



Safety is the cornerstone upon which we build mission success.

Integrating Quantitative Risk Assessment into System Safety to Support Decision- making

NASA Risk Management Conference 2004

October 26, 2004

Homayoon Dezfuli, Ph.D., Manager of System Safety, OSMA, NASA HQ
hdezfuli@nasa.gov (202) 358-2174

William Vesely, Ph.D., Manager of Risk Assessment, OSMA, NASA HQ
william.e.vesely@nasa.gov (202) 358-1556



Safety is the cornerstone upon which we build mission success.

Introduction

- **In this presentation, several enhancements to system safety practices at NASA are discussed:**
 - **Carry out more effective assessments**
 - Better orient system safety analyses toward mission objectives
 - Use more quantitatively-based safety analysis techniques
 - Better integrate risk assessments into safety analyses
 - **Communicate more effectively**
 - Roll-up the results to help the decision-makers evaluate the implications of safety findings
 - Explicitly resolve the uncertainties in the analyses
 - **Enhance the decision-making process**
 - Better identify the factors and values entering in the decision
 - Expand the coordination and collaboration with other stakeholders



Safety is the cornerstone upon which we build mission success.

Principal Objective of System Safety (NPR 8715.3)

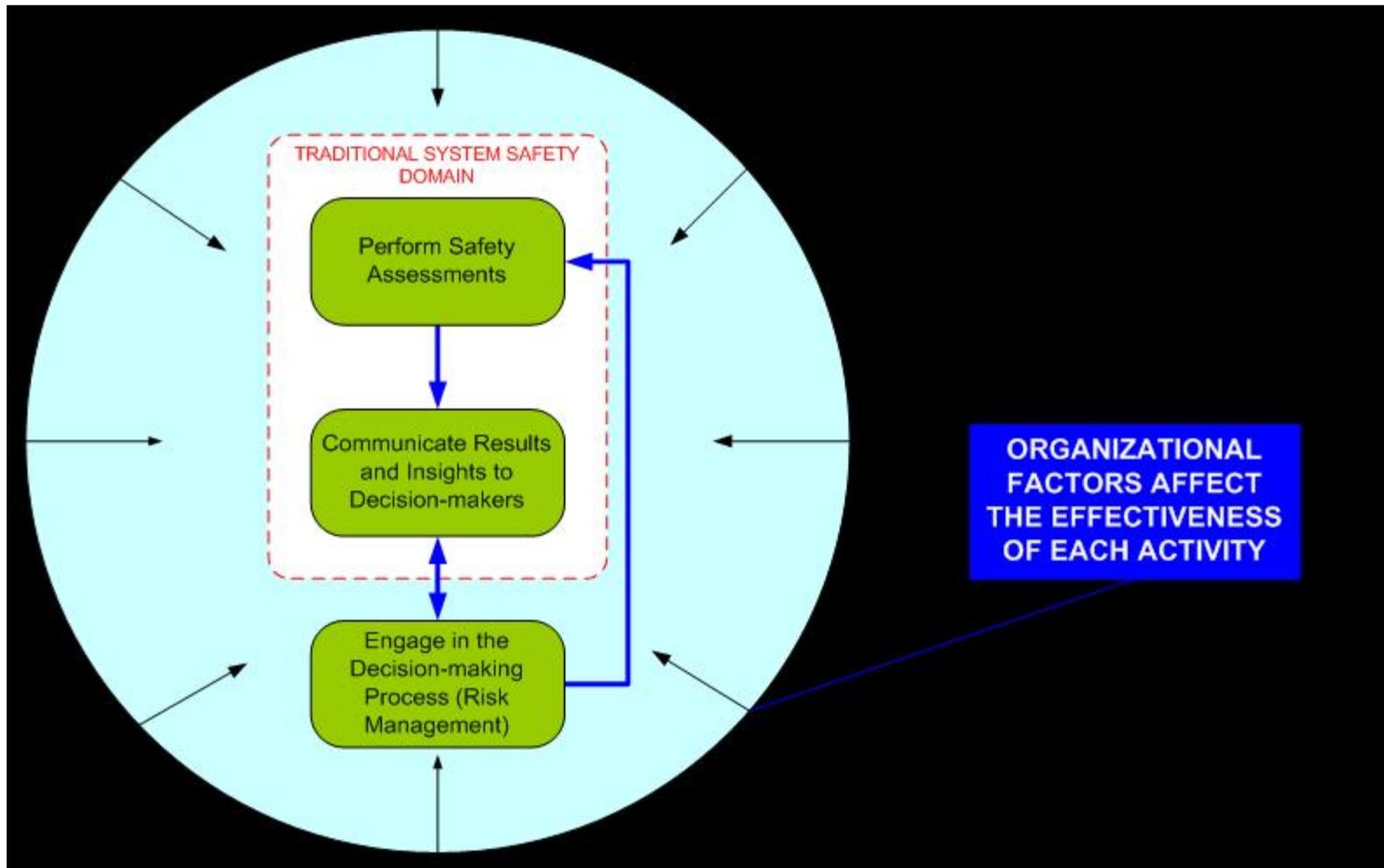
The principal objective of a system safety activity is to provide for an organized, disciplined approach to the early identification and resolution of risks impacting personnel, hardware, or mission success to a level that is as low as reasonably achievable.





