Evolution of Risk Management at NASA and the Philosophy of Risk Acceptance

Presented to
The Institute of Medicine's Committee on Ethics Principles and Guidelines for Health Standards for Long Duration and Exploration Spaceflights

July 25, 2013
Washington, DC

Homayoon Dezfuli, Ph.D.
NASA Technical Fellow for System Safety
Office of Safety and Mission Assurance
NASA Headquarters
Outline

• Evolution of Risk Management (RM) at NASA
  – RM = CRM ===> RM = RIDM + CRM

• Risk Tolerance
  – Acceptance of performance uncertainty

• Accounting for Unknown and Underappreciated Risks
  – Because of completeness uncertainty, prudent risk management will incorporate margin into the safety thresholds to which the project is being managed, especially early in its life cycle
  – These margins may be “burned down” as the development matures

• NASA’s Process for Handling Risk Acceptance through Deviations and Waivers

• Introduction of Opportunity Management into Decisions about Deviations and Waivers
  – Balancing safety against other performance areas needs to be established at the Agency level
  – These guidelines then drive implementation of the “As Safe as Reasonably Practical” requirement
Historical Perspective on NASA Risk Management (RM)

• No “formal,” systematic RM process in NASA until mid-1990s.

• Then came the “Continuous Risk Management” or “CRM” process:
  – Originally developed by Carnegie Mellon University for the Department of Defense
  – Brought increased attention to risk over the next decade
  – Stressed management of individual risk issues during implementation
  – Risks were identified via brainstorming
  – Individual risks were analyzed qualitatively and arrayed on a “risk matrix” of severity vs. likelihood
RM Approach After 2008

- In 2008, we took the next step in the evolution of RM by revising our Risk Management Directive, NPR 8000.4
- NPR 8000.4A evolved NASA’s risk management to entail two complementary processes:
  - **Risk-Informed Decision Making (RIDM)**
    - To inform systems engineering decisions through better use of risk and uncertainty information in selecting among alternatives and establishing baseline performance requirements
  - **Continuous Risk Management (CRM)**
    - To manage aggregate performance risks over the course of the development and implementation phases of the life cycle to assure that requirements related to safety, technical, cost, and schedule are met

\[ RM = \text{RIDM} + \text{CRM} \]
RM Approach After 2008 (Cont.)

• Inclusion of RIDM in RM has the effect of increasing emphasis on analysis and decision-making
  • Development of requirements based on aggregate performance measures such as Probability of Loss of Crew (P(LOC)), Payload Capability (Kg), Time to Completion (Days), Total Program Cost ($)
  • Risk measured in terms of confidence in being able to meet each performance requirement
  • Confidence measured in terms of the aggregation of uncertainties in the quantification of the performance measures
  • Uncertainties defined down to the level of uncertainties in models used and in the inputs to the models

• CRM was expanded to be a tool for managing aggregate performance risks
  • Evaluation of the effects of individual risks on the aggregate performance measures
  • Determination of corresponding risk drivers
  • Mitigation of risk drivers that most significantly affect the likelihood of not meeting the aggregate performance requirement
Relationship Between RIDM and CRM

- Selection of an alternative (e.g., a design concept) includes specification of baseline performance requirements
- CRM processes manage the risk of not achieving that performance baseline, until the baseline is changed
- Per 8000.4A, each organizational unit’s authority for risk acceptance is spelled out in its Risk Management Plan, with the concurrence of the higher-level unit
Risk Tolerance

• The paradigm for RM = RIDM + CRM introduced the concept of risk tolerance
  – Within NASA’s Risk Management framework, “risk tolerance” (a.k.a. acceptance) is the amount of uncertainty (or lack of confidence) accepted in the argument that the system meets an aggregate performance requirement
  – There is a separate risk tolerance for each aggregate performance requirement
Risk as the Effect of Propagating Uncertainties in the Quantification of Performance Measures

- Uncertainty distributions are obtained for quantities such as input parameters and model results.
- Integrated models for technical performance, safety, cost, and schedule are run using a Monte Carlo process to obtain output uncertainty distributions for key PMs.
- The output distributions provide the basis for determining the risk of not meeting each performance requirement.
- The effect on risk of scenarios that are unknown or underappreciated have to be considered in decision-making, as well, since they are not included in the models (by definition).
Accounting for and Managing Unknown and Underappreciated Risks

