Overview of NASA's System Safety Approach in the Context of Risk-informed Decision Making

Presented at the Trilateral Safety and Mission Assurance Conference

Noordwijk, The Netherlands

April 14-16, 2008

Homayoon Dezfuli, Ph.D.
Manager, System Safety, Office of Safety and Mission Assurance
NASA Headquarters
hdezfuli@nasa.gov

Background

- In July 2006, NASA issued NASA Procedural Requirement (NPR) 8715.3A "NASA General Safety Program Requirements"
- The requirements for system safety were revised significantly
- The changes were introduced to improve the conduct of system safety technical processes
- The new system safety requirements advocate a proactive, analytic-deliberative, risk-informed approach to safety to enable the integration of system safety activities with Systems engineering and risk management processes

Traditional Approach vs. Risk-based Approach to Safety

Traditional "Deterministic" Approaches

- Traditional safety metrics (e.g., safety margin, failure tolerance)
- Conservatism in hazard and risk analysis (worst case consequence)
- Probabilities are not quantified
- Special attention to identification of hazard causes
- <u>Incomplete</u>

Risk-based Approaches

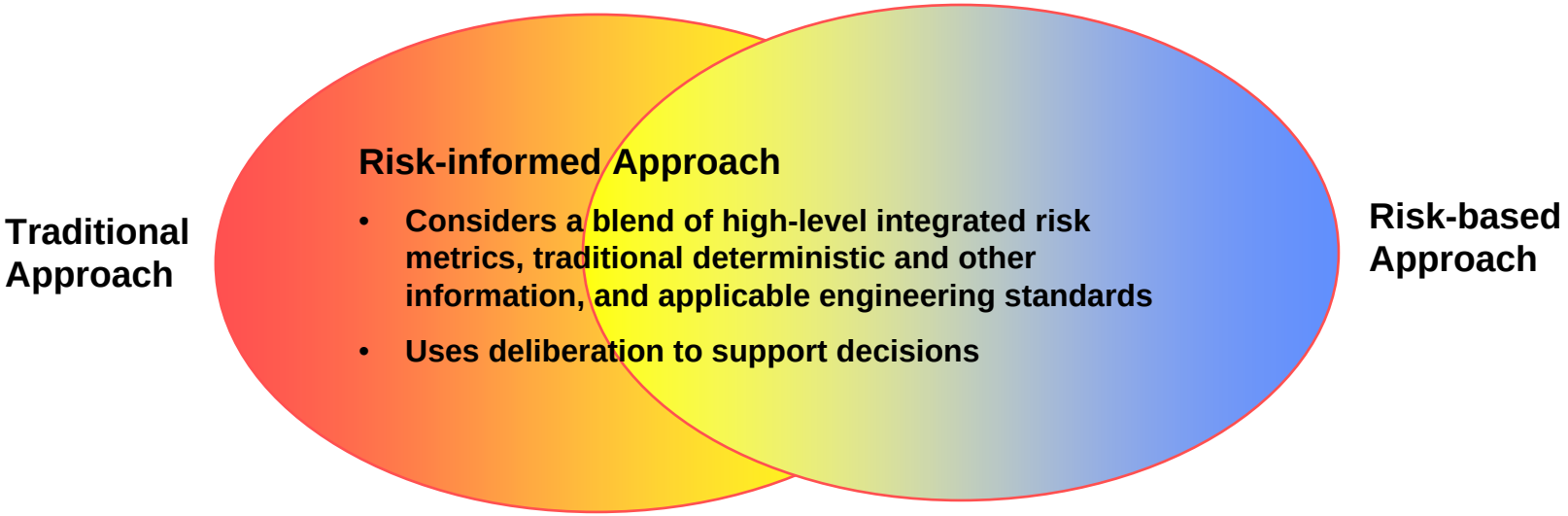
- High-level integrated risk metrics (e.g., probability of loss of crew)
- Advocate realism in hazard and risk analysis (scenario-based modeling)
- Probabilities and uncertainties are quantified
- Special attention to characterization of uncertainties
- <u>Incomplete</u>

Both approaches assume engineering standards are being met

- Analysis is often hardware-centric
- Uncertainties are not acknowledged
- Interactions among hazards and controls are not systematically analyzed

- Is the scenario list complete?
- Are the models used reasonable?
- Are the value of parameters used in the models reasonable?