Safety is the cornerstone upon which we build mission success.

Key Activities of the System Safety Process





Safety is the cornerstone upon which we build mission success.

MORE EFFECTIVE ASSESSMENTS



Safety is the cornerstone upon which we build mission success.

Orienting System Safety Assessments Toward Mission Safety

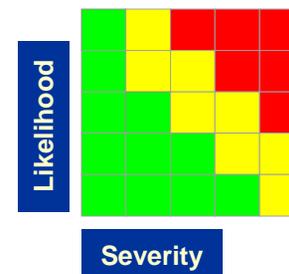
- **A mission-oriented approach to system safety should be employed**
 - **Provides focus for safety assessments**
 - Steers safety assessments toward the fundamental objectives of the mission (big picture)
 - Eliminates stove-piped safety assessments
 - **Promotes integration and coordination of safety assessments**
 - Captures systems interactions in safety assessments
 - Promotes integration of safety assessments with other assessments
 - Cost
 - Schedule
 - **Fosters better communication of safety issues**
 - Helps the decision-makers to appreciate the significance of safety issues in terms of the big picture



Safety is the cornerstone upon which we build mission success.

Traditional System Safety Assessment Techniques

- Analyst postulates a failure or a deviation and assesses its consequences
 - Typically one failure or deviation is analyzed at a time
- Analyst qualitatively judges how often a failure or deviation can occur
- Analyst qualitatively judges the severity of the outcome or assumes the worst-case outcome
- Instead of systematically quantifying risk, analyst maps each analyzed failure into one of three risk categories (**Green**, **Yellow**, **Red**)

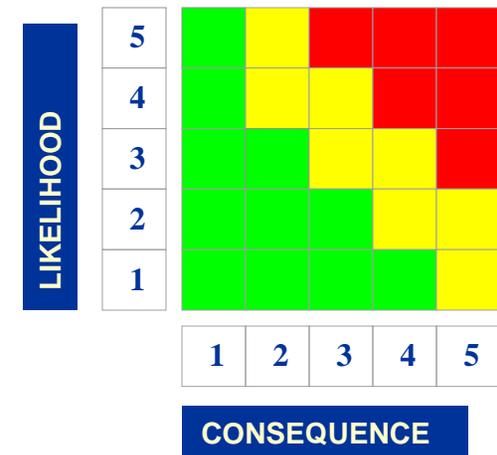




Safety is the cornerstone upon which we build mission success.

Limitations of Traditional Risk Analyses

- Uses bottom-up modeling approach
- Failure dependencies are not modeled and evaluated
- Completeness of all important potential accident scenarios cannot be achieved
- Ambiguity in the consequence and likelihood scales arises
- Without a more quantitative scale foundations, risks end up inappropriately lumped up in bins
- Having one consequence scale is not applicable to all projects and may change from project to project
- Risk matrix is unsuitable for combining risks to obtain aggregate risk
- Risk matrix cannot handle more than one risk item at a time
- Risk matrix cannot identify risk priorities
- Uncertainties are not formally accounted for



Legend:

- 1 – very low
- 2 – low
- 3 – moderate
- 4 – high
- 5 – very high



Safety is the cornerstone upon which we build mission success.