- The new paradigm for system safety (NASA/SP-2010-580) has introduced the concept of safety performance margins to be used by decision-makers to compensate for the unavoidable presence of unknown and known but underappreciated (UU) risks
  - Margin is meant to allow for the difference between the mean calculated value of the safety performance measure (e.g., P(LOC)) obtained from model, simulation, and testing, and the true mean value (including effects of UU risks)
  - Safety performance margin (estimated from historical experience) provides a rational basis for deriving verifiable probabilistic safety requirements on known risks

- Known risks are managed by applying controls that are designed to mitigate identified adverse scenarios

- UU risks are managed by controlling the factors that produce them (e.g., design philosophy, organizational and programmatic factors)

- Safety thresholds are developed as a matter of agency policy
- Realistic safety goals, meant to be applied to the mature system, are developed from historical experience
Implementation of Risk Acceptance through Deviations and Waivers

• In implementation, acceptance of a risk that exceeds the DM’s risk tolerance may occur by approving a deviation or waiver request

• The NASA deviation and waiver process is described in NPR 7120.5E: “NASA Space Flight Program and Project Management Requirements”
  • At the program/project level, deviation and waiver approvals are normally decided by the various Technical Authorities

• Corroboration may be required from higher levels of NASA depending upon the importance of the mission and of the core requirement being debated

• For matters involving human safety risk, the actual risk taker(s), e.g., astronauts, need(s) to formally consent to taking the risk and the responsible program, project, or operations manager needs to formally accept the risk

• RIDM and CRM inform the deviation/waiver process
  • RIDM initially informs the process of developing core safety requirements at the beginning of a program/project
  • RIDM and CRM continue to inform decisions about re-baselining existing requirements when deviations or waivers are sought
Introduction of Opportunity Management into Decisions about Deviations and Waivers (Work in Progress)

• To make an informed decision about deviating from or waiving a requirement, the safety risk incurred by not meeting the core requirement has to be weighed against the risk of not capitalizing on an opportunity that would advance a key agency goal
  • For example, a waiver or deviation from the standard for radiation dose may be justified by the importance of the mission if the only way to meet the standard involves an unacceptably high weight and cost penalty
  • Need to establish agency level guidelines for how to determine the balancing point between the safety risk and the worth of the opportunity

• The process of balancing safety risk against the worth of the opportunity is encapsulated within the “As Safe As Reasonably Practicable” (ASARP) philosophy (Refer to NASA/SP-210-580)
  • It is necessary to show that the only ways to further reduce the safety risk incur unacceptable penalties in the ability to achieve a key agency goal
  • Informed consent of those affected is an essential component of ASARP
Design Tradeoffs Involve Weighing Risks against Strategic Opportunities

- Typically, the more the program/project contributes toward achieving the Agency’s strategic goals, the more the Agency might be willing to accept the risk of not meeting technical, safety, cost, and schedule requirements.
- The acceptable tradeoff between risk and opportunity is determined at the Agency level on a specific case-by-case basis and involves the informed consent of the stakeholders.

![Safety Risk Versus Opportunity](image)

- **Risk of Not Meeting P(LOC) Reqmt.**
- **P(LOC)**
- **Degree of Progress**
- **DM’s Risk Tolerance**
- **Proposed Change**

**NOTIONAL**
Acknowledgments

This presentation is partly derived from the following sources:

NASA NPR 8000.4A
NASA/SP-2010-576
NASA/SP-2011-3422
NASA/SP-2010-580
SUPPLEMENTARY CHARTS
Principles of Adequate Safety

- An adequately safe system is one that adheres to the following fundamental safety principles:
  - Meeting minimum tolerable levels of safety (i.e., aggregate risk)
    - Below the minimums the system is considered unsafe
    - Minimums may be applied to any safety performance measure, e.g., P(LOC), P(LOM), P(LOV), \( E_c \), P(environmental contamination)
    - Minimums may evolve from initial thresholds to long-term goals
  - Being as safe as reasonably practicable (ASARP)
    - Decisions affecting safety are risk-informed
    - Safety is prioritized within constraints on operational effectiveness, schedule, and cost