A PROPOSED RISK-INFORMED DECISION-MAKING FRAMEWORK FOR NASA

Michael Stamatelatos, NASA Headquarters
Homayoon Dezfuli, NASA Headquarters
George Apostolakis, Massachusetts Institute of Technology

(Presented at the Eight International Conference on Probabilistic Safety Assessment and Management (PSAM 8,) New Orleans, USA, May 14-18, 2006)

ABSTRACT

The January 2004 Presidential Directive to NASA to adopt a goal-oriented space exploration program poses many challenges. These include sustained and affordable human and robotic space programs to explore the Solar System starting with a human return to the Moon and subsequent human exploration of Mars. Meeting the exploration technical and safety goals while meeting programmatic constraints related to cost and schedule involves making complex decisions. In this paper, we propose a risk-informed decision-making framework to better manage uncertainties and to better balance competing priorities that decision makers face routinely during the various phases of the program execution. In this framework, stakeholder expectations related to technical performance attributes, such as safety, reliability, and mission performance, as well as for programmatic performance attributes, such as cost and schedule, can be defined in terms of a set of performance measures (PMs) that need to be quantitatively assessed and monitored during the entire life-cycle of the program. Risk-informed decision making, as described in this paper, is the formal process of analyzing various decision alternatives with respect to their impact on the PMs, of assessing uncertainty associated with their degree of impact, and of selecting the optimal decision alternative using formal decision theory and taking into consideration program constrains, stakeholder expectations, and the magnitude of uncertainties. The proposed framework is based on an analytic-deliberative decision-making methodology that consists of three major steps: (1) formulation and selection of decision alternatives, (2) analysis and ranking of decision alternatives, and (3) selection of the best decision alternative. These steps are linked and are supported by a deliberation process in which the decision-makers scrutinize the initial set of decision alternatives and results of the analysis of decision alternatives to ensure that they are meaningful and that important concerns not captured by the analysis are considered.

ACRONYMS

AHP	Analytic Hierarchy Process
NASA	National Aeronautics and Space Administration
MAUT	Multi-attribute Utility Theory
PI	Performance Index
PM	Performance Measure
QRA	Quantitative Risk Assessment

INTRODUCTION

In January 2004, President George W. Bush announced the New Vision for Space Exploration directing NASA to embark on a comprehensive space exploration program that would advance the Nation's scientific, security, and economic interests. The goals of the exploration program are "safe, sustained, affordable human and robotic exploration of the Moon, Mars, and beyond ... for less than one percent of the federal budget." Implementation of the exploration goals requires development of a constellation of new systems that include earth-to-orbit, in-space and surface transportation systems, surface and space-based infrastructures, power generation, communications systems, maintenance and science instrumentation, and robotic investigators and assistants. The design and development of these systems will involve many decisions that require weighting/trading various competing programmatic and technical considerations against one another. The success of missions pursued using future space exploration systems and infrastructure is achieved by ensuring that technical objectives of the missions are accomplished safely within the constraints of cost and schedule and consistent with stakeholder expectations. The primary considerations that should factor into each design and operational decision are the following:

Mission Technical Objectives– Future space exploration systems and infrastructures should be designed and operated to ensure that technical objectives of exploration missions will be accomplished in a sustainable manner and on schedule. These systems must also be able to operate in an environment of considerable uncertainty throughout their life-cycles. These uncertainties arise from policy redirections, budgetary and organizational changes, and traditional technical and supply chain issues [1]. The design attributes for sustainability include flexibility (ability to adapt) and extensibility (ability to evolve).

Affordability – Future space exploration systems, infrastructure, and missions pursued using them should be affordable. The cost components that should be addressed include design and development cost, technology development cost, operation cost, and facility cost.

Safety – Future space exploration systems, infrastructure, and missions pursued using them should be safe. Safety is a NASA core value. NASA defines the term "safety" broadly to include human safety (public and workforce), environmental safety and assets safety.

Stakeholder Expectations – Future space exploration systems, infrastructure, and missions pursued using them should be able to adapt to (or be robust to) emerging political, technical, and budgetary changes and to evolve over time to continue to meet long term needs of intra-agency and extra-agency stakeholders.

This paper will discuss how NASA can address these attributes in an integrated framework which is based on an analytic-deliberative decision-making methodology [2]. While all above-mentioned attributes are important and to some extent dependent on each other, we will focus in this paper on how our proposed approach impacts mission technical objectives and safety.