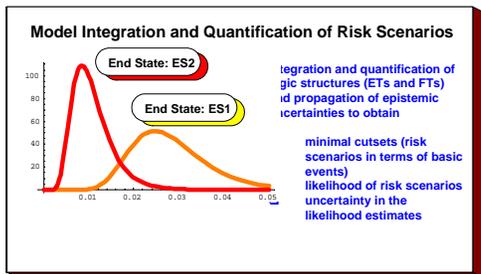
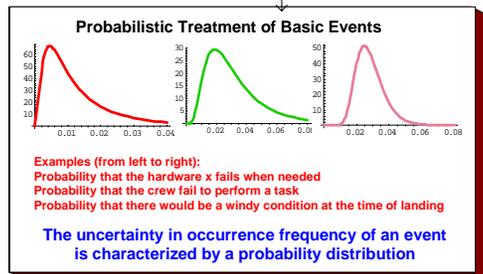
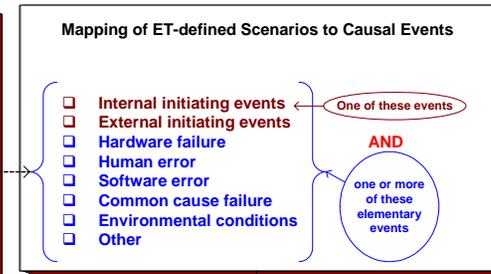
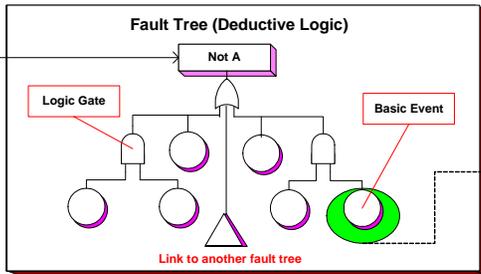
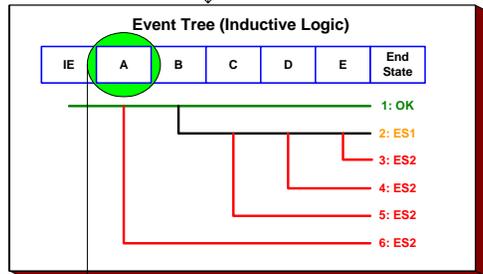
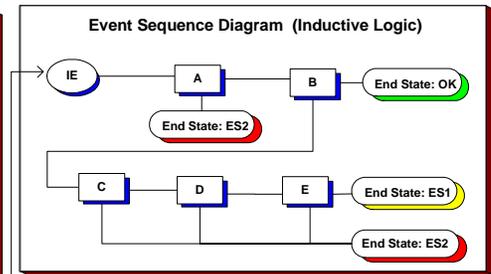
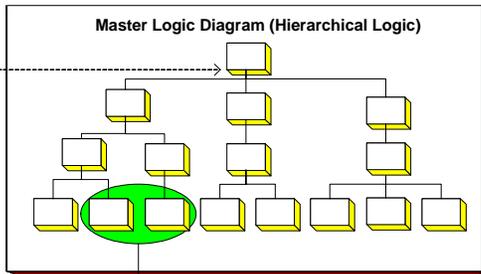
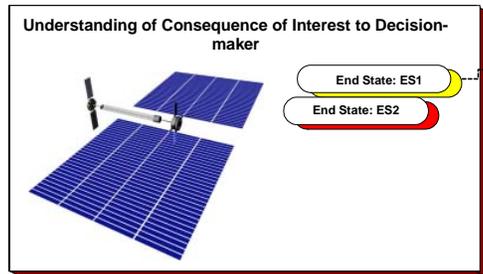
Incorporation of more Quantitative Techniques into Traditional System Assessments

- **Quantitative risk assessment (QRA) should be used whenever possible to complement qualitative assessment of hazards.**
 - Traditional system safety analyses (hazard analysis, fault tree analysis, and FMEA) are to be integrated into a coherent assessment process
- **Quantitative Risk Assessment has been shown to be a useful tool to quantify risk metrics relating to the likelihood and severity of events adverse to safety or mission success**
 - Identifies a complete set of credible system failure modes
 - Captures interactions between events/systems/crews in an integrated modeling framework
 - Quantifies uncertainties and identifies what the system safety analysts know or do not know
 - Facilitates decision-making by identifying the dominant risk contributors, so that risk management decisions are targeted toward risk significant hazards



Safety is the cornerstone upon which we build mission success.

Quantitative Risk Assessment Process



- Communicating Risk Results and Insights to Decision-maker**
- Displaying the results in tabular and graphical forms
 - Ranking of risk scenarios
 - Ranking of individual events (e.g., hardware failure, human errors, etc.)
 - Insights into how various systems interact
 - Tabulation of all the assumptions
 - Identification of key parameters that greatly influence the results
 - Presenting results of sensitivity studies
 - Proposing candidate mitigation strategies



Safety is the cornerstone upon which we build mission success.

