Evolution of Risk Management at NASA in the Context of Achieving Adequate Safety

Presented at the
DOE 2012 Nuclear Safety Workshop

Bethesda, Maryland
September 20, 2012

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

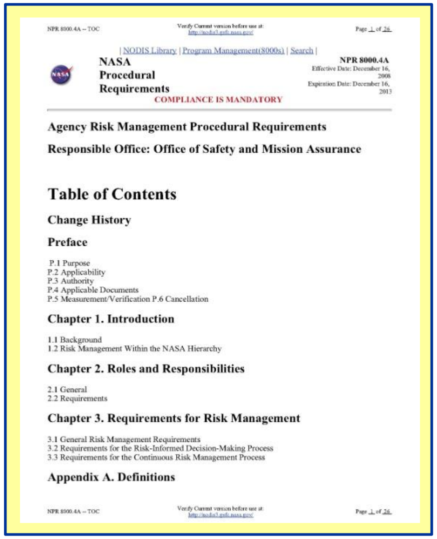
Outline

- Historical Perspective on NASA Risk Management (RM)
- RM Approach After 2008
- Future Direction of RM at NASA
  - The Concept of "Adequate Safety"
  - The Issue of Risk Analysis Completeness

    (Rationale for Future Trends in RM)
- Summary

Acknowledgments

This presentation is partly derived from the following sources:



NPR 8000.4A -- TOC

Verify Current version before use at:
http://nodis3.gsfc.nasa.gov/

Page 1 of 26

| NODIS Library | Program Management(8000s) | Search |

NASA
Procedural
Requirements

NPR 8000.4A
Effective Date: December 16, 2008
Expiration Date: December 16, 2013

COMPLIANCE IS MANDATORY

Agency Risk Management Procedural Requirements

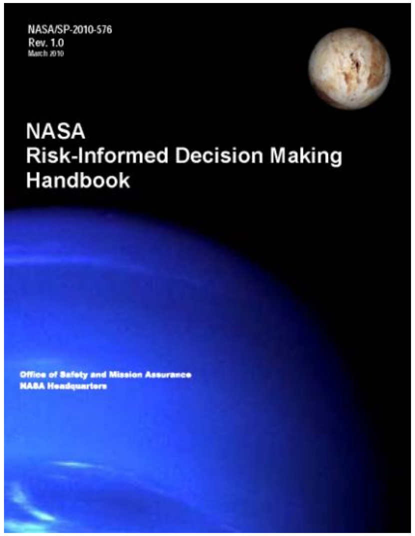
Responsible Office: Office of Safety and Mission Assurance

Table of Contents

NPR 8000.4A -- TOC

Verify Current version before use at:
http://nodis3.gsfc.nasa.gov/

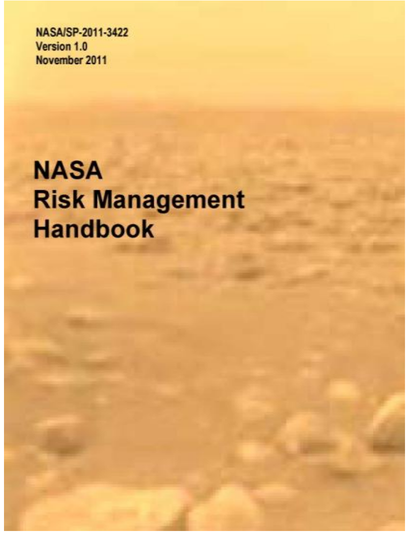
Page 1 of 26



NASA/SP-2010-576
Rev. 1.0
March 2010

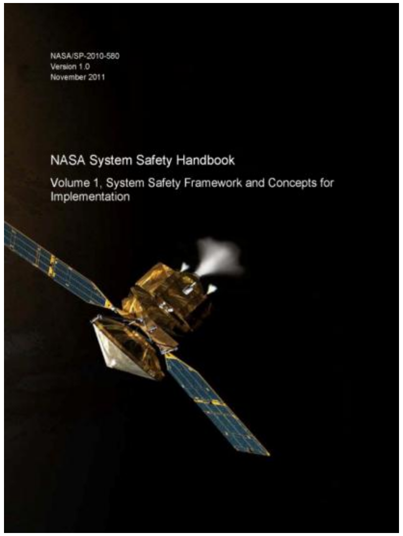
NASA
Risk-Informed Decision Making
Handbook

