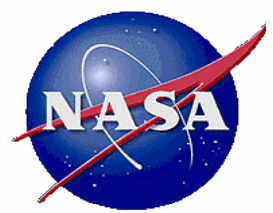


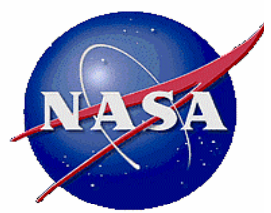
NASA's Risk Management Approach

Workshop on Risk Assessment and Safety Decision Making Under Uncertainty

September 21-22, 2010
Bethesda, Maryland

Homayoon Dezfuli, Ph.D.
NASA Technical Fellow
NASA Headquarters

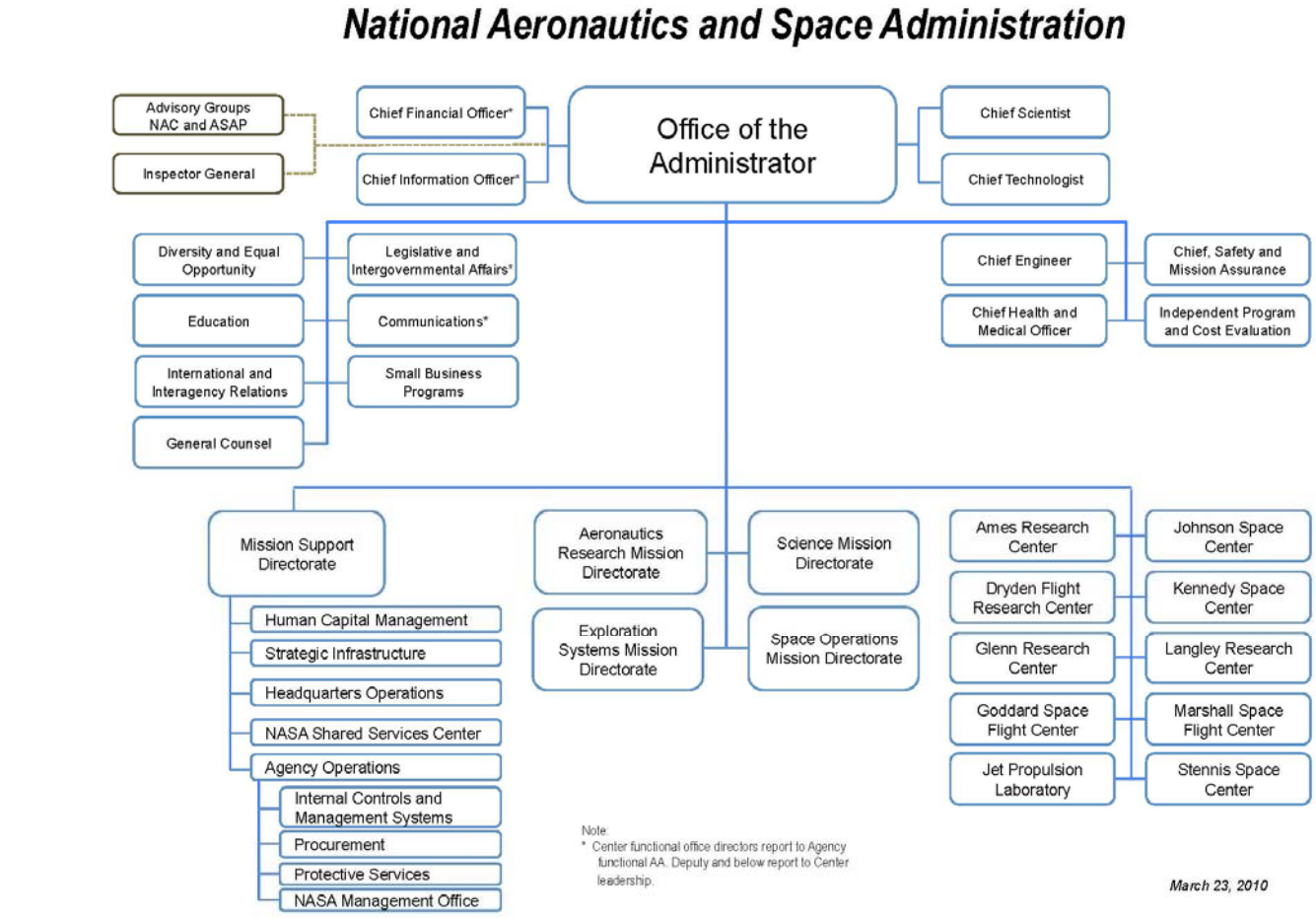
Outline



- NASA Organization
- Evolution of Risk-related Policy and Guidance Documents
- NASA's Risk Management Approach
- Safety Goals and Thresholds for Human Space Flights

NASA Organization Structure

National Aeronautics and Space Administration



www.nasa.gov

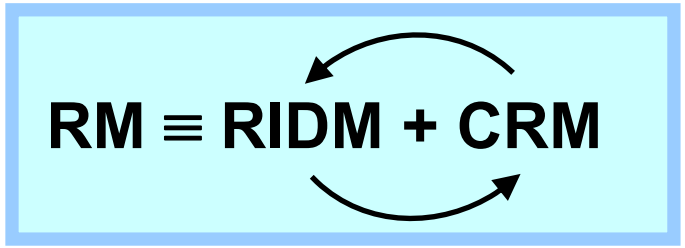
Evolution of Risk-related Policy and Guidance Documents