Limitations of QRA

- **Human reliability modeling is still evolving**
- **Software failures are only partially modeled**
- **Design errors are modeled only in specific scenarios**
- **Influence of safety culture is not modeled**
 - Reliance on updating of models to reflect new information
- **Estimated probabilities and consequences can have larger uncertainties**
 - Uncertainties are assessed and quantified, which is a benefit
 - Relative risk contributors generally are most accurately resolved



Safety is the cornerstone upon which we build mission success.

QRA Quality

- **QRA is ambitious: It models the whole system including hardware failures, human performance, software, and relevant physical phenomena**
- **QRA results and insights are input to a decision-making process**
- **Defining an acceptable QRA for a specific application a priori requires knowledge of QRA capabilities/powers and knowledge of the problem**
- **Peer review is an essential part of QRA**



Safety is the cornerstone upon which we build mission success.

EFFECTIVE COMMUNICATION



Safety is the cornerstone upon which we build mission success.

Need for Effective Communication of Safety Issues

- **Risk communication provides the link between system safety assessments and risk management**
 - The analyst should clearly identify what he/she knows or does not know
 - a very clear and concise tabulation of all known limitations and constraints associated with the assessment
 - identification of key assumptions that greatly influence the results of the assessment
 - The analyst should always present results in the context of the big picture (i.e., mission objectives)
- **Credibility is the key for influencing the decision-makers**
 - A clear assessment of uncertainties and their impacts



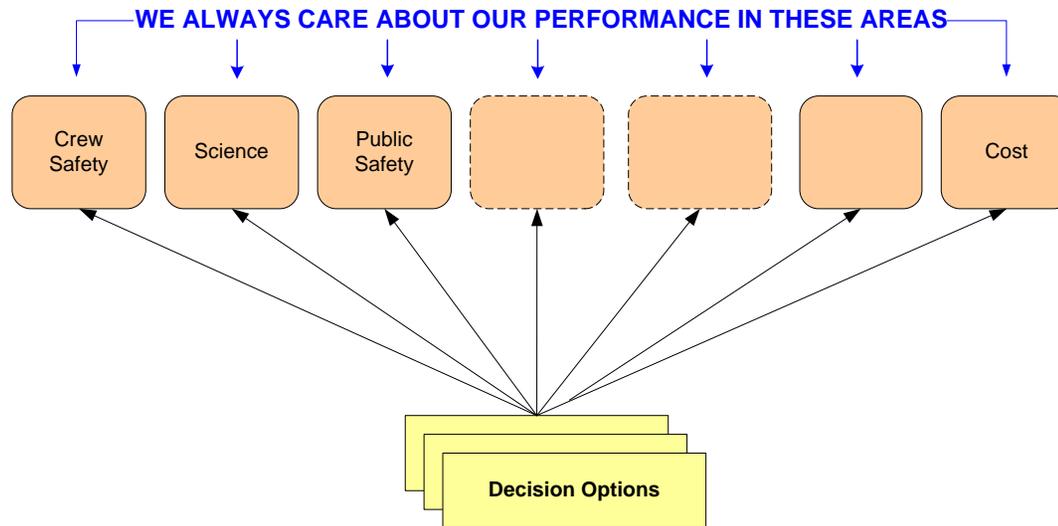
Safety is the cornerstone upon which we build mission success.

ENGAGEMENT IN DECISION- MAKING



Safety is the cornerstone upon which we build mission success.

Our Decisions Influence and are Influenced by Many Factors



Decision situations

- Designing new systems.
- Making changes to existing systems.
- Extending the life of existing systems.
- Changing requirements.
- Responding to mishaps in real time.
- Allocating resources.
- Initiating research programs to reduce uncertainty.
- Other



Safety is the cornerstone upon which we build mission success.

NASA is Moving to a Risk-informed Decision-making Environment

- **NASA's 2003 Strategic Plan States:**

“Decision-making in the face of uncertainties that affect cost, schedule, and technical parameters demands that our managers understand the impact of trade-offs on the potential for program success. Our managers must have the information and training they need to make well-informed decisions, and our stakeholders must be able to see how we arrive at key missions decisions. We must develop modern tools for cost and risk analysis.” Page A-3: Implementation Strategy 5

- **Incorporating System Safety activities in a risk-informed decision-making framework is required according to the Agency's strategic plan**



Safety is the cornerstone upon which we build mission success.

