New Thrust for Probabilistic Risk Assessment (PRA) at NASA

Risk Analysis for Aerospace Systems II: Mission Success Starts with Safety, Arlington, VA, October 28, 2002

Michael G. Stamatelatos, Ph.D.
Manager, Agency Risk Assessment Program
NASA Headquarters, OSMA
E-mail: mstamate@hq.nasa.gov
Phone: (202) 358-1668

Preamble: Risk Is Inevitable

It is impossible to win
the great prizes of life
without running risks

Theodore Roosevelt

Therefore, risk must be understood, assessed and managed

Definitions of Risk

- **Risk is the measure of the probability and severity of adverse effects.**

  Lowrance, Of Acceptable Risk

- **Risk is a set of triplets that answer the questions:**

  1) What can go wrong? (accident scenarios)

  2) How likely is it? (probabilities)

  3) What are the consequences? (adverse effects)

  Kaplan & Garrick, Risk Analysis, 1981

- **Risk is the probability that a project will experience undesirable consequences.**

  NASA-NPG: 7120.5A

Importance of Probability

It is remarkable that a science which began with the consideration of games of chance should become the most important object of human knowledge

Pierre Simon, Marquis de Laplace (1749-1827), in his book "Analytic Theory of Probabilities"

Risk is Two-Dimensional

Risk always involves the likelihood that an undesired event will occur.

Risk should consider the severity of consequence of the event, should it occur.

Qualitative or Quantitative

Qualitative or Quantitative

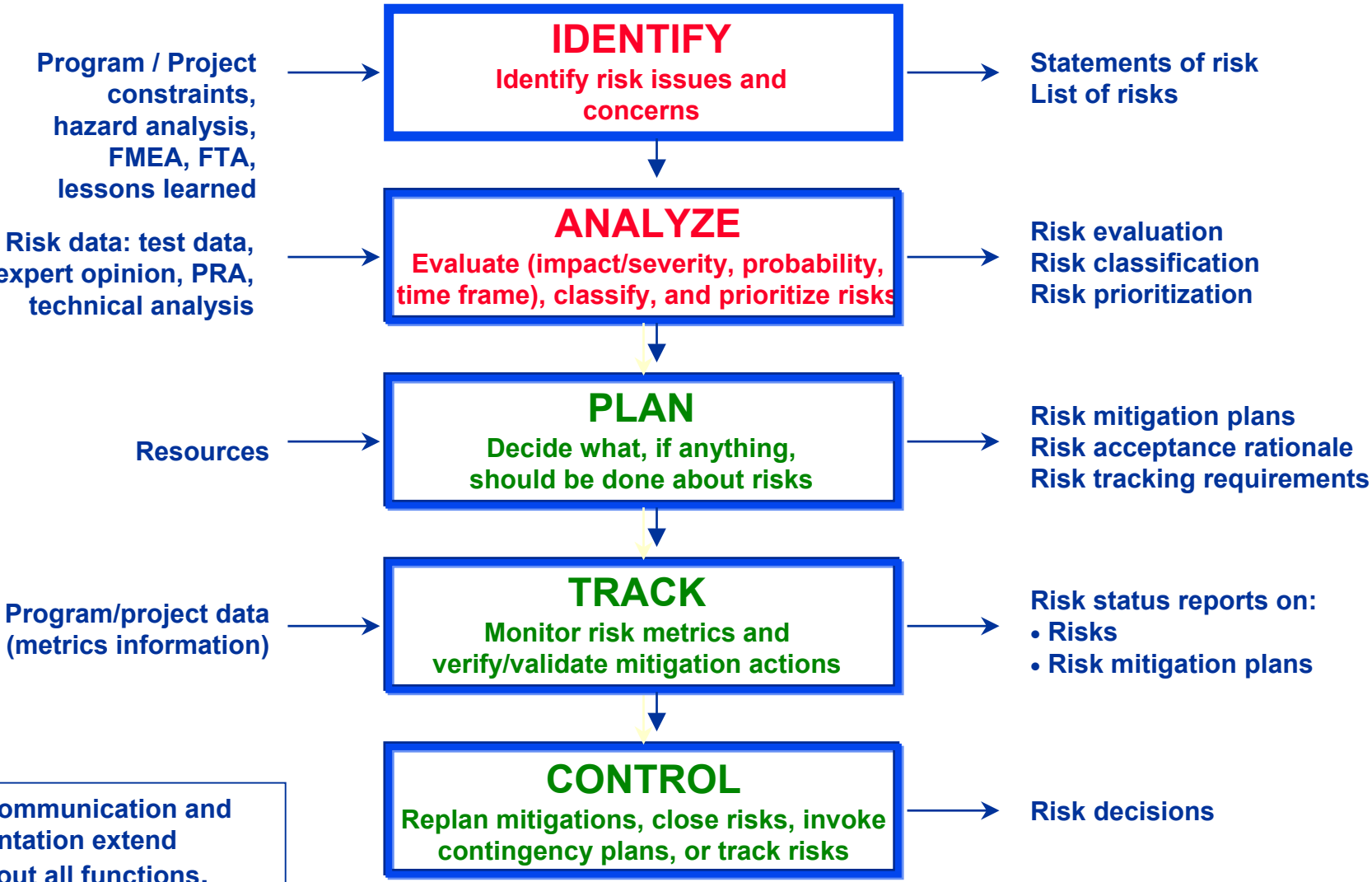
Risk = Likelihood and Severity

NASA Manages Risk on a Daily Basis

- As a technological pioneer, NASA has, explicitly or implicitly, evaluated, accepted and managed risks throughout its existence.

- Mission Success Starts with Safety of:
  - ✓ The public;
  - ✓ Astronauts and pilots;
  - ✓ NASA workforce; and
  - ✓ High-value equipment and property

NASA Risk Management Process



Note: Communication and documentation extend throughout all functions.

NASA Risk Management and Assessment Requirements

- **NPG 7120.5A, NASA Program and Project Management Processes and Requirements**
  - The program or project manager shall apply risk management principles as a decision-making tool which enables programmatic and technical success.
  - Program and project decisions shall be made on the basis of an orderly risk management effort.
  - Risk management includes identification, assessment, mitigation, and disposition of risk throughout the PAPAC (Provide Aerospace Products And Capabilities) process.
- **NPG 8000.4, Risk Management Procedures and Guidelines**
  - Provides additional information for applying risk management as required by NPG 7120.5A.
- **NPG 8705.x (draft) PRA Application Procedures and Guidelines**
  - Provides guidelines on how to apply PRA to NASA's diversified programs and projects

Risks that We "Accept," Implicitly or Explicitly

- *Annual Individual Fatality Risks in Sports*
  - Hang Gliding: 8×10^{-4}
  - Power boat racing: 8×10^{-4}
  - Mountaineering: 7×10^{-4}
- *Annual Individual Occupational Fatality Risks*
  - Mining: 9×10^{-4}
  - Fire fighting: 8×10^{-4}
  - Police: 2×10^{-4}
- *Annual Individual Fatality Risks due to Accidents*
  - Motor vehicles: 2.4×10^{-4}
  - Falls: 6.2×10^{-5}
- *Annual Cancer Fatality Risks*
  - All cancers: 3×10^{-3}