Risk-informed Approach to Safety



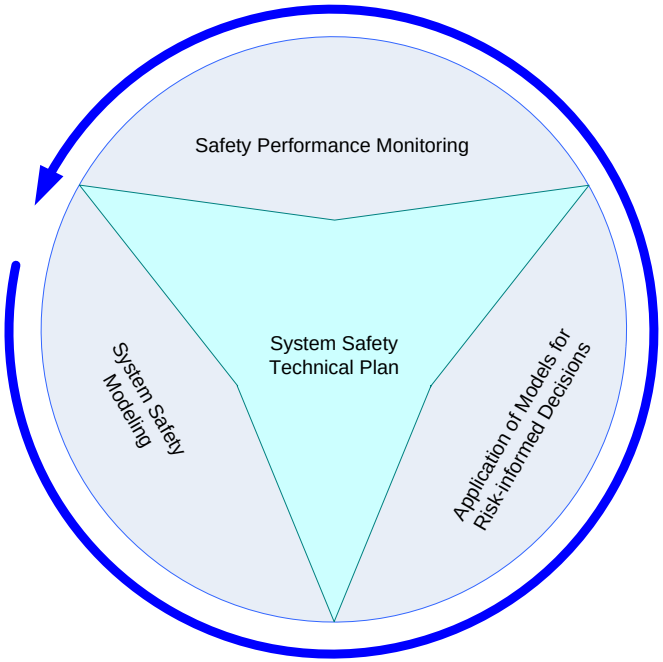
- **Decision making is risk-*informed*, not *risk-based***
- **Traditional and modern safety and risk analysis (e.g., Probabilistic Risk assessment) should complement each other**

Highlights of NASA's System Safety Approach

System Safety Lexicon Issues

- **Clarifying what is "system safety?"**
  - **Is a technical discipline -- a multidisciplinary engineering function**
  - **Involves modeling and analysis -- inclusive of the Hazard Analysis and Probabilistic Risk Assessment (PRA)**
  - **Supports design and operational decisions -- must be continuously active throughout the lifecycle of the system**
- **Providing *operational* definitions for some key terms such as**
  - **Hazard**
  - **Safety**
  - **Risk**
  - **Risk-informed**
  - **Risk-based**
  - **Uncertainty**
  - **Risk Scenario**
  - **Performance Measure**

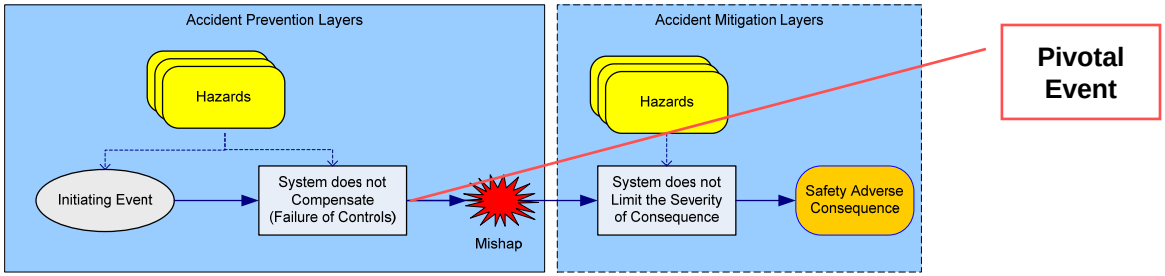
Key Attributes of the System Safety Approach