Why Risk-Informed and not Risk-based Decision Making?

- Risk assessment by itself techniques does not account for everything of importance to the decision-maker
- Analytic/Deliberative Process:
 - Multi-attribute Analysis uses rigorous, replicable methods, evaluated under the agreed protocols of an expert community - such as those of disciplines in the natural, social, or decision sciences, as well as mathematics, logic, and law - to arrive at answers to factual questions.
 - Stakeholders Deliberation is any formal or informal process for communication and collective consideration of issues.

National Research Council, Understanding Risk, 1996



Safety is the cornerstone upon which we build mission success.

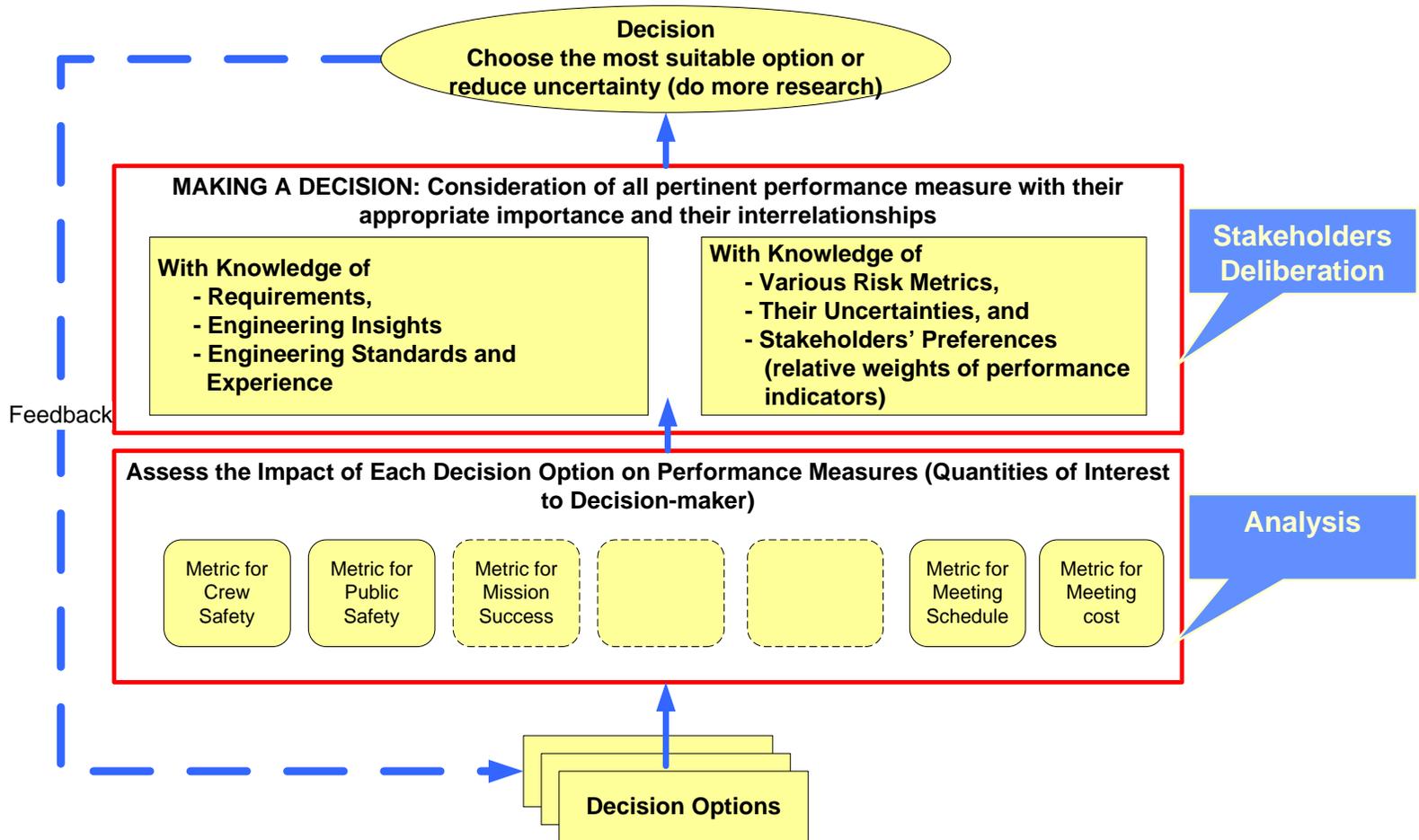
How Risk-informed Decision-making Works

- **Consequences of decision options are modeled in terms of the performance measures (PM) relating to the program fundamental objectives**
