Matching Risk Analysis Methods and Tools to the Decision Support Needs and the Technology

Presented by:
Bob Youngblood

Collaborators:
Martin B. Sattison, Curtis L. Smith

Idaho National Laboratory

www.inl.gov

INL
Idaho National Laboratory

Overview

- This talk will
  - survey the range of modeling techniques applied in venues such as the Department of Energy, NASA, process plants, and NRC, relating the techniques to the problem attributes,
  - address the data needs, and
  - address issues of interpretation of risk analysis results, and the application of risk analysis in the formulation of safety cases,

  with a view to development of a practical approach to the problem of pipeline integrity.

Acknowledgments

The talk owes a great deal to long collaboration with colleagues at the INL, and clients at NRC and NASA

Opinions expressed in this talk are those of the presenters, not necessarily the opinions of INL or its clients

Why Decision Analysis? (=> Why Risk Analysis?)

Idaho National Laboratory

- High Stakes — High stakes are involved in the decision, such as significant costs, significant potential safety impacts, or the importance of meeting the objectives.
- Complexity — The actual ramifications of alternatives are difficult to understand without detailed analysis.
- Uncertainty — Uncertainty in key inputs creates substantial uncertainty in the outcome of the decision alternatives and points to risks that may need to be managed.
- Multiple Attributes — Greater numbers of attributes cause a greater need for formal analysis.
- Diversity of Stakeholders — Extra attention is warranted to clarify objectives and formulate performance measures when the set of stakeholders reflects a diversity of values, preferences, and perspectives.

What questions are we answering with risk analysis? Examples:

- Is this facility (system, design, operating practice) safe enough to be allowed to operate?
- What makes this facility (system, design, operating practice, …) safe enough to be allowed to operate? **Under what conditions is it safe?**
  - Systems, structures, & components (SSCs), operating procedures, operators, training, …
  - … shown by analysis to meet safety requirements (potentially including a demonstration of being "as safe as reasonably practicable")

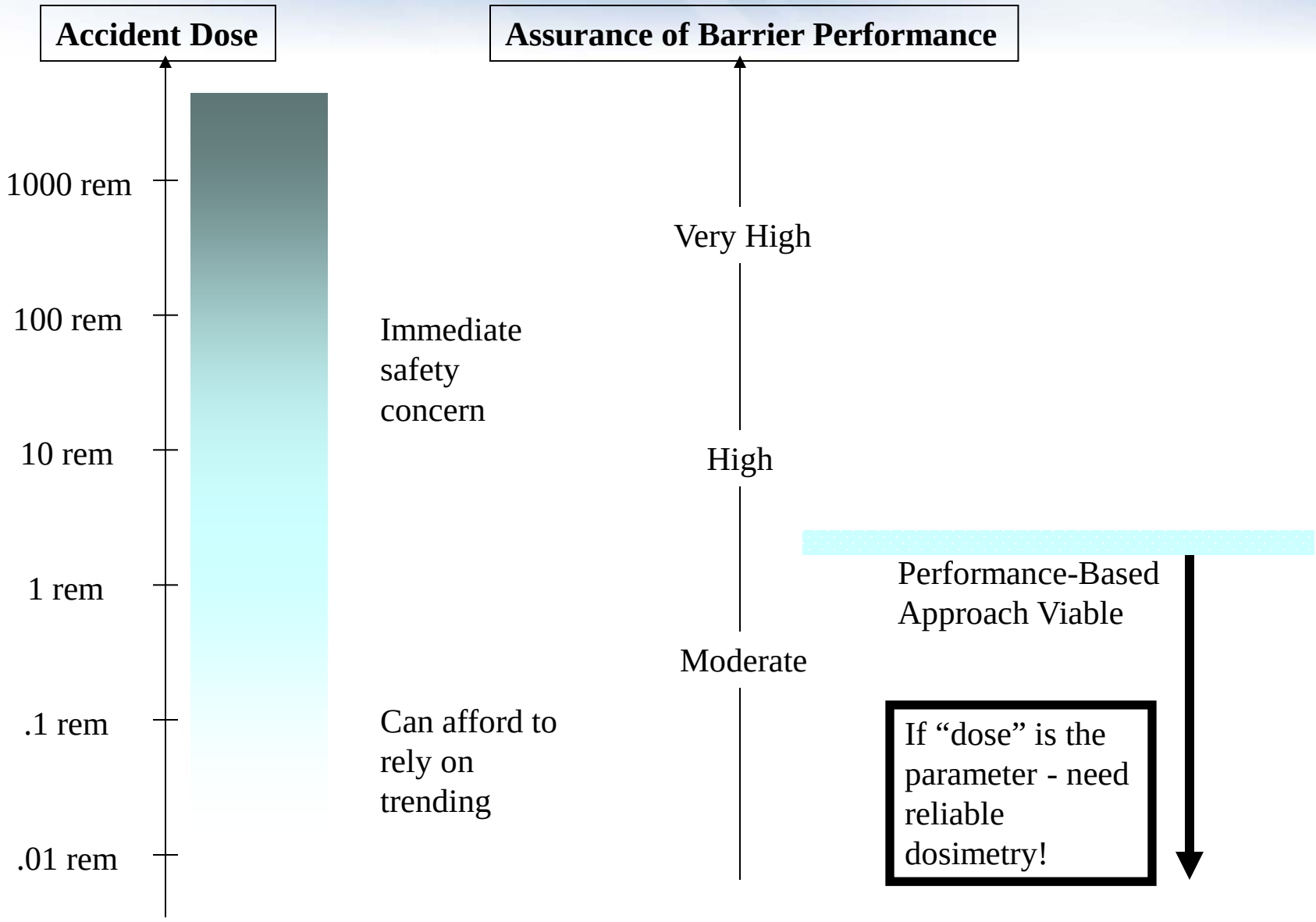
The analysis that answers these questions is a roadmap to what has to be achieved in order to actually attain the desired level of safety.

