A PARADIGM SHIFT IN SYSTEM SAFETY PROCESSES AT NASA

Homayoon Dezfuli[(1)] and Michael Stamatelatos[(2)]

NASA Headquarters, Office of Safety and Mission Assurance
[(1)] Email: hdezfuli@nasa.gov
[(2)] Email: michael.g.stamatelatos@nasa.gov

(Presented at the 7th National Space Systems Engineering & Risk Management Symposium, Los Agnels, CA, Feb. 2008)

Abstract

Recent years have seen significant advances in the state of risk analysis at NASA. These advances are reflected both in the state of practice of risk analysis within programs and projects, and in the status of several NASA requirements and procedural documents. However, although risk analysis are intended to support system safety processes, the practice of system safety modeling within NASA has not evolved comparably to the practice of risk analysis. Partly in response to this disparity and with the objective of better integrating system safety activities with system engineering and risk management processes, NASA has significantly changed the requirements for system safety. The new requirements are designed to ensure that system safety technical processes have the following characteristics:

- Hazard analysis uses accident scenario modeling technique.
- Safety-related performance measures (PMs) are formulated to support risk trade studies.
- Probabilistic Risk Analysis (PRA) techniques are used to quantify PMs.
- Uncertainties are evaluated and characterized.
- Hazard analysis and PRA models are collectively constitute system safety models to support decision processes.

In this way, the ongoing implementation of system safety activities supports the attainment of a holistic and risk-informed decision-making environment within NASA. This paper will provide an overview of system safety process changes that are being implemented at NASA.

Background

Until 2006, the conduct of system safety practice at NASA was governed by a set of requirements stipulated mainly in Chapter 3 of Reference [1.] These requirements called for identification of hazards and assessments of associated risks by considering their probability of occurrence and severity of consequences. For managing safety-related risks, the requirements advocated the risk reduction principle of "as low as reasonably achievable" (ARARA) and the application of the Continuous Risk Management (CRM) process and risk matrices. A brief description of these tools is provided below.

The CRM Process

As illustrated in Figure 1, CRM [2] is an iterative and adaptive process consisting of the following steps:

Identify –*Identify* risk by identifying hazards having adverse consequences on safety.

Analyze – Estimate the likelihood and consequence components of the risk through *Analysis* and prioritize risks.

Plan – *Plan* what should be done to eliminate or reduce the risks, and provide the planning to the appropriate levels of program management for a decision to eliminate, further reduce, or accept the risk.

Track – *Track* program performance compared to the plan (i.e., track the results of the corrective actions and continue to verify and validate their effectiveness.)

Control – Given an emergent risk issue, execute the appropriate *Control* action, and verify its effectiveness.

Communicate and Document – This is an element of each of the previous steps. Focus on understanding and communicating all risk information throughout each program phase.

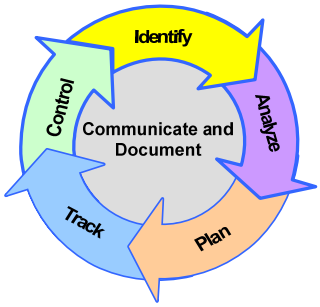

Figure 1: The CRM Process

Risk Matrices

Reference [1] introduces the concept of risk matrices and Risk Assessment Codes (RACs) to categorize and communicate risk issues. Figure 2 shows the setup of probability and consequence definitions for a "4x5" matrix [1.] In this setup, the probability range is subdivided into five "probability levels." Similarly, the consequence range is subdivided into four severity levels. By discretizing probability and consequence severity, risk tolerability regimes are then defined. Figure 2 shows five regimes. The RAC is a numerical expression of comparative risk determined by an evaluation of both the potential severity of a condition and the probability of its occurrence. RAC`s are assigned a number from 1 to 7. According to Reference 1, the RAC number is intended to serve as a means to prioritize corrective actions, e.g., RAC 1 is unacceptable and mitigation actions must be taken immediately or operations terminated, RAC 2`s must be addressed before RAC 3`s, etc.

Description of Consequence Severity Levels		
I	Catastrophic	A condition that may cause death or permanently disabling injury, facility destruction on the ground, or loss of crew, major systems, or vehicle during the mission.
II	Critical	A condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, equipment, or flight hardware.
III	Moderate	A condition that may cause minor injury or occupational illness, or minor property damage to facilities, systems, equipment, or flight hardware.
IV	Negligible	A condition that could cause the need for minor first aid treatment. A condition that subjects facilities or flight hardware to more than normal wear and tear.