- 2002 – Issuance of PRA Procedures Guide
- 2004 – Issuance of NPR 8705 "Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects"
- 2006 – Issuance of NPR 7123.1 "Systems Engineering Processes…"
- 2006 – Revision of NPR 8715.3A "NASA General Safety Program Requirements," Rewrite of System Safety Requirements (Chapter 2)
- 2007 – Revision of NPR 7120.5D "Space Flight Project Management Processes…"
- 2007 – Reissue of NASA/SP-2007-6105 "NASA Systems Engineering Handbook"
- 2008 – Reissue of NPR 8705.2B "Human-Rating Requirements for Space Systems"
- 2009 – Issuance of NPD-1000.5 "Policy for NASA Acquisition"
- 2009 – Revision of NPR 8000.4A "Agency Risk Management Requirements"
- 2009 – Issuance of NASA/SP-2009-569, "Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis"
- 2010 – Issuance of NASA/SP-2010-576 "NASA Risk-informed Decision Making Handbook"

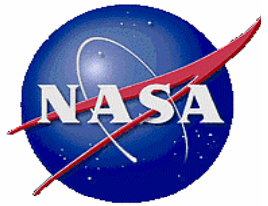
Emerging themes:
- Integrated perspective of risk analysis
- Scenario-based modeling of risk
- Better treatment of uncertainties

Risk Management Policy

- **NASA Policy Directive (NPD) 1000.5 (2009) states: "*It is NASA policy to incorporate in the overall Agency risk management strategy a risk-informed acquisition process that includes the identification, analysis, and management of programmatic, infrastructure, technical, environmental, safety, cost, schedule, management, industry, and external policy risks that might jeopardize the success with which the Agency executes its acquisition strategies.*"**
- **NPR 8000.4A (2009), Agency Risk Management Procedural Requirements, evolves NASA's risk management approach to entail two complementary processes:**
  - **Risk-informed Decision Making (RIDM)**
    - To risk-inform direction-setting decisions (e.g., space architecture decisions)
    - To risk-inform the development of credible performance requirements as part of the overall systems engineering process
  - **Continuous Risk Management (CRM)**
    - To manage risk associated with the implementation of baseline performance requirements



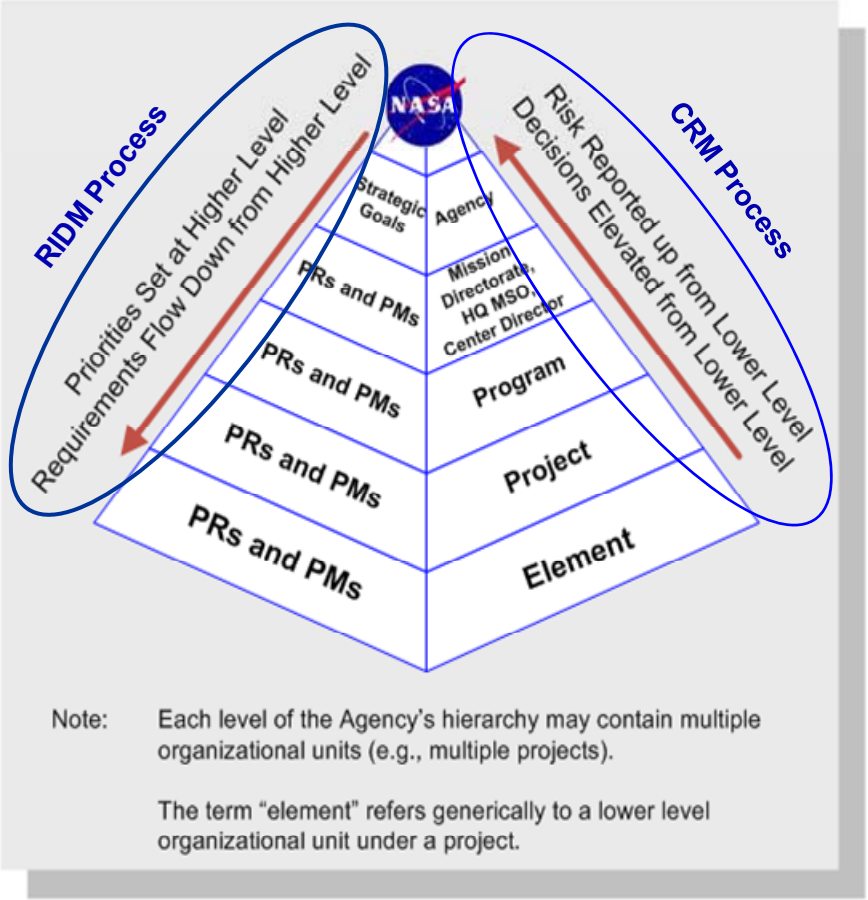
Motivating Factors for New RM Approach



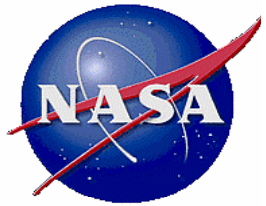
- To manage risk in a holistic and coherent manner across the Agency
  - Agency strategic goals explicitly drive RM activities at all levels
  - All risk types and their interactions are considered collectively during decision-making
  - Implementation of RM in the context of complex institutional relationships (programs, projects, centers, contractors, …)
- To better match the stakeholder expectations and the "true" resources required to address the risks to achieve those expectations
  - Better comprehension of the risk that a decision-maker is accepting when making commitments to stakeholders
  - Having an integrated perspective of risks when analyzing competing alternatives
- To better establish close ties between the selected alternative and the requirements derived from it
  - Derivation of achievable requirements through systematic characterization of uncertainties

The RM Process Begins with NASA Strategic Goals

- Within NASA's organizational hierarchy, high-level objectives (NASA Strategic Goals) flow down in the form of progressively more detailed performance requirements, whose satisfaction assures that objectives are met
- RIDM is designed to maintain focus on strategic goals as decisions are made throughout the hierarchy
- CRM is designed to manage "risks" in the context of requirements

