.

This definition of risk was chosen due to its simplicity and the fact that it lends itself to evaluation as a FOM. Risk may be quantified in terms of the following measures:

1) **Likelihood** – Probability that the risk event will occur.
2) **Consequence** – A measure of the cost (usually in dollars or schedule) to the mission if the risk event occurs.

Given these two measures, an overall Expected Risk Value may be calculated as:

Vr = Likelihood × Consequence.[1]

This is the expected cost of accepting a particular risk.

According to this document, Risk Management consists of two complementary processes: Risk Informed Decision Making (RIDM) and Continuous Risk Management (CRM). For conceptual design purposes, RIDM is the use of risk as a FOM for making design decisions. This document defines CRM as the process used for managing risks associated with design implementation, plans, and processes. RIDM and CRM as defined by NASA are explained in the next section.

B. Risk Management at NASA

Risk Management at NASA is guided by specification *NPR 8000.4A.* This NASA standard describes two complementary processes required for Risk Analysis at NASA: RIDM and CRM.

Risk Informed Decision-Making is defined as follows:

1) Identification of Decision Alternatives
2) Risk Analysis of Decision Alternatives to Support Ranking
3) Selection of a Decision Alternative Informed by (not solely based on) Risk Analysis[2]

According to NPR 8000.4A, CRM consists of the following steps:

1) **Identify** – Identify contributors to risk (shortfalls in performance relative to the baseline performance requirements).

Note: Sometimes the relationship between an identified risk and performance measures is indirect, but risks within the proper scope of CRM are addressed precisely because they may affect one or more performance measures.

2) **Analyze** – Estimate the probability and consequence components of the risk through analysis, including uncertainty in the probabilities and consequences and, as appropriate, estimate aggregate risks.

3) **Plan** – Decide on risk disposition and handling, develop and execute mitigation plans, and decide what will be tracked.

4) **Track** – Track observables relating to performance measures (e.g., technical performance data, schedule variances).

5) **Control** – Control risk by evaluating tracking data to verify effectiveness of mitigation plans, making adjustment to the plans as necessary, and executing control measures.

6) **Communicate and document** – Communicate and document the above activities throughout the process.[3]

III. Pre-Phase A Design

Space systems concepts encompass a wide variety of devices and fabrications. These include launch vehicles to take payloads into Earth orbit, satellites to perform Earth orbit missions, manned and unmanned landers to take payloads to extra-terrestrial surfaces, and surface systems to provide surface support. All are designed to fulfill mission objectives, either individually or as part of an overall architecture. The design process begins with one or more mission objectives.

At the Pre-Phase A stage, mission objectives are broad statements with little detail. 'Land a small crew on the Moon to study its geology' is a typical Pre-Phase A mission objective. Refining the general objective of the study of Lunar Geology to include details such as exact mission duration, surface location, tools required, number of crew etc. will require a great deal of future analysis. This level of detailed analysis is done in later levels of design, starting with Phase A. Usually broad assumptions about these details are agreed upon with the study customer and include in the initial Ground Rules & Assumptions document for the study.

Pre-Phase A design groups, such as the NASA Marshall Spaceflight Center (MSFC) Advanced Concepts Office, use initial mission objectives to provide a conceptual level spacecraft design in a few weeks or less. The distinguishing features of conceptual design are described below:

1) **Large Breadth** – Most Pre-Phase A groups can design a very wide variety of vehicles, space systems and surface systems.
2) **Low Depth** – In general, Pre-Phase A is the design of the concept at the subsystems level (Power, Propulsion, Avionics, etc) from components (Solar Cells, Rocket Motor, Star Tracker) that are either sized from models or selected from an existing hardware catalog.
3) **Quick Turnaround** – Studies are typically performed in time-frames of days or weeks and may include multiple vehicle or subsystem trades.
4) **Low to Moderate Fidelity** – Mission Design elements typically have contingencies greater than 5% while design concept masses typically have contingencies of 20% or more[4].

Design decisions made at the Pre-Phase A level include:

1) **Basic Mission Planning Decisions** – Determining optimum launch windows, required flight operations and maneuvers, Delta-V estimates for propulsive maneuvers, target orbits, and trajectories.
2) **Concept Level Go-Forward Decisions** – Down-selecting among competing concepts based on FOM scoring, feasibility analysis, and architecture decisions.
3) **Individual Concept Design Decisions** – Making Configuration decisions and decisions involving component or subsystem selection to realize an optimal design.

IV. Risk Analysis for Pre-Phase A Design

C. Benefits of Risk Analysis in Pre-Phase A

Risk Analysis affords several benefits to the Pre-Phase A design process. As mentioned previously, RIDM includes using risk assessment as a component of decision making. When system designers make choices regarding which system type to include or which components to select, risk should be a factor guiding those decisions. In the conceptual design process, this means using assessed risk as one of several FOMs considered, such as performance, mass, etc. In the same way, risk should be a FOM used in selecting among competing concepts in architecture studies. For example, if four lander concepts are being considered for a particular Mars mission, overall risk should be one of the factors influencing the decision of which lander to use. The relative weight given to risk as a deciding factor may be mission-dependent and might change over time, but risk should always be a factor.

Risk Analysis can be useful in planning future project activities. As previously mentioned, Pre-Phase A is the initial phase of mission and space systems concept development. The products of a Pre-Phase A study guide the activities in later developmental stages and limit their scope. By uncovering potential problems or recognizing a high degree of uncertainty in specific areas, Risk Analysis can help project planners assess the personnel, resources, and level of effort required for future development. This is useful in guiding both strategic and tactical planning activities.

To be of benefit in a Pre-Phase A study, Risk Analysis must provide scores that are objective and compare the risks of decision alternatives in a study. For example, using risk as a FOM in deciding whether or not to choose a specific propulsion system over a competing one, the risks of both systems must be scored in a way that easily determines which alternative incurs the most risk. Pre-phase A Risk Analysis must also include information that will allow technical experts to investigate mitigation or other disposition alternatives in future studies.

D. Reluctance to Perform Pre-Phase A Risk Analysis

Despite the benefits of Risk Analysis in a Pre-Phase A study, comprehensive risk assessment is seldom performed unless there is a requirement for a risk product. Some NASA programs, such as New Frontiers, require Risk Analysis as part of the response to an Announcement of Opportunity [5.] Therefore, most conceptual design teams at NASA have procedures for performing risk assessment when it is required. However, even when a risk product is required, in-depth Risk Analysis methods for conceptual design are still lacking. Virtually all conceptual design studies include a system component breakdown with a mass statement. There is no such equivalent for risk at the Pre-Phase A level.