Description of Probability Levels	
A	Likely to occur immediately
B	Probably will occur in time
C	May occur in time
D	Unlikely to occur
E	Improbable to occur

Severity Level	A	B	C	D	E
I	1	1	2	3	4
II	1	2	3	4	5
III	2	3	4	5	6
IV	3	4	5	6	7

Probability Estimate

Figure 2: A Typical Risk Matrix

Motivations for Making Changes to the System Safety Practice

In January 2004, President 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.

Against this backdrop, the Office of Safety and Mission Assurance conducted an internal review of representative hazard and risk analysis for several NASA programs to determine whether the state-of-practice of system safety is adequate to support transition to and implementation of the

Exploration Program. This review, which was conducted in 2005, revealed semantic and methodological problems in the practice of system safety and a lack of rigor in safety model development activities. The review found the system safety practice at NASA had remained grounded in the modeling approach of the 1970s. Despite the fact that NASA had made significant progress in developing Probabilistic Risk Assessment models for its missions [3, 4, 5], these modeling activities have not been integrated with system safety modeling efforts. Key review findings include:

- The key term *hazard* is defined and understood differently by various system safety analysts. Sometimes the term is used to characterize a single undesired event (e.g., a failure), a hazardous condition (e.g., a pressurized tank), an undesired consequence of some events (e.g., loss of a critical function), or a cause of a failure event (e.g., a manufacturing defect). The variability in the definition of hazard not only has introduced inconsistencies in the characterization and reporting of hazards, it also has promoted an *ad hoc* approach to the analysis of hazards and their risks.
- There is a tendency to use risk assessment in a confirmatory way, when a design is already on the table, rather than as analysis-in-the-loop (so to speak). As a result, system safety activities have significant limitations in influencing early design decisions.
- The risk assessment and management approach is not based on an integrated risk perspective. The approach places emphasis on identification of individual "risks" and on accountability for action items associated with particular "risks." Without modeling the *overall* risk, there is no analytical basis for using system safety models in the risk tradeoff studies.
- Additionally, for the following reasons, the use of risk matrices in decision-making was found to be problematic in the following areas [6]:
    - If the risk matrix is viewed as the deliverable, rather than the underlying risk analysis, there is a temptation to substitute subjective completion of the form for careful risk analysis.
    - The linguistic definitions for probability levels, although referring to an inherently probabilistic concept are often subject to different interpretations.
    - The matrix deals with individual risks, not with aggregate risks (i.e., *overall* risk). This supports assignment of specific "track" and "control" action items to individuals, but does not furnish proper perspective to decision-makers.
    - Consequence types are often not discriminated. Inclusive consequence severity levels (e.g., human safety and asset safety together) short-circuit the ability to perform risk trade studies.
    - Uncertainties are not acknowledged and characterized. A risk is assumed to exist within one likelihood range and consequence range, both of which are assumed to be known.
    - The desire to balance likelihood against consequence drives safety decisions. A rare but severe risk contributor may warrant a response different from that warranted by a frequent, less severe contributor, even though both have the same expected consequences.

These findings prompted NASA to institute major changes in the system safety practice. The new system safety requirements are stipulated in Chapter 2 of NPR 8715.3B: NASA General Safety Program Requirements [7]. These requirements advocate a proactive, analytic-

deliberative, risk-informed approach to safety to enable the integration of system safety activities with system engineering and risk management processes. The highlights of the system safety modelling framework and associated key safety terms and concepts that govern the new requirements are provided below. From here on the term "8715.3B" refers to Chapter 2 of NASA NPR 8715.3 [7.]

New NASA System Safety Framework

Key System Safety-related Terms and Concepts

To achieve an adequate level of common understanding and interpretation of new requirements, 8715.3B provides *operational* definitions for key safety-related terms and concepts that are used in the language of the requirements. Examples of key terms are:

System -- one integrated entity that performs a specified function and includes hardware, software, human elements, and the environment within which the system operates.

Hazard -- a state or a set of conditions[1], internal or external to a system, that has the potential to cause harm. Generally, one or more additional conditions need to exist or additional events need to occur in conjunction with the existence of the hazard in order for an accident[2] or mishap[3] with consequences adverse to safety[4] to result.