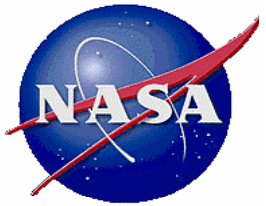


Definition of Risk in the Context of Mission Execution per NPR 8000.4



- **Risk is the expression of the potential for performance shortfalls, which may be realized in the future, with respect to achieving explicitly established and stated performance requirements**
  - **The performance shortfalls may be related to any one or more of the following mission execution domains:**
    - **Safety**
    - **Technical performance**
    - **Cost**
    - **Schedule**
  - **Every performance requirement has a risk associated with it based on the uncertainty of achieving it**

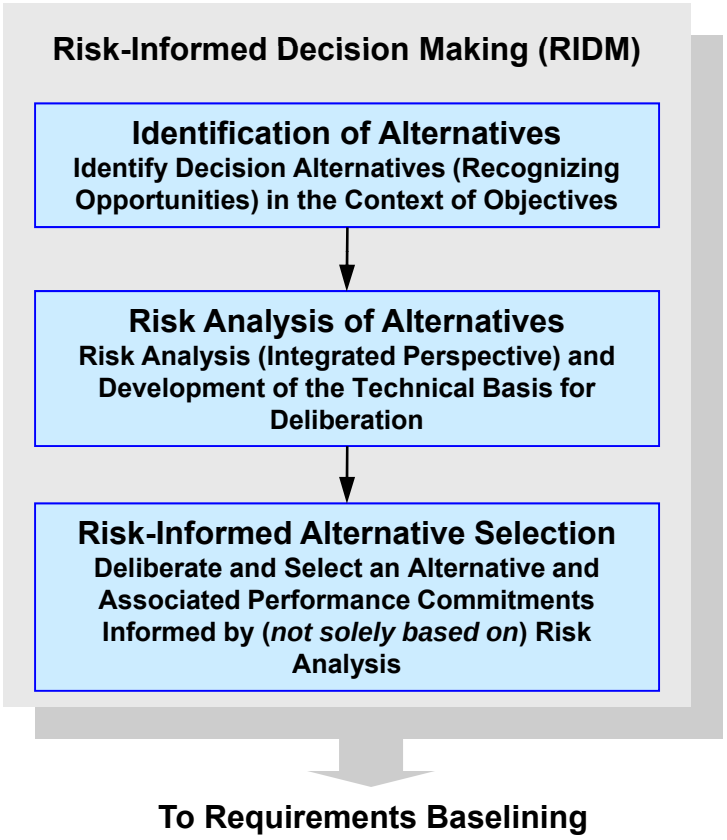
What is RIDM and When is it Invoked?



- **A risk-informed decision-making process that uses a diverse set of performance measures (some of which are model-based risk metrics) along with other considerations within a *deliberative* process to inform decision making.** ***Paragraph A.14 of NASA NPR 8000.4A***
  - **Within RIDM, decisions are informed by an integrated risk perspective rather than being informed by a set of individual "risk" contributions whose cumulative significance is not understood**
  - **A decision-making process relying primarily on a narrow set of model-based risk metrics would be considered "risk-based"**
- **RIDM is invoked for key decisions such as architecture and design decisions, make-buy decisions, and budget reallocation (allocation of reserves), which typically involve requirements-setting or rebaseling of requirements**

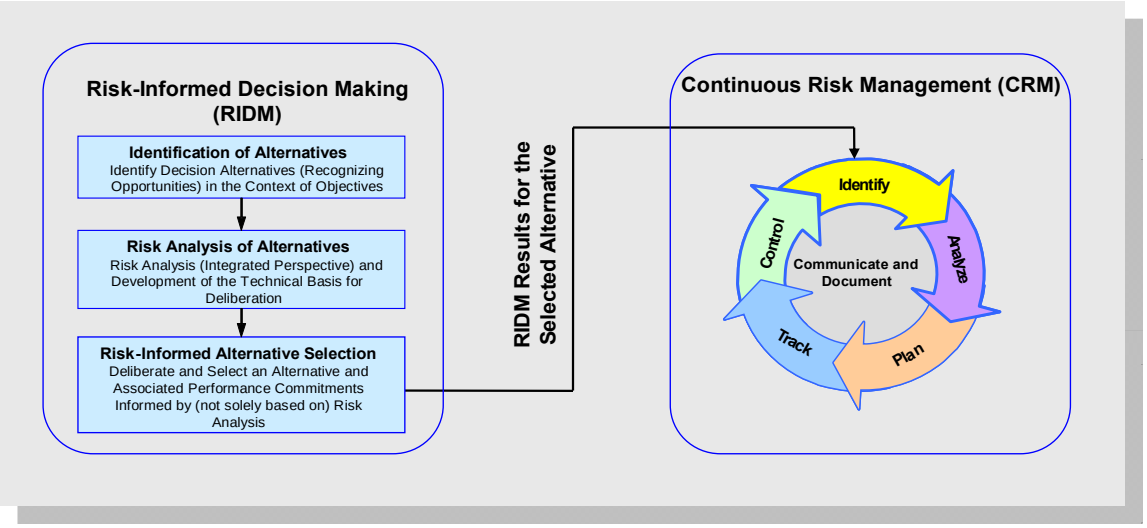
The RIDM Process as Defined in NPR 8000.4A