One reason for this lack of established risk methodology in conceptual design is the widely accepted notion that risk identification and assessment is time-consuming and expensive. In order to use risk as a viable FOM for evaluating design decisions in a Pre-Phase A design, a risk methodology that utilizes a quick and easy approach to assess the risk of each design alternative is needed. This paper proposes both a methodology and a tool for assessing risk at the conceptual design level.

Another reason for this lack of an established risk methodology at the Pre-Phase A level is the belief that the fidelity at which risk may be assessed at the conceptual level is very low. There is the perception that large amounts of error in risk evaluation make it meaningless. The degree of error in risk assessment is usually not as large as it is perceived to be. Even with fairly large errors, risk scores are nevertheless useful as a basis for comparison and as a criterion for deciding between design alternatives.

Debating actual likelihood and consequence numbers and deciding on an agreed-to range for them can be done by the design team. After determining the range, the risks can be scored on both the low and high ends. The design team or individual analyst should either have a good idea of which alternative incurs more risk, or determine that the risk is not a feasible FOM for choosing either one. In the latter case, notes can made in the resulting risk plan and the choice deferred for later studies.

Discipline experts in a conceptual design environment often see formal Risk Analysis as unnecessary due to their knowledge of the technology and application of it in their respective fields. Most engineers consider risk in some fashion when making design choices, and most design engineers feel that they have good judgment in deciding which design choices are risky and which are safe. In fact, all risk assessment is ultimately based on expert knowledge; an expert engineer *does* know a lot about the risk factors in his/her discipline. However, there is a tendency in a large, complex system to overlook small details buried deep in the design unless the expert utilizes a rigorous process to consider all risk possibilities. An expert orbital mechanic, for instance, might know that lunar orbits are unstable over long periods of time due to perturbations in the density of the interior of the moon, but the engineer may not consider this problem unless explicitly made aware that the lunar loiter duration of a mission is extremely long.

There is some resistance to Risk Analysis in Pre-Phase A studies based in bureaucratic inertia. As previously noted, most Pre-Phase A studies do not include a rigorous Risk Analysis. Conceptual design teams tend to perform studies in a similar manner. They also tend to resist substantive changes to the team’s established design processes.

E. Basic Requirements for Pre-Phase A Risk Analysis

One purpose of this paper is to propose a Risk Analysis process specifically for Pre-Phase A design studies. The paragraphs that follow outline basic requirements for Risk Analysis at the conceptual design level and address the problems explained above.

The Risk Analysis process must be adaptable to a wide variety of concepts. Most Pre-Phase A design teams perform design studies based on a wide array of missions and elements. The team on which the authors serve has designed Earth-to-orbit vehicles (manned and unmanned), satellites for science missions, solar-electric tugs, nuclear-electric interplanetary vehicles, space stations, Mars and lunar landers, lunar surface habitats, space telescopes and fusion propulsion vehicles. Any risk assessment method must be adaptable to that range of technology and application.

The Risk Analysis process must support RIDM**.** To meet NPR8000.4a objectives, risks must be scored in a way that facilitates use as a FOM in evaluating decisions. To accomplish this goal, risk scores must be evaluated as thoroughly, accurately, and objectively as possible. Scores must also be comparable to those evaluated for other competing alternatives.

The Risk Analysis process must be performed as quickly as other analyses used in Pre-Phase A conceptual design. Each discipline expert will be able to contribute to the Risk Analysis process quickly and efficiently. This does not imply that the discipline expert will perform the Risk Analysis. A risk analyst can perform Risk Analysis for all disciplines if given input from each discipline expert.

The Risk Analysis process must provide data for inclusion into a risk plan for CRM. The process must also preserve all qualitative information regarding risks (i.e. risk statements, mitigation options, etc.) and allow users to edit them for inclusion in other studies.

F. Source Taxonomy-Based Risk Identification

The proposed Risk Analysis process in this paper contains four principal elements listed below:

1) Source Taxonomy-based Risk Identification
2) Risk Value Scoring
3) Major Risks Report
4) Initial Risk Management Plan

The first step in analyzing risk is identifying the risks to be assessed. The Source Taxonomy-Based Risk Identification method begins with a taxonomy, or breakdown, of the possible sources of uncertainty and/or risk in the concept. The risk analyst develops a questionnaire based on this taxonomy for each discipline expert to answer. Each question asks the discipline expert about the applicability of a risk source to some aspect of the concept under development. The answers to the questionnaire reveal the risks related to each risk source[6]. In theory, each type of space system concept (i.e. satellite, launch vehicle, etc.) could have a different taxonomy. However, in practice the top levels of the taxonomy are nearly identical for all projects. There are four principal risk sources at the top level of the taxonomy: 1) Requirements, 2) Mission Operations, 3) Design and Integration, and 4) Testing and Qualification.

The source of risk regarding requirements is the uncertainty in mission objectives and requirements as conveyed by a study customer. This does not refer to mistakes or accidental omissions in the requirements, but rather necessary uncertainty in the objectives and requirements due to lack of analysis or specific commitment at higher management levels. If the President, for instance, has not decided how extensive a lunar exploration program he intends to propose to the Congress, there will be a large amount of uncertainty in the requirements of a lunar lander study. Requirements risks can also come from inadequate requirement detail, forcing customers or designers to make too many assumptions. Another requirements-related risk is that the requirements set may change after the design has been completed, forcing the program to re-design at additional cost and schedule delay. Risk is also incurred when there is uncertainty regarding the feasibility of objectives or derived.

Mission Operations is a source of risk. Each mission operation must be evaluated for feasibility in the context of the overall mission. Some operations and maneuvers carry inherent risk. For instance, the probability of a successful robotic landing on Mars is around 50%, based on prior experience. Risk can also come from a lack of flight experience or from known loss experience. Uncertainty concerning consequences of an operation on other aspects of the mission can introduce risk, as well.

Design and Integration is another source of risk. Each component included in the design concept may have risk associated with it. Lack of technological maturity introduces reliability risks. Component availability introduces risk when there is uncertainty that a component can be obtained within required cost and schedule constraints. Integration is also an area where risk can be introduced due to known integration issues regarding redundancy and fault tolerance of integrated assemblies.

Testing and Qualification become a source of risk due to uncertainty in procedures and/or facilities for testing each space system component. This is not caused by mistakes in test planning or accidental omissions but caused by necessary uncertainty in testing or test planning due to factors beyond the customer's knowledge or control. Inadequite test objectives introduce risk when a test plan is incomplete or cannot be written until a later date. An example is a surface drill that cannot be tested due to inadequate data concerning the surface to be drilled. Test Feasibility introduces risk when there is uncertainty as to whether component testing is feasible given current facilities.