Safety (in the context of risk-informed decision making) -- an overall mission and program condition that provides sufficient assurance that accidents will not result from the mission execution or program implementation, or, if they occur, their consequences will be mitigated. This assurance is established by means of the satisfaction of a combination of deterministic requirements and risk criteria.

Risk (in the context of risk-informed decision making) -- a set of triplets [8]: *accident scenarios* involving hazards; associated *frequencies*; and associated adverse *consequences*. Each triplet is a statement about the likelihood of realizing a postulated accident scenario with the type and magnitude of potential adverse consequences. The "triplet" concept of risk is operationally useful because it makes clear that in order to define, assess and manage risk it is necessary to produce three components of risk: undesired scenarios, their probabilities, and their consequences. The expression for risk as a set of triplets is:

$$Risk \equiv \{< accident\ scenario,\ frequency, consequence >\}$$

Uncertainties (in the context of risk assessment) -- 8715.3B defines two types of uncertainty:

[1] 8715.3 B uses the term "state" or "condition" in a broad sense to include any intrinsic property and characteristic of the material, system, or operation that could, in certain circumstances, lead to an adverse consequence.
[2] 8715.3B uses the term "accident" in the context of risk assessment methodology because of its wide acceptance in the practice of this methodology.
[3] The term "mishap" is NASA's preferred generalization of an accident.
[4] NASA uses the term "safety" broadly to include human safety (public and workforce), environmental safety, and asset safety.

- Epistemic uncertainty: that uncertainty associated with incompleteness in the risk analyst's (or analysts') state of knowledge. There are two categories of epistemic uncertainty: parameter uncertainty[5] and model uncertainty.[6]
- Aleatory uncertainty (variability): that uncertainty associated with variation or stochastic behavior in physical properties or physical characteristics of the system being modeled[7].

The expanded representation of the risk triplets that accounts for epistemic uncertainties is shown below. It is also shown notionally in Figure 3.

$$Risk \equiv \{< accident\ scenario,\ frequency\ and\ its\ uncertainty, consequence\ and\ its\ uncertainty >\}$$

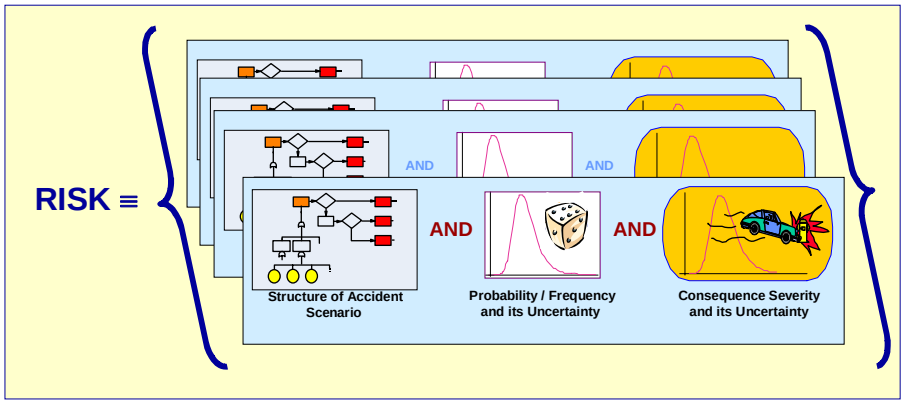

Figure 3: Expressing Risk as a Set of Triplets

Performance Measure (PM) -- a quantifiable metric used to characterize performance of the decision alternatives with respect to a particular fundamental objective.

Safety PM -- a quantifiable metric used to characterize performance of the decision alternatives with respect to a particular safety objective. Safety PMs can be defined in terms of the probability of a consequence type of a specific magnitude (e.g., probability of general public deaths or injuries) or the expected magnitude of a consequence type (e.g., the number of public deaths or injuries). Probability of Loss of Mission P(LOM) and Loss of Crew P(LOC) are two particularly important PMs for manned apace missions. Because an actuarial basis does not exist for predicting these probabilities, modelling is needed to quantify them.

Risk-informed Decision Making -- a decision process that accepts modern risk analysis results as one input. In this process, decisions are informed by a range of inputs including performance measures (e.g., integrated risk metrics).

