Risk-informed Approach to System Performance and Safety

Robert A. Bari

Presented at

NASA

February 2, 2007

Brookhaven Science Associates
U.S. Department of Energy

BROOKHAVEN NATIONAL LABORATORY

Outline

- The Risk Informing Process
- Applications to Materials and Waste
- Applications to Proliferation Risk
- Applications to Space Exploration
- Summary

Nuclear Materials and Waste

- Risk: Potential to cause harm; includes notion of both likelihood and consequence
- Risk Informed Decision Making = RIDM
- RIDM: SECY-98-0144 definition:

  A “risk-informed” approach to regulatory decision-making represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to health and safety.

RIDM Definition

Has 3 elements:

- Consider risk insights
- Other factors include consideration of uncertainty, defense-in-depth, safety margins, cost-benefit, etc. identified in regulatory analysis guidance, e.g., NUREG/BR-0058 and NUREG/BR-0184
- Focus on design/operational issues important to health and safety

Examples of Risk Insights

- Risk to individual member of public from licensed activity is negligible* (likelihood of dose/health effect < goal)
- Risk to individual worker from a proposed change is unacceptably high (likelihood of dose/health effect > applicable limit)
- Risk Reduction [in units of collective dose x $2000/person-rem] > cost of implementation

* Need a risk level to define negligible.

Recipients of Risk and Consequence Measures

- Recipients of risk include:
  - General public
  - Facility/Process and Co-located workers
  - Environment
- Consequence measures may include:
  - Radiation dose
  - Chemical exposure
  - Radiation health effects (early fatality, early injury, fatal latent cancers, non-fatal cancers) and chemical health effects (mortality, morbidity)
  - Land contamination
  - Monetary costs of protective/mitigative measures

Risk Methods

- Methods include:
  - Integrated Safety Assessment: used for fuel cycle facilities under Part 70 (NUREG-1513, NUREG-1520, NUREG-1718)
  - Performance Assessment: used for HLW repository under Part 63
  - Barrier/Hazard Analysis: used for industrial/medical materials facilities and devices (NUREG/CR-6642)
  - Probabilistic Risk Assessment: generally used for power reactors but may be usefully applied in certain circumstances to other complex facilities
- Risk method used will depend on:
  - the technical complexity of the facility in question
  - the safety issues to be resolved
  - the time frame for developing the information needed by the decision maker.