Office of Safety and Mission Assurance
NASA Headquarters



NASA/SP-2011-3422
Version 1.0
November 2011

NASA
Risk Management
Handbook



NASA/SP-2010-580
Version 1.0
November 2011

NASA System Safety Handbook

Volume 1, System Safety Framework and Concepts for Implementation

NASA NPR 8000.4A

NASA/SP-2010-576

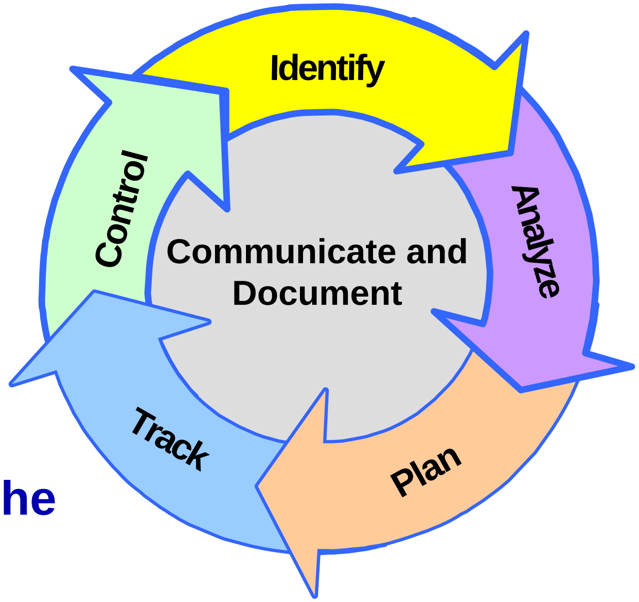
NASA/SP-2011-3422

NASA/SP-2010-580

Historical Perspective on NASA Risk Management (RM)

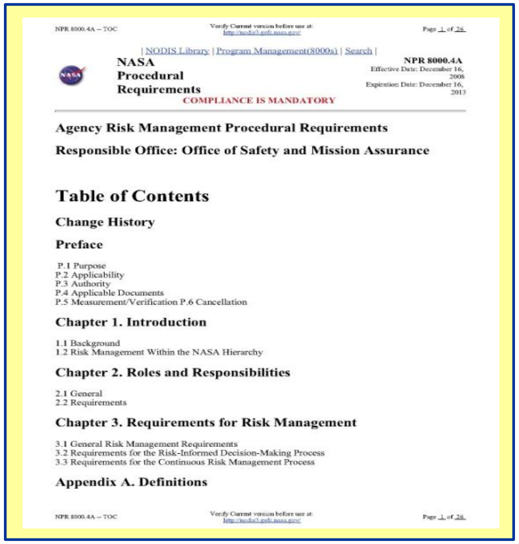
- No "formal," systematic RM process in NASA until mid-1990s.

- 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 not normally seen as scenario-based
  - Individual risks were analyzed qualitatively and arrayed on a "risk matrix" of severity vs. likelihood
  - Mitigations were typically devised without a focus on performance requirements



RM Approach After 2008

- In 2008, we took the next step in the evolution of RM by revising our Risk Management directive, **NPR 8000.4A, *Agency Risk Management Procedural Requirements***



NPR 8000.4A -- TOC | Verify Current version before use at: http://nodis3.gsfc.nasa.gov/ | Page 1 of 26

| NODIS Library | Program Management(8000s) | Search |

NASA
Procedural
Requirements

NPR 8000.4A
Effective Date: December 16, 2008
Expiration Date: December 16, 2013

COMPLIANCE IS MANDATORY

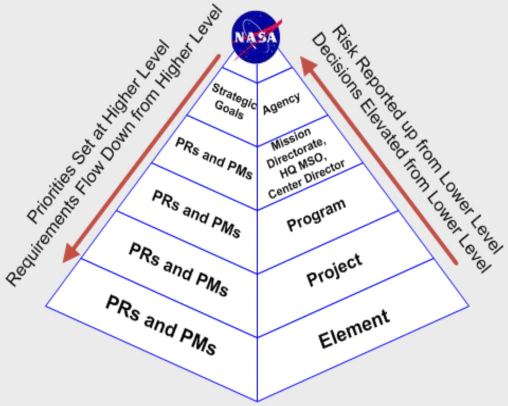
Agency Risk Management Procedural Requirements

Responsible Office: Office of Safety and Mission Assurance

Table of Contents

NPR 8000.4A -- TOC | Verify Current version before use at: http://nodis3.gsfc.nasa.gov/ | Page 1 of 26

- Agency strategic goals drive RM activities at all levels
- All risk types are considered collectively during decision-making, and
- RM activities are coordinated horizontally and vertically, across and within programs, projects, and institutions


Priorities Set at Higher Level
Requirements Flow Down from Higher Level
Strategic Goals
Agency
PRs and PMs
Mission Directorate, HQ MSO, Center Director
PRs and PMs
Program
PRs and PMs
Project
PRs and PMs
Element
Risk Reported up from Lower Level
Decisions Elevated from Lower Level

Note: Each level of the Agency's hierarchy may contain multiple organizational units (e.g., multiple projects).

The term "element" refers generically to a lower level organizational unit under a project.

PR: Performance Requirement
PM: Performance Measure

NPR 8000.4A Definition of Risk is Based on Meeting Performance Objectives

> "Risk is the potential for performance shortfalls, which may be realized in the future, with respect to achieving explicitly established and stated performance requirements."