The Risk Analysis questionnaire will contain questions about each risk source in the described taxonomy for every mission operation and concept component to which it applies. Each discipline expert will answer the questions related to that expert's specific discipline. Answers to each question indicate which, if any, risks are indicated. A list of possible risks is then compiled based on the questionnaire answers.

G. Vetting the Risk List

This list of possible risks will not usually be in an acceptable final form. The design team and risk analyst will review the list to eliminate any risks with a likelihood so low as to be considered insignificant (e.g. communications satellite being struck by a meteor) or that the team agrees to omit for other reasons (risks inherent to all designs, for example). The team will combine risks with common root causes so that risks are as causally independent as possible because there is a natural tendency to find interdependent risks with most risk identification methods. This occurs when an underlying risk cause manifests itself in multiple disciplines or project phases. For example, solar particle exposure risks in high earth orbits that are identified for science instrumentation may be identified for solar arrays separately by a different discipline expert. In such a case, it is desireable to combine the risks into a single 'Solar Particle Exposure' risk with a single likelihood value for the purposes of risk scoring, but list the comprising risks separately for risk mitigation and planning purposes. This may be accomplished by adding a combined risk above the comprising risks in the worksheet, and changing the likelihood of each comprising risk to "*" in order to indicate that the risk is a 'child' risk to the combined risk listed above it. The team will also add any new risks that arise during the discussion process.

H. Risk Value Scoring

The remaining risks are then assigned likelihood and consequence values by discipline experts. The likelihood values will be probabilities expressed as a number in the open interval 0-1. The consequence values, on the other hand, will be in loss units. These may be in any units as long as the same units are used for all risks in the study and the units quantify the consequence of the risk event. The units must also be a linear measure of the consequence such that a 50% probability of a consequence of **2x** is seen to have the same expected value as a 100% probability of a consequence of **x.** The most frequent units used are schedule days and $. After the likelihood and consequence values are agreed upon, the risk may be scored as the expected risk value **(Likelihood × Consequence).**

Aggregate risk scores can be computed that represent the total risk posed by multiple identified risks (perhaps the risks found in a particular vehicle subsystem).

If Pr_1 represents the likelihood of Risk 1,
Pr_2 the likelihood of Risk 2,
Pr_n the likelihood of Risk n

And

Cr_1 represents the Consequence of Risk 1,
Cr_2 the Consequence of Risk 2,
Cr_n the Consequence of Risk n

And the probabilities of all risks to be combined are causally independent of one another and not mutually exclusive.

$$\textbf{Aggregate Likelihood} = 1 - ((1 - Pr_1)\times(1 - Pr_2)\times\ldots\times(1 - Pr_n)) = 1 - \Pi_{i=1,n}(1-Pr_i)$$

In similar fashion an aggregate expected Risk Value can be computed:

If $Vr_1 = Cr_1 \times Pr_1$ represents the Expected Risk Value of Risk 1,
$Vr_2 = Cr_2 \times Pr_2$ the Total Risk Value of Risk 2,
$Vr_n = Cr_n \times Pr_n$ the Total Risk Value of Risk n

$$\textbf{Aggregate Risk Value} = Vr_1 + Vr_2 + \ldots + Vr_n = \Sigma_{i=1,n} Vr_i$$

Since

$$\textbf{Risk Value = Likelihood × Consequence}$$

Then

$$\textbf{Aggregate Consequence} = \frac{\textbf{Aggregate Risk Value}}{\textbf{Aggregate Likelihood}}$$

Note that this Aggregate Consequence is not a real consequence; it is for comparison purposes only. To see the actual composition of risk values, comparing risks as pairs (Likelihood, Consequence) is sometimes beneficial. This will provide a comparable Consequence number.

I. Major Risks Report

After the risks have been scored, a document is compiled listing all of the major risks (those that have significant risk values) and their scores. Discipline experts then add two sections to each risk. One is a context section elaborating on the risk and its context in the mission, and the second is a list of possible disposition options for the risk, such as mitigation, de-scope, etc.

Any combined risk scores deemed significant should also be listed with a discussion of their significance. This Major Risks Report represents a customer deliverable.

J. Initial Risk Management Plan

The Initial Risk Management Plan contains an initial plan for managing a project's risk as it goes forward. If the Pre-Phase A design study is part of a proposal, a Risk Management Plan will likely be required as a separate proposal section. This document contains three major sections as follows:

1) A summary of the risk disposition options listed in the Major Risks Report.
2) A list of problems that need further research (other than performing analytical studies).
3) A discussion of further analytical studies that need to be performed in order to mitigate risk.

V. Advanced Concepts Evaluating Risk Tool

To expedite the Pre-Phase A Risk Analysis process within NASA MSFC's Advanced Concepts Office, a computational tool was developed for use by both discipline experts and risk analysts. This tool is called Advanced Concepts Evaluating Risk Tool (ACERT) and is applicable to any group or organization engaged in conceptual design who wish to assess risk in an expedient, efficient manner. The major objectives of ACERT are described in this section. One such objective is to identify and assess risks by discipline and/or design subsystem. Identifying risks in logically grouped parts and combining the results later is often convenient. ACERT will allow individual analysts to perform initial risk identification separately and to do any reasonable portion as an individual run. The risks may be edited and combined later. Another objective is to identify risks in a rigorous and structured manner. ACERT will guide each discipline expert by asking a structured series of questions (generally multiple choice) and will use the answers to generate suggested risks. Automating parts of the Risk Analysis process is facilitated by ACERT, which automates the generation of risk suggestions and provides facilities for computing individual and combined risk scores. Users can easily edit risk information by adding or deleting risks from the risk list. In addition, a user can edit all fields for each risk. ACERT also allows users to compute risk scores for any portion of the design or mission operations and provides facilities to compute combined risk scores for any group of risks.

Users can configure all aspects of tool behavior within ACERT’s performance scope. Users can develop their own taxonomy, compose questions to be asked, compose and maintain rules that guide the way in which questions are asked and the way in which risk suggestions are generated, including the verbiage of the risk statements. ACERT will not enforce or provide a specific set of rules for identifying risks other than those inherent in the tool’s limitations, unless specifically configured in that manner.