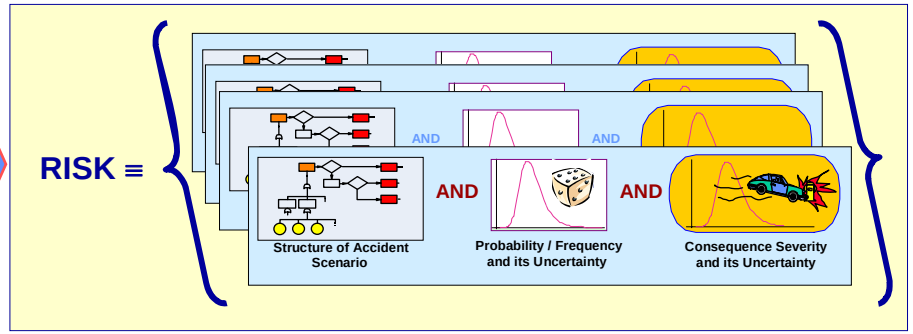
Source: NPR 8715.3

- **Uses graded approach to system safety modeling**
  - **Use qualitative and quantitative risk analysis techniques in a complementary fashion**
- **Adopts scenario-based hazard analysis (HA)**
  - **Recognition and characterization of uncertainties**
  - **Quantification of aggregate risks**
- **Informs systems engineering (SE) and risk management (RM) decisions**
  - **Treatment of safety-related aggregate risks as performance measures (PMs)**
  - **Consideration of safety PMs within the trade space to support design and operational decisions**
  - **Monitoring safety performance**

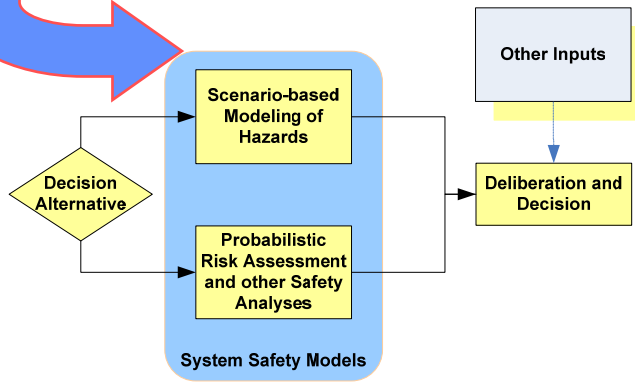
Key Attributes of the System Safety Approach (cont.)



Scenario-based Approach for Hazard Analysis



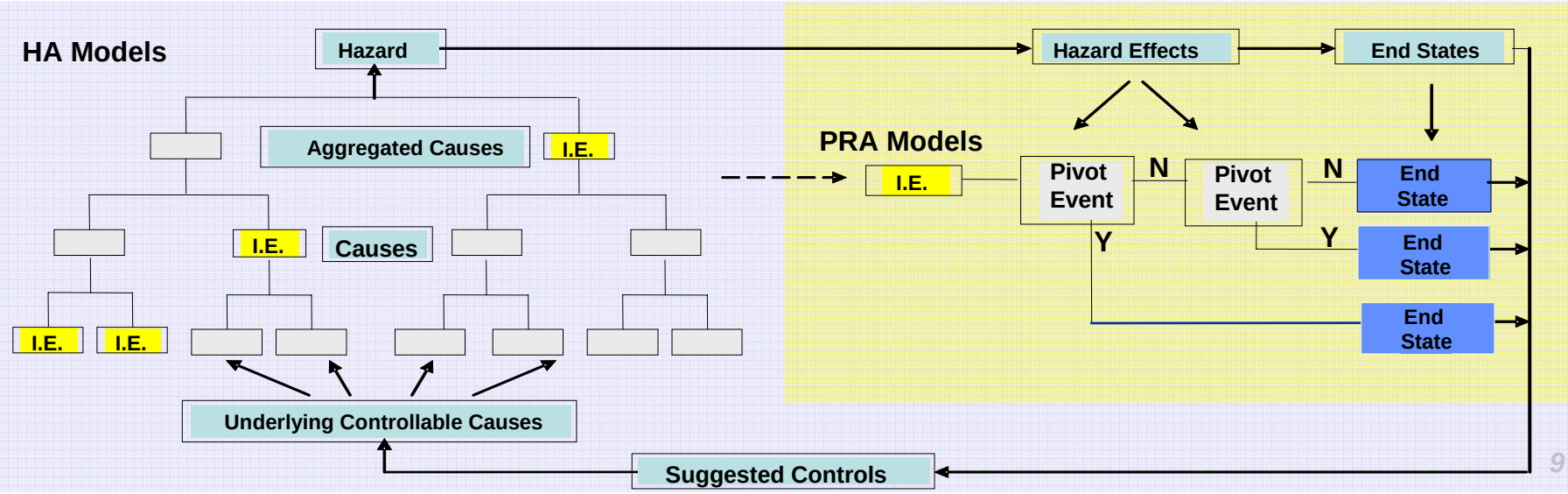
Model-based Assessment of Risk and Uncertainties