Probabilistic Risk Assessment (PRA) -- a scenario-based risk assessment technique that quantifies the likelihoods of various possible undesired scenarios and their consequences, as well

[5] This is uncertainty in the value of a parameter of a risk model, conditional on the mathematical form of that model.
[6] This is uncertainty in whether the risk model adequately represents the behavior of the system being analyzed.
[7] Aleatory uncertainty is manifested, for example, in the variability of the time at which a failure will occur. Another example is the variations in material properties resulting from variability in manufacturing processes.

as the uncertainties in the likelihoods and consequences [9.] PRA can be applied to quantify Performance Measures.

Scenario-based Modeling of Hazards

8715.3B advocates scenario-based analysis hazards as a modeling framework. In the scenario-based modeling approach, illustrated in Figure 4 an initiating event is identified for each hazard along with the necessary enabling events that result in undesired consequences. The enabling events often involve the failure of or lack of protective barriers or safety subsystems (controls). The resulting accident scenario is the sequence of events that is comprised of the initiating event and enabling events that lead to the adverse consequences. Scenarios can be classified according to the type and severity of the consequences (i.e., according to their end states). In the scenario-based modeling framework, a linkage between hazards and adverse consequences of interest is established. 8715.3B emphasizes the need for the modeling of the characteristics of this linkage (i.e., how the presence of a hazard is linked with the occurrence of other events (e.g., hardware failures, software error, human errors, or phenomenological events) leading to the formation of a mishap.) As part of this modeling, the following items need to be addressed:

- How a hazard enables or contributes to the causation of initiating events[8].
- How a hazard enables or contributes to the loss of the system's ability to compensate for (or respond to) initiating events.
- How a hazard enables or contributes to the loss of system's ability to limit the severity of the consequences.

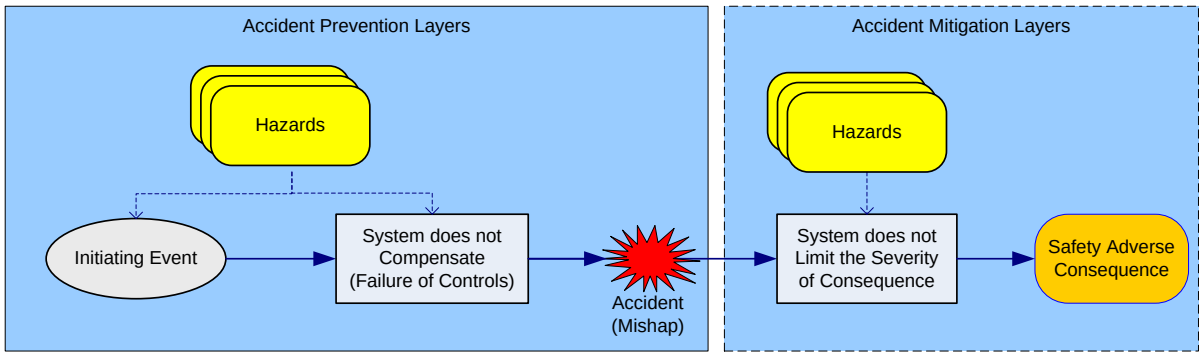

Figure 4: Scenario-based Modeling of Hazards

Analyzing hazards, in relation to the above enabling conditions, supports risk management activities that involve prevention (reduction of frequency) of adverse accident scenarios (ones with undesired consequences), and the promotion of favorable scenarios. 8715.3B identifies the following risk management strategies:

- Elimination of an accident scenario (e.g., hazard or initiating event elimination.)

[8] For example, the presence of fuel vapor in the crew module of a spacecraft is an enabling condition that may result in a fire (an initiating event) which is the starting point of an accident scenario. The cause of the fire is a spark or other igniters.

- Reduction of the likelihood of an accident scenario through design and operational changes (hazard control.)
- Reduction of the severity of the accident consequence (hazard mitigation.)
- Improvement of the state-of-knowledge regarding key uncertainties that drive the risk associated with a hazard (uncertainty reduction to support implementation of the above strategies.)

System Safety Domain

According to 8715.3B, the system safety domain is fundamentally a multidisciplinary system engineering function that should be active continuously throughout the lifecycle of the Program in maintaining and conducting safety analyses of hazards to support decisions. The system safety domain is inclusive of the Hazard Analysis and Probabilistic Risk Assessment Domains. The Hazard Analysis and Probabilistic Risk Assessment Domains are the subsets of the systems safety models which are to be used to support decisions.