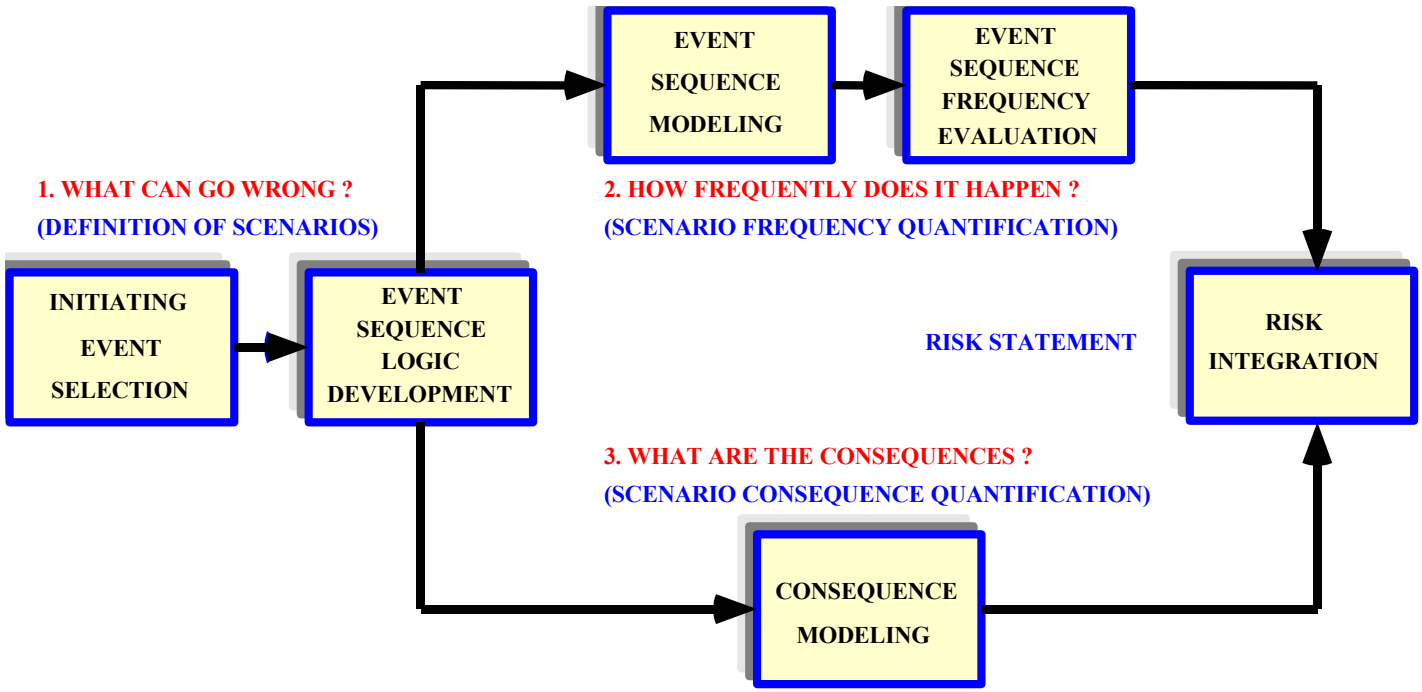
} From Wilson & Crouch, *Risk/Benefit Analysis,* 1982

NASA Integrated Action Team (NIAT) Defines

Acceptable Risk is the risk that is understood and agreed to by the program/project, Governing Program Management Council (GPMC), and customer sufficient to achieve defined success criteria within the approved level of resources.

- Each program/project is unique.
- Acceptable risk is a result of a knowledge-based review and decision process.
- Management and stakeholders must concur in the risk acceptance process.
- Effective communication is essential to the understanding of risk.
- Assessment of acceptable risk must be a continuing process.

PRA Answers Three Basic Questions



PRA is generally used for low-probability and high-consequence events for which insufficient statistical data exist. If enough statistical data exist to quantify system or sub-system failure probabilities, use of some of the PRA tools may not be necessary.

PRA Helps Prevent the Unexpected

One should expect that the expected can be prevented, but the unexpected should have been expected

Augustine Law XLV

Interactive Failures in Complex Systems Lead to Normal Accidents

In his 1984 book "Normal Accidents," Charles Perrow, a Yale sociology professor, states that:

- High-technology undertakings with their highly complex, tightly coupled systems lead to "normal accidents"
- Most engineers can identify and counteract single points of weakness in complex systems
- Difficulties arise when two or more components in complex systems interact in unexpected ways; these hidden flaws are the so-called "interactive failures."

The Three Mile Island and the Mars Polar Lander are both examples of accidents resulting from such interactive failures.

Traditional Safety Assessments

- "Established" good engineering practices
- Hazard analyses dealing with consequence only without regard to likelihood
- Deterministic (phenomenological) "what-if" analyses postulating maximum credible accidents

Unfortunately, traditional safety assessments are usually not sufficient to predict and mitigate all important safety risks

Insufficiency of Traditional Analyses

- The focus tends to be on single high-consequence events without the perspective of their likelihood
- Even after a mishap/accident, the focus is to fix mainly the problems that led to that mishap/accident
- Completeness of potential accident scenarios cannot be achieved
- There is no formal way to examine sequences of higher probability events, each of which has low consequence, but all together form a high-consequence scenario
  - Experience has shown this situation to be a dominant cause of accidents and mishaps (e.g., Three Mile Island, Challenger, Chernobyl)

Reasons Why Some People Oppose PRA

- Many people do not understand what probability values "really" mean
- Many engineers lack formal probability and statistics training
- Most engineering analyses are deterministic analyses of models, not of real systems
- The fact that risk assessment is built on uncertainty is seen as a weakness, not as a strength. PRA recognizes uncertainties based variability of observables and lack of knowledge
- People tend to think that lack of data is a reason not to perform a PRA, but the exact opposite is true