- Performance shortfalls may be related to institutional support for mission execution or to any one or more of the following mission execution domains:
  - Safety (e.g., avoidance of injury, fatality, destruction of key assets, environmental damage)
  - Technical (e.g., thrust or output, amount of observational data acquired)
  - Cost (e.g., execution within allocated cost)
  - Schedule (e.g., meeting milestones)

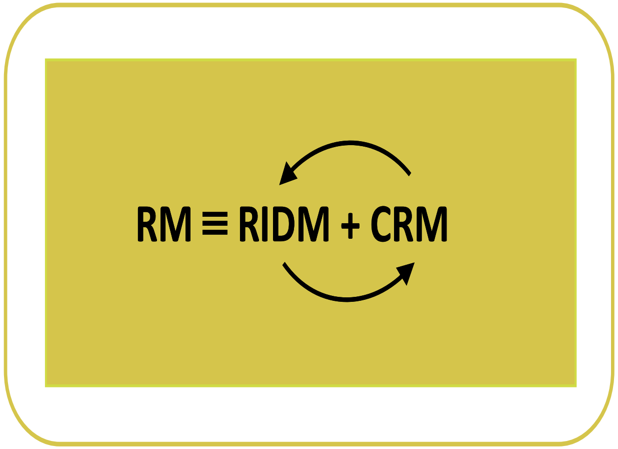
Today RM is Viewed as the Interaction of RIDM and CRM

- NPR 8000.4A (Dec. 2008), evolved NASA RM to entail two complementary processes:
  1. Risk-Informed Decision Making (RIDM) and
  2. Continuous Risk Management (CRM)

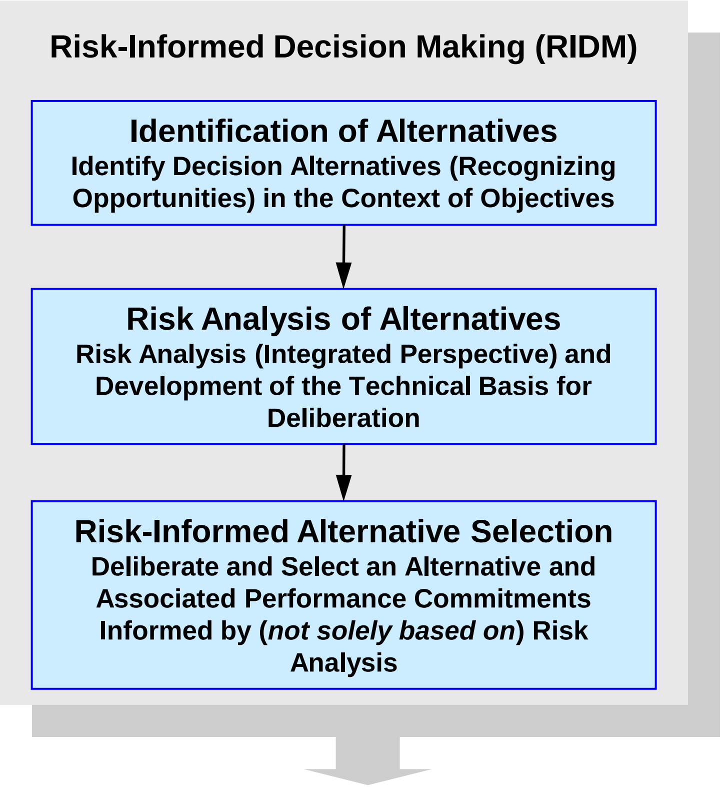
- The result is a RM approach that is proactive, integrated, coherent, and supportive of the management of aggregate performance risk

RIDM informs systems engineering decisions through better use of risk and uncertainty information in selecting among alternatives and establishing baseline performance requirements

CRM manages 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 ≡ RIDM + CRM

The RIDM Process and its Themes



Risk-Informed Decision Making (RIDM)

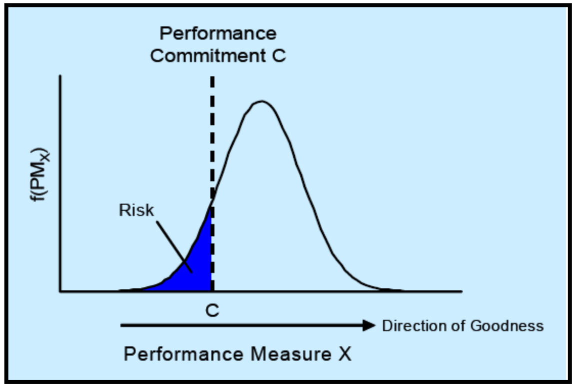
Identification of Alternatives
Identify Decision Alternatives (Recognizing Opportunities) in the Context of Objectives

Risk Analysis of Alternatives
Risk Analysis (Integrated Perspective) and Development of the Technical Basis for Deliberation

Risk-Informed Alternative Selection
Deliberate and Select an Alternative and Associated Performance Commitments Informed by (*not solely based on*) Risk Analysis