The Risk Informing Process

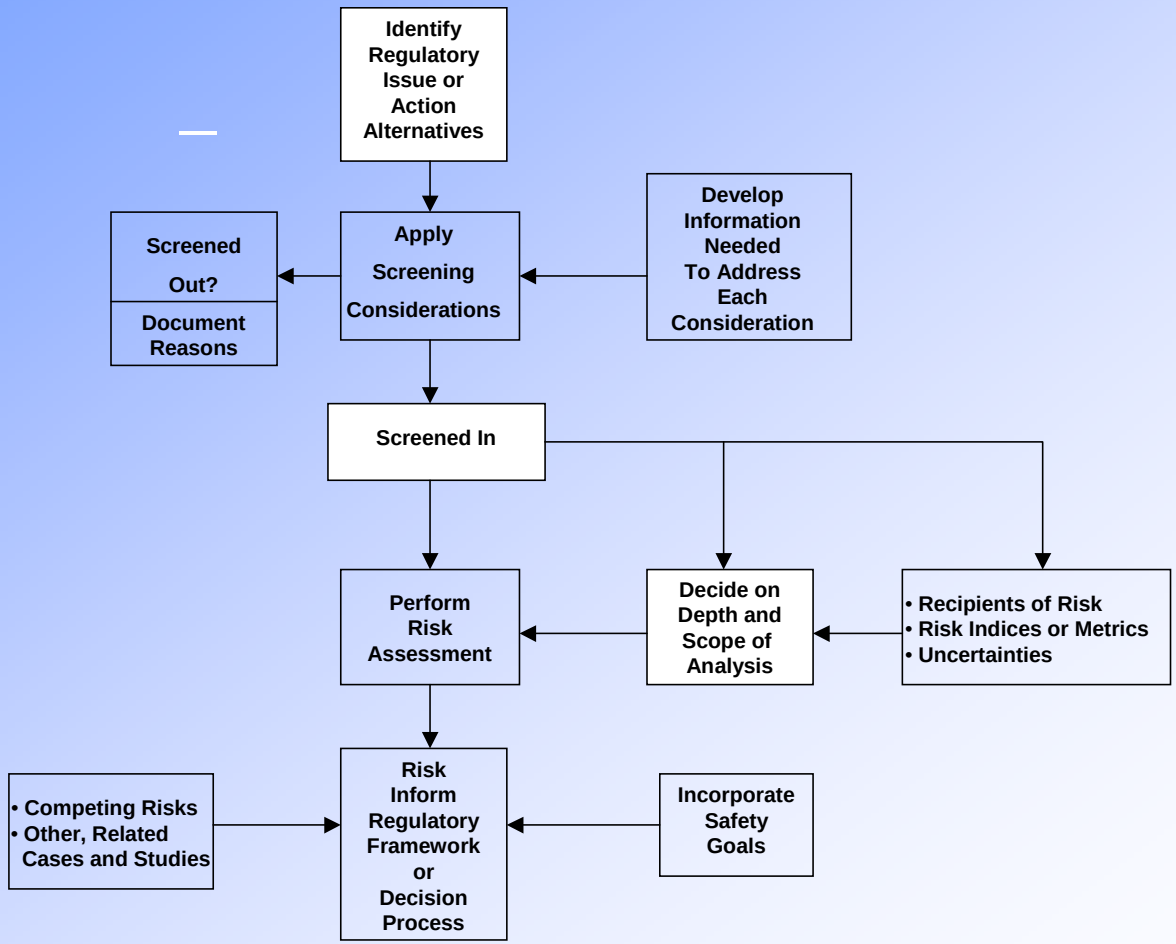


Figure 1: Risk-Informing Process

Process for Risk-informed Decision Making

- Identify safety issue / action alternatives
- Develop information and then apply screening process to determine if the issue should/can be risk informed
- If screened in, perform/adapt a suitable risk assessment identifying the risk metrics, the risk-affected population, the factors contributing to uncertainties, and the scope/depth of analysis needed
- Incorporate considerations related to uncertainty, defense-in-depth, safety margins, and risk guideline aspects
- Assess any information on competing risks or from related cases and studies that bears on the decision

Use of Quantitative Guidelines

- Limited quantitative guidance on allowable accident risk to individuals applicable to non-reactor facilities/activities
- In risk-informing a particular decision some guidance is useful where additional regulatory attention to reduce risk is not needed
- Stated in terms of radiation health effect risks, risk guidelines are aspirations: not regulatory limits, not default ALARA levels

Risk Guidelines

- Are used to better inform decision making on particular issues.
- Quantitative guidelines based on qualitative safety aspirations establish the *metrics* for quantifying safety and provide the *measurable scale* for determining the level of safety that is being achieved.
- Guidelines can be used to:
  - reduce unnecessary conservatism in purely deterministic approaches,
  - identify areas with insufficient conservatism in deterministic analyses, and
  - provide the bases for identifying the need for additional requirements or regulatory actions.

Example Public Quantitative Health Guidelines

- Individual Public Acute (QHG 1): The risk of prompt fatality to an individual member of the public due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed 5E-7 per year. This is one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. public are generally exposed.

- Individual Public Latent (QHG 2): The risk of latent cancer fatality to an individual member of the public due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed 2E-6 per year. This is one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.

- Individual Public Injury (QHG 3): The risk of severe injury to an individual member of the public due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed 1E-6 per year. This is one-tenth of one percent (0.1 percent) of the sum of severe injury risks resulting from other accidents to which members of the U.S. public are generally exposed.

Example Worker Quantitative Health Guidelines

- Individual worker acute (QHG 4): The risk of prompt fatality to a worker due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed 1E-6 per year. This is approximately 1% of the prompt fatality risk in all higher risk industries combined.

- Individual worker latent (QHG 5): The risk of latent cancer fatality to a worker due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed 1E-5 per year. This is 0.5% of the annual risk of cancer from all other causes.

- Individual worker injury (QHG 6): The risk of severe injury to a worker due to inadvertent or accidental exposure from nuclear materials and waste activities should be less than 5E-6 per year.