THE ELEMENTS OF RISK-INFORMED DECISION-MAKING

Mission success is achieved by ensuring that technical objectives of the mission are accomplished safely within the constraints of cost and schedule and consistent with stakeholder expectations. Safety is one of NASA's core values. Ensuring safety involves the following high-level safety objectives[1]:

- Protecting public health
- Protecting workforce health
- Protecting the environment
- Protecting mission assets (systems and infrastructures needed to execute a mission) and public properties.

In order to properly support key design and operational decisions, it is necessary that design and operational alternatives not analyzed only with respect to their impact on the mission's technical and programmatic objectives, but also with respect to their impact on these high-level safety objectives[3].

The existing NASA decision-making process can be depicted as shown in Figure 1.

Figure 1: Traditional decision-making process

The decision options (alternatives) may refer to design or operational options. Each option is subjected to traditional engineering analysis. This means that the option is evaluated against relevant NASA requirements. The analysis is mostly deterministic and uncertainties, which remain unquantified, are managed using traditional methods such as safety factors.

The results of the engineering analysis are subjected to a deliberative process in which their validity and insights gained are discussed and a decision is made based on the overall judgment of the decision makers. It is important to note that the decision is the result of a combination of analysis and deliberation.

We now have the technology of quantitative risk assessment (QRA), which allows us to view the system as an integrated whole and to develop accident scenarios along with their frequencies. The role in decision making of this rigorous approach to safety risk is depicted in Figure 2.

[1] NASA defines safety broadly as "freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment."

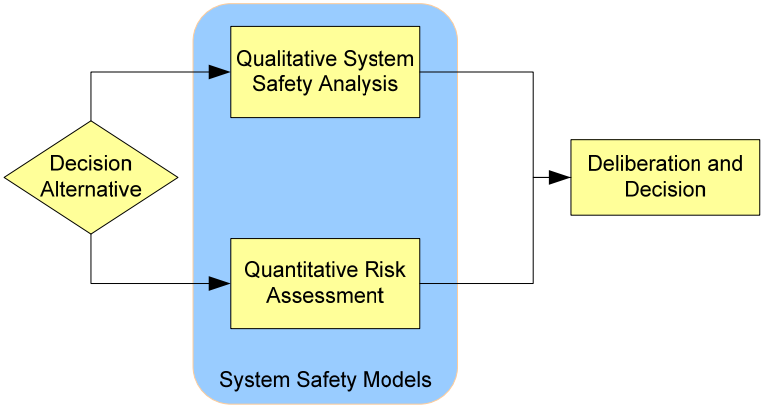

Figure 2: The Role of System Safety Models in Decision making

Figure 2 shows clearly that QRA supplements the results of traditional analyses and does not replace them. The deliberation that takes place before the decision is made utilizes the insights and results from both the traditional "deterministic" analyses and those from the risk assessment. Possible conflicts between these results are resolved during the deliberation. Even though we emphasize the deliberation after the various analyses have been completed, it is understood that the stakeholders deliberate throughout the process, including the choice of decision alternatives.

It is evident that the deliberation at the end of the process imposes a heavy burden on the decision makers who must consider subjectively the impact of each decision option on various metrics that represent mission success as well as on metrics that represent safety considerations. It would be desirable to move as much of this burden from the deliberation to the analysis. We do this by introducing decision theory and modifying Figure 2 as shown in Figure 3.

Conceptually, the analytical-deliberative decision making process consists of three major steps as shown in the circular flow diagram in Figure 3. The three steps are (1) Formulation and selection of decision alternatives, (2) Analysis and ranking of Decision Alternatives and (3) Selection of the best decision alternative. The circular flow indicates that these steps are linked and are supported by the deliberation as shown in Figure 3.

A brief discussion of the steps shown in Figure 3 follows.