Early PRA History at NASA

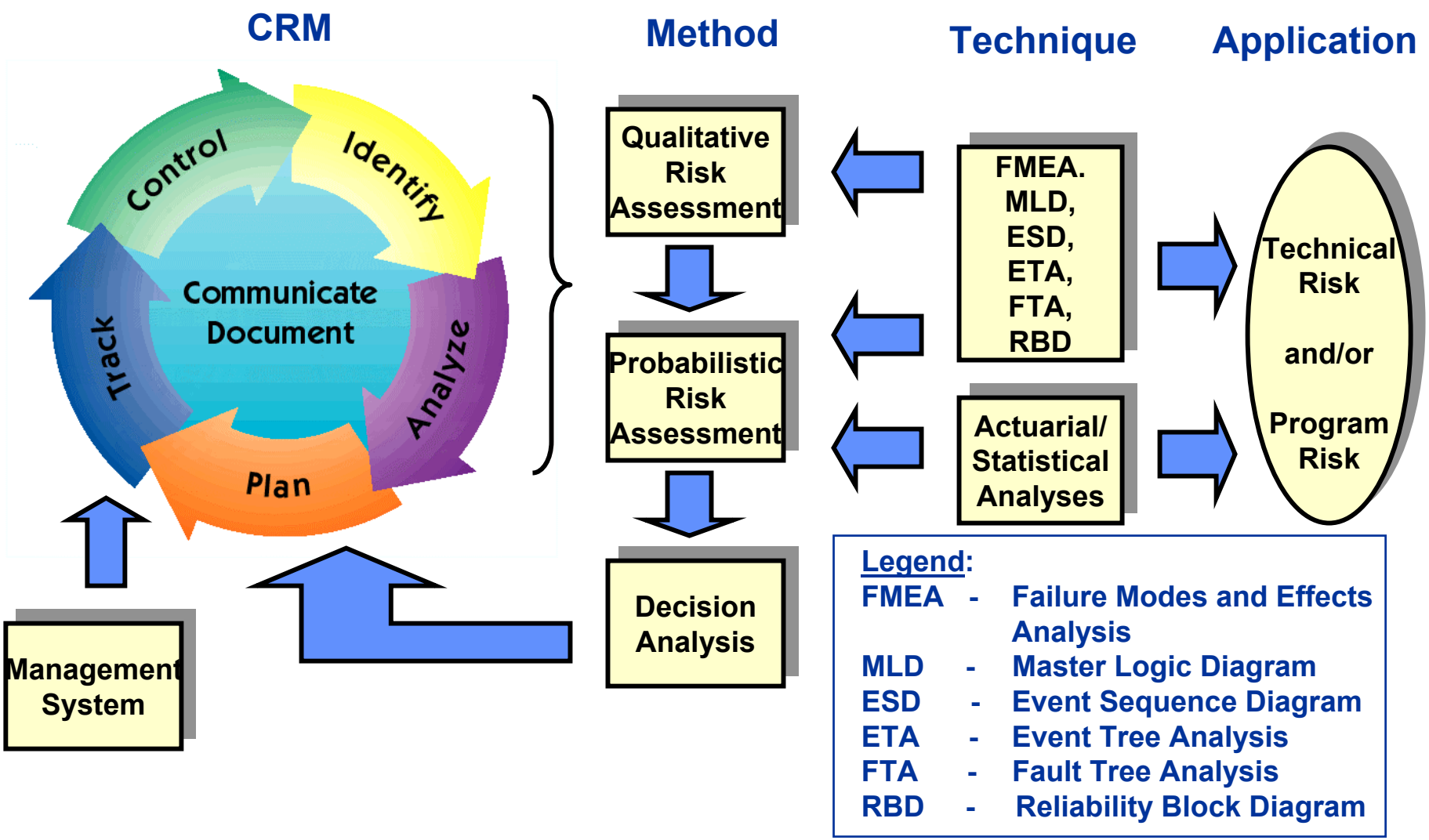
- Early Apollo program estimate of mission success probability was very low. This was bad news.
- However, between 1969 and 1972, 6 out of 7 successful Apollo missions demonstrated high mission success probability.
- This discrepancy caused dissatisfaction with PRA at NASA.
- October 29, 1986 - The "Investigation of the Challenger Accident" by the Committee on Science and Technology of the House of Representatives criticized NASA for not "estimating the probability of failure of the various [Shuttle] elements."
- January 1988 - In the "Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management," the Slay Committee recommended that "probabilistic risk assessment approaches be applied to the Shuttle risk management program at the earliest possible date."

PRA Returns to NASA

- More than a dozen PRA studies were performed for NASA between 1987 and 1995
- PRA work performed in support of nuclear payload missions including Galileo, Ulysses and Cassini.
- Then, on July 29, 1996, the NASA Administrator stated:

  "Since I came to NASA [1992], we've spent billions of dollars on Shuttle upgrades without knowing how much they improve safety. I want a tool to help base upgrade decisions on risk."
- The Administrator wanted to know if the Shuttle was "safe enough" and how to make it safer. NASA then began development of a tool to answer these questions. This is how QRAS was born.

Relationship Between Risk Management and Probabilistic Risk Assessment (PRA)



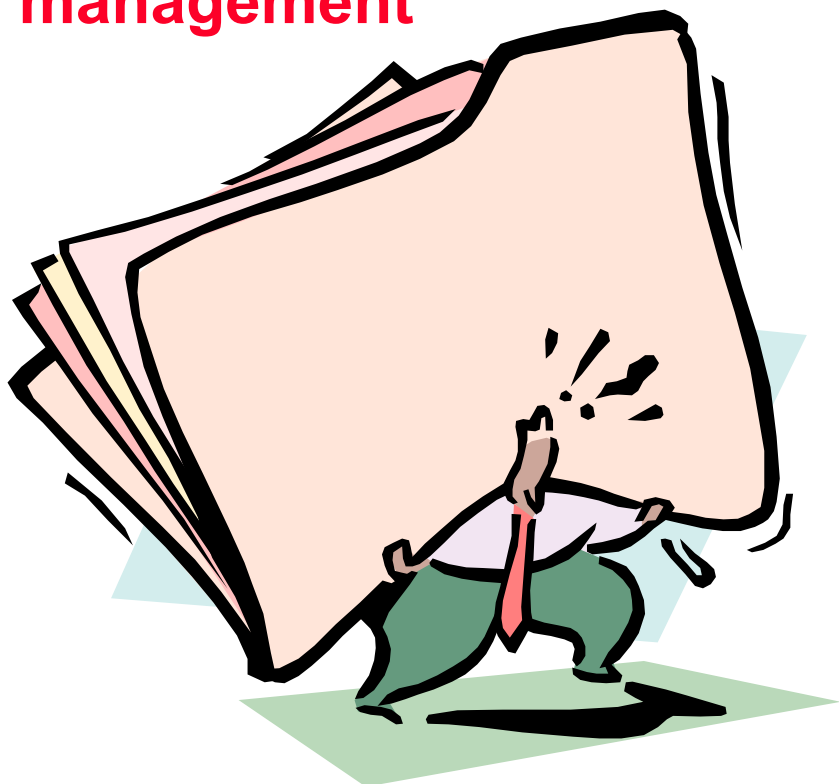
PRA Throughout Product Life Cycle

- **PRA in Design**
  - Design seeks to optimize programs, missions, or systems to meet objectives and requirements within given constraints
  - PRA evaluates risk of alternative designs, relative risks of subsystem contributors and identifies how risks can be minimized through design change or other means
- **PRA in Operation**
  - Normal operation, normal and accident operating procedures, and maintenance can cause increased risks
  - PRA is eminently suited to assess these risks as well as to guide and optimize "configuration management" for minimum risk
- **PRA for Upgrade**
  - Improvements in design can result in risk increase
  - PRA can evaluate upgrade alternatives and show the least risky ones
- **PRA for Decommissioning**
  - End of life presents situations when safety can be compromised and regulatory requirements breached
  - PRA can guide the removal-from-service process to accomplish it safely and within regulatory constraints

Important PRA Benefits

- Improve safety in design, operation, maintenance and upgrade (throughout life cycle);
- Ensure mission success;
- Improve performance; and
- Reduce design, operation and maintenance costs.

- The greatest value of PRA is that it is a decision-support tool for management



Major Historic PRAs and Associated Measures

- **Reactor Safety Study:** The first probabilistic risk assessment of a modern electricity-generating nuclear power plant, US AEC, WASH-1400, 1975: Health and safety risks of nuclear power plants.

  Measures: Triggered regulatory requirements to improve nuclear power reactor safety; it also lay the foundations of the current Nuclear Regulatory Commission (NRC) risk-informed regulation.

