Uncertainty in the Context of Risk Acceptance Decision-Making at NASA: Thinking Beyond "The Model"

Presented at the 27th Annual Regulatory Information Conference

Bethesda, MD
March 10, 2015

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

Acknowledgments

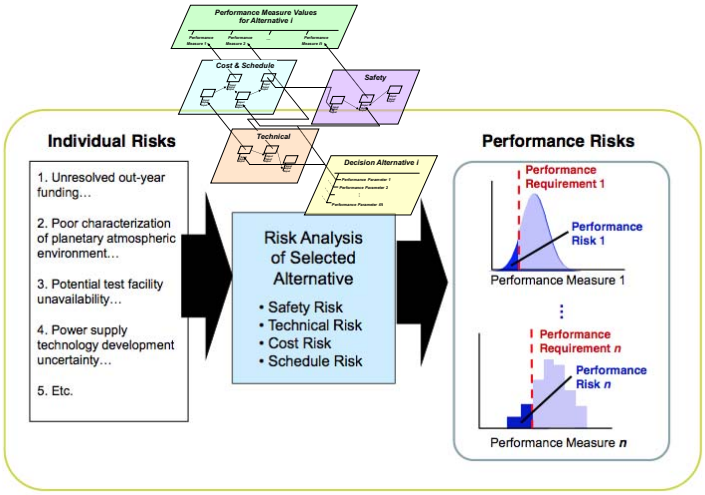
- Opinions expressed in this presentation are not necessarily those of NASA
- Most of the present discussion is based on work performed by the Office of Safety and Mission Assurance in conjunction with NASA System Safety Handbook, Volume 1 (NASA/SP-2010-580) and NASA System Safety Handbook, Volume 2 (NASA/SP-2014-612 (draft))
- The presentation has benefited from discussions with Dr. Robert Youngblood of INL and Mr. Chris Everett of Information Systems Laboratories

Overview

- In the NASA risk management context, "risk" means "potential for falling short of performance requirements"
  - E.g., a particular value of Probability of Loss of Crew (P(LOC)) might be a safety performance requirement (threshold for maximum acceptable risk)
  - The risk is the probability that the "actual" P(LOC) > the threshold
  - Roughly analogous to MIL-HDBK-189C *consumer risk*: the probability of accepting a system when the true reliability is below the technical requirement
- In a mission context, the scope of performance requirements spans the domains of safety, technical, cost, and schedule
- Specifying acceptable levels of performance for a given system is a question of requirements setting and relates to policy decisions (not a topic of this presentation)
- Uncertainty about what the "actual" performance of a system is, or will be, relates to epistemic uncertainty, and *is* a topic of this presentation
- At issue is the need to make sure that the decision maker (DM) is adequately apprised of *all* the relevant uncertainty when making risk acceptance decisions
  - For the above example, in order to justify a risk acceptance decision, DM needs assurance (enough confidence) that P(LOC) < "threshold"

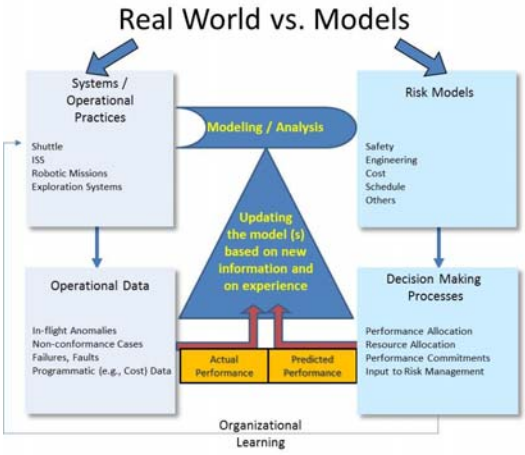
Risk Models

- Risk model development (synthetic analysis) attempts to forecast performance within a probabilistic framework that accounts for known, quantifiable sources of epistemic uncertainty.