1. *Formulation and Selection of Decision Alternatives*: In this step the decision alternatives are generated by quantitative and qualitative analyses, past experience, as well as engineering judgment. Unacceptable alternatives are removed after deliberation and based on criteria such as Violation of flight rules (unless the decision problem is to change the flight rules); Violation of safety standards (unless the decision problem is to change the standards) and Other requirements.
2. *Analysis and Ranking of Decision Alternatives* -- In this step, the screened alternatives are ranked using Multi-attribute Utility Theory (MAUT) supported by quantitative models such as quantitative risk assessment (QRA), cost, and schedule. We will elaborate on this step further later.
3. *Actual Decision making* -- The final decision can be made only after a deliberation takes place (that is, we are describing a risk-*informed* rather than risk-*based* process). Deliberation is necessary because there may be aspects of the particular decision that cannot be considered in a formal way. For example, since MAUT only ranks decision alternatives, we may want to ensure that the chosen alternative complies with safety goals, if any. As usual, deliberation can be formal or informal.

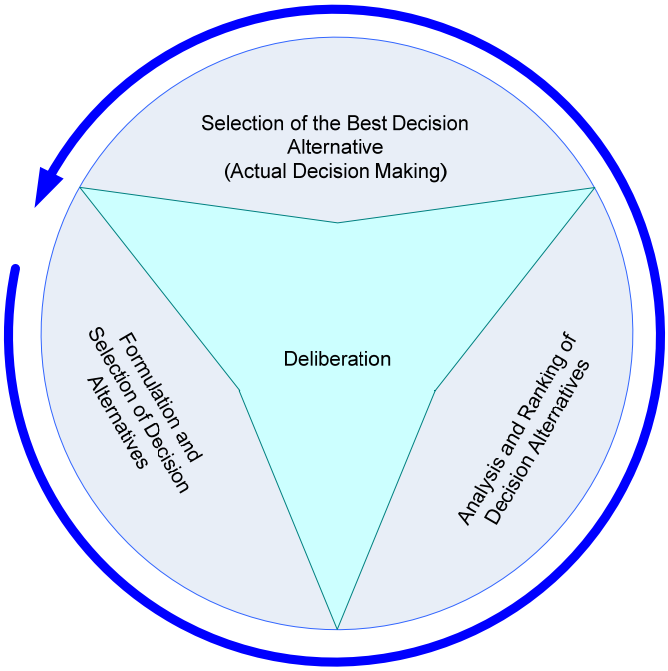

Figure 3: Expanded Analytical-Deliberative Decision-making Process

We recognize that the deliberation may lead to the conclusion that none of the original alternatives is acceptable. The insights gained from Step 2 may lead to the formulation of additional decision alternatives, in which case we go back to Step 1 as indicated by the feedback loop.

If the deliberation concludes that the original decision alternatives were satisfactory, then a decision is made. The top options from Step 1 are evaluated and one of them is selected.

We now return to Step 2, in which decision theory and various assessment models are utilized. Figure 4 depicts the process embedded in this step.

The top tier of this tree is "Mission Success." The idea is to evaluate the impact on this ultimate objective of each decision alternative listed in the diamond at the bottom of the figure. Since "Mission Success" is very general, a hierarchical approach is employed develop quantitative metrics that will measure the achievement of this top-level objective. The next tier in the tree lists the general objective categories that constitute mission success, i.e., "ensure meeting technical objectives," "ensure affordability," "ensure safety," and "ensure stakeholder support. At the next tier, these categories are elaborated upon further by listing a number of objectives. Thus, the category "ensure safety" becomes the four objectives: "protecting public health," "protecting workforce health," "protecting environment," and "protecting mission and public assets." Finally, the next tier of the tree, labeled "potential adverse consequences," shows quantitative metrics for each objective. For example, two metrics for the objective "protecting environment" are: "earth contamination" and "planetary contamination." These metrics, also called Performance Measures (PMs), allow quantitative assessment of the impact of each decision alternative on the objectives. This hierarchical, tree-like structure shows the objectives that the decision maker values in making the decision. It provides a convenient structure for:

- Identification of safety PMs (measures of safety adverse consequences) and other technical and programmatic PMs in the context of the program's high-level objectives
- Formulating risk tradeoff studies.