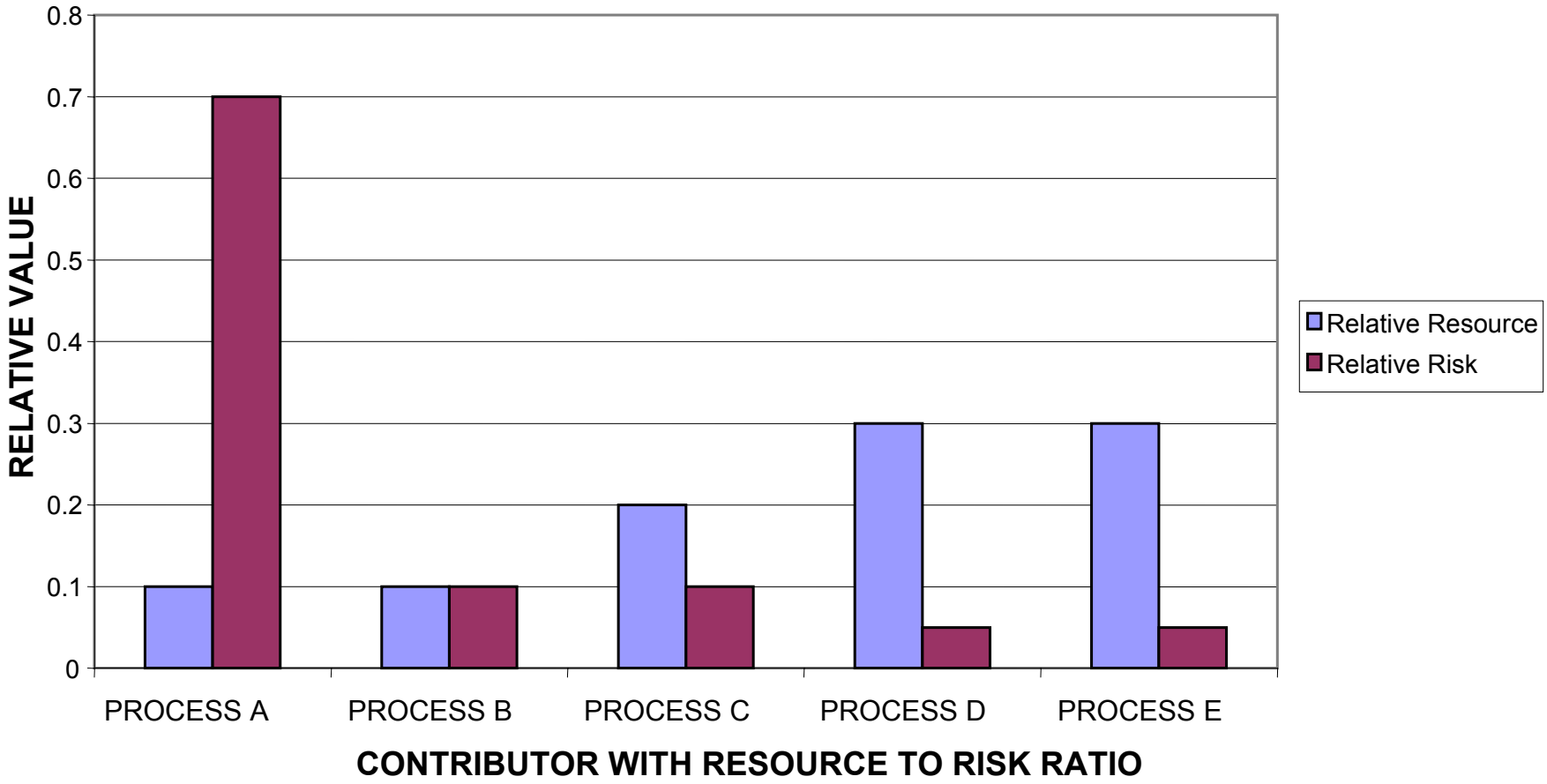
- **Canvey Island:** One of the first major modern quantitative risk assessments, UK, 1978: Health and safety risks of petrochemical installations on the highly industrial north bank of the Thames River.

  Measures: Implemented important risk reduction measures including relocation of a large butane storage facility.

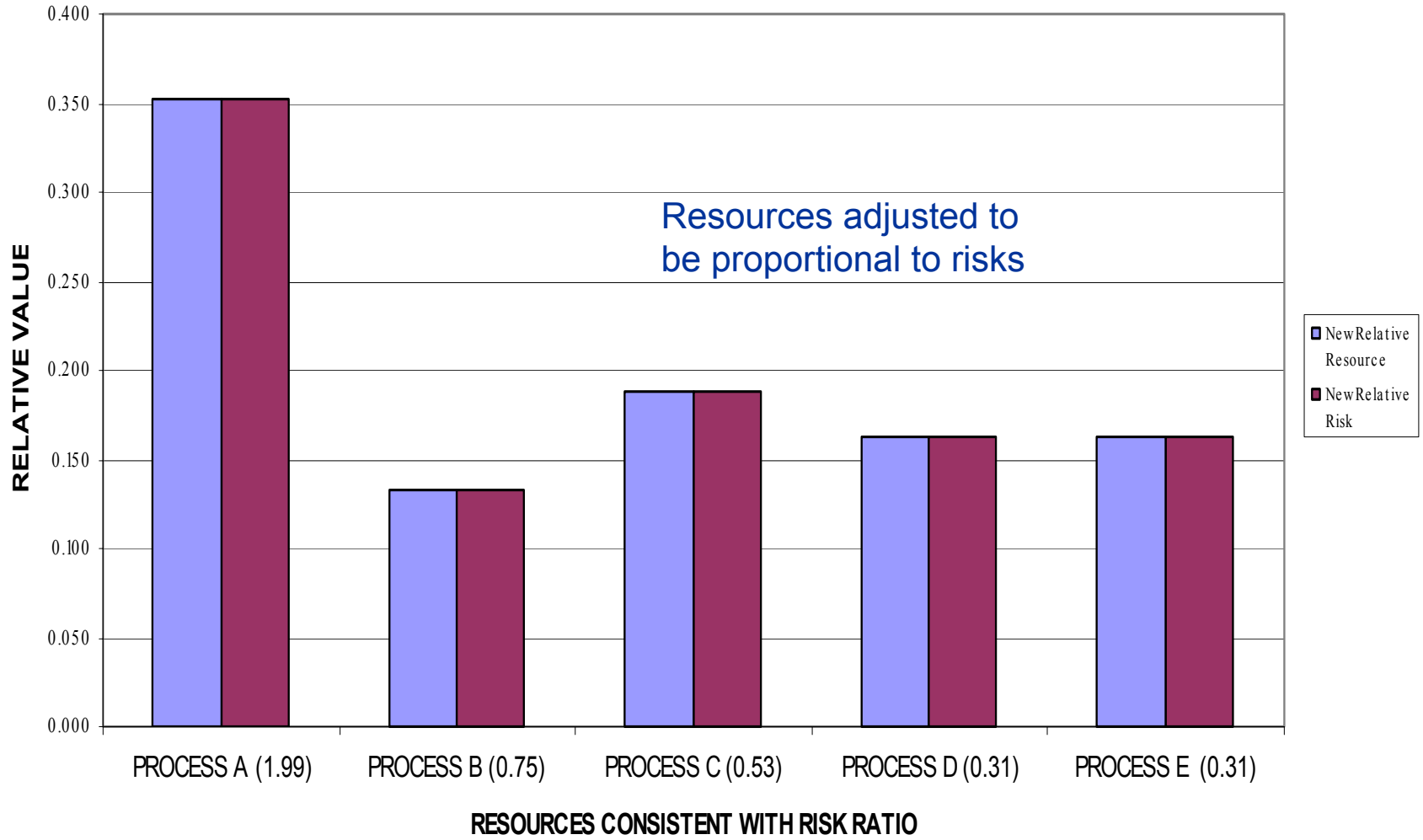
- **Chemical Munitions Demilitarization:** US Army, 1996: Comparative assessment of several options including on-site, regional, centralized.