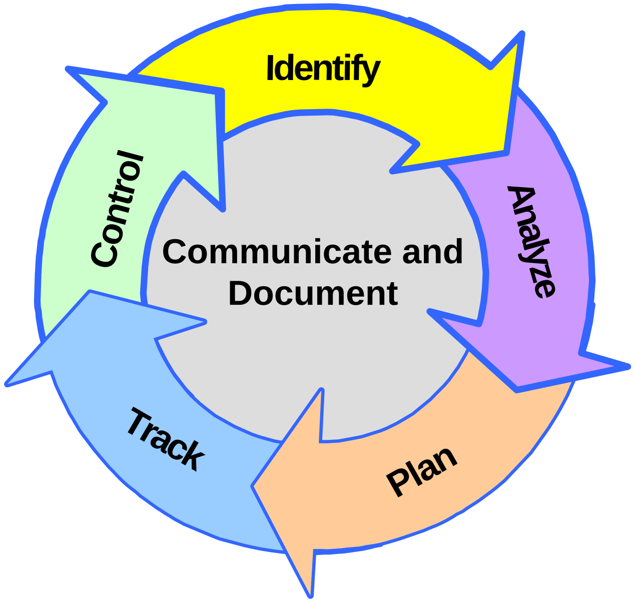
To Requirements Baselining

- **The importance of considering multiple objectives across all mission execution domains (safety, technical, cost, schedule)**
- **The importance of close ties between the selected alternative and requirements derived from it**
  - Match commitment levels with the decision maker's risk tolerance limits



  - Develop achievable requirements
- **The importance of a documented decision rationale**

The CRM Process and its Themes



- CRM process is oriented toward keeping the potential for performance shortfalls within tolerable limits

- At the micro level, the process is largely unchanged
  - However, the context within which CRM operates is now defined explicitly
  - All “risks” managed within an organizational unit are pegged to the performance requirements that that unit is working to
- Risk Statements are now defined in a manner that supports a scenario-based understanding of individual risks
- The significance of individual risks is analyzed by integrating them into a risk model that quantifies performance risk
- Risk responses are based on addressing the most important causes of performance risk (i.e., the risk drivers)

FUTURE DIRECTION OF RM AT NASA

The Concept of “Adequate Safety”

- The trigger for dealing with the issue of “adequate safety” was the NASA Aerospace Safety Advisory Panel (ASAP) Recommendation 2009-01-02a:

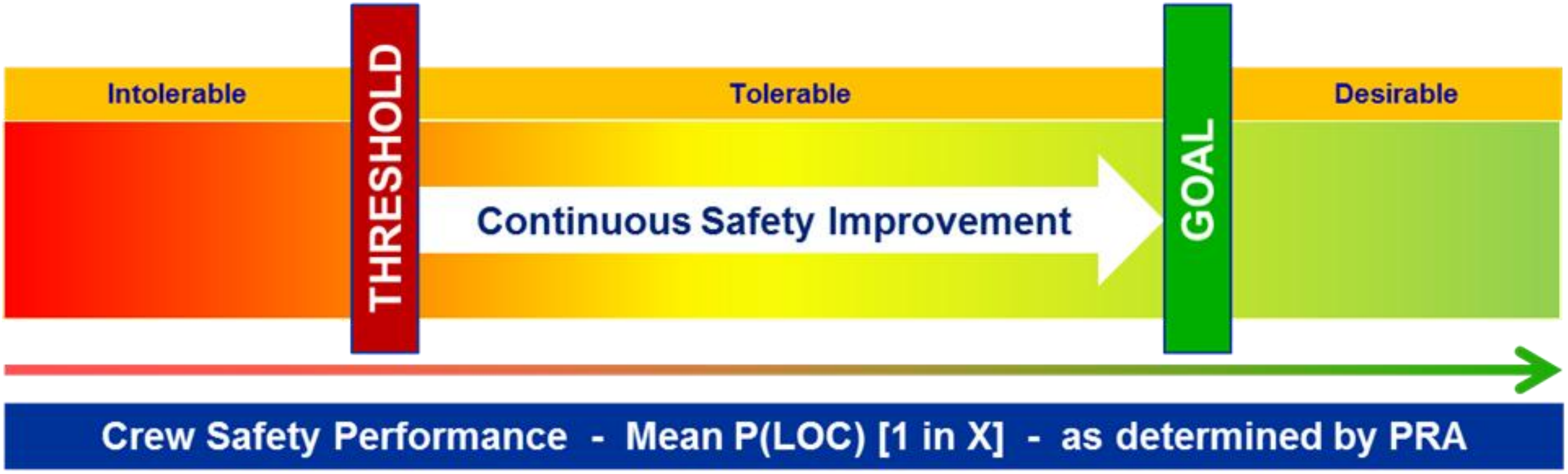
  > “The ASAP recommends that NASA stipulate directly the acceptable risk levels—including confidence intervals for the various categories of activities (e.g., cargo flights, human flights)—to guide managers and engineers in evaluating “how safe is safe enough.”