Intolerable Risk

"Fix At Any Cost"

Regulatory Limit

REQUIREMENT

Tolerable Risk

"Fix If Cost Beneficial"

Risk Guideline

ASPIRATION

Insignificant Risk

"Do Not Fix"

Risk-Informed Decision Making

- Use Three-Region Risk Acceptance Diagram
  - Intolerable high risk region (excessive likelihood of exceeding some regulatory limits)
  - Tolerable (intermediate) risk region where benefit-cost trade offs may be used to reduce risk
  - Insignificant risk region where no further risk reduction is needed
- Apply Decision Algorithms
  - Analogs of guidance in RG 1.174 and NUREG/BR-0058
  - Applicable to changes in the facility licensing basis to allow small risk increases or mandate risk reduction
- Consider factors other than risk, e.g., defense-in-depth and safety margins, in making decision
- Can be used directly on QHGs or on “surrogates” if they exist

Nature/Types of Issues Needing Risk-Informing

- Licensing application reviews of new facilities or new processes at existing facilities
- Establishing safety envelope of conditions of operation
- Reducing undue burden

The Screening Process

- Benefits (e.g., maintaining or enhancing safety, increasing regulatory efficiency, improving communication)
- Feasibility (availability of data and models, startup costs, and legislative, judicial, and related issues) of implementing a risk-informed approach
- Gather information needed to address each of the screening elements

Decision Making on Licensee Requests

- Identify risk metric(s) affected by licensee request
- Map baseline value of risk onto risk acceptance diagram
- Evaluate change in risk (ΔRisk) due to licensee request
- Use logic matrix to help risk-inform decision

Decisions Making on New Requirements

- Identify risk metric(s) affected by potential new requirement
- Value-impact analysis for NMSS arena outlined in NUREG/BR-0184
- Safety goal evaluation: Analog to NUREG-BR-0058
- Develop logic matrix similar to NUREG-BR-0058

Proliferation Risk

An international group is developing and demonstrating a methodology for the systematic evaluation of Generation IV nuclear energy systems with respect to proliferation resistance and physical protection

- Major Tasks
  - Characterize relevant proliferation and security threats
  - Specify measures for expressing a system's proliferation resistance (PR) and physical protection (PP)
  - Develop a methodology to assess/quantify the measures
    - Methodology will be implemented in a software-based evaluation tool (called the "Implementation Guide")

Some Important Definitions

- Proliferation resistance is that characteristic of a nuclear energy system that impedes the diversion or undeclared production of nuclear material, or misuse of technology, by the host State in order to acquire nuclear weapons or other nuclear explosive devices.

- Physical protection is that characteristic of a nuclear energy system that impedes the theft of materials suitable for nuclear explosives or radiation dispersal devices, and the sabotage of facilities and transportation, by sub-national entities and other non-host State adversaries.

Assessment Paradigm

CHALLENGES → **SYSTEM RESPONSE** → **OUTCOMES**

Threats ***PR & PP*** ***Assessment***

Intrinsic
- Physical & Technical Design Features

Extrinsic
- Institutional Arrangements

Proliferation, theft and sabotage involve **<u>competing</u> adversary and defender forces**. Important to recognize both perspectives and the human interplay.

PR & PP Measures

PR measures

- ***Proliferation Technical Difficulty (TD)***
- ***Proliferation Time (PT)***
- ***Proliferation Cost (PC)***
- ***Detection Probability (DP)***
- ***Fissile Material Type (MT)***
- ***Detection Resources Efficiency (DE)***

PP measures

- Probability of Adversary Success (Ps)

- Consequences (C)

- Physical Protection Resources (PPR)

Threat Space

Proliferation Resistance

- Concealed diversion from declared flows and inventories
- Overt diversion from declared flows and inventories (abrogation)
- Concealed material production or processing in declared facilities
- Overt undeclared material production or processing in declared facilities (abrogation)
- Production using dedicated clandestine facilities