  Measure: Selected the on-site demilitarization as least risky.

NASA Example of Imbalance between Resources and Risks (Before PRA)



Rebalance: No Risk Increase but 44% Resource Reduction (After PRA)

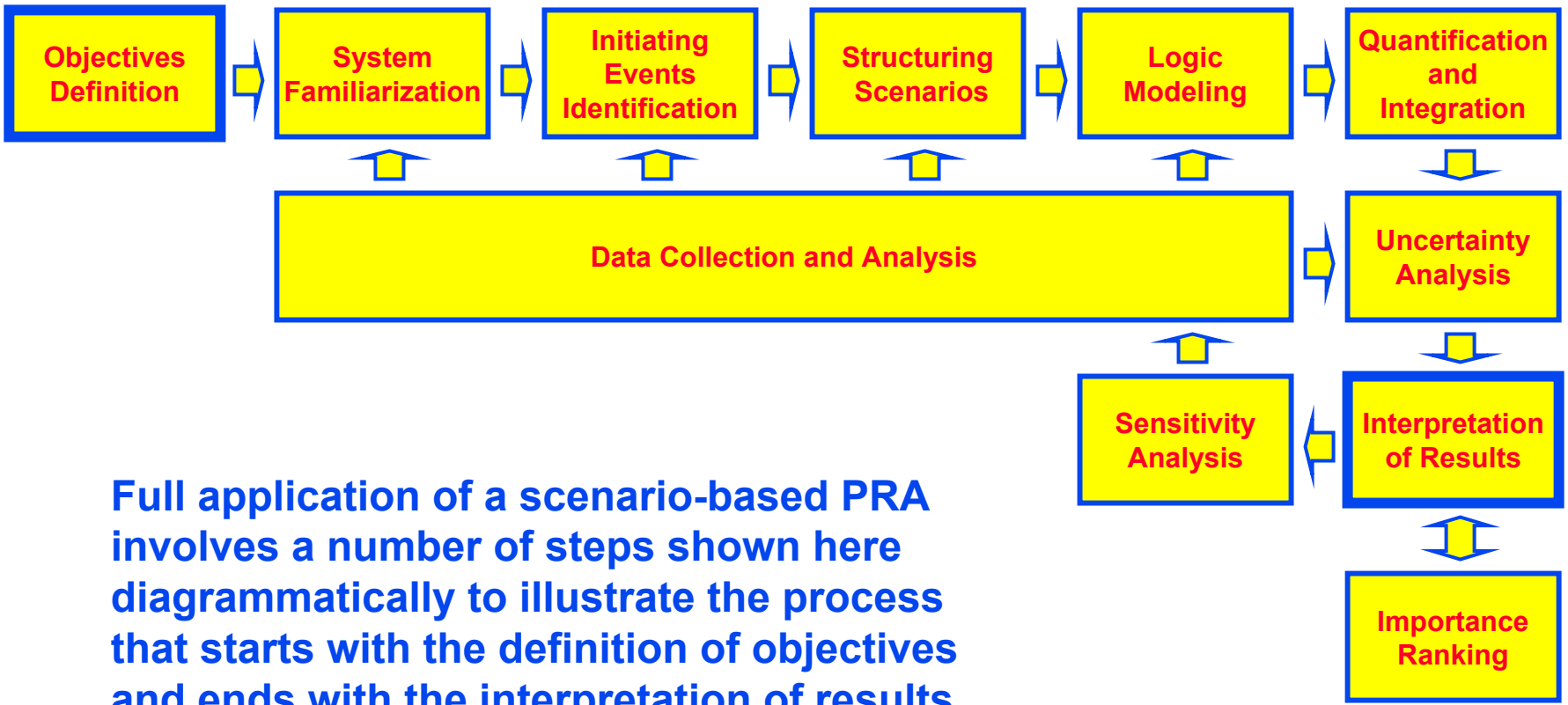


Example of Trade-off for Management Decision (International Space Station PRA)

Postponed maintenance activities based on ISS PRA

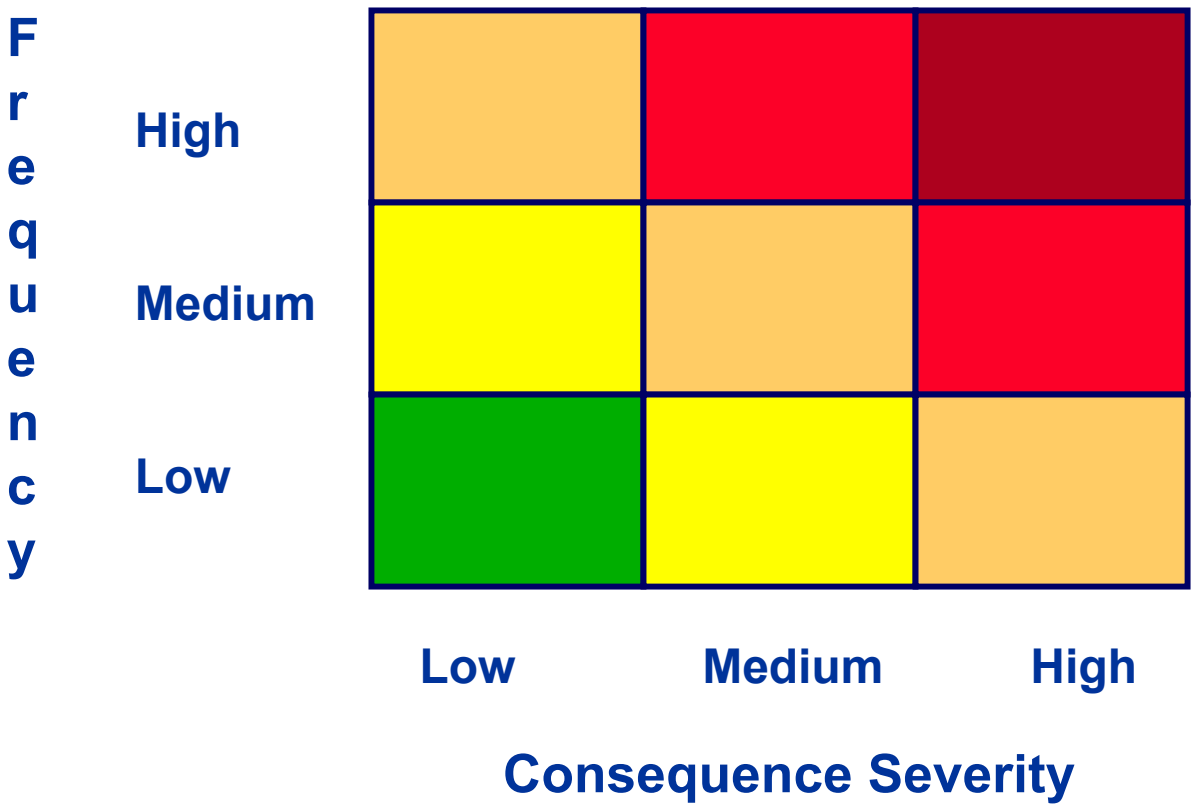
- What are the risks in delaying maintenance actions until Orbiter arrives in order to increase the number of hours the crew can devote to science?
- Analysis showed that deferring all maintenance would decrease the number of science hours available because of increased probability of evacuation.
- PRA showed that science hours can be increased when maintenance is focused on risk drivers.