- NASA accepted the ASAP recommendation and committed to establishing safety thresholds and goals for human space flight
  - Safety threshold expresses an initial minimum tolerable level of safety
  - Safety goal expresses expectations about the safety growth of the system in the long term
- Achieving an adequately safe system requires adherence to the following fundamental safety principles:
  - The system meets or exceeds a minimum tolerable level of safety; below this level the system is considered unsafe
  - The system is as safe as reasonably practicable (ASARP)

Meeting or Exceeding a Minimum Tolerable Level of Safety

Standard of "Minimally Safe Initially"
Less than this would be "intolerable"

Standard of "Minimally Safe for Long Term Operation"
Less than this is tolerable, conditional on continuous safety improvement



Crew Safety Performance - Mean P(LOC) [1 in X] - as determined by PRA

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

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

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

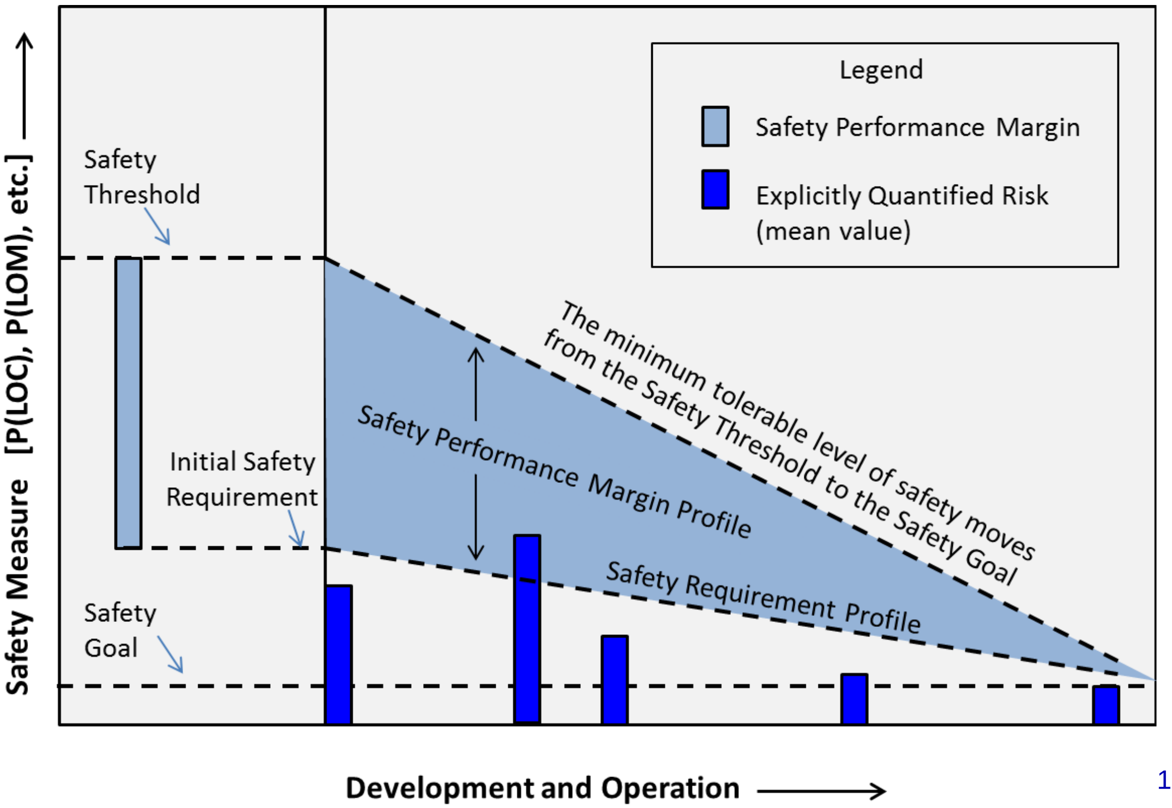
PRA:	Probabilistic Risk Assessment
P(LOC):	Probability of Loss of Crew

The Issue of Risk Analysis Completeness
(Rationale for Future Trends in RM)

- **Safety goals and thresholds represent expectations about actual risk, including both known and unknown/underappreciated (UU) sources of risk**
  - ***Known sources of risk*** are amenable to explicit quantification via synthetic, scenario-based methods of analysis (e.g., PRA), and actuarial methods (when sufficient data are available)
  - ***UU sources of risk*** are not amenable to synthetic analysis or direct actuarial characterization, yet are historically recognized as significant contributors to risk
    - They tend to remain latent in the system until revealed by operational failures, precursor analysis, etc.
    - They tend to be most significant early in the system life cycle
    - They disproportionally reflect organizational issues and/or complex intra-system interactions