The Role of System Safety Models in Decision Making

System safety as defined by 8715.3B is inherently risk-informed [10.] As shown in Figure 5, probabilistic risk assessment complements qualitative hazard analysis and does not replace it. The deliberation that takes place before a decision is made utilizes the insights and results of both the qualitative analyses and the probabilistic risk assessment. Possible conflicts between these results maybe resolved during the deliberation. This process of decision making is therefore risk-*informed*, not risk-*based*. It is important to note that the decision is the result of a combination of analysis and deliberation. 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 PMs that represent technical and programmatic objectives as well as on metrics that represent safety considerations. Consequently, it would be desirable to move as much of this burden as possible from the deliberation to the analysis, and to begin such analysis as early as possible during the design.

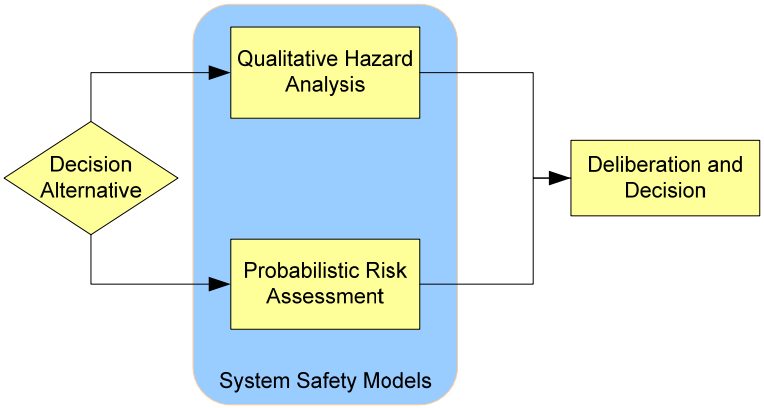

Figure 5: The Role of System Safety Models in Decision Making

To facilitate the deliberation, 8715.3B provides the hierarchical tree of Figure 6, which shows how system safety models along with other models are utilized to assess the impact of a decision alternative on safety and other objectives.