Elements of a Scenario-Based PRA

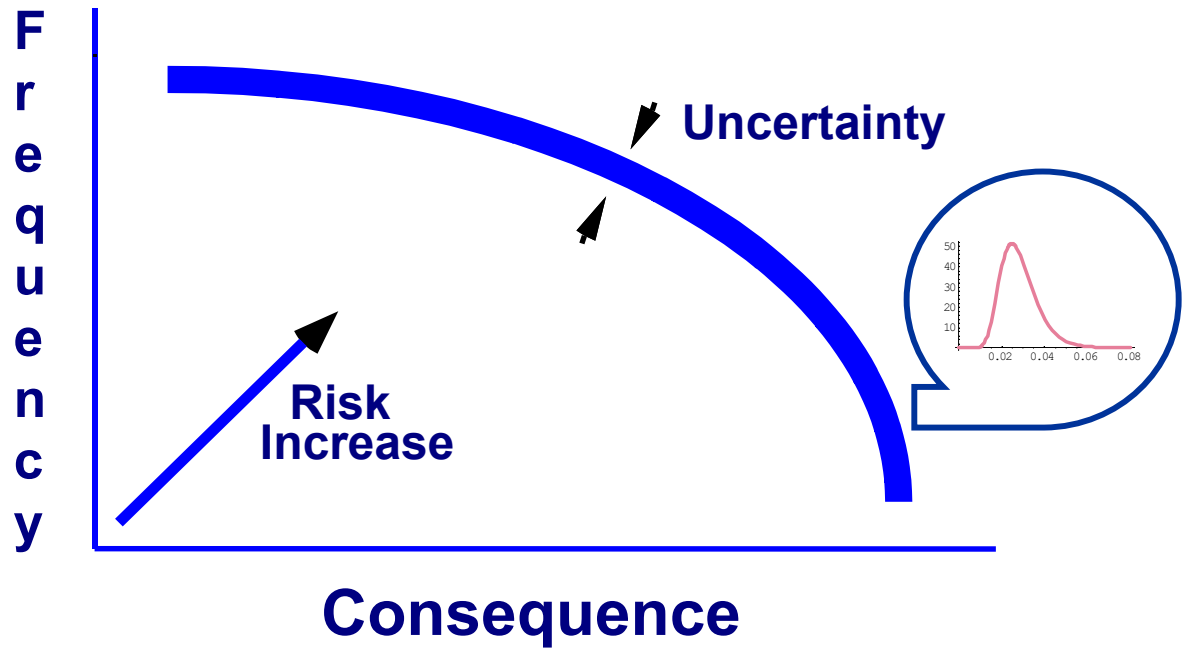


Full application of a scenario-based PRA involves a number of steps shown here diagrammatically to illustrate the process that starts with the definition of objectives and ends with the interpretation of results.

Qualitative (Level) Risk Representation



Graphic Representation - Risk Curve



In mathematical terms, the risk curve is the complementary cumulative distribution function (CCDF); i.e., the frequency of exceeding a given consequence severity

Areas of PRA Application at NASA

- Design and Conceptual Design (e.g., 2nd Generation Reusable Launch Vehicles, Mars missions, NSI)
- Upgrade (Space Shuttle)
- Development/construction/assembly (e.g., International Space Station); Important findings
  - MMOD: lead contributor to loss of station (LOS) risk
  - Illness in space: lead contributor to loss of crew (LOC) risk
- Requirements for safety compliance (e.g., nuclear payload missions like Mars '03; NSI, Mars Sample Return)

Two Major NASA PRA Programs

Space Shuttle Development Roadmap

Goals and Objectives	97	02	07	12
1 Fly Safely	1 vehicle loss in 148 flights	1 vehicle loss in 250 flights	1 vehicle loss in 325 flights	1 vehicle loss in 500 flights

International Space Station PRA

- **1999 -- The NASA Advisory Council recommended, the NASA Administrator concurred, and the ISS Program began a PRA.**
  - **The modeling will be QRAS-compatible.**
  - **First portion of PRA (through Flight 7A) - delivered in Dec. 2000; Second portion (through Flight 12A) delivered in July 2001.**

ISS PRA End States

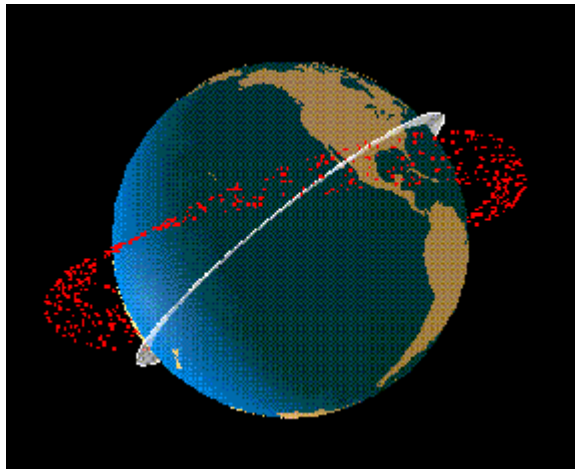
- **End State definitions were developed in concert with program concerns: *Critical End States***
- ***Other Undesired End States* are by-products of performing the PRA**

- Station and Crew are Functional (OK)
  - This end state signifies that the station is still working with the flight rule constraints
- Critical End States
  - Loss of Station and Crew (LOS)
    - Catastrophic loss of the station and crew
  - Loss of Crew (LOC)
    - Resultant loss of a crew-member
    - Also includes the inability to evacuate the station due to evacuation end state and the unavailability of either Soyuz or Orbiter to perform such a task
  - Evacuation End States (EVAC)
    - Emergency Evacuation
    - Flight Rule Evacuation
    - Medical Evacuation
- Other Undesired End States (OUE)
  - Loss of Module (LOM)
    - The shut down of any pressurized module as dictated by flight rule or as result of MMOD
  - Loss of System (LOSys)
    - The loss of either US or RS distributed systems
    - Loss of a function such as
      - ability for Orbiter, Progress, or Soyuz to dock
      - ability to reboost
      - insufficient O_2 or N_2 reserves
  - Collision (COL)
    - Impact of the Orbiter, Progress, or Soyuz

Interesting Results of the ISS PRA

- Illness in space is the main risk contributor to Loss of Crew (LOC)
- Micro-meteoroids and orbital debris (MMOD) are the main risk contributors to Loss of Station (LOS)

MMOD Risk Modeling



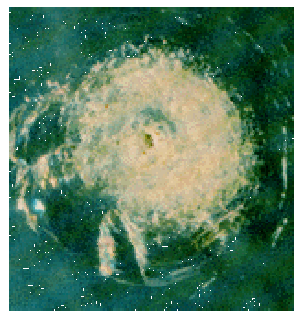
- MMOD = Micro- Meteoroid and Orbital Debris
- Micro-Meteoroid is a term generically used to refer to any kind of small-size (order of cm in diameter or less) body traveling in space outside of the Earth atmosphere.
- The term Orbital Debris generally refers to material that is on orbit as the result of space initiatives, but is no longer serving any function.

Risk from Orbital Debris

MMOD generally move at high relative speed with respect to operational spacecraft.