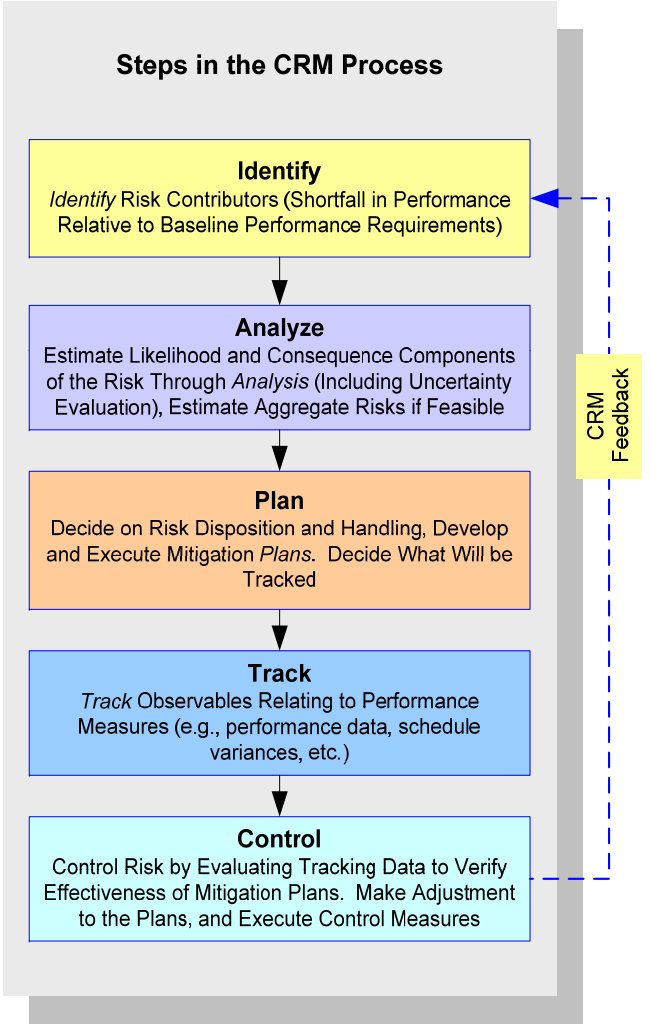
- Identification of decision alternatives (*decision context*) and considering a sufficient number and diversity of performance measures to constitute a comprehensive set for decision-making purposes
- *Risk analysis* is defined broadly in NPR 8000.4A as uncertainty analysis of performance associated with the alternative
- *Selection* of a decision alternative *informed by* (not solely based on) *Risk Analysis results*.



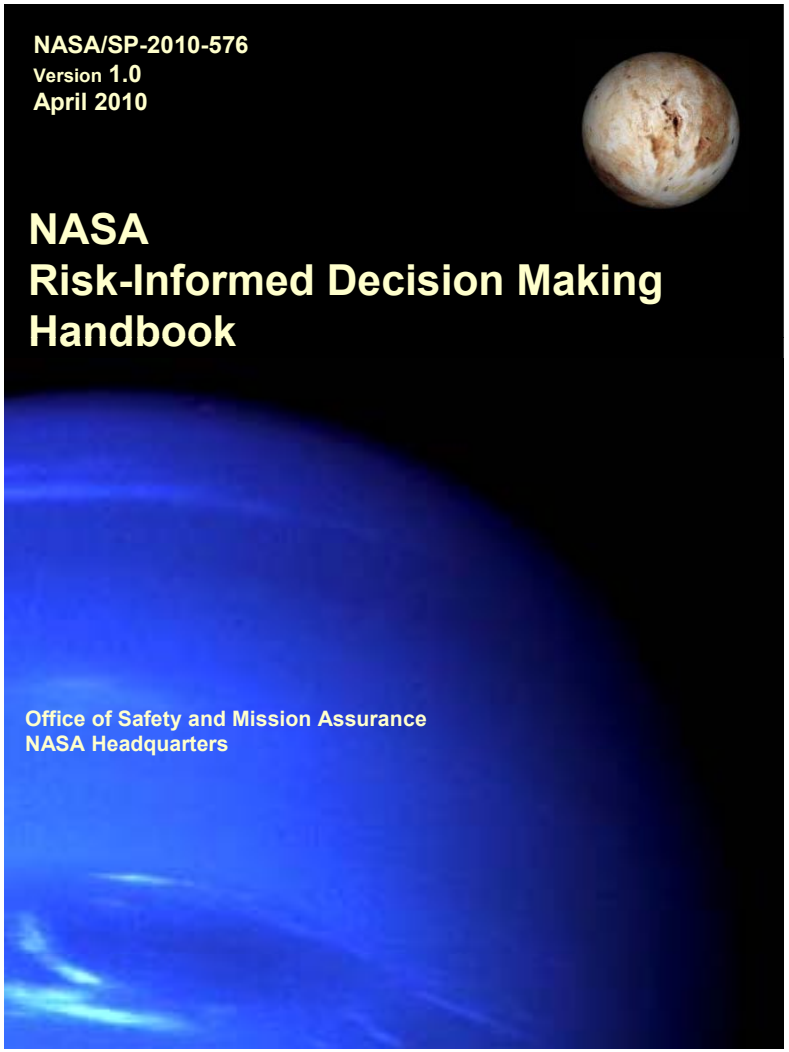
The Continuous Risk Management (CRM) Process

- Is initiated by the results of the RIDM process:
  - The risk analysis for the selected alternative
  - An initial risk list
- Focuses on meeting performance requirements
  - By managing performance margins over time so that associated performance requirements are not violated
  - By "burning down" (over time) the risk of violating performance requirements
  - By means of mitigation actions





RIDM Process Steps
Based on NASA/SP-2010-576



Risk-Informed Decision Making (RIDM)

Part 1 - Identification of Alternatives
- Step 1 – Understand Stakeholder Expectations and Derive Performance Measures
- Step 2 – Compile Feasible Alternatives

Part 2 - Risk Analysis of Alternatives
- Step 3 – Set the Framework and Choose the Analysis Methodologies
- Step 4 – Conduct the Risk Analysis and Document the Results