Risk-informed Decision Making

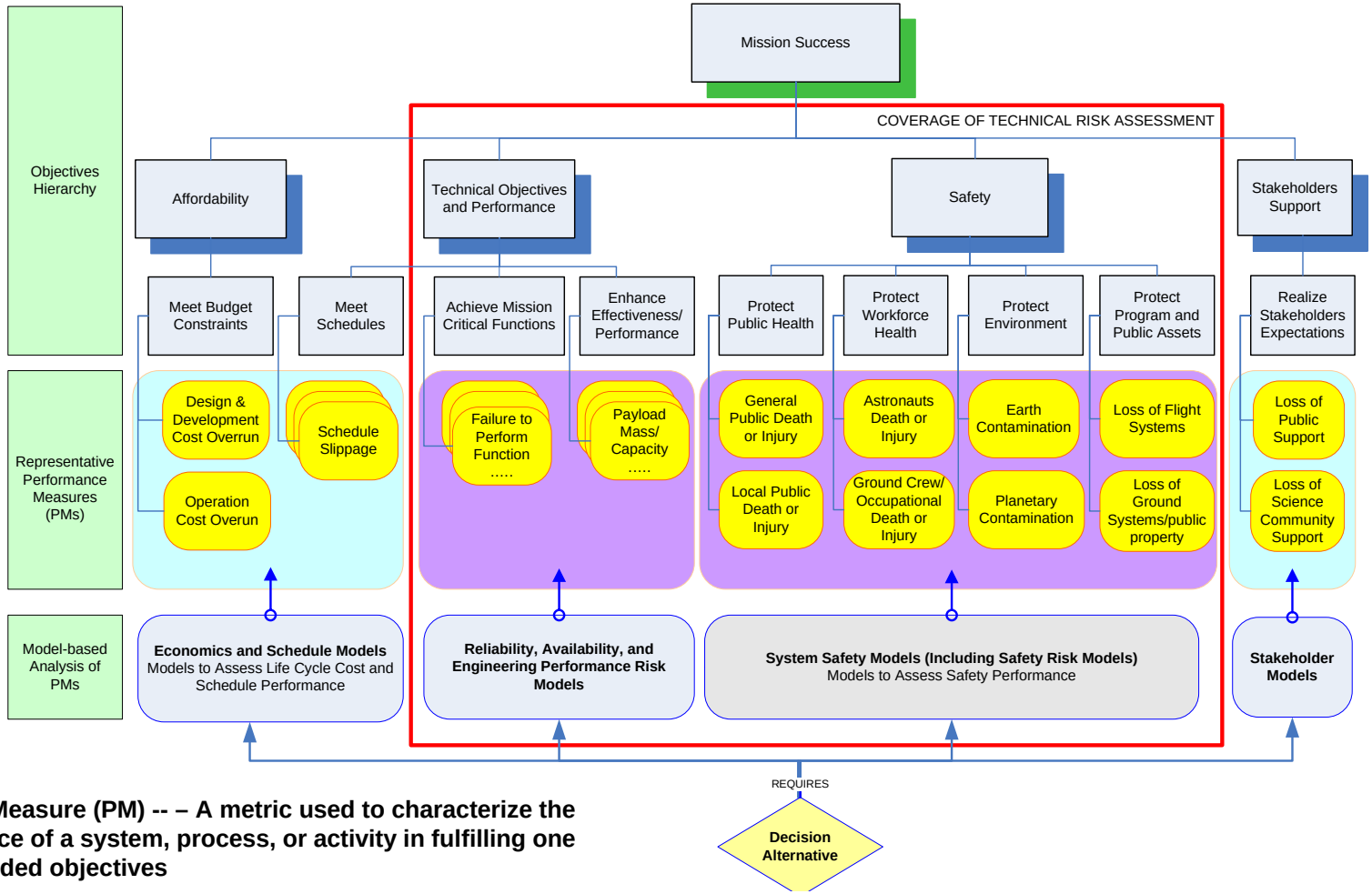
Integration of Hazard Analyses with Probabilistic Risk Assessments

- HAs provide PRAs with initiating events (I.E.), pivot events, and end states
- HAs provide a priority ranking of scenarios based on mostly qualitative factors
- PRAs provide detailed quantitative analysis (including uncertainty) of the high priority scenarios
- Quantitative results for decisions on how to add, change, or enhance controls
- Iteration occurs if needed to account for new or modified controls