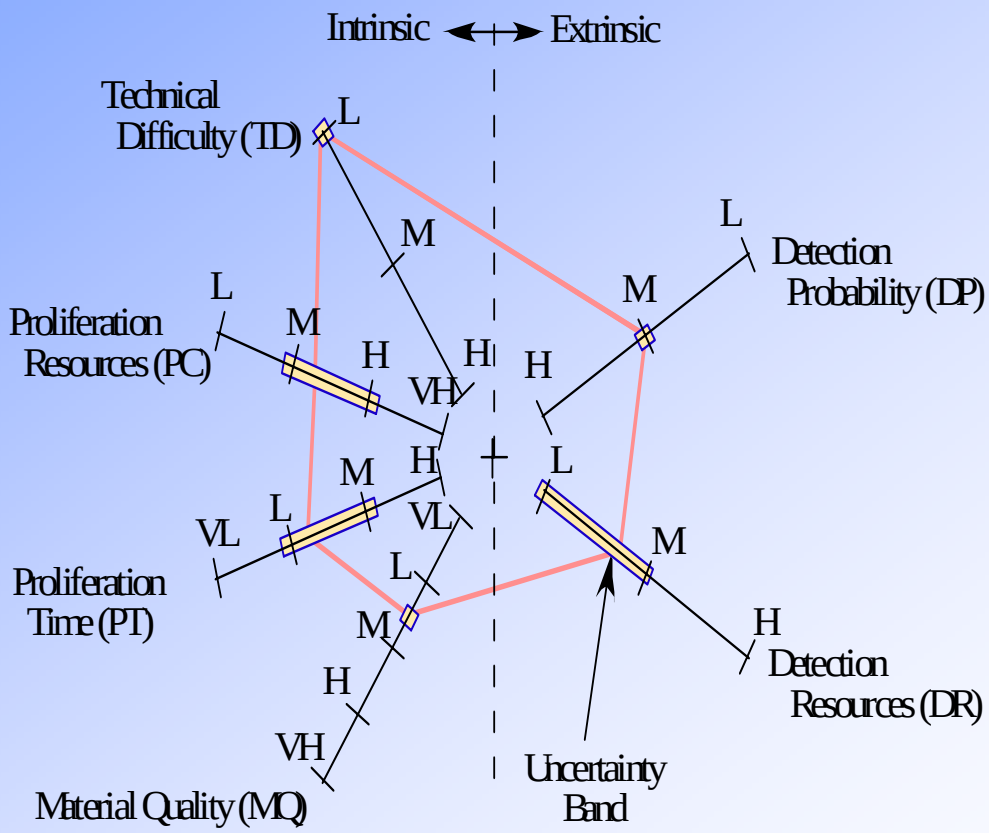
Physical Protection

- Theft of nuclear weapons-usable material from facilities or transport
- Theft of hazardous radioactive material from facilities and transport for use in a radioactive dispersal device (dirty bomb)
- Sabotage at a nuclear facility or transport with the intention to release radioactive material to harm the public, damage facilities, or disrupt operations.

System Response

- Pathway analysis: Intuitive way to describe & analyze proliferation, theft, or sabotage scenarios and to identify vulnerabilities
- *Segmentation & Decomposition, then Re-aggregation*
- Pathways: Potential sequences of events followed by the proliferator or adversary to achieve its objectives
  - Along any pathway the proliferant state or adversary will encounter various difficulties, barriers, or obstacles, all of which are collectively called “proliferation resistance” or “physical protection robustness”
- Considers time-dependent aspects and uncertainty

Spider Diagram for Six PR Measures



Application of Markov Model to Proliferation Resistance Evaluation

- Scenarios are represented by discrete stages.
- Each stage represents the end point of a major activity module.
- Transition between stages (or sub-stages) is modeled as a Markov random process.
- Detection, failure, or success of proliferation activity are modeled as transitions to 'absorbing' states.
- Instantaneous probability of detection is used to model on-demand detection, e.g. at the transition between major stages.
- Allows study of either the overall system or the selected portion of the fuel cycle