Part 3 - Risk-Informed Alternative Selection
- Step 5 – Develop Risk-Normalized Performance Commitments
- Step 6 – Deliberate, Select an Alternative, and Document the Decision Rationale

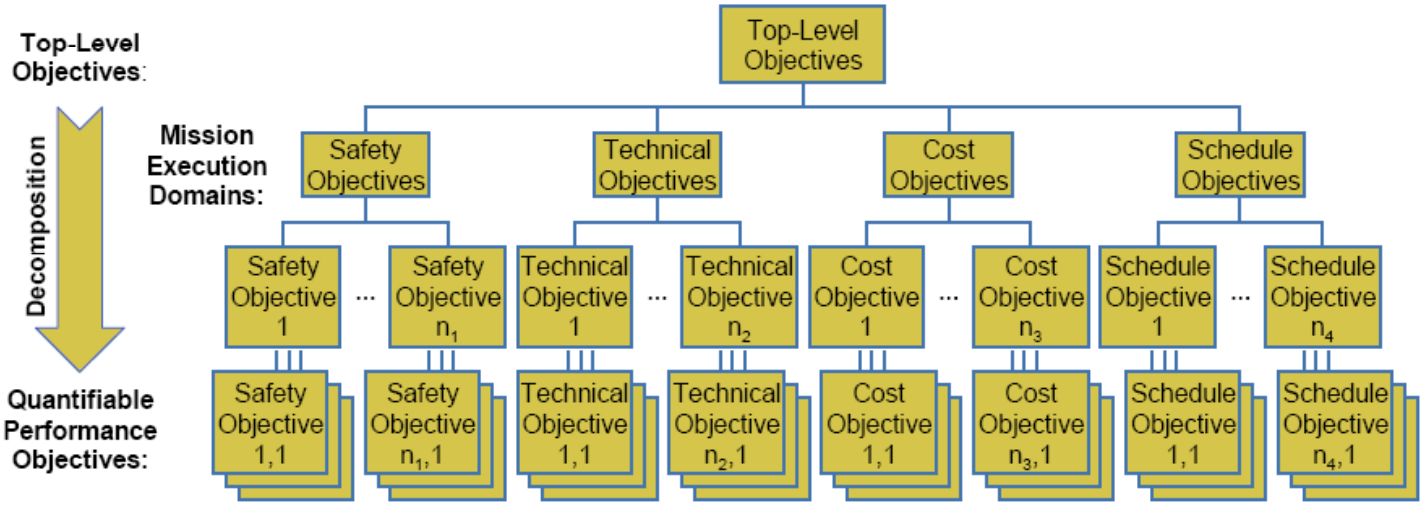
To Requirements (Re)Baselining

http://www.hq.nasa.gov/office/codeq/doctree/SP2010576.htm

RIDM Process – Part 1

Understand Stakeholder Expectations and Derive Performance Measures

- An objectives hierarchy is constructed by subdividing the top-level objectives into more detailed objectives, thereby clarifying the intended meaning.
- At the first level of decomposition, the top-level objective is partitioned into the mission execution domains of Safety, Technical, Cost, and Schedule.
- Within each domain, the objectives are further decomposed until appropriate quantifiable performance objectives are generated.