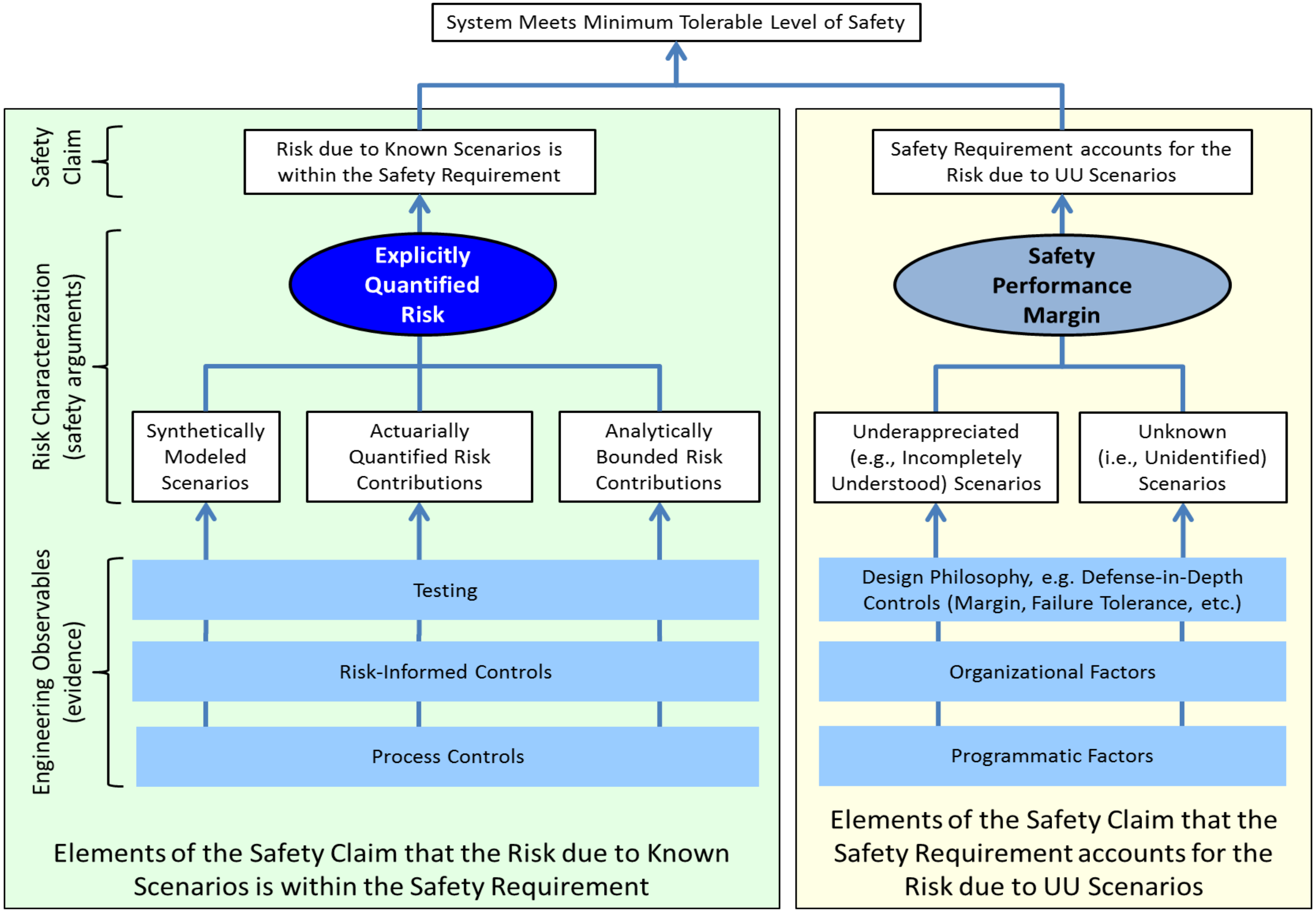
Accounting for Unknown/Underappreciated Risks

- ASAP and others have raised the need to consider the gap between *known* risk and *actual* risk when applying NASA safety thresholds and goals
- We have developed the concept of safety performance margin, based on historical discrepancies between calculated and demonstrated safety performance
- Safety performance margin accounts for UU risks
- It provides a rational basis for deriving verifiable requirements on known risk, e.g., using PRA mean values


Legend
Safety Performance Margin
Explicitly Quantified Risk (mean value)
Safety Threshold
Initial Safety Requirement
Safety Goal
The minimum tolerable level of safety moves from the Safety Threshold to the Safety Goal
Safety Performance Margin Profile
Safety Requirement Profile
Safety Measure [P(LOC), P(LOM), etc.]
Development and Operation

Managing Known and UU Risks

- The structure of a safety claim that the system meets the minimum tolerable level of safety is the conjunction of two sub-claims:
  1. The risk due to known scenarios is within the safety requirement; and
  2. The safety requirement accounts for the risk due to UU scenarios