K. Tool Overview

ACERT is implemented as a Microsoft Office Excel workbook. There are three worksheets that provide input to the tool to specify information about the mission and concept. The first worksheet allows for entry of miscellaneous information about the mission. ACERT can be configured for a wide variety of possible entries on this sheet, but each entry must be an individual value (number or string). The second worksheet is used to input System Breakdown Structure (SBS) data regarding the space concept design of major systems and their constituent components. The third input worksheet is a sequence of operations listing, in order of occurrence, major mission operations.

An Excel macro is provided to launch a rule-based expert system to identify the risks. If this macro is run while the SBS input worksheet is active, then the system will use the appropriate rules to identify risks related to the SBS elements. ACERT will ask a series of question for each SBS element in turn and generate a separate workbook with risk suggestions that may be copied back to the tool’s risk list. If the macro is run while any other worksheet is active, it will use appropriate rules to identify risks associated with the operations and general mission inputs and again generate a separate workbook with risk suggestions that the user may copy into the ACERT risk list.

Excel editing and computation facilities are used to manage the risk list. A macro function called **AggregateLikelihood(<Range>)** is provided to compute the likelihood of combined risks.

All of the files that configure the tool are text files and may be edited with a text editor. The inference rules that drive risk generation are all available in the tool launch directory, as are the risk statement templates. HTML tags may be used in the risk statement templates to display simple text effects like italics, bold, etc.

L. Initial Tool Inputs

The initial input worksheets mentioned above are included in the ACERT workbook. Each must have the correct sheet name and must be in a specific format.

The **Mission** worksheet is used to input values for user-specified mission variables. The user can create **if…then** rules that drive the risk identification. In those rules, the user can take the variables defined on this worksheet to make decisions. The worksheet format is shown in Table 1below:

Table 1. Mission Worksheet

Value
Demo Mission
Earth Orbit
15 Days

For example, when configuring risk rules, a user might write a rule such as the following:

MissionTooLong::if[Duration > 14 then risk[“MissionTooLong”, “MISSION”, 0.1]];

This rule would cause the risk in the rule above to be generated during risk identification since the variable **Duration** is given a value of 15 on the **Mission** worksheet. These variables are available for use in the text of questions or in the text of risk statements.

The worksheet named **SBS** is used to provide a breakdown structure for the portion of the design concept for which risks are identified. The format for this worksheet is shown in Table 2 on the next page.

Table 2. System Breakdown Structure Worksheet

4.0	**Power**	
	4.1	Power Distribution Unit
	4.2	Cabling
	4.3	Fuel Cell Power System
	4.4	H2 Tank
	4.5	O2 Tank
	4.6	Water Tank
5.0	**Mechanisms**	
	5.1	Thrust Vector Control
6.0	**Avionics**	
	6.1	Attitude Control System
	6.2	Command and Data System
	6.3	Instrumentation
	6.4	Communications System
	6.5	Avionics Cabling

The SBS format shown above is the minimal format. Other columns may be included for convenience, but they will be ignored by the risk identification system. The deepest-level elements of this structure (the ones that have no sub-elements, such as ‘4.1 Power Distribution Unit’ above) are the **components** in the breakdown, while the other elements are **assemblies.** The breakdown may be as many as three levels deep, with two levels of assembly and one level of component.

When the risk identification macro is run with the **SBS** worksheet active, a specific set of rules will be checked for each component in the SBS in order to identify risks for that specific component. For each assembly, a different set of rules will be checked to find risks associated with the integration of the components into the assembly above it. In all rules, the variable **SBSItem** will have the string value of the item description (e.g. ‘Power Distribution Unit’) and the variable **ItemID** will have the string value ‘SBS’ concatenated with the SBS item number (e.g. for the Power Distribution Unit, ‘SBS4.1’). In the rules, these variables are typically used either in asking questions or identifying risks generated.

The input worksheet named **Operations** is used to provide a sequence of operations for identifying operations risks. The format for this worksheet is shown below in Table 3:

Table 3. Operations Worksheet

Sequence	Operation
1	Launch-to-Low Earth Orbit
2	Low Earth Orbit Loiter
3	Trans-Lunar Injection
4	Mid Course Correction
5	Lunar Orbit Injection
6	Lunar Descent
7	Lunar Landing

When the risk identification macro is run with the **Operations** worksheet active, a specific set of rules will be checked for each operation listed on this worksheet to identify risks for that operation. In all rules, the variable **OPSItem** will have the string value of the item description (e.g. ‘Launch to Low Earth Orbit’) and the variable **ItemID** will have the string value ‘OPS’ concatenated with the item number (e.g. for the Launch to Low Earth Orbit operation, ‘OPS1’). In the rules, these variables are typically used either in asking questions or identifying generated risks

M. Risk Identification System

The risk identification system ACERT uses to generate risk suggestions is a backward-chaining rule-based inference engine written in the Java programming language. Backward-chaining systems use a set of **if…then** rules to make decisions or to follow plans. The set of rules together is called a **Rule Base.** In ACERT, rules are used to decide whether particular risks apply to a mission or design concept.

There are three distinct rule bases used in ACERT. The **Operations** rule base contains a set of rules to find risks in the sequence of operation found on the **Operations** input worksheet. The rule base is applied to each operation in turn to decide if any risk identified by that rule base applies to the operation. Any that apply are added to a risk list. An HTML file containing the actual risk statement is generated from a template file, which can be used in other documents. Similarly, the **Design** rule base contains a set of rules to find risks in the **SBS** elements. Just as with the **Operations** rule base, these rules are applied to each element of the **SBS** in turn to decide if any known risks apply to that **SBS** element. Any risks found are added to the list. A third rule base, the **Project** rule base, contains a set of rules to find other risks that apply to the mission, design concept, or project as a whole.

When a user clicks on the **Risk Identification** button on the **Quick Access** toolbar, an Excel Visual Basic for Applications macro is run. This macro first checks to see which worksheet is currently active. If the worksheet named **SBS** is active, the macro writes the SBS information to a text file. If another worksheet is active, the macro writes the information on the **Operations** worksheet to a text file. In either case, the macro launches the backward-chaining system as a separate process. In the case where the **SBS** information is being processed, the **Design** rule base is applied to each **SBS** element. In the case where the **Operations** data is being processed, the **Operations** rule base is applied to each operation in turn, and then the **Project** rule base is applied.

After the risk identification macro has completed, a new workbook is opened containing a list of the risks found. This list is in the same format as the master risk list maintained in the ACERT workbook. The user may then copy any or all risks from the new workbook into the master list using the clipboard.