PR & PP Paradigm using Markov

Generic PR & PP Paradigm

Threat → Response → Outcomes

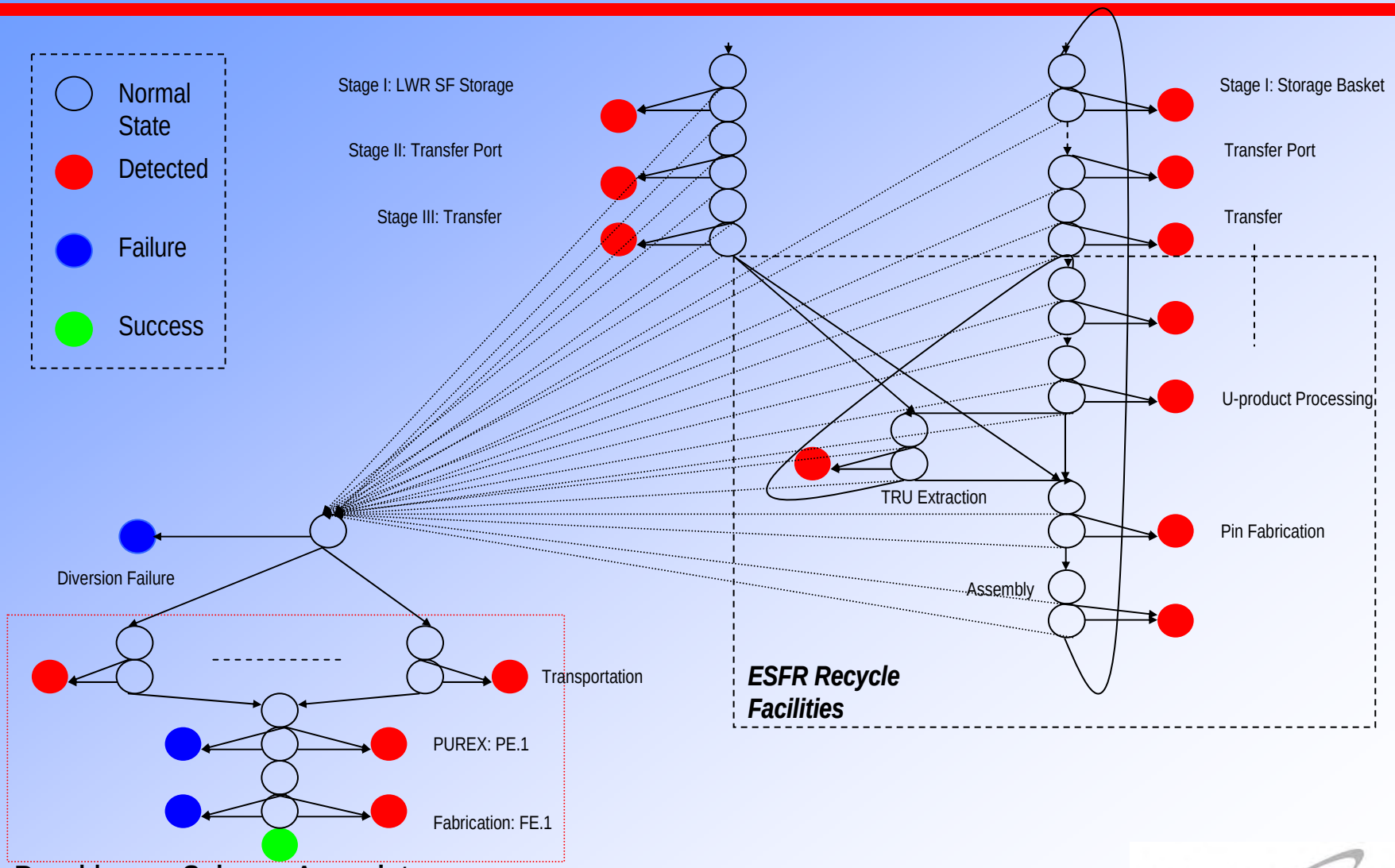
Markov Model Formulation

- Assumes proliferator targets
- A particular MQ (Material Quality)
- Sufficient resources to carry out missions