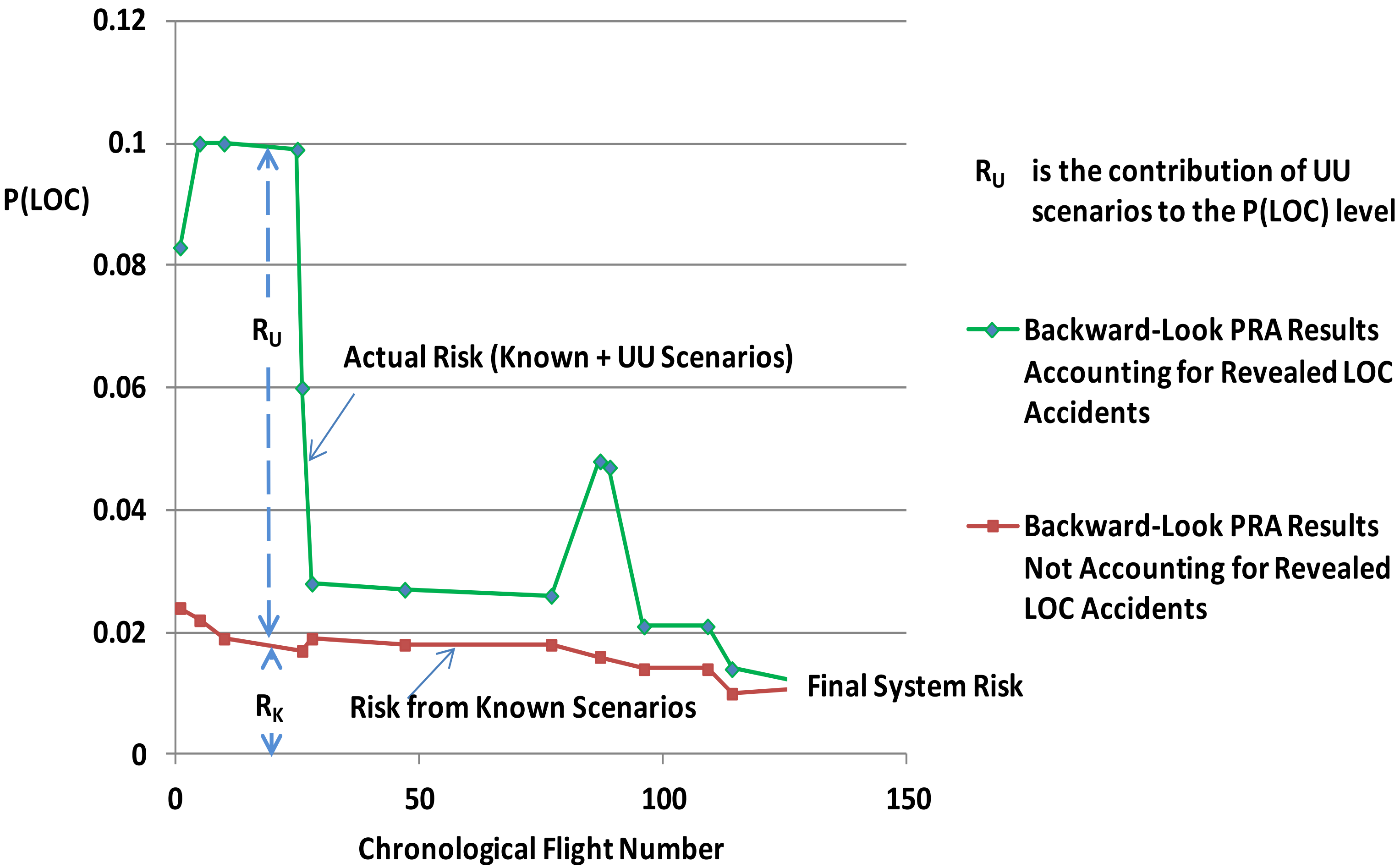

System Meets Minimum Tolerable Level of Safety
Safety Claim
Risk due to Known Scenarios is within the Safety Requirement
Risk Characterization (safety arguments)
Explicitly Quantified Risk
Synthetically Modeled Scenarios
Actuarially Quantified Risk Contributions
Analytically Bounded Risk Contributions
Engineering Observables (evidence)
Testing
Risk-Informed Controls
Process Controls
Elements of the Safety Claim that the Risk due to Known Scenarios is within the Safety Requirement
Safety Requirement accounts for the Risk due to UU Scenarios
Safety Performance Margin
Underappreciated (e.g., Incompletely Understood) Scenarios
Unknown (i.e., Unidentified) Scenarios
Design Philosophy, e.g. Defense-in-Depth Controls (Margin, Failure Tolerance, etc.)
Organizational Factors
Programmatic Factors
Elements of the Safety Claim that the Safety Requirement accounts for the Risk due to UU Scenarios