N. Using the Tool to Score Risks

The workbook constructed by the risk identification system contains the individual risk scoring formula in the **Risk Value** column. To combine risks, the user can use the **AggregateLikelihood(<Range>)** function to compute the probability that any combined risks in <Range> will occur and the **Sum(<Range>)** function to compute the Risk Value of the combined risks in <Range>.

O. Tool Configuration

Almost all tool behavior can be configured by the user, within the scope of the tool capabilities. Each rule base is configured in a separate plain text file with a **.rul** extension. The rule format is unique to the tool. To specify a risk, the **then** clause of a rule uses a **risk** primitive that specifies the risk name and a template file used in generating a risk statement. This template file is also a text file that contains the text of the risk statement, along with tags containing variable names. When a risk is generated, the variable values are substituted for the names. **HTML** tags may also appear in the text to implement formatting effects like bold (<b> tag), italic (<i> tag), and other formatting. The entire statement should be enclosed in a paragraph element (<p>…</p>) so that the risk statement will appear as a separate paragraph in documents that contain other information.

P. Tool Status

ACERT is currently undergoing initial testing at the Advanced Concepts Office, Marshall Space Flight Center in Huntsville, AL. At present, only the most basic rules have been included in the rule bases; more will be added as the tool becomes more widely used. Rules that need to be added include more operations risks based on failure experience with each type of maneuver. ACERT contains questions that break down the operations sequence to a reasonable level of detail. However, adding all known risks associated with each operations scenario still needs to be done. Another task that remains to be done is to add rules to look for known risks that are already documented. There are several lists of these available; however rules for them need to be added. Initial testing and the first round of improvements are scheduled to be completed by the end of the fiscal year.

Q. Risk Tool Identification Validation Testing

To compare the risk identification performance of the risk tool to other risk identification processes, the list of risks found in a previous Pre-Phase A study was compared to a list of risks generated by this risk tool inference engine and applied to the same study.

The study was a pre-proposal study for an Aitken Basin Lunar Sample Return Mission performed as part of a proposal effort to the New Frontiers program. The basic mission plan was to send a robotic lander to the rim of the Aitkin Basin near the Moon's South Pole, land there with minimal contamination of the lunar surface, drill a 1m deep core sample, collect surface regolith with a robotic arm, place the samples in a return canister, and return the canister safely to Earth.

Risk Analysis was required for the proposal and was performed by the Advanced Concepts Office at the NASA Marshall Space Flight Center in conjunction with NASA Ames Research Center and industry partners over a three day period. On the first day, the design team held a risk workshop which included presenting the mission plan, concept of operations, and each vehicle concept design to a selected team of discipline experts recruited from proposal industry partners. These discipline experts had not been directly involved in either the mission analysis or the vehicle designs. On the second day, the discipline experts were tasked with evaluating risks for each element presented in an individual discipline. They were given a risk format template to complete for each. On the third day, the discipline experts met with the design team to review the risks and finalize the major risks list. After vetting the risk list and combining similar and inter-dependent risks, 17 risks were found. Four were considered to be of too little significance to be reported. This left 13 reportable risks.

To test the rule-based risk identification system in ACERT, the rule bases were run against study mission operations and SBS specifically looking for each of the 13 risks found in the prior study. Because the author running the tool was not an expert in all required disciplines, a risk was considered identified by the tool if it was generated by an appropriate answer to a question asked by the system. Appropriate is defined as a choice of answers that led to the generation of the risk under evaluation and would be a reasonably expected choice for a discipline expert. For instance, if a risk involving a propulsion system assembly was found by the existing rule-base, only if the propulsion expert correctly answered a question about communications software was the risk not considered found. If correct answers to all questions could be expected from a propulsion expert, that risk was considered found.

The following three results were then tabulated: risks found, risks findable, and risks not findable. Risks found is defined as the number of risks found in the original study that were also found by the rule-based identification method assuming 'appropriate' answers to risk questions. Risks findable is defined as the number of risks found in the original study that were not found by the rule-based method, but could be found by adding one or more rules to any of the rule bases. Risks Not Findable included the number of original risks for which a rule could not easily be written to find with a rule-based system. Proving that no such rule exists would be difficult, but it is unlikely that the automated risk identification system would ever find such a risk. Results: Found 8, Findable 4, and Not Findable 1.

This test was limited in scope, thus caution must be used in drawing conclusions from it. This test provides only an indication of how efficient the tool methodology is at finding risks identified by an older, more time-consuming method. There are also likely to be a number of risks found by rule-based analysis that would be less likely to be found using other methods; however this has not been tested. There is also the problem that the rule-based analysis was performed by one engineer who is qualified in only two disciplines involved in the study. In normal practice, the rule-based tool would be used by each discipline expert individually and the risks combined with possibly the addition of others in a group setting. The test methodology was chosen to overcome this problem to some degree by allowing inclusion in the 'Found' category of risks that would be found given appropriate expert answers to existing questions.

The real purpose of the initial test was to derive a sense of the types of risk a taxonomy-based, rule-driven system is unlikely to find. Meaningful data was obtained in this regard. The one 'Not Findable' risk concerned the deposition of lunar sample material into the return canister, which is shown below:

Risk Statement:

If the robotic arm is unable to deposit samples in the sample canisters due to triboelectric charging effects, then the sample may be lost.

Context:

Lunar dust is known to be "sticky", and charging effects cause it to clump together. This could pose a problem for getting the samples into sample canisters.

There is a similar problem with Martian regolith, and this became a serious issue for the Mars Phoenix lander, which was unable to use several of its sample ovens because of difficulties in depositing samples due to sample clumping caused by triboelectric charging.

In this case, it was concluded that the risk was not likely to be identified by the backward-chaining system due to the reasons listed below:

1) The root cause of the risk – triboelectric charging – is not directly related to structure or function of the arm.
2) If the sample particulate were denser or larger, the charging effect might not cause a problem regardless.
3) Important factors like composition and properties of Lunar regolith friction generated during sample collection, etc. are not available to the automated tool.

In short, this risk was identified because of two distinct factors, both necessary to the risk inference. The first is the experience of the Mars Phoenix Lander Team. No one anticipated the sample transfer problems that the Phoenix Lander experienced. Understanding of the problem came about due to experience with it. The second critical factor was the higher reasoning ability of the human expert in recognizing the important similarities in the lander equipment and in the properties of the regolith on both the Moon and Mars. One could argue that this is not beyond the ultimate capabilities of a backward-chaining system; rules could be entered describing all sorts of regolith, robotic arms, electrostatic effects, etc., but it seems far fetched that such an enormous rule base could be developed to implement a Pre-Phase A risk identification tool. Such a tool would be so time-consuming if it did have such a rule base as to be unusable.