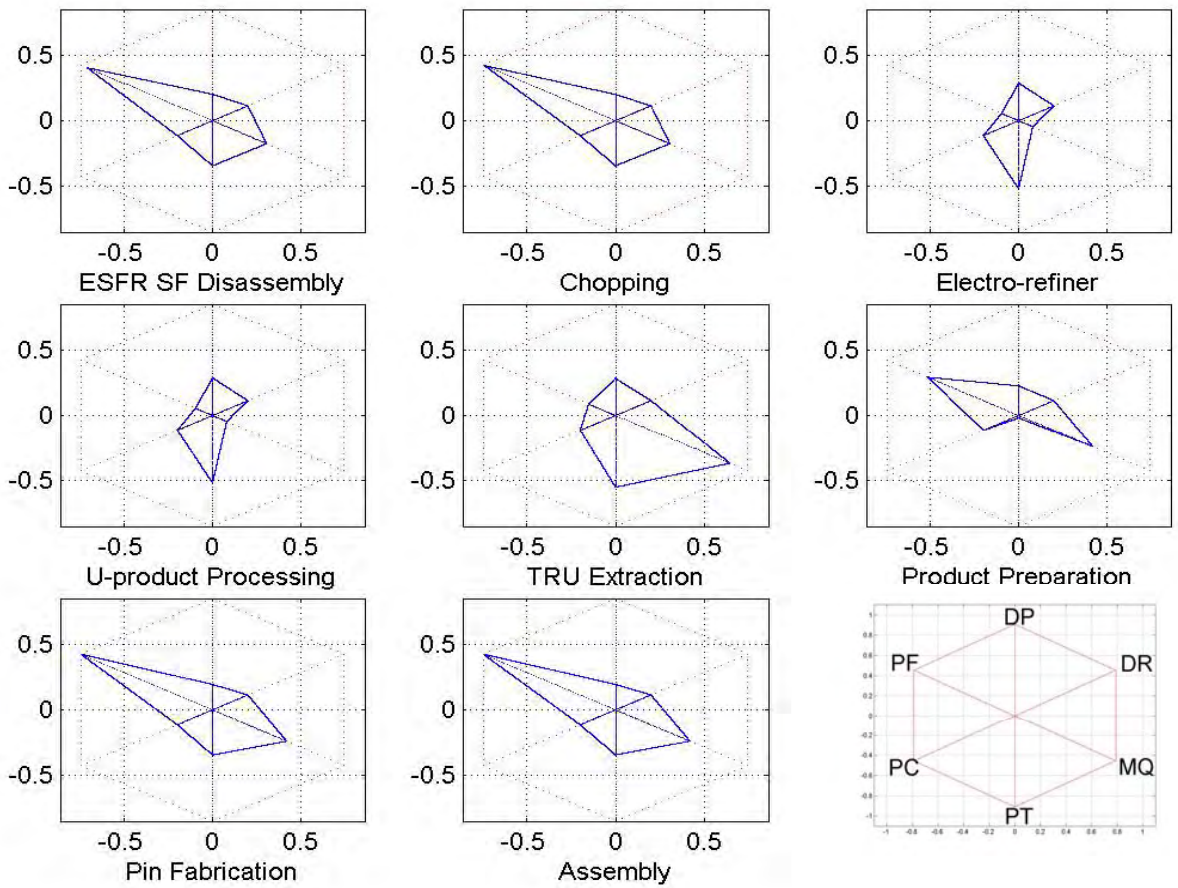
- Defines pathways to proliferation based on material stocks and flows design features
- Assumes safeguards approaches, false alarm, and intrinsic barriers
- Assumes the existence of clandestine facilities in which material can be processed and weapons can be fabricated

- Calculates
  - ✓ Detection probability at each stage of potential proliferation
  - ✓ Probability of technical failure of the proliferator
  - ✓ Probability of proliferation success
- Can Calculate
  - ✓ Least time to proliferation
  - ✓ Least cost to proliferation

Markov Model for ESFR



Sample Results: Spider Diagrams



DP: Detection probability; PF: Proliferation failure probability; PC: Proliferation cost;
PT: Proliferation time; MQ: Material quality; DR: Detection resources

Observations from Preliminary Markov Results

- No dominant scenario for all six measures
- Intrinsic barriers have significant impacts on Proliferation Time and Proliferation Failure probability and minor impacts on other measures
- Safeguards have significant impacts on both Detection Probability and Proliferation Failure probability (however, in different directions, i.e., Detection Probability and Proliferation Failure probability do not increase simultaneously but their sum increases) and no impact on other measures
- Diversion rates above certain value do not have significant impacts on Detection Probability (due to uncertainty model for MUF safeguards) but do on Proliferation Failure probability and Proliferation Time
- Generic approaches to modeling intrinsic barriers, false alarms, extrinsic barriers, concealment approach are integrated in Markov approach

"Standards for Analysis"

- Consider pathways/scenarios as well as the barriers that impede progress along each pathway
- Include an explicit threat definition
- Consider both the aspects of interest to the adversary and the defender
- Recognize that PR and PP are multi-dimensional (multi-measure)
- Demonstrate that the analysis is methodical in order to provide depth and coverage