Summary

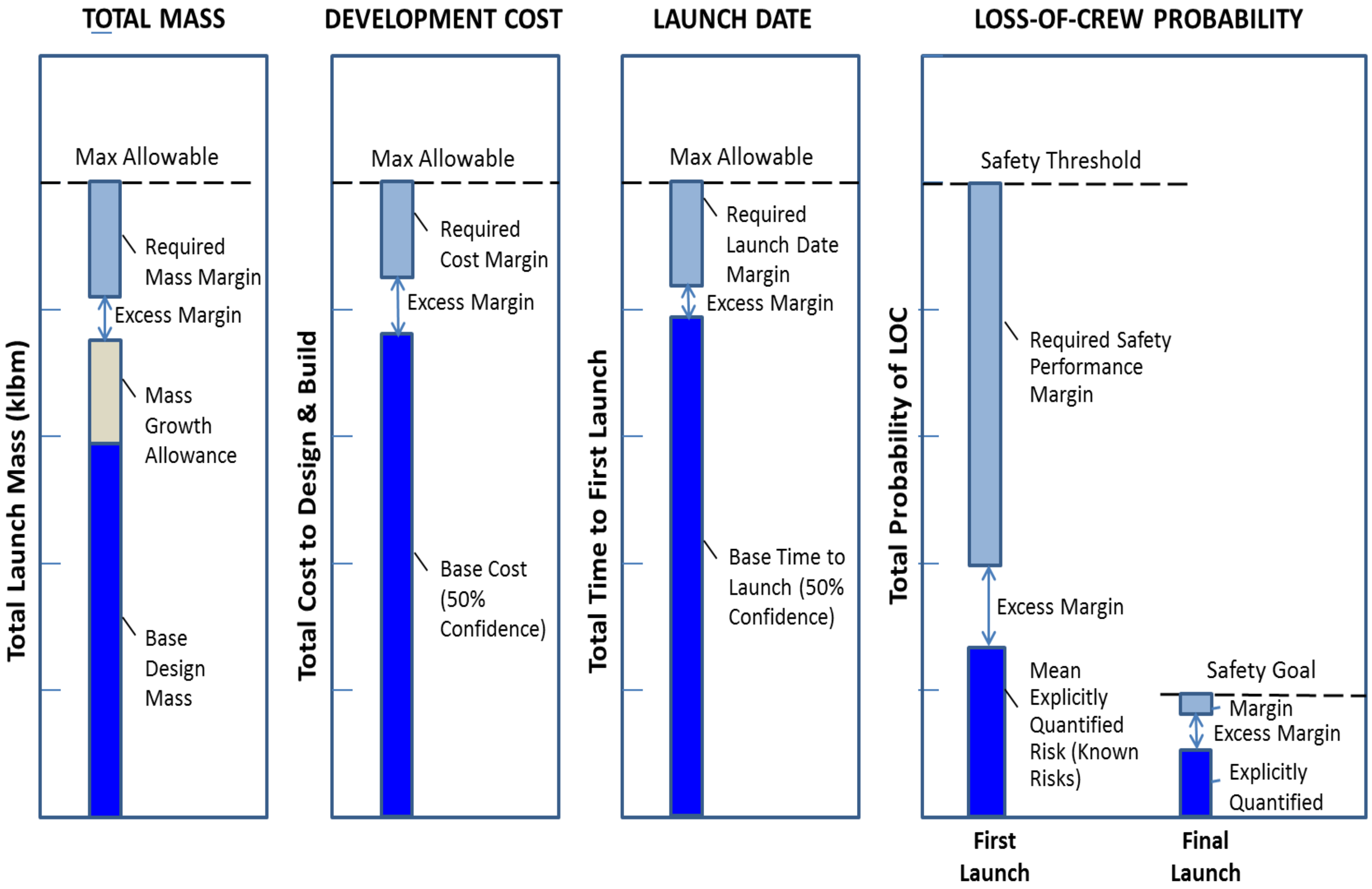
- Our RM approach is still evolving
- NPR 8000.4A laid the foundation for moving towards a more coherent and proactive RM approach
- Our new RM handbook (NASA/SP-2011-3422) lays the groundwork for considering multiple objectives in an integrated fashion across all mission execution domains (safety, technical, cost, schedule)
- The focus moves from the management of individual risks toward the management of aggregate performance risk
- Our safety threshold and goal policy gives impetus to address unknown or underappreciated (UU) risks
- We are exploring ways for characterizing and managing UU risks
- We still need to address institutional and enterprise risks

Backup Slides

Contribution of UU Scenarios to Shuttle Risk



Relationship of Safety Performance Margins to System Engineering Margins



TOTAL MASS
Max Allowable
Required Mass Margin
Excess Margin
Mass Growth Allowance
Base Design Mass
Total Launch Mass (klbm)
DEVELOPMENT COST
Max Allowable
Required Cost Margin
Excess Margin
Base Cost (50% Confidence)
Total Cost to Design & Build
LAUNCH DATE
Max Allowable
Required Launch Date Margin
Excess Margin
Base Time to Launch (50% Confidence)
Total Time to First Launch
LOSS-OF-CREW PROBABILITY
Safety Threshold
Required Safety Performance Margin
Excess Margin
Mean Explicitly Quantified Risk (Known Risks)
Safety Goal
Margin
Excess Margin
Explicitly Quantified
Total Probability of LOC
First Launch
Final Launch