Low Earth orbit (< 2,000 km) average relative impact velocity is 10 km/s (~ 22,000 mi/hr)

- **@ 10 km/s a 1.3 mm diameter aluminum particle has same kinetic energy as a .22-caliber long-rifle bullet**
- **4-mm-diameter crater on windshield of Space Shuttle orbiter, produced by a fleck of white paint approximately 0.2 mm in diameter estimated to be traveling at a relative velocity of 3-6 km/sec at impact**



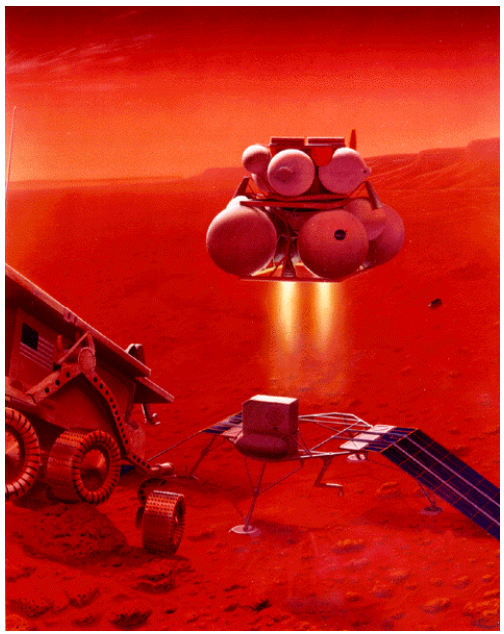
For Space Shuttle, typical MMOD risk is approximately the same as the risk form all other causes combined (~1/250)

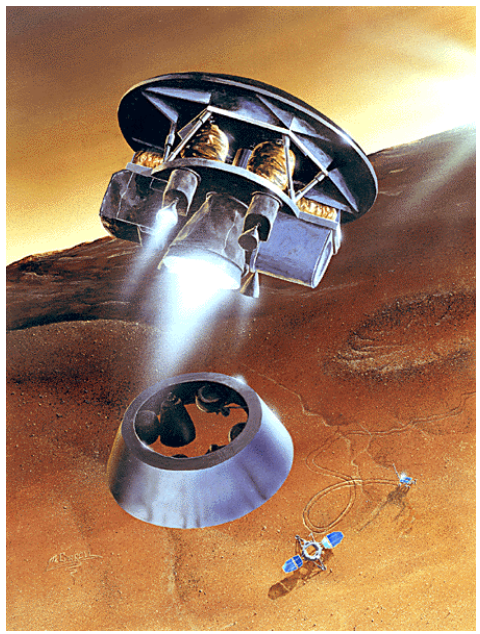
Nuclear Launch Approval Requirements

- **National Environmental Protection Act**
  - requires Environmental Impact Statement (EIS) to address mission potential environmental impacts
- **Presidential Directive / NSC-25**
  - defines launch approval process for missions carrying nuclear material; actual approval is to be granted, after consideration of launch risk, at the Executive Office level
    - process requires safety evaluation of space nuclear systems by the responsible program
    - independent technical review of evaluation executed by responsible program is conducted by the Interagency Nuclear Safety Review Panel (INSRP)

Mars Sample Return Mission

- Mission must meet a Planetary Protection Program (PPP) criterion of $<10^{-6}$ probability of Earth contamination upon return of sample
- PRA is used to evaluate mission compliance with the PPP criterion





Who at NASA Needs More Expertise in PRA?

- **Practitioners to**
  - Assess vulnerabilities
  - Improve design
  - Improve operation
- **Managers to**
  - Timely and cost-effectively manage projects and programs throughout life cycle
- **Decision makers to**
  - Support decisions to satisfy/enhance mission safety and productivity cost-effectively

Focus for PRA Capability Enhancement

In-house expertise

to perform, manage and use PRAs to make sound decisions

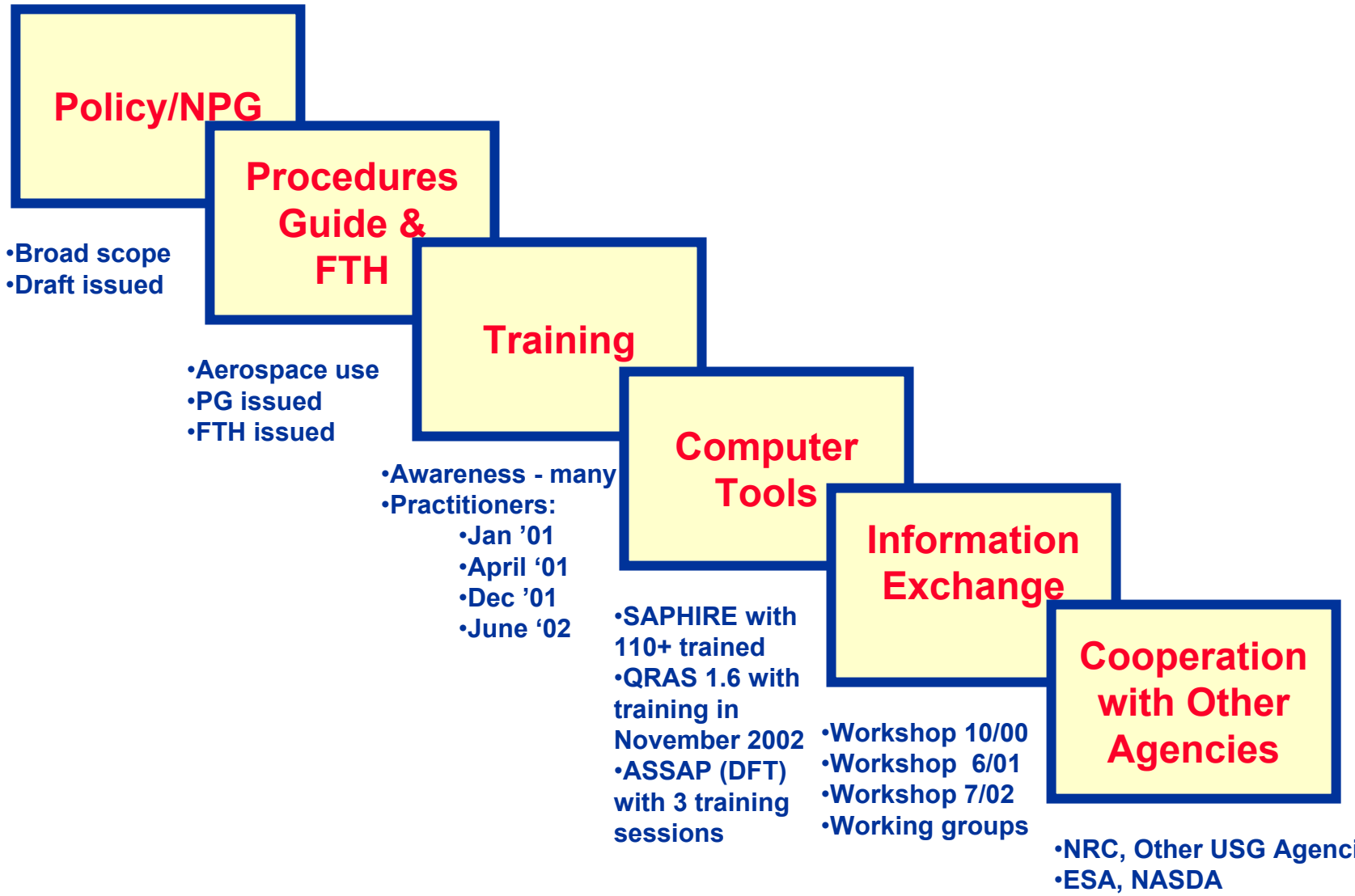
In-house ownership and corporate memory

of PRA methods, tools, databases and results

Transfer of PRA technology

from expert consultants to in-house personnel and managers who need to understand, manage, oversee, and use PRA to make decisions