 - PMs are attributes or their surrogates that are measurable
 - Example: PM for crew safety can be the probability of loss of crew
 - Example: PM for ELV performance can include capability and reliability
- **Preferences (relative weights of key performance measures) are obtained from each stakeholder**
 - Incorporating the stakeholders' views into the decision-making process
- **Decision options are ranked according to their desirability**
 - Comparing the consequences of decision options on the PMs
- **The most suitable decision option is selected through deliberations amongst stakeholders**
 - Deliberation is any formal or informal process for communication and collective consideration of issues



Safety is the cornerstone upon which we build mission success.

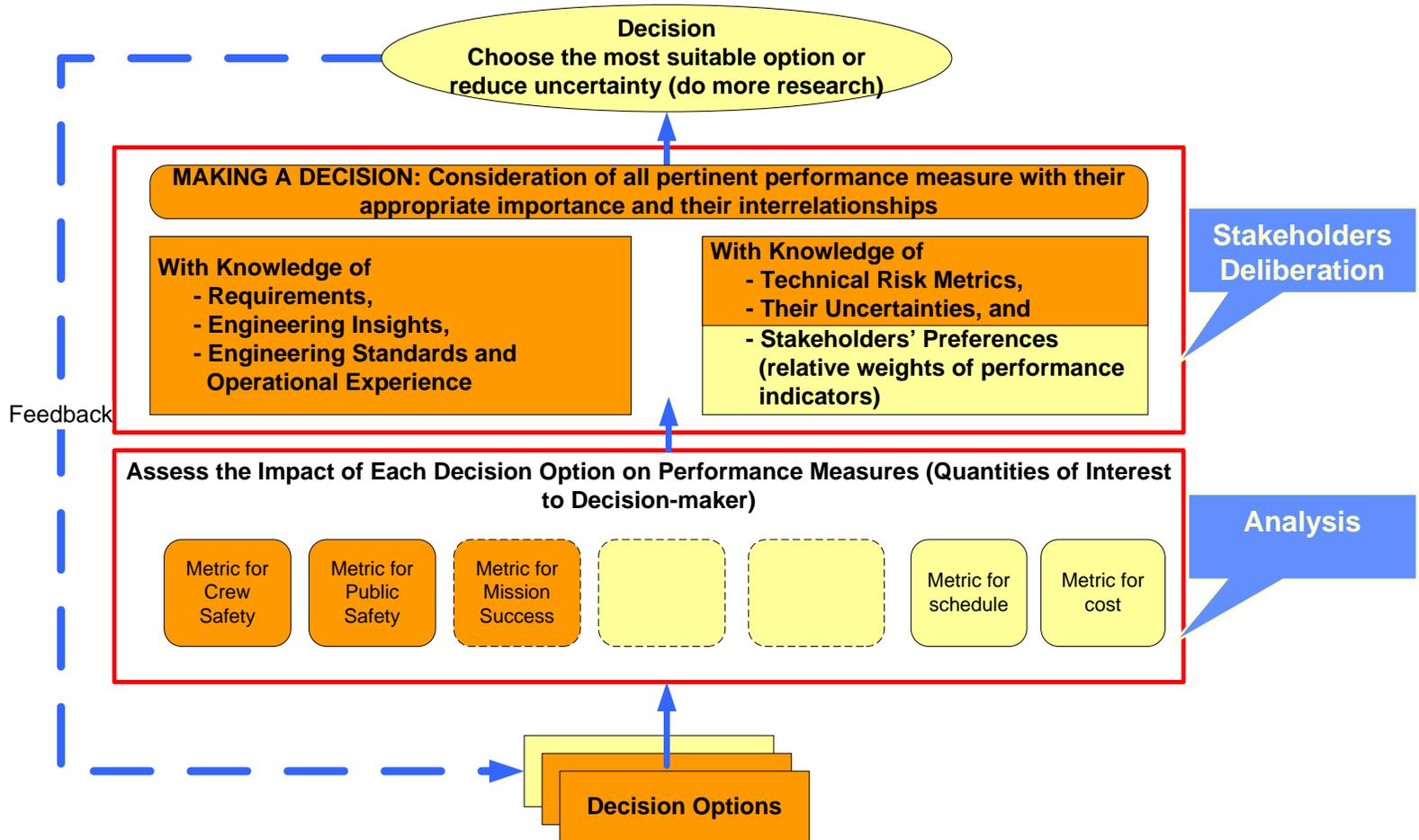
A Risk-informed Decision-making Framework





Safety is the cornerstone upon which we build mission success.