Perspectives on PR&PP

- Introduce PR&PP at earliest stages of design

  - A tool for "Safeguards & Protection by Design"

- Focus on user needs: Provide decision options for Designers , Policy Makers and Inspectors
- Foster the establishment of a PR & PP culture
- Thus work needs to be continually sustained in this area – *not just a "one-shot" report or study*

  It's not the numbers…it's the process and the insights derived

Space Exploration Initiative

- Interagency (NASA/DOE/DOD) initiative during late 1980s-early 1990s
- Development of an overarching policy for safety functional requirements for nuclear propulsion systems

Recommended Safety Policy

- Safety is of paramount importance
- ALARA approach advocated
- Establish stringent design and operational requirements
- Ensure protection of individuals and environment
- Be consistent with applicable regulations, standards and research

Recommended Safety Policy (2)

- Establish comprehensive safety program
- Include continual monitoring, evaluation of safety performance, provide independent oversight
- Clear lines of authority, responsibility, communication
- Foster a safety consciousness in participants through SEI program

Recommended Safety Requirements

- Reactor Start-Up

1. No operation prior to space deployment, except low power testing
2. Remain shutdown prior to planned orbit

- Inadvertent Criticality

Preclude for both normal and credible accidents

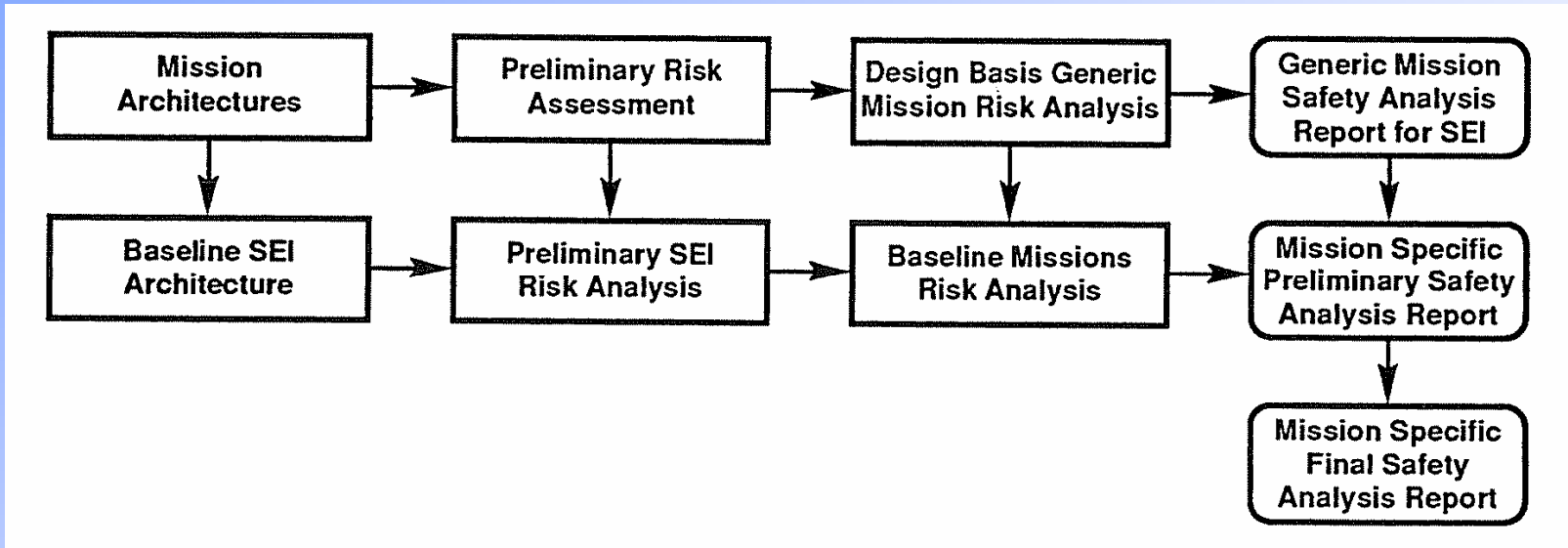
Recommended Safety Requirements (2)