  - *System capability, reliability, availability, …*

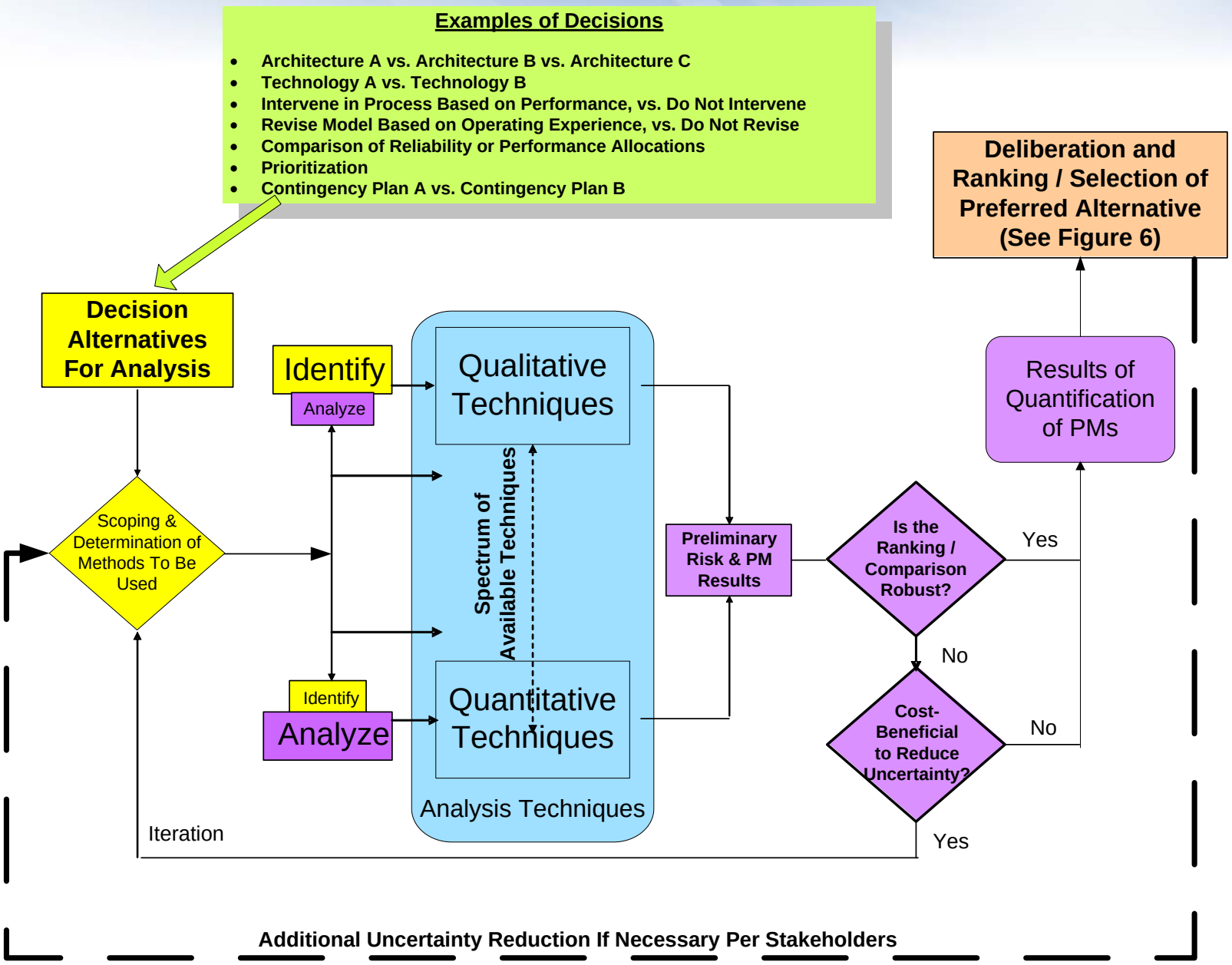
Do we need an integrated model of aggregate risk?