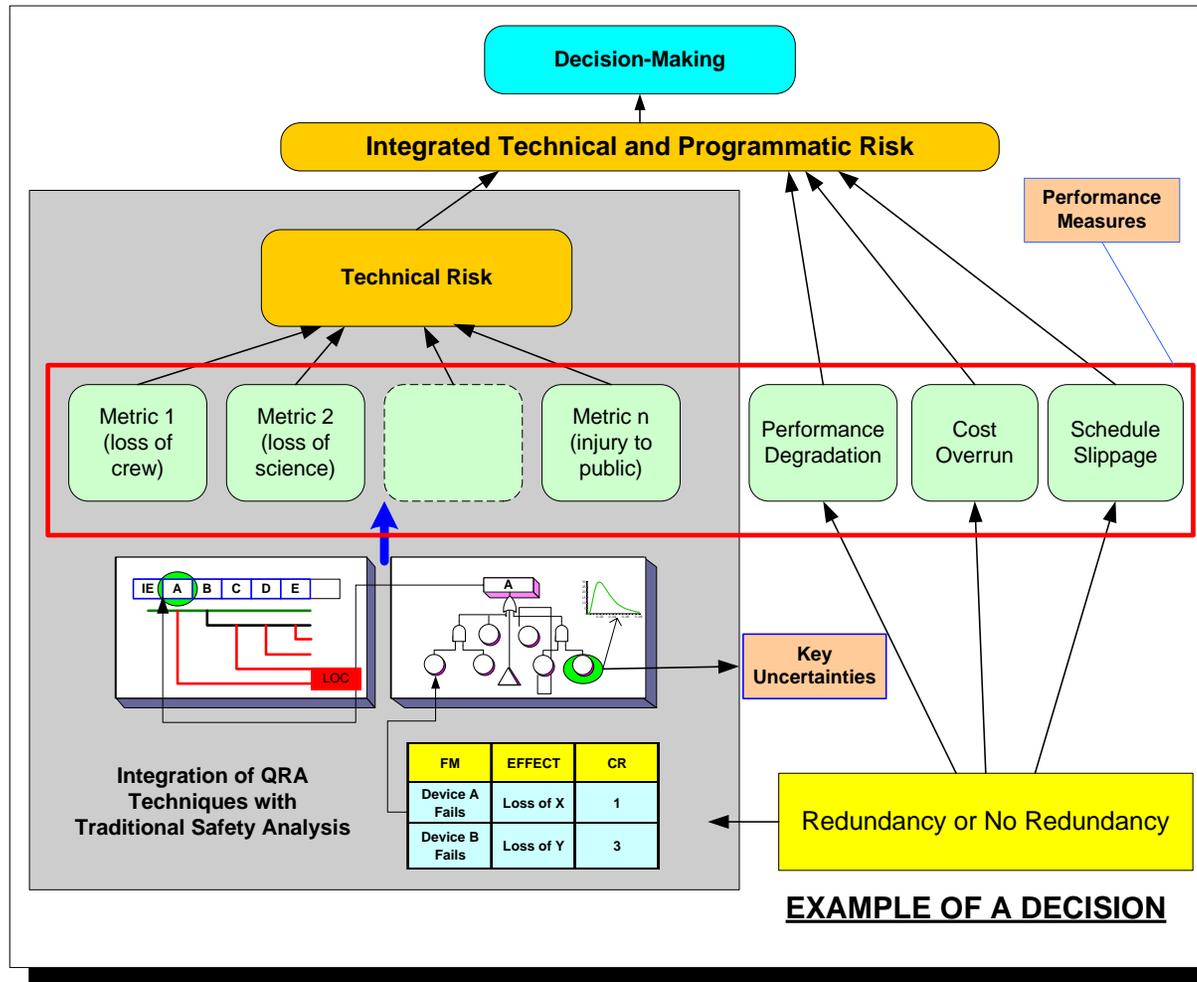
System Safety Involvement in Decision-making





Safety is the cornerstone upon which we build mission success.