VI. Conclusion

The use of a simplified taxonomy-based Risk Analysis process for Pre-Phase A design is being tested in the Advanced Concepts Office at MSFC. The goal of significantly reducing the time required to analyze risk has been achieved to the extent that RIDM at the Pre-Phase A level has been determined achievable. The process has so far appeared to be useful in a wide variety of designs, although its actual application has been limited.

Limited data on effectiveness seems to bear out what was initially assumed – that taxonomy-based risk identification, although it doesn’t find all types of risks, is well-suited to finding the sorts of risk that impact Pre-Phase A design decisions. A close look at design decisions made in Pre-Phase A will reveal that they are high level decisions (e.g. choice among flight maneuvers, choice of solar array panels, choice of tank geometry, etc.) as opposed to the more unstructured problems faced in research laboratories or at more detailed design levels. Taxonomy-based risk identification generally works well for informing those decisions because the uncertainty (and hence risk) involved in those decisions is based on general, abstracted flight experience with the selected components or maneuvers (or lack thereof). Rule-based systems tend to be effective at abstracting experience with known choices, while taxonomy-based risk identification provides an adequate job of covering that risk space.

Further development on ACERT is planned and will make the tool more robust and user friendly. The rule-bases will also be expanded beyond their present scope. ACERT is currently undergoing intensive testing on actual studies within the NASA MSFC Advanced Concepts Office, which will provide excellent data for future development efforts to improve and expand the tool.

Acknowledgments

The authors thank NASA MSFC Advanced Concepts Office Manager Reginald Alexander for approving the development and use of ACERT in the Advanced Concepts Office. The authors appreciate Risk Experts and Systems Engineers John P. McCullough and Thomas R. McInnis of the Jacobs Engineering, Science, and Technical Services Group for reviewing this material and providing valuable feedback.

References

[1] The Aerospace Corporation, “Risk management Quick Reference Card”, URL:http://www.aero.org/education/tai/documents/RiskMgtQuickRef.pdf, 2003, p. 2

[2] NASA Office of Safety and Mission Assurance, “Agency Risk Management Procedural Requirements”, NASA NPR8000.4A, 2008, p. 6

[3] NASA Office of Safety and Mission Assurance, “Agency Risk Management Procedural Requirements”, NASA NPR8000.4A, 2008, pp. 7,8

[4] Goddard Space Flight Center, “Rules for the Design, Development, and Operation of Flight Systems”, NASA GSFC-STD-1000 Rev E, 2009, p. 14

[5] NASA, “Announcement of Opportunity – New Frontiers 20009”, NASA NNH09ZDA007O, 2009, p.B-19

[6] Carr, Marvin J., Konda, Suresh L., Monarch, Ira, Ulrich,F. Carol, Walker, Clay F.,”Taxonomy-Based Risk Identification”, Technical Report CMU/SEI-93-TR-6,ESC-TR-93-183, Software Engineering Institute, Carnegie Mellon University, Pittsburg 1993, pp. 7,8

Risk Evaluation in the Pre-Phase A Conceptual Design of Spacecraft

AIAA Space 2009 Conference

8/31/2010

Jacobs Engineering, Science, & Technical Services to NASA Marshall Space Flight Center, Advanced Concepts Office

Leo Fabisinski and C. Dauphne Maples

Outline

- Introduction
- Risk Management Overview
- Risk Management at NASA
- Pre-Phase A Conceptual Design
- Risk Analysis in Pre-Phase A: Benefits vs. Reluctance
- Requirements for Risk in Conceptual Design
- Proposed Risk Analysis Process for Pre-Phase A
- Advanced Concepts Evaluating Risk Tool (ACERT)
- Conclusions

Introduction

- **NASA defines the initial conceptual design stage as Pre-Phase A, per NPR 7120.5, the NASA Systems Engineering Handbook**
- **Pre-Phase A is the phase where objective, high-level design decisions are made**
- **Design decisions are made using Figures of Merit (FOMs), which are agreed-upon measures that are**
  - Objective
  - Comparable
  - Easily Evaluated
- **This presentation asserts that risk is a FOM that should be considered in Pre-Phase A decision-making**

Risk Management Overview

- **Risk is defined as Any Possible Future Event**
  - Whose occurrence is uncertain
  - That may result in a failure to meet a mission requirement
- **Risk is often quantified as**
  - Likelihood – Probability of occurrence (0.0 to 1.0)
  - Consequence – Cost (in $, Time, etc.) of occurrence
- **Total Risk Value = Likelihood * Consequence**

Risk Management at NASA

- **NASA specification NPR 8000.4A defines Risk Management as a two-fold process**
  - Risk Informed Decision Making (RIDM)
  - Continuous Risk Management (CRM)
- **RIDM consists of three processes that**
  - Identify decision alternatives
  - Perform risk analysis on each decision alternative to support ranking
  - Use risk analysis results to help select a decision alternative (selection informed by risk analysis – not solely based on it)
- **CRM is an iterative process made up of six steps**
  - Identify risks
  - Analyze to estimate likelihood and impact
  - Plan future tasks in consideration of risk disposition (Mitigation, Acceptance, etc.)
  - Track observables and FOMs to assure requirements will be met
  - Control risk by implementing risk mitigation plans in the ongoing project
  - Communicate and Document the above activities throughout the process

Pre-Phase A Conceptual Design

- **Large Breadth of Concepts**
  - Launch Vehicles
  - Satellites
  - Fusion-Powered Inter-Planetary Vehicles
- **Low Depth – not a detailed design**
- **Quick Turn-Around – typically performed in weeks**
- **Low to Moderate Fidelity – 5% to 20% Contingency**
- **Basic Mission Decisions**
  - Launch Windows
  - Target Orbits (e.g. 600 km, 28° Circular)
  - Flight Operations
- **Determine Feasibility of Specific Concepts for Go-Forward Decisions**
- **Decide which concepts are best suited to the mission by virtue of their FOM scores**

Risk Analysis in Pre-Phase A: Benefits vs. Reluctance

- **Benefits of implementing Risk in Pre-Phase A**
  - Aids in evaluating Concept Design Decisions when used as a FOM
  - Informs the planning of the crucial Phase A Study that will culminate in a Preliminary Design Review
  - Guides Project Management in allocating resources to solve potential problems early
- **Reluctance to use Risk as a FOM in Pre-Phase A**
  - Time-Consuming, Expensive
  - Low Fidelity of Risk Likelihood, Consequence
  - Unnecessary