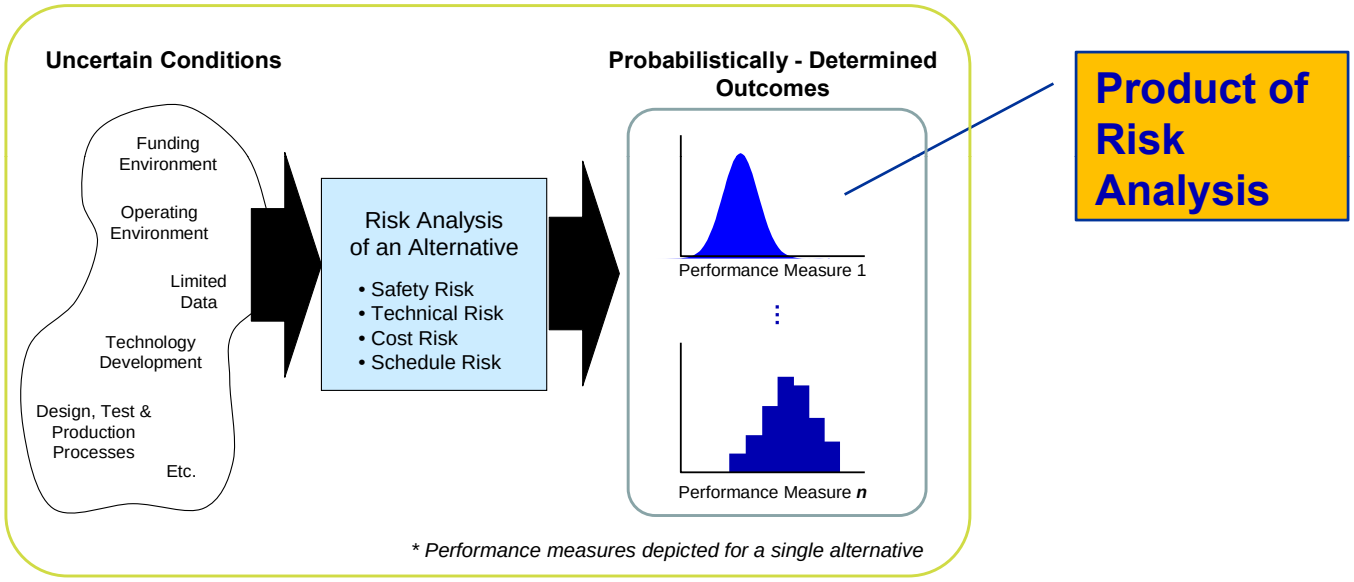


Notional Objectives Hierarchy

RIDM Process – Part 2

Risk Analysis of Alternatives

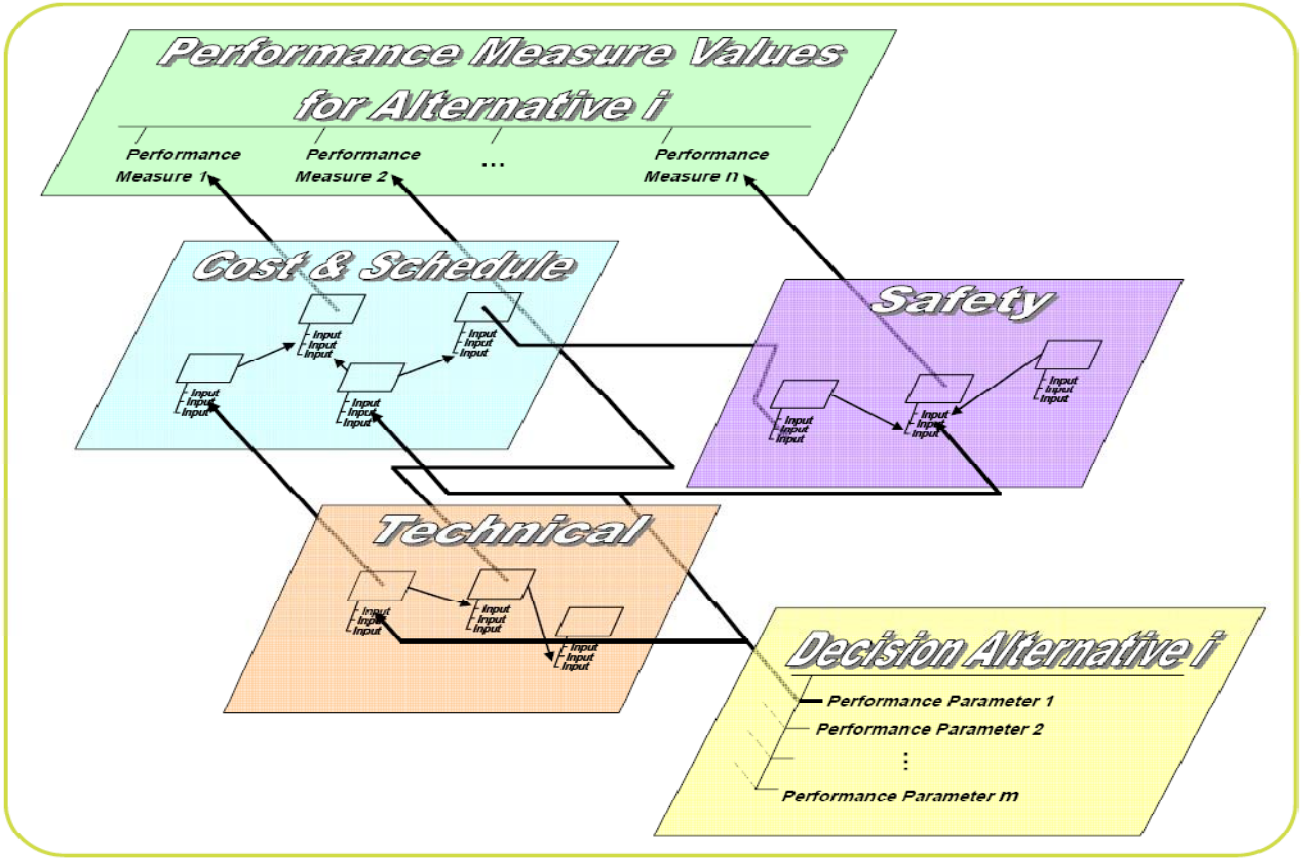
- **The goal is to develop a risk analysis framework that integrates domain-specific performance assessments and quantifies the performance measures**
  - **Risk Analysis -** probabilistic modeling of performance



- **Establishing a transparent framework that:**
  - Operates on a common set of **performance parameters** for each alternative
  - Consistently addresses uncertainties across mission execution domains and across alternatives
  - Preserves correlations between performance measures

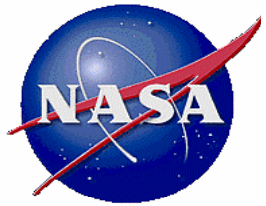
Setting Risk Analysis Framework

- **Detailed domain-specific analysis guidance is available in domain-specific guidance documents like the *NASA Cost Estimating Handbook*, the *NASA Systems Engineering Handbook*, and the *NASA Probabilistic Risk Assessment Procedures Guide***