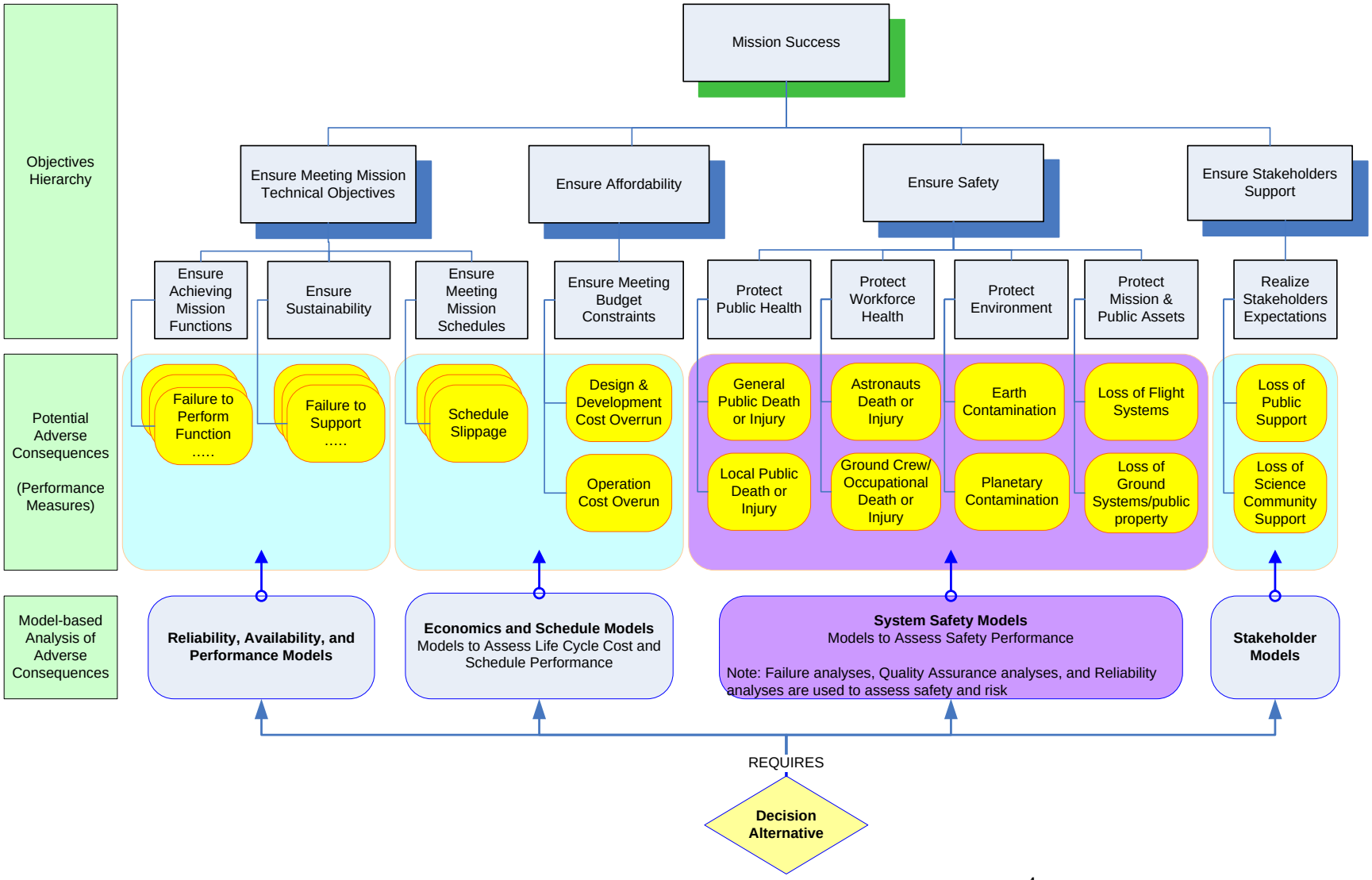

Figure 4: The Role of Various Analyses for Ranking of Decision Alternatives[4]

- Capturing of decision-maker's preferences.
- Ranking of decision alternatives according to their desirability [5] (based on consideration of PMs and preferences.)
- Deliberation that is required as part of the decision-making process.

To develop a more quantitative approach, we note that the PMs (adverse consequences), in general, are not valued equally by the decision maker. This leads to the assignment of weights w_i to the PMs. These weights represent the decision maker's judgments and values. They can be assigned directly or, preferably, using structured methods such as the Analytic Hierarchy Process (AHP). These weights must be normalized to unity, i.e.,

$$\sum_{1}^{N_{PM}} w_i = 1 \qquad \text{Equation (1)}$$

where N_{PM} is the number of performance measures.