Source: NASA System Safety Training Modules (under development by ARES)

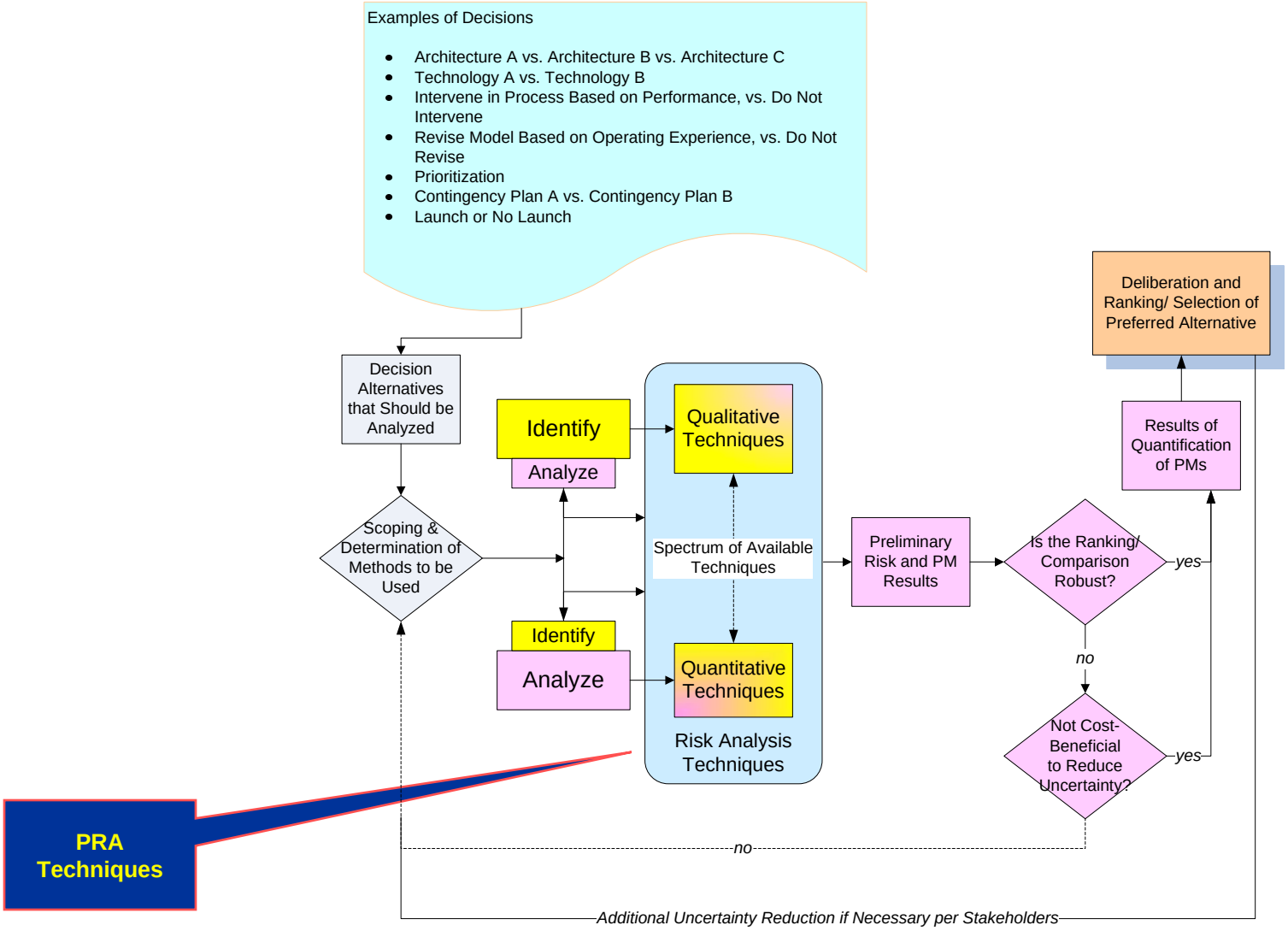
The Role of System Safety Models and Other Models in Trade Studies to Support Decisions



Performance Measure (PM) -- – A metric used to characterize the performance of a system, process, or activity in fulfilling one of its intended objectives

- **Technical performance (e.g., thrust or output)**
- **Mission performance (amount of observational data acquired)**
- **Safety performance (probability of crew injury)**
- **Cost performance (amount of cost overrun), and so on**