Real World vs. Models

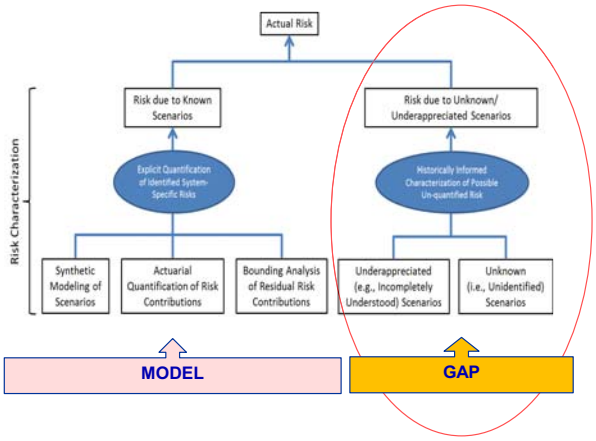
- Risk models must be constantly and critically reexamined for consistency with system configuration/ operation, and updated with relevant information (e.g., accident precursor analysis…) to ensure the closest correlation and fastest convergence between the "real world" and the "risk model"



The Gap

- However, in NASA contexts there is typically a gap between the real world and the model that is initially dominating and does not converge until long after most major decisions have been made
  - Executing first-of-a-kind missions with first-of-a-kind hardware
  - Employing systems that operate at the edge of engineering capability
- This gap is the domain of so-called Unknown and/or Underappreciated (UU) risks
- UU risks live outside the model due to:
  - Model incompleteness
  - Being outside the scope of the model
  - Violating the model assumptions
  - Remaining latent in the system until revealed by operational failures, precursor analysis, etc.
  - Tending to be most significant early in the system life cycle
  - Disproportionally reflecting complex intra-system and environmental interactions

How Significant is the Gap?



UU scenarios have historically represented a significant fraction of actual risk, especially for new systems

Launch System Reliability Trends

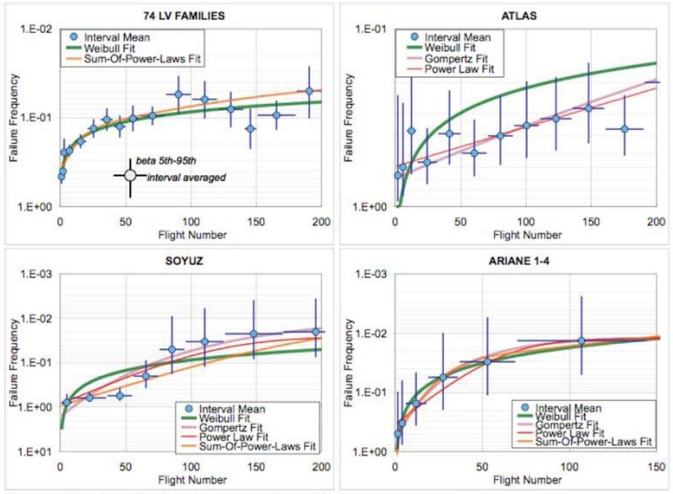
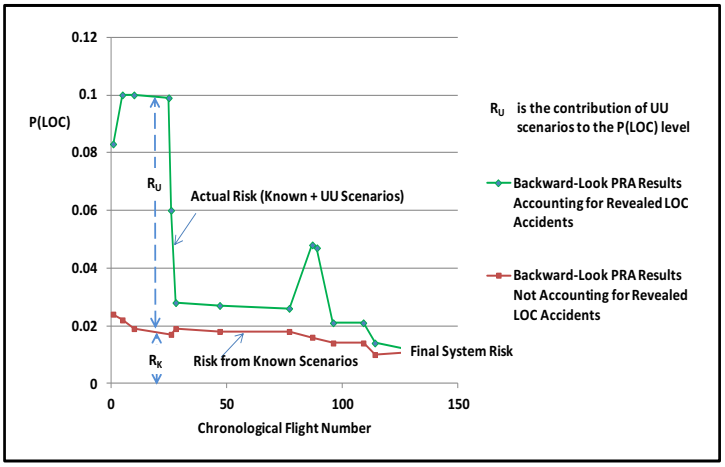


Figure 3. Model matches to selected examples of historical growth curves

Source: *Morse et al., "Modeling Launch Vehicle Reliability Growth as Defect Elimination," AIAA Space Conference and Exhibition (2010).*