Requirements for Risk in Conceptual Design

- Must support Risk Informed Decision Making (RIDM) for Pre-Phase A decisions
- Must be quick and easy to implement
- Must be adaptable to a wide variety of concepts
- Must be capable of producing a Risk Plan useful for further studies (CRM)

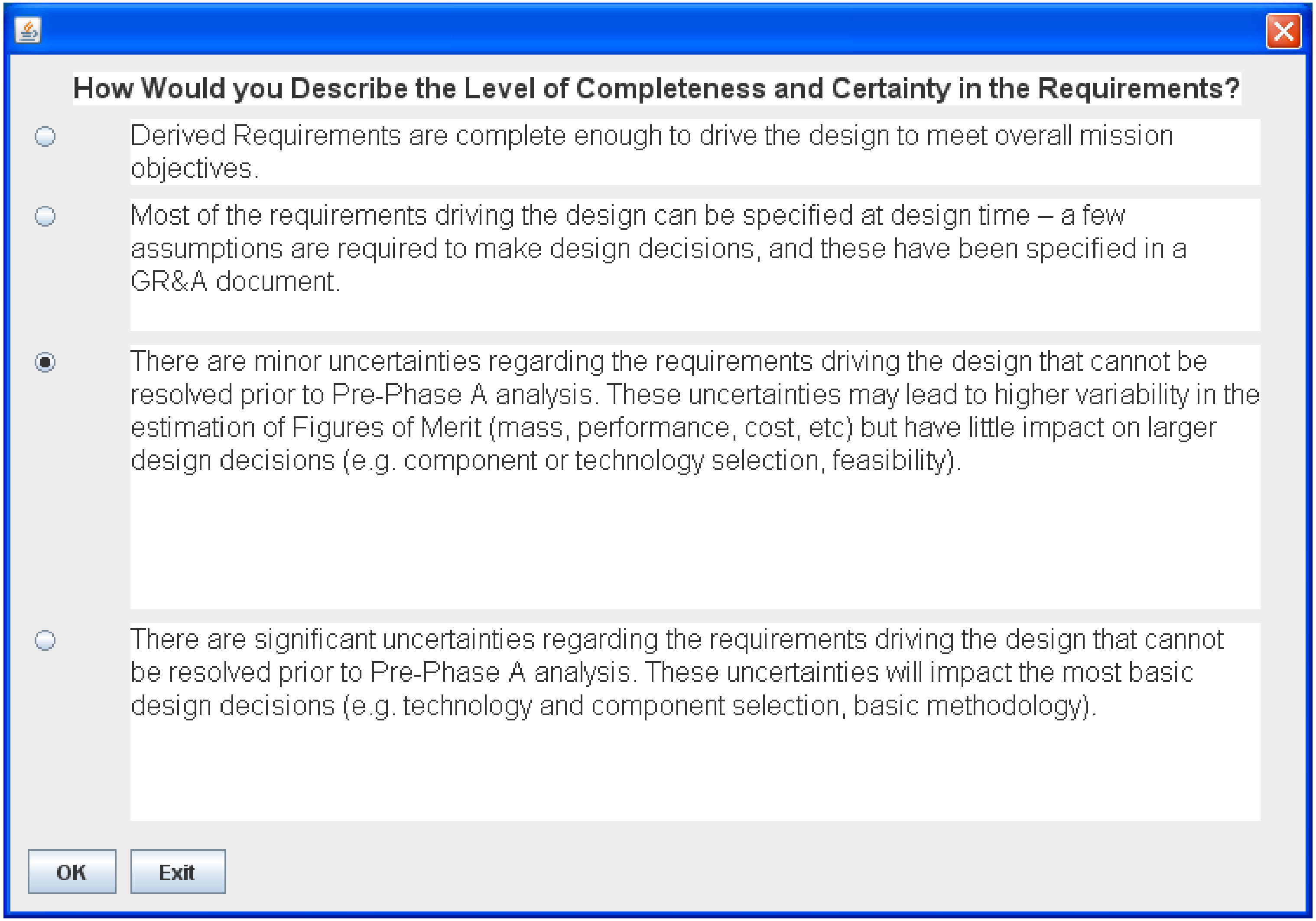
Proposed Risk Analysis Process for Pre-Phase A

- **Source / Taxonomy-Based Risk Identification**
  - Based on the following sources of Risk uncertainty
    - Requirements
    - Mission Operations
    - Design & Integration
    - Testing & Qualification
- **Risk Value Scoring**
  - If there is both a Likelihood and Consequence score for an individual risk, we may calculate:

    Risk Value = Likelihood × Consequence

    To determine the expected value (cost) of the risk
- **Major Risk Report**
  - A list of significant risks to be carried forward that have significant Likelihood and Consequence and cannot be mitigated in Pre-Phase A
- **Initial Risk Management Plan**
  - Dispositions Options for Each Major Risk
  - Recommends Disposition Strategy
  - Outlines contingencies and lists issues that require further research
  - Provides recommendations for planning next design cycle

Sample question evaluating requirements risk in the Advanced Concepts Evaluating Risk Tool (ACERT)



How Would you Describe the Level of Completeness and Certainty in the Requirements?

○ Derived Requirements are complete enough to drive the design to meet overall mission objectives.

○ Most of the requirements driving the design can be specified at design time – a few assumptions are required to make design decisions, and these have been specified in a GR&A document.

● There are minor uncertainties regarding the requirements driving the design that cannot be resolved prior to Pre-Phase A analysis. These uncertainties may lead to higher variability in the estimation of Figures of Merit (mass, performance, cost, etc) but have little impact on larger design decisions (e.g. component or technology selection, feasibility).

○ There are significant uncertainties regarding the requirements driving the design that cannot be resolved prior to Pre-Phase A analysis. These uncertainties will impact the most basic design decisions (e.g. technology and component selection, basic methodology).