Risk Analysis of Decision Alternatives



Example: Performance Measures used in NASA's Exploration Systems Architecture Study (ESAS)

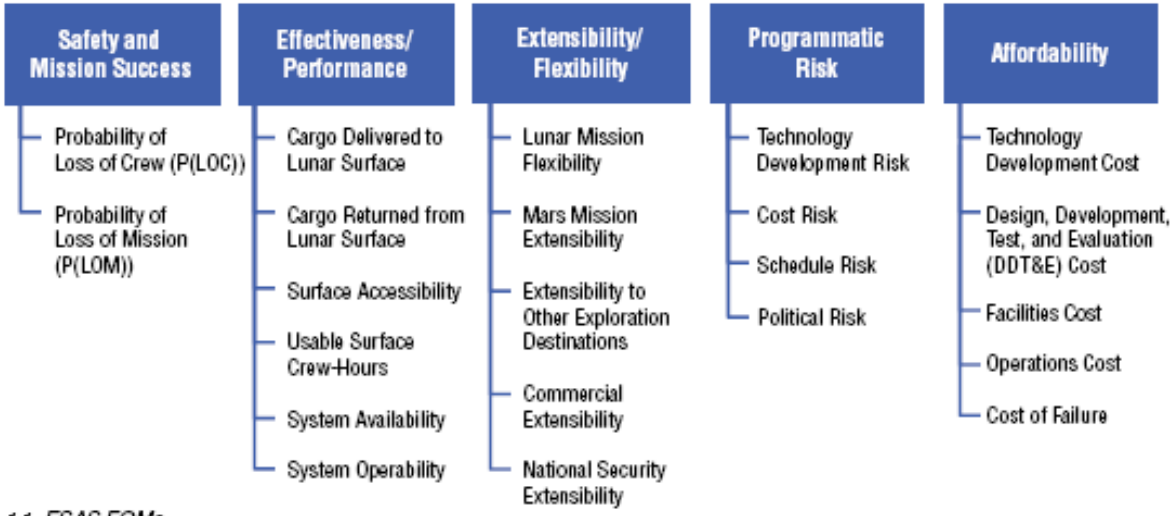


Figure 1-1. ESAS FOMs

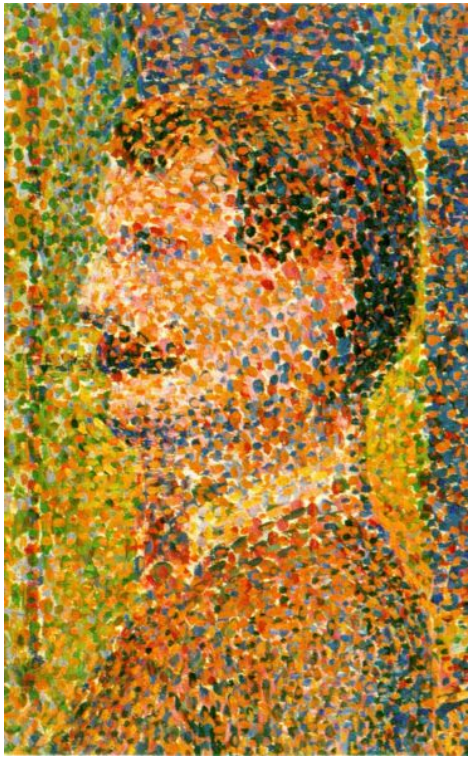
In ESAS study, the performance measures were referred to as "Figures of Merit (FOMs)"

The various trade studies conducted by the ESAS team used a common set of FOMs for evaluation. Each option was quantitatively or qualitatively assessed against the FOMs shown in **Figure 1-1**. FOMs are included in the areas of: safety and mission success, effectiveness and performance, extensibility and flexibility, programmatic risk, and affordability. FOMs were selected to be as mutually independent and measurable as possible. Definitions of each of these FOMs are provided in **Appendix 2D, ESAS FOM Definitions**, together with a list of measurable proxy variables and drivers used to evaluate the impacts of trade study options against the individual FOMs.