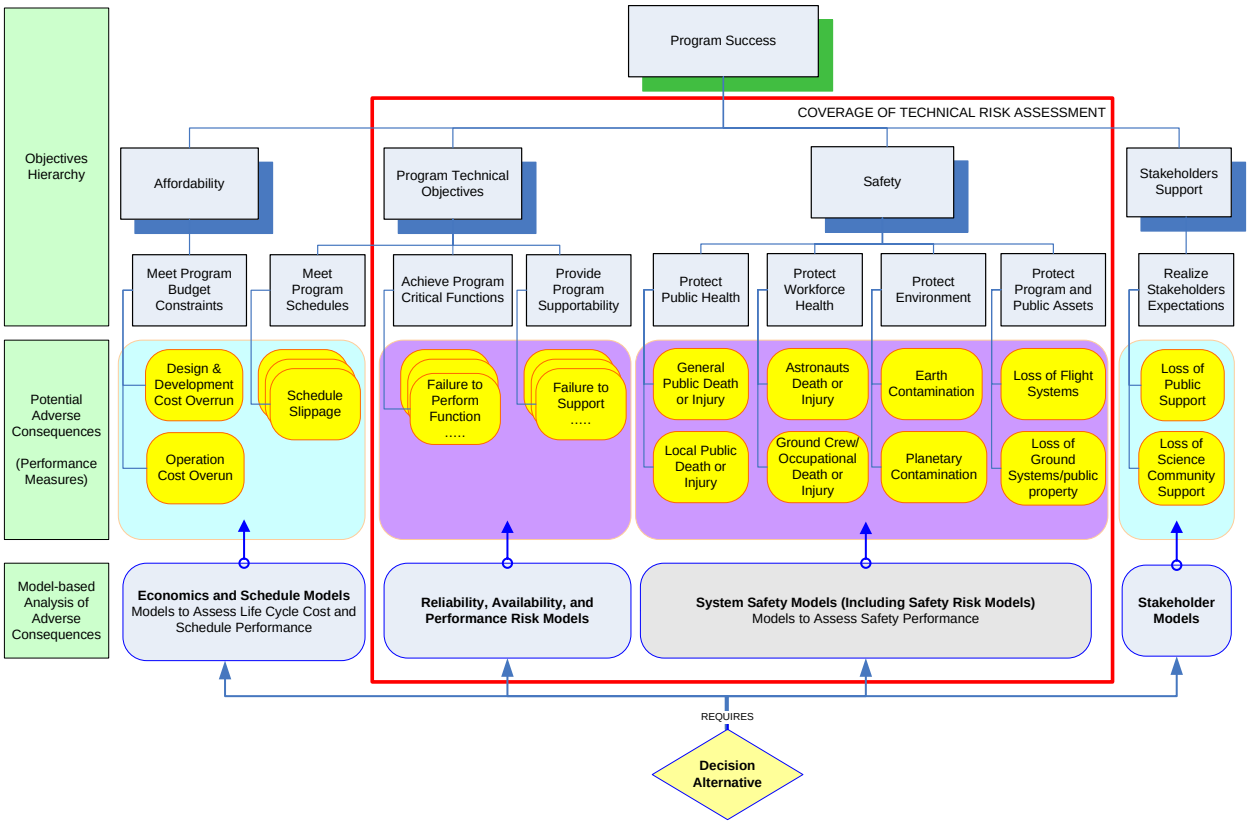

Figure 6: The Role of System Safety Models and Other Models in Risk-informed Decision Making

The top tier of this tree is “Program Success.” The idea is to evaluate the impact on this ultimate objective of each decision alternative shown as the diamond at the bottom of the figure. Since “Program Success” is very general, a hierarchical approach is employed to 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 program success, i.e., “Affordability,” “meet program technical objectives,” ”Safety,” and “Stakeholder support.” At the next tier, these categories are elaborated upon further by listing a number of objectives. Thus, the category “Safety” becomes the four objectives: “Protect public health,” “Protect workforce health,” “Protect environment,” and “Protect assets.” 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:

- Identifying safety PMs and other technical and programmatic PMs in the context of the program's high-level objectives.
- Formulating risk tradeoff studies.
- Capturing decision maker's preferences.
- Ranking decision alternatives according to their desirability (based on consideration of PMs and preferences.)
- Deliberating that is required as part of the decision-making process.

Scope of System Safety Activities

8715.3B advocates a graded approach to system safety. That is, the level of formality and rigor that is involved in implementing the system-safety processes should match project potential consequences, life cycle phase, life cycle cost, and strategic importance. To assist in determining the scope of activities for safety evaluations as a function of project characteristics 8715.3B provides two tables. The categorization scheme identified in Table 1 is used to determine a project priority. This table is similar to Table 1 from NPR 8705.5 [11.]

Table 1: Criteria for Determining the Project Priority

<table>
<tr><th>CONSEQUENCE CATEGORY</th><th colspan="2">CRITERIA / SPECIFICS</th><th>Project Priority Ranking</th></tr>
<tr><td rowspan="4">Human Safety and Health</td><td rowspan="3">Public Safety</td><td>Planetary Protection Program Requirement</td><td rowspan="7">I</td></tr>
<tr><td>White House Approval (PD/NSC-25)</td></tr>
<tr><td>Space Missions with Flight Termination Systems</td></tr>
<tr><td colspan="2">Human Space Flight</td></tr>
<tr><td rowspan="4">Mission Success (for non-human rated missions)</td><td colspan="2">High Strategic Importance Projects</td></tr>
<tr><td colspan="2">High Schedule</td></tr>
<tr><td colspan="2">High Cost (See NPR 7120.5[12])</td></tr>
<tr><td colspan="2">Medium Cost (See NPR 7120.5)</td><td>II</td></tr>
<tr><td colspan="2">Low Cost (See NPR 7120.5)</td><td>III</td></tr>
</table>

Once the project priority is determined, the scope of system safety modeling is determined using Table 2. Projects identified as "Priority I" ranking from Table 1 are generally the most visible and complex of NASA's product lines. Because of this, the system safety technical processes for Priority I projects must include probabilistic risk assessment as specified in NPR 8705.5 [11.] For Priority II or III projects, Table 2 provides latitude to adjust the scope of system safety modeling. This graded approach to the application of system safety modeling also operates on

another dimension. That is, the level of rigor and detail associated with system safety modeling activities must be commensurate with the availability of design and operational information. The two-dimensional nature of the graded approach is intended to ensure that allocation of resources to system safety technical activities considers the visibility and complexity of the project and to ensure that the level of rigor associated with system safety models follows the level of maturity of the system design.