Advanced Concepts Evaluating Risk Tool

- Java programming language used to develop ACERT
- Excel workbook-based interface
- Excel macro launches a rule-based (backward-chaining) system to identify risks
- Rules written and maintained in any of 3 text files
- Initial inputs include Mission, Operations, and Design information

Advanced Concepts Evaluating Risk Tool

- **Risk statements are edited in Excel and scored with VBA custom formula functions**
- **ACERT can be customized by editing configuration information**
  - Risk Identification Rules
  - Risk Statement Templates
- **System asks questions based on**
  - Mission Inputs
  - Systems Breakdown Structure
  - Operations Sequence

ACERT Mission Worksheet

- **The Mission Worksheet is the first of 3 initial input files in ACERT**
  - User defined Mission Variables
  - Can be used in rules (also user-defined)
  - Can be inserted into risk descriptions

Mission Worksheet

Variable	**Value**
Mission	Demo Mission
Type	Robotic Lunar
Duration	27 days
LaunchMass	35,500 kg
LaunchVehicleCapacity	50,000 kg

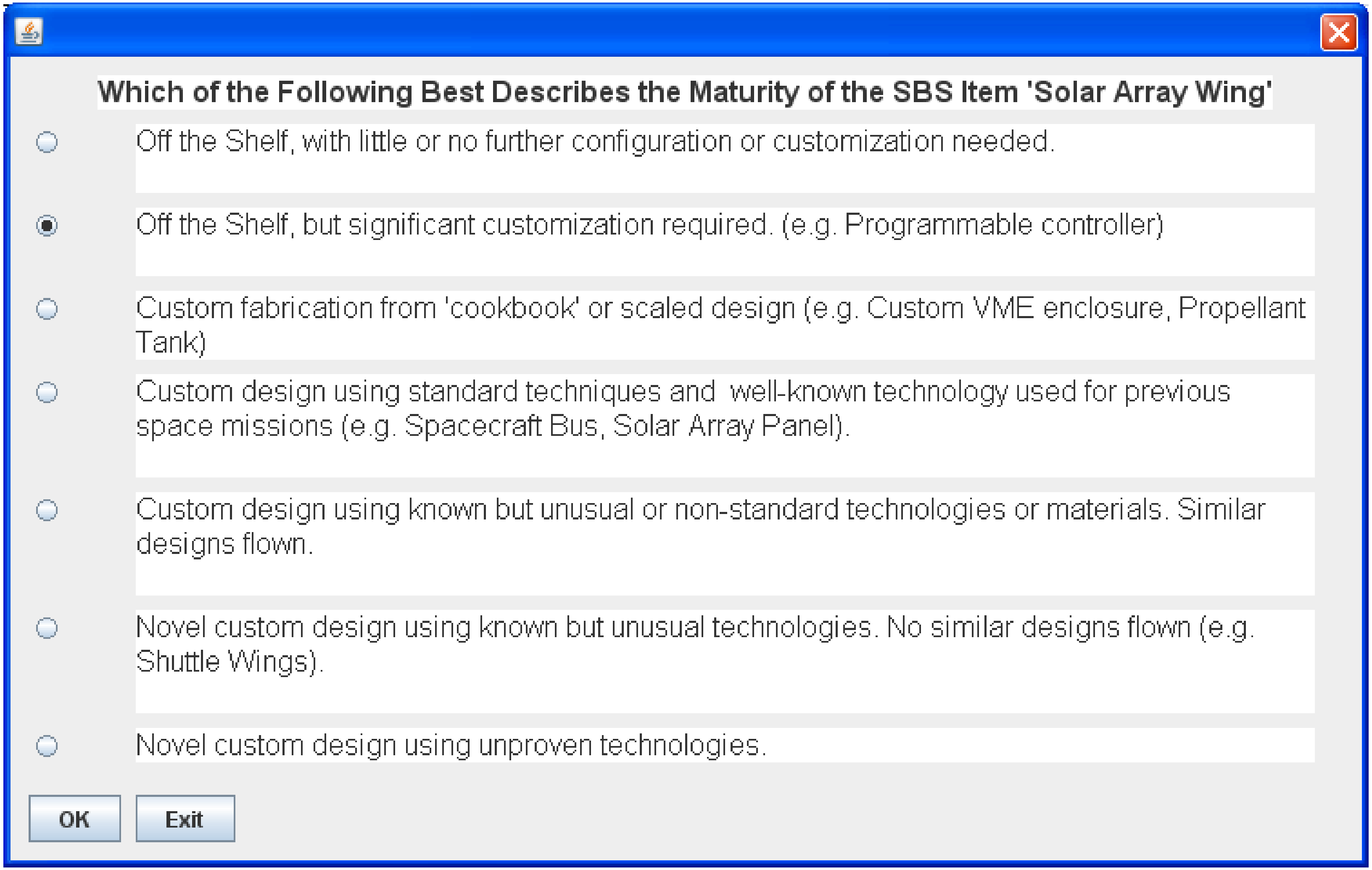
Advanced Concepts Evaluating Risk Tool (ACERT)

- **The System Breakdown Structure Worksheet is the second of 3 initial input files in ACERT**
  - Drives Risk identification for design, testing, and integration
  - Traditional multi-level component breakdown of design concept

System Breakdown Structure Worksheet

4.0	**Power**	
	4.1	Power Distribution Unit
	4.2	Cabling
	4.3	Fuel Cell Power System
	4.4	H2 Tank
	4.5	O2 Tank
	4.6	Water Tank
5.0	**Mechanisms**	
	5.1	Thrust Vector Control
6.0	**Avionics**	
	6.1	Attitude Control System
	6.2	Command and Data
	6.3	Instrumentation
	6.4	Communications System
	6.5	Avionics Cabling

Sample question evaluating a component in the Power Subsystem via the SBS Workbook



Which of the Following Best Describes the Maturity of the SBS Item 'Solar Array Wing'

○ Off the Shelf, with little or no further configuration or customization needed.

● Off the Shelf, but significant customization required. (e.g. Programmable controller)

○ Custom fabrication from 'cookbook' or scaled design (e.g. Custom VME enclosure, Propellant Tank)

○ Custom design using standard techniques and well-known technology used for previous space missions (e.g. Spacecraft Bus, Solar Array Panel).

○ Custom design using known but unusual or non-standard technologies or materials. Similar designs flown.

○ Novel custom design using known but unusual technologies. No similar designs flown (e.g. Shuttle Wings).

○ Novel custom design using unproven technologies.

Advanced Concepts Evaluating Risk Tool (ACERT)

- **The Operations Worksheet is the third of 3 initial input files in ACERT**
  - Appears on the Operations Worksheet
  - Drives Risk evaluation on Operations

Operations Worksheet	
Sequence	**Operation**
1	Launch to LEO
2	LEO Loiter
3	TLI
4	Mid Course Correction
5	Lunar Orbit Injection
6	Lunar Descent
7	Lunar Landing

Conclusions

- **A taxonomy-based Risk Identification and Assessment System can be done in Pre-Phase A**
- **This can be implemented using a tool, such as ACERT**
- **ACERT facilitates calculating Risk as a FOM quickly enough to be useful for Pre-Phase A studies**
- **Future work is needed on ACERT**
  - Add more rules to the ACERT rule bases
  - Extend ACERT capabilities
  - Perform more testing