Source: ESAS Report

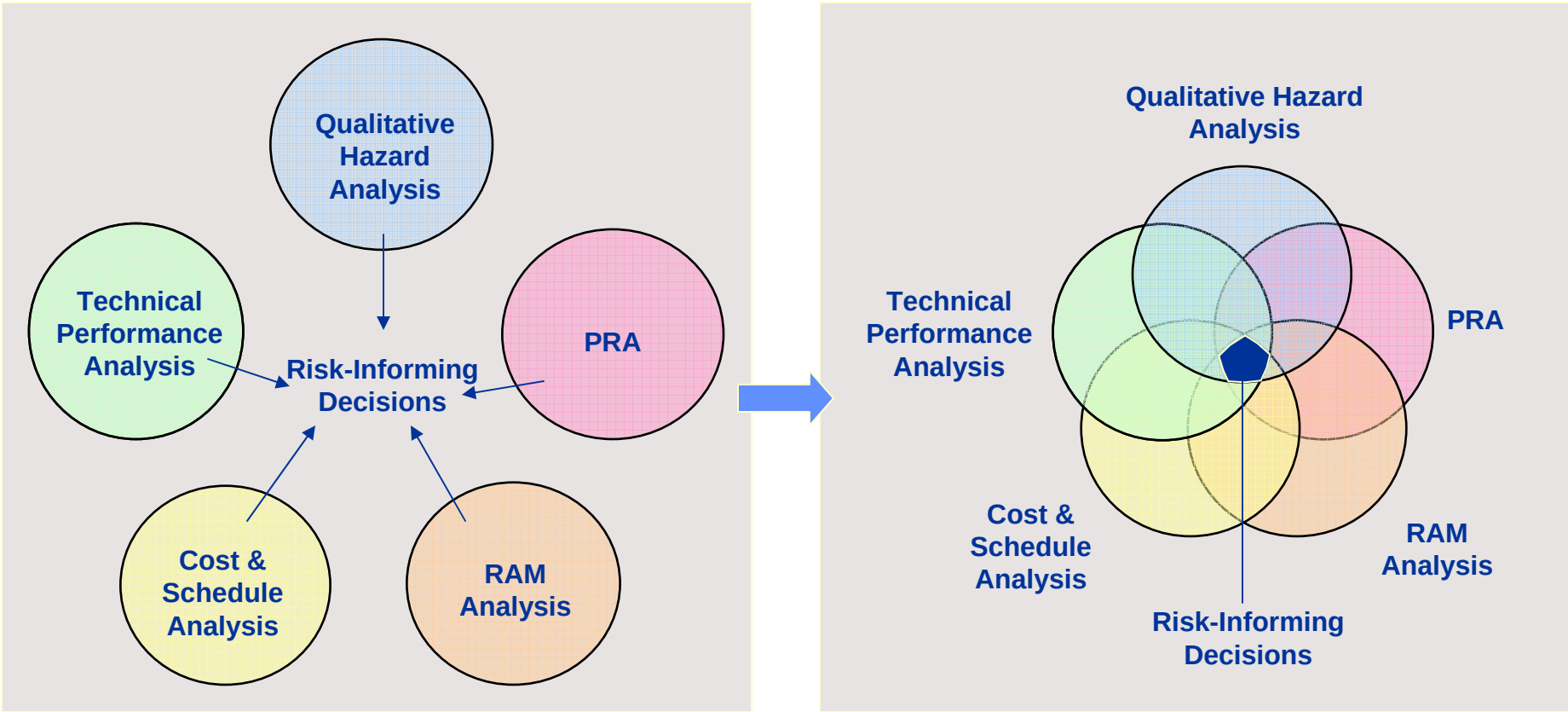
The Path From Pointillistic Safety Modeling to Integrated Safety Modeling

Need for a coherent *safety* picture, as opposed to a pointillistic portrayal of hazards and controls



Pointillism is a style of painting in which small distinct points of primary colors create the impression of a wide selection of secondary colors

The Path from Fission to Fusion



PRA: Probabilistic Risk Assessment

RAM: Reliability and Maintainability

Source: NASA System Safety Training Modules (under development by ARES)

Summary

- **The system safety approach at NASA is risk-informed and based on analytic-deliberative decision making methodology**
- **It is designed to integrate system safety modeling activities with systems engineering and risk management processes in an analytical framework**
- **The analytic nature of the methodology promotes model-based analysis of hazards and their associated risks and explicit treatment of uncertainties**
- **The deliberative aspect of the approach allows the consideration of deterministic and other information**