Table 2: Graded Approach to System Safety Modeling

Priority Ranking	Scope (The level of rigor and details are commensurate with the level of design maturity)
I	Probabilistic risk assessment (per NPR 8705.5) supported by qualitative system safety analysis
II	Qualitative system safety analysis supplemented by probabilistic risk assessment where appropriate
III	Qualitative system safety analysis

Core Requirements for System Safety Processes

8715.3B groups the requirements in relation to technical processes that represent system safety activities. Conceptually, these technical processes are shown in the circular flow diagram in Figure 7. They are (1) system safety modeling, (2) life cycle applications of models for risk-informed decisions and, (3) monitoring safety performance. The circular flow indicates that these technical processes are linked and are performed throughout the project life cycle. According to 8715.3B, a System Safety Technical Plan is required to guide the technical processes and establish roles and responsibilities. This plan is established early in the formulation phase of each project and is updated throughout the project life cycle.

Summary

The system safety changes being implemented at NASA are designed to integrate system safety modeling activities with system engineering processes in an analytical framework. The expected benefits of these changes are to improve the analytical basis for safety management decisions and safety risk trade studies. These changes would allow system safety models be used for assessing safety impact of design decisions, prioritizing safety issues, prioritizing research to reduce uncertainty, and risk management. NASA is in the process of developing a procedural handbook to facilitate the implementation of the new system safety requirements.

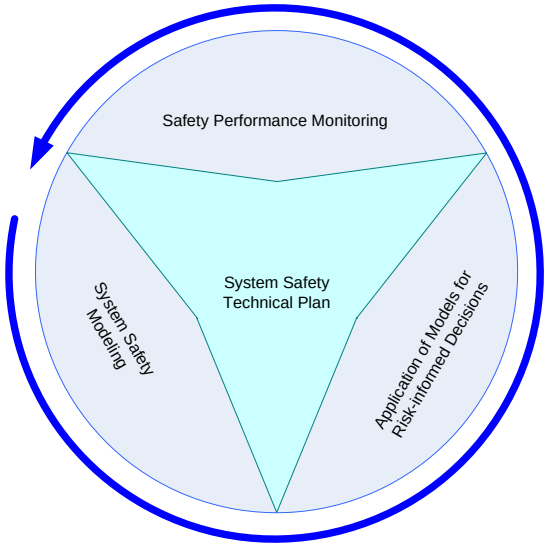

Figure 7: The System Safety Technical Processes

References

1 NASA NPR 8715.3, “NASA Safety Manual w/Change 2," March 31, 2004, Expiration Date: January 24, 2006.

2 NASA NPR 8000.4, “Risk Management Procedural Requirements,” April 25, 2002, Expiration Date: April 25, 2008.

3 Space Shuttle Probabilistic Risk Assessment, Volume II, Rev. 1: Model Integration Report, Johnson Space Flight Center, January 2005.

4 Probabilistic Risk Assessment of the International Space Station: Phase II – Stage 7A Configuration, Volume II – Data Package, Futron Corporation, 2000.

5 Pluto/New Horizons Interagency Nuclear Safety Review Panel Safety Evaluation Report of August 2005.

6 H. Dezfuli, et al., “Managing Risk Within A Decision Analysis Framework,” Second IAASS Conference, Chicago, May 14-16, 2007.

7 NASA NPR 8715.3, “NASA General Safety Program Requirements,” Revision Level: B, Effective Date: April 4, 2007, Expiration Date: April 4, 2012.

8 S. Kaplan and B.J. Garrick, “On the Quantitative Definition of Risk,” Risk Analysis, 1, 11-27, 1981.

9 M.G. Stamatelatos., et al., “Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners,” Version 1.1, Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC, August 2002.

10 M.G. Stamatelatos, et al., “A Proposed Risk-Informed Decision-Making Framework for NASA,” Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management, New Orleans, LA, May 14-18, 2006.

11 NASA NPR 8705.5, “Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects, Effective Date: July 12, 2004, Expiration Date: July 12, 2009.

12 NASA NPR 7120.5, “NASA Program and Project Management Processes and Requirements,” Revision Level: D, Effective Date: 03/06/2007, Expiration Date: 03/06/2012.