- Radiological Release and Exposure
- Disposal
- Entry
- Safeguards

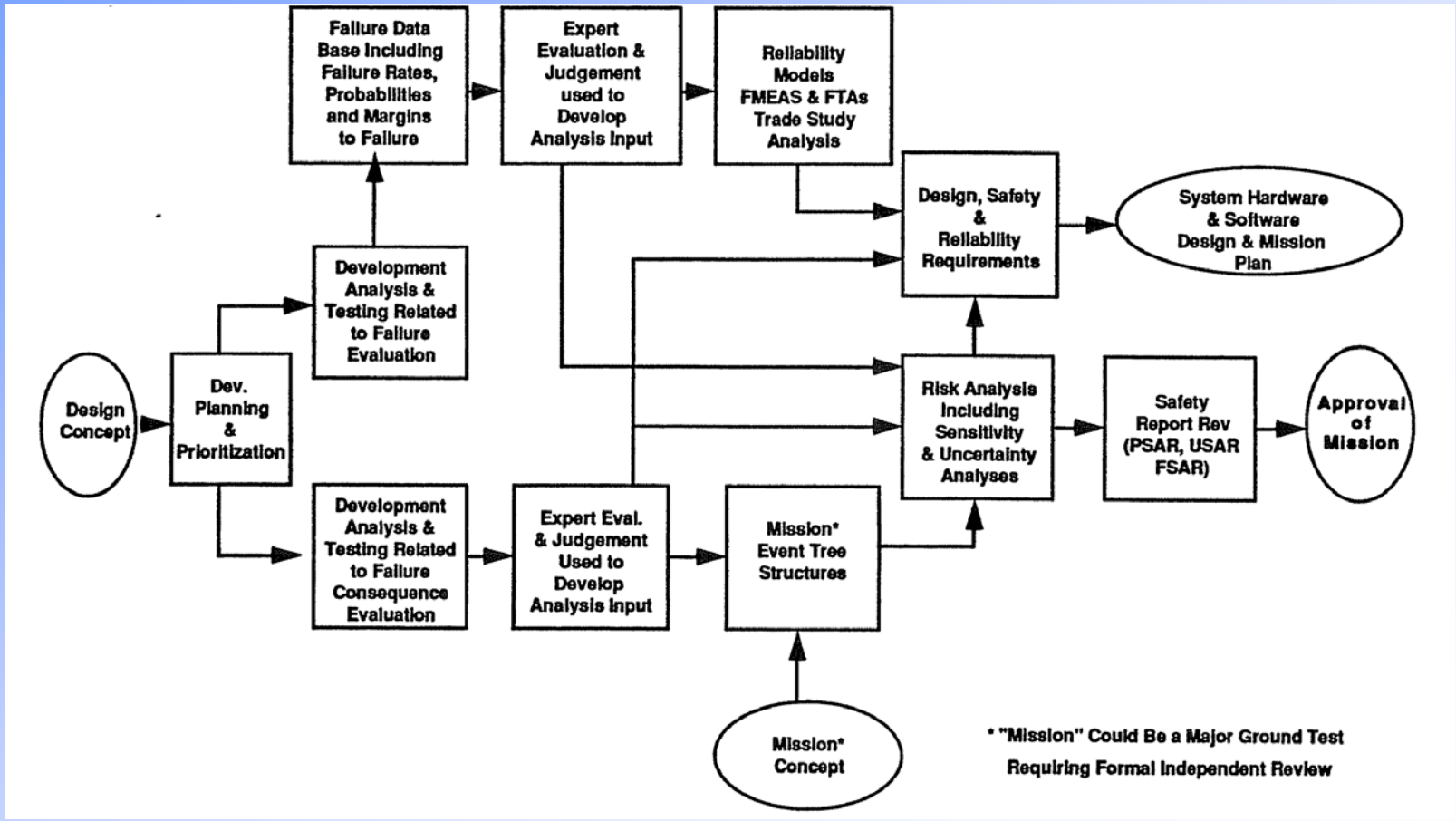
Recommended Guidelines

- Risk & Reliability
- Operational Safety
- Flight Trajectory and Mission Abort
- Space Debris and Meteoroids

Role of Risk and Safety Analysis



Detailed Risk and Reliability Approach



BROOKHAVEN NATIONAL LABORATORY

Summary

- Risk-informed approaches have been used in various applications
- Disciplined, systematic approaches can be a valuable adjunct to traditional design, operational, and safety methods
- The approach should supplement the traditional approaches, not replace them
- Decisions should be consistent with existing regulations and standards