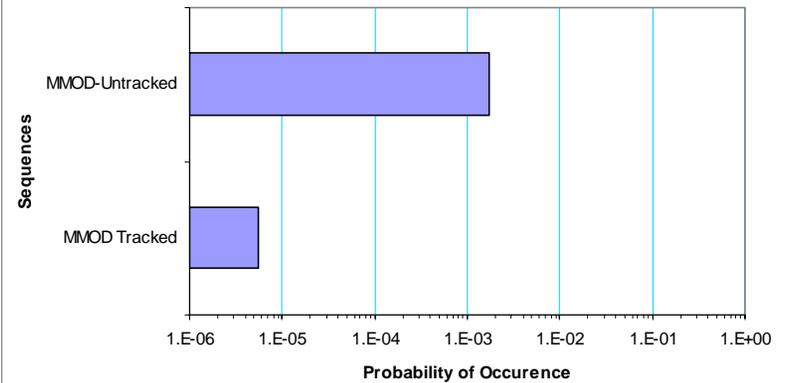
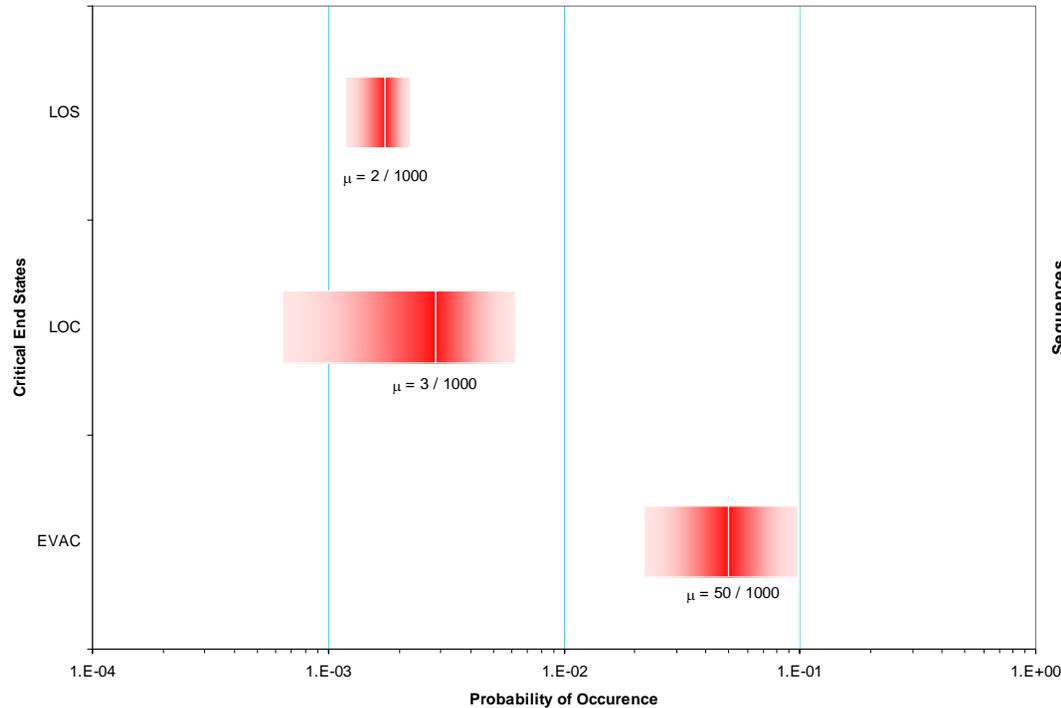
Integration of Quantitative Risk Assessment with Traditional System Safety Analyses





Safety is the cornerstone upon which we build mission success.

Representative QRA Results (International Space Station Probabilistic Risk Assessment; Phase II, Stage 7A)



LOS: Loss of Station
LOC: Loss of Crew
EVAC: Evacuation
MMOD: Micrometeoroids and Orbital Debris



Safety is the cornerstone upon which we build mission success.

In Summary, System Safety Analyses Can be Strengthened to Meet NASA's Goals

- **To better meet NASA's fundamental goal of "ensuring safety and mission success":**
 - We need to integrate system safety analysis and risk assessment
 - We need to better identify how each activity relates to the overall objective of ensuring safety and mission success
 - We need to better incorporate quantitative assessments into safety analysis to provide sounder risk assessments
 - We need to move toward risk-informed decision-making and we need to better engage all stakeholders in the decision process
- **We need to do this by working together to address these important areas**