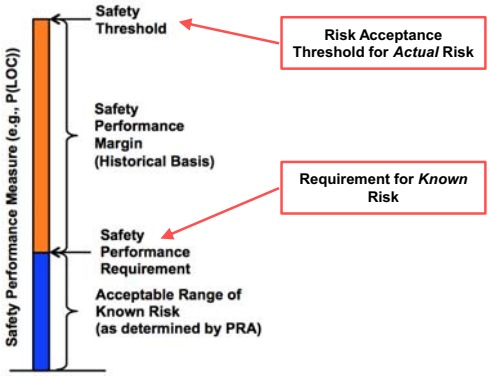
Results of Retrospective Analysis on Shuttle Risk



Source: *Shuttle Risk Progression: Use of the Shuttle Probabilistic Risk Assessment (PRA) to Show Reliability Growth, Teri L Hamlin et al. (AIAA, 2010) (downloadable from http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110004917_2011004008.pdf)*

Accounting for Unknown/Underappreciated Risks

- Aerospace Safety Advisory Panel (ASAP) and others have identified the need to consider the gap between *known* risk and *actual* risk when applying NASA safety thresholds and goals
- We use the concept of safety performance margin to account for UU risks
  - Based on historical discrepancies between initially-calculated and eventually-demonstrated safety performance
  - Provides a rational basis for deriving probabilistic requirements on known risk



The Case for the "Risk-informed Safety Case"

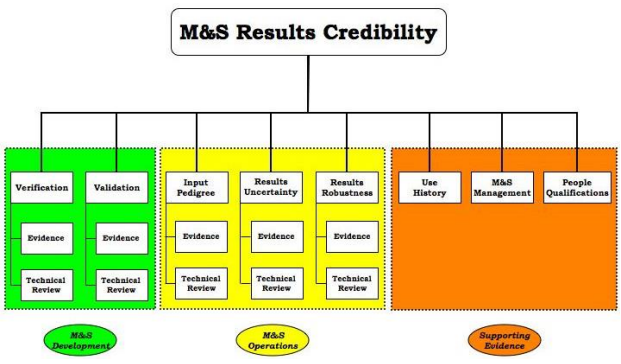
- Informed risk acceptance decision making must go beyond the model to be adequately risk-informed
- The "case" that the system risk is within the safety threshold must be made by a coherently-stated argument with supporting evidence – hence a "Risk-Informed Safety Case (RISC)"
  - Substantiation that UU risks (UU uncertainties) are adequately managed via application of best practices and a defense-in-depth philosophy to:
    - Minimize the presence of UU scenarios (e.g., via margin, programmatic commitments)
    - Maximize discovery of UU hazards (e.g., via testing, liberal instrumentation, monitoring, and trending, anomaly investigation, Precursor Analysis, use of best safety analysis techniques)
    - Provide broad-coverage safety features (e.g., abort capability, safe haven, rescue)
  - Substantiation that the known risk (calculated by PRA) is within the specified safety performance requirement
    - Known risks are managed by applying controls that are designed to mitigate identified adverse scenarios
- The RISC is the totality of the "uncertainty story" about the "actual" safety performance of the system
  - presented and defended by the provider at key decision points
  - provides the DM with a rational basis for identifying assurance deficits (inadequacies in the evidentiary support of the safety claims)
  - involves serious consideration of things that live outside traditional risk models (e.g., organizational and management factors)

Unknown / Underappreciated

Known

The Model as Evidence

- The risk model counts as (major) evidence in the case.
- But how good is it? To what extent can the DM rely on it?
- NASA-STD-7009, Standard for Models and Simulation (M&S) presents a framework for assessing the credibility of models and simulations in the context of the uses to which they are put
- The credibility assessment is presented with the model and model results, as an integral part of the case



Summary

- **In general:**
  - When a system is being acquired or licensed, someone (acquirer, licensing authority) is making a risk-acceptance decision…
    - Potentially affecting a range of stakeholders (public, workers, …) in different ways (safety, performance, cost, schedule …)
  - The decision is informed by some combination of modeling, analysis, *experience with the subject system, experience with related technology, and, in some cases, a sense of the provider's (or the applicant's) capability*
  - The responsible decision-maker has to have a sense of the uncertainties affecting the decision, *including the limitations of the model*
- **At NASA:**
  - The challenge is to execute high-stakes, first-of-a-kind missions that are subject to significant uncertainty in all domains (safety, performance, cost, schedule)
  - As in other complex, high-stakes undertakings, modeling is a vital ingredient in the development process
  - But responsible risk-acceptance decision-making requires the decision-maker to think beyond the model