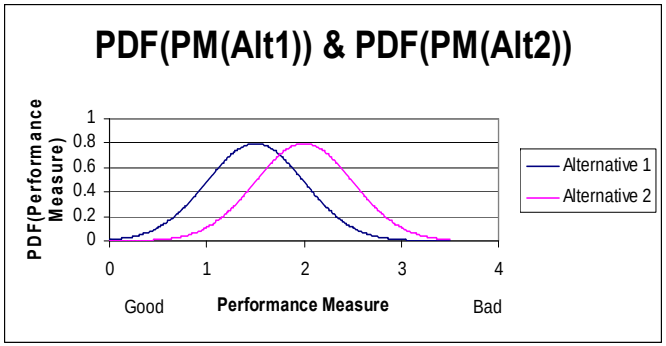


RIDM Process – Part 3

Risk-informed Alternative Selection



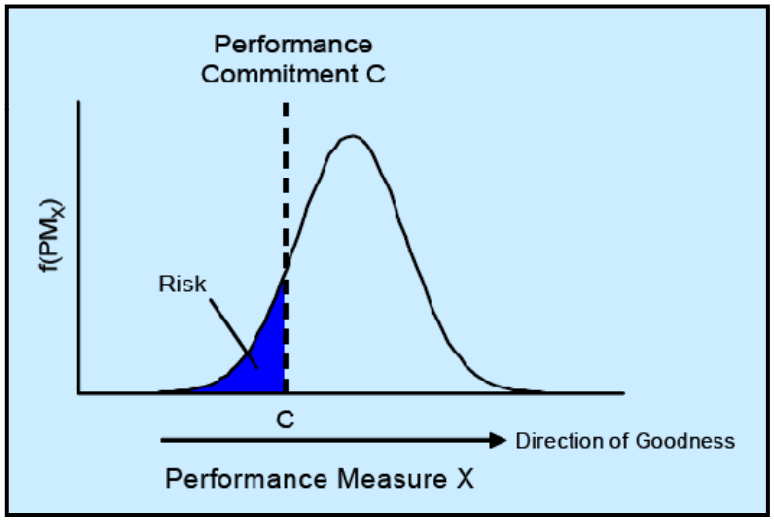
- **Performance measure pdfs constitute the fundamental risk analysis results.**
- **However, there are complicating factors for performance measures that are expressed as pdfs:**
  - The pdfs for different alternatives may overlap, preventing a definitive assessment of which alternative has superior performance



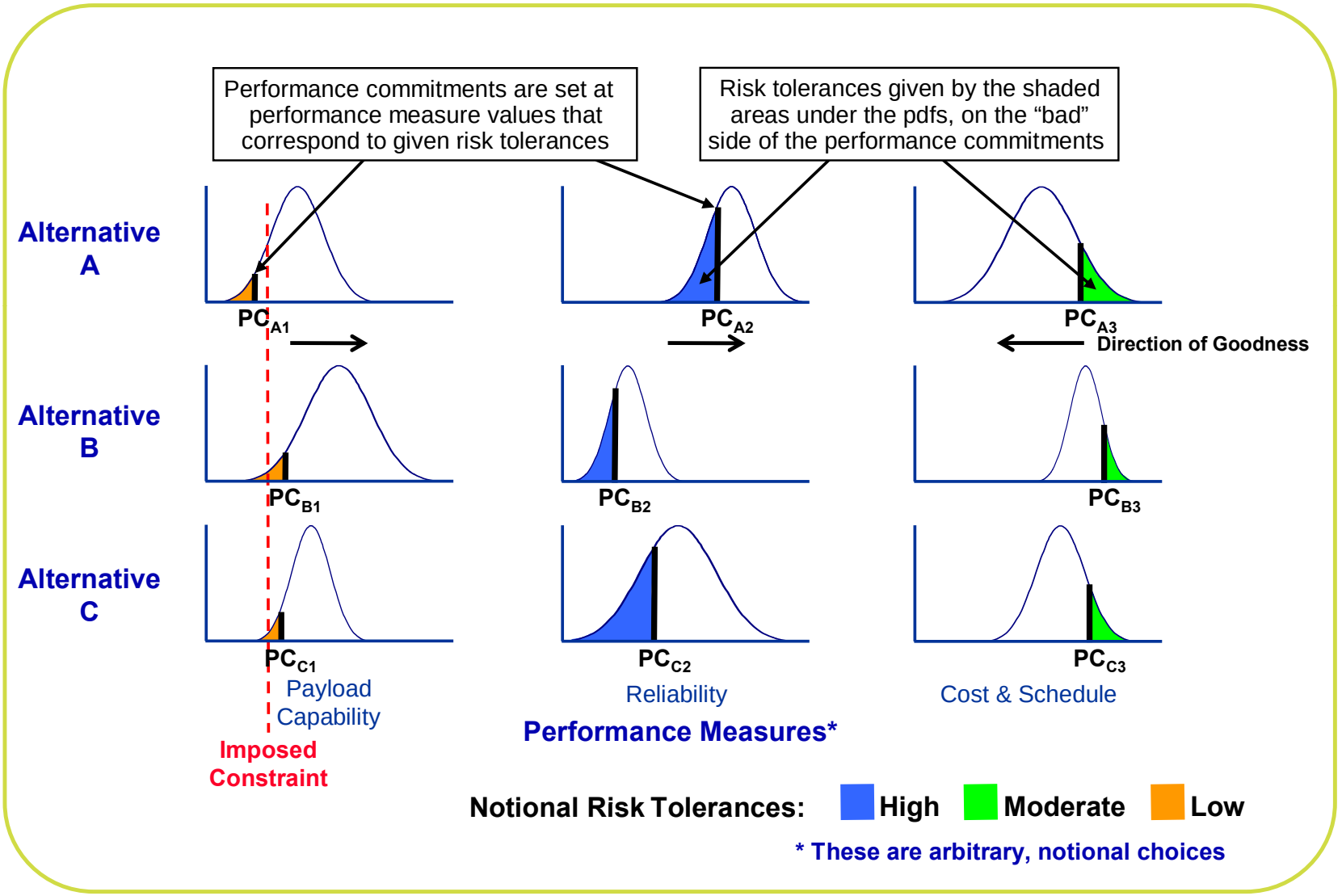
  - Different pdfs may exceed imposed constraints at different percentiles, thereby comingling issues of performance with issues of success