Accomplishments to Date

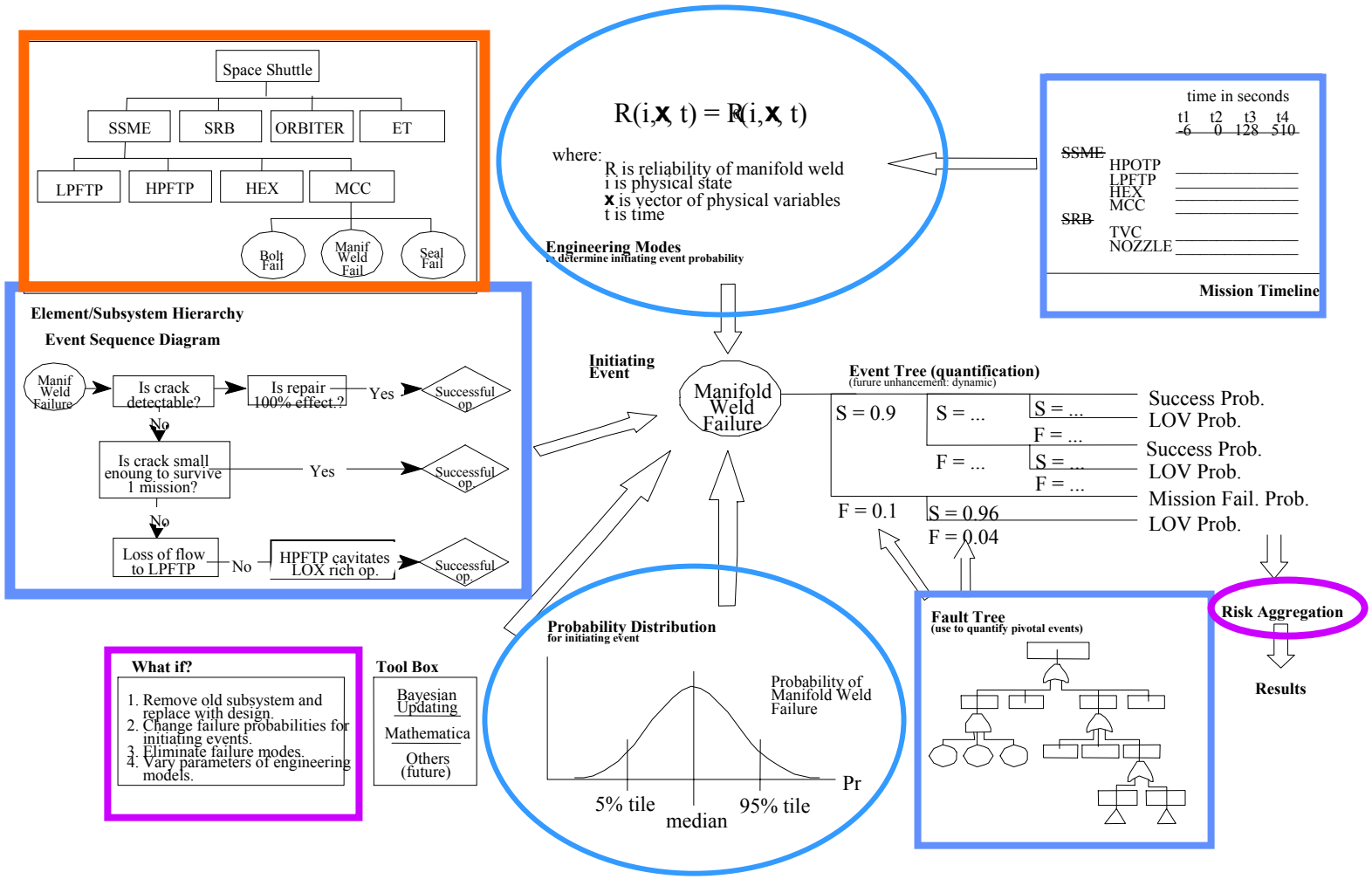


NASA PRA Policy Requirements

CONSEQUENCE CATEGORY	CRITERIA / SPECIFICS		NASA PROGRAM/PROJECT (Classes and/or Examples)	PRA SCOPE*
Human Safety & Health	Public Safety	Planetary Protection Program Requirement	Mars Sample Return	F
		White House Approval (PD/NSC-25)	Nuclear payload (e.g., Cassini, Ulysses, Galileo)	F
	Human Space Flight		International Space Station	F
			Space Shuttle	F
			Crew Return Vehicle	F
Mission Success (for non-human rated missions)	High Strategic Importance		Mars Program	F
	High Schedule Criticality		Launch window (e.g., planetary missions)	F
	All Other Missions		Earth Science Missions (e.g., EOS)	L
			Space Science Missions (e.g., SIM)	L
			Technology Demonstration and Validation (e.g., EO-1)	L

LEGEND (*) : F = Full Scope; L = Limited Scope or Simplified PRA

NASA QRAS Methodology



QRAS 1.7 Capabilities

- System (Physical or Functional) Hierarchy
- Mission Phases
- Event Sequence Diagrams (ESD)
- Automatic conversion of ESDs to Event Trees
- Fault Tree linking through ESDs
- Inter-system and Intra-system Common Cause Failure Modeling and Quantification
- Use of Binary Decision Diagrams (BDD) for exact quantification of top event probabilities

Training on QRAS 1.7 is planned for Nov./Dec. 2002
at University of Maryland, College Park, MD

NASA Special PRA Methodology Needs

- **Broad range of programs**: Conceptual non-human rated science projects; Multi-stage design and construction of the International Space Station; Upgrades of the Space Shuttle
- **Risk initiators** that vary drastically with type of program
- **Unique design and operating environments** (e.g., microgravity effects on equipment and humans)
- **Multi-phase** approach in some scenario developments
- **Unique external events** (e.g., micro-meteoroids and orbital debris)
- **Unique types of adverse consequences** (e.g., fatigue and illness in space) and associated **databases**
- Different quantitative methods for **human reliability** (e.g., astronauts vs. other operating personnel)
- Quantitative methods for **software reliability**

Projects for PRA Capability Development

- Galileo/ASSAP – dynamic fault tree (DFT) program
- QRAS 1.7 – Training in Nov./Dec. 2002
- Incorporation of DFT capability into an integrated PRA program (SAPHIRE, QRAS)
- Develop/integrate MMOD module into PRA program (SAPHIRE, QRAS)
- Dynamic PRA capability (DARE, UMD effort funded by ECS)
- NASA-wide PRA database
- PRATMAD – NASA-wide group on PRA tools, methods, and data

Vision for the Future

- Improve risk awareness at NASA
  - Conduct PRA/QRA training for project managers, astronauts and operational personnel
- Develop a corps of NASA PRA experts
- Adopt agency-wide risk informed culture
  - PRA to become a way of life for safety and technical performance improvement and for cost reduction
  - Implement risk-informed management process
- Transition PRA from curiosity object to NASA baseline method for safety assessment
- Make NASA a leader in PRA