The final issue that remains is how we can evaluate quantitatively the impact of each decision alternative on the PMs. Some of them, such as "astronaut death or injury" have natural scales, i.e., the number of such deaths or injuries. Others, such as those referring to mission functions, may not have such natural scales. Finally, these scales are fundamentally different. Even if we assess the number of public deaths and the degree of contamination of the earth and planets, we have the problem of combining such assessments into one scalar number that will allow us to rank the decision alternatives according to their total impact. We solve this problem by introducing dimensionless scales that represent the value to the decision maker of various levels of impact. We call these "disutilities."

An example involving cast is shown in Table 1. The potential costs are placed in four categories. Each category is assigned a disutility value that reflects the decision makers attitude. In this example, the disutility scale is linear (from 0 to 1.0), although it does not have to be so.

Table 1: An Example of the Disutilities for the Performance Measure "Cost Overrun"

Cost Overrun	**Disutility ($\bar{u}$)**
In excess of $10M	1.00
Between $5M and $10M	0.75
Between $1M and $5M	0.50
Between $0.5M and $1M	0.25

The impact of each decision option on each PM is assessed (see Figure 4) in terms of the corresponding disutility. For example, a decision alternative may lead to a cost of $6M, in which case the disutility for this PM would be 0.75. If there is uncertainty involved, we will calculate the average disutility. For example, the decision alternative may lead to a cost overrun of $6M with probability p and to a cost overrun of $0.80M with probability (1-p). Then $\bar{u}$, the average cost disutility for this decision alternative would be 0.75p + 0.25(1-p).

By calculating the expected disutilities for each decision alternative j, we can define a scalar quantity that represents the overall average disutility of that alternative as follows:

$$\overline{PI}_j = \sum_{i=1}^{N_{PM}} w_i \overline{u_{ij}} \qquad \text{Equation (2)}$$

where

$\overline{PI}_j$ is the average Performance Index associated with decision alternative j
w_i is the weight of the ith PM, and
$\overline{u_{ij}}$ is the average disutility of decision alternative j with respect to PM_i

The Performance Indices can be used to rank the decision alternatives according to how undesirable they are to the decision maker. From the definition of Equation (2), we conclude that the inequality $\overline{PI}_j > \overline{PI}_k$ means that the decision maker assesses that decision alternative j is of higher disutility, i.e., is less desirable, than decision alternative k.

CONCLUDING REMARKS

Generally speaking, it is virtually impossible to improve something effectively unless one can measure it. The same concept applies to safety. In occupational safety, safety enhancement can be measured by the reduction in the rate of mishaps or accidents. For complex systems, it is neither practical nor cost-effective to keep trying safety measures until the most successful ones are found. For new designs, this approach in not only cost ineffective; it is impossible because of the inability to assess safety beneficial design changes on the basis of engineering judgment or on failure modes and effects analyses coupled with hazards analyses. Systematic and cost-effective safety improvement begins with the definition of safety performance measures, safety-related variables that can be evaluated and monitored.

An important step in a complex decision process is the deliberation among stakeholders. Stakeholders are individuals or entities that have a stake (something to gain or to lose) from the outcome of the decision process. For a complex system at NASA this may include, as appropriate, within NASA, the program/project manager, NASA management, project/program personnel, NASA astronauts, and NASA workforce. Outside NASA, stakeholders may include the affected public as well as political and other important community figures.

The deliberation process is a crucial part of the decision-making process since it evaluates results and makes explicit all the pros and cons associated with the decision alternatives. The proposed framework provides both qualitative and quantitative information that will prove useful to the deliberation among the stakeholders.

REFERENCES

[1] Taylor, C., et. al., "Paradigm Shift in Design for NASA's Space Exploration Initiative: Results from MIT's Spring 2004 Study," Massachusetts Institute of Technology, Cambridge MA 02139.

[2] "Understanding Risk: Informing Decisions in a Democratic Society," National Academy Press, Washington, DC, 1996.

[3] NASA Draft General Safety Program Requirements, NPR 8715.3, 2006.

[4] Dezfuli, H., "Role of System Safety in Risk-informed Decision Making," The NASA Risk Management Conference 2005, Orlando, Florida, December 7, 2005.

[5] Pagani, L., Smith, C., and Apostolakis, G., "Making Decisions for Incident Management in Nuclear Power Plants Using Probabilistic Safety Assessment," Risk, Decision and Policy, 9:271-295, 2004.