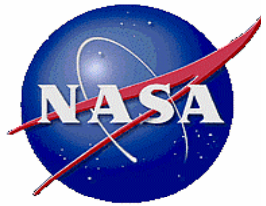
Performance Commitment

- **Mean values are used in many different contexts to compare alternatives, but this approach can:**
  - **Produce values that are strongly influenced by the tail ends of the pdfs**
  - **Introduce significant probabilities of falling short of imposed constraints, even when the mean values meet imposed constraints**
- **A *Performance Commitment* is the level of performance whose probability of not being achieved matches the decision maker's risk tolerance**
  - **Anchors the commitment the decision maker (DM) is willing to make for that performance measure**
- **Performance commitments support a risk-normalized comparison of decision alternatives, at a level of risk tolerance determined by the decision maker.**



Deliberation of the Merits of Each Alternative in the Context of Performance Commitments (notional)





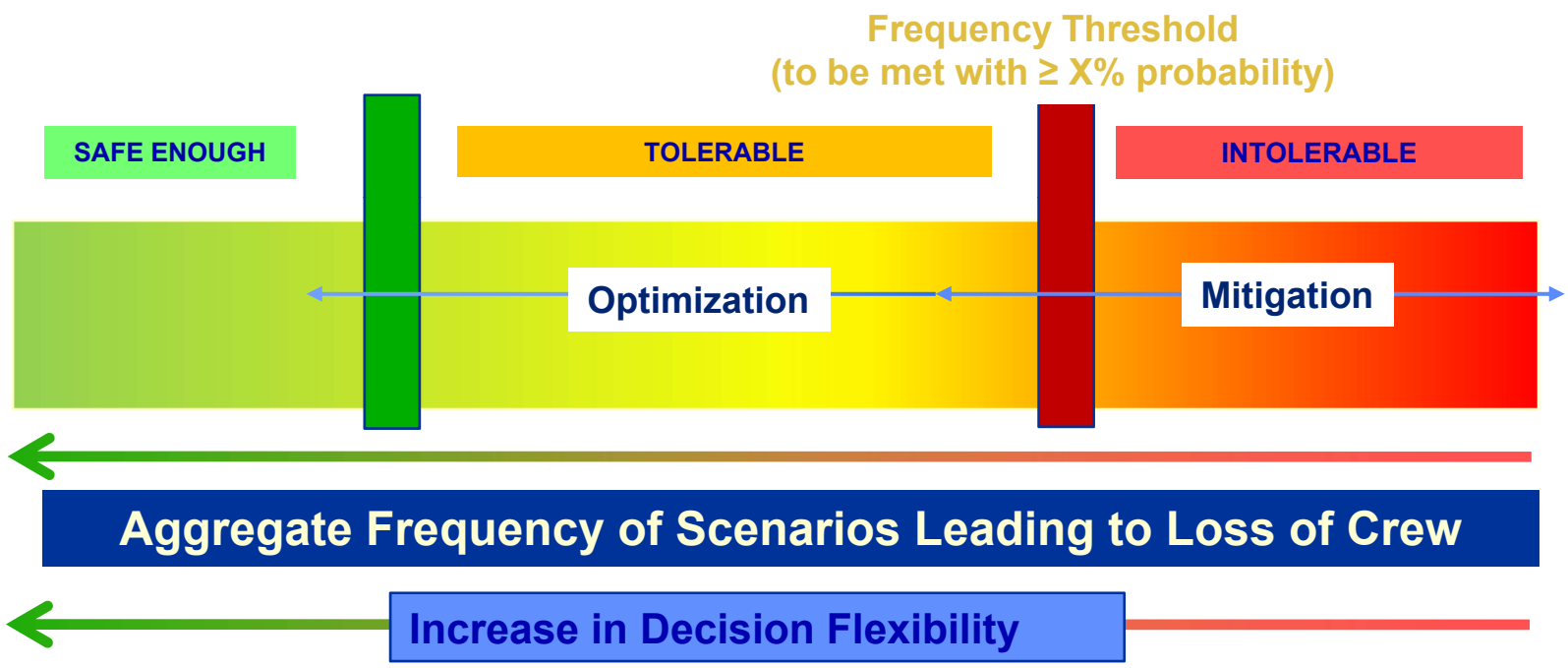
Safety Thresholds and Safety Goals

- Safety performance, like technical performance, schedule and cost is now a key acquisition parameter for human spaceflight
- We are developing safety goals and thresholds for human space flight to low earth orbit
  - Safety Goals are desirable safety performance levels for driving safety improvements
  - Safety Thresholds are criteria for risk acceptability decisions; not meeting these values is not tolerable
  - Both goals and thresholds are defined in terms of aggregate risks
    - Help designers with safety performance allocation
    - Help decision makers to deal with safety-related decisions
      - Risk acceptance
      - Risk mitigation
      - Safety optimization

Safety Regimes and Safety Decisions to be Made

Standard of "Optimally and Sufficiently Safe"
More than this May have diminishing return
GOAL

Standard of "Minimally Safe Level"
Less than this would be "intolerable"
TRESHOLD



- Keep alert for enhancements, but focus more on maintaining the good safety level that has been been achieved

- Actively pursue safety improvements via risk tradeoff studies
- Actively identify unaccounted-for hazards via precursor analysis

- Don't proceed with the acquisition
- Fix design or operation to meet the threshold.

References

- *Probabilistic Risk Procedures Guide for NASA Managers and Practitioners*, 2002.
- NPD 1000.5, *Policy for NASA Acquisition,* 2009.
- NPR 8000.4, *Agency Risk Management Procedural Requirements*, 2009.
- NPR 8705.2, *Human Rating Requirement for Space Systems*, 2009.
- NASA/SP-2009-569, *Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis*, 2009
- NASA/SP-2010-576, *NASA Risk-Informed Decision-Making Handbook*, 2010.
- NASA/SP-2011-XXX, *System Safety Guidebook* (Under development by NASA Office of Safety and Mission Assurance)