- What sorts of trade studies / prioritization exercises do we need to perform?

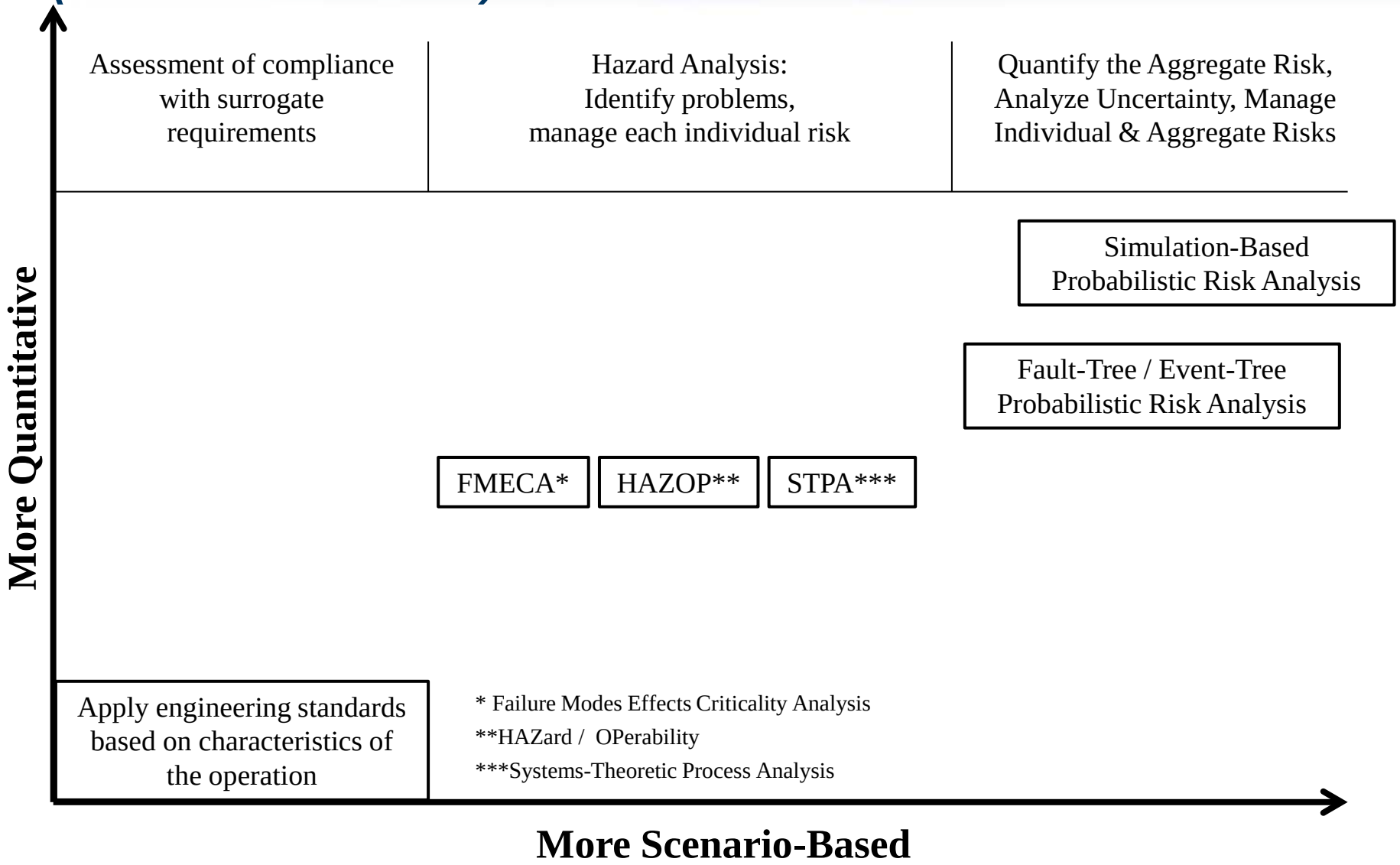
Level Of Assurance Needed As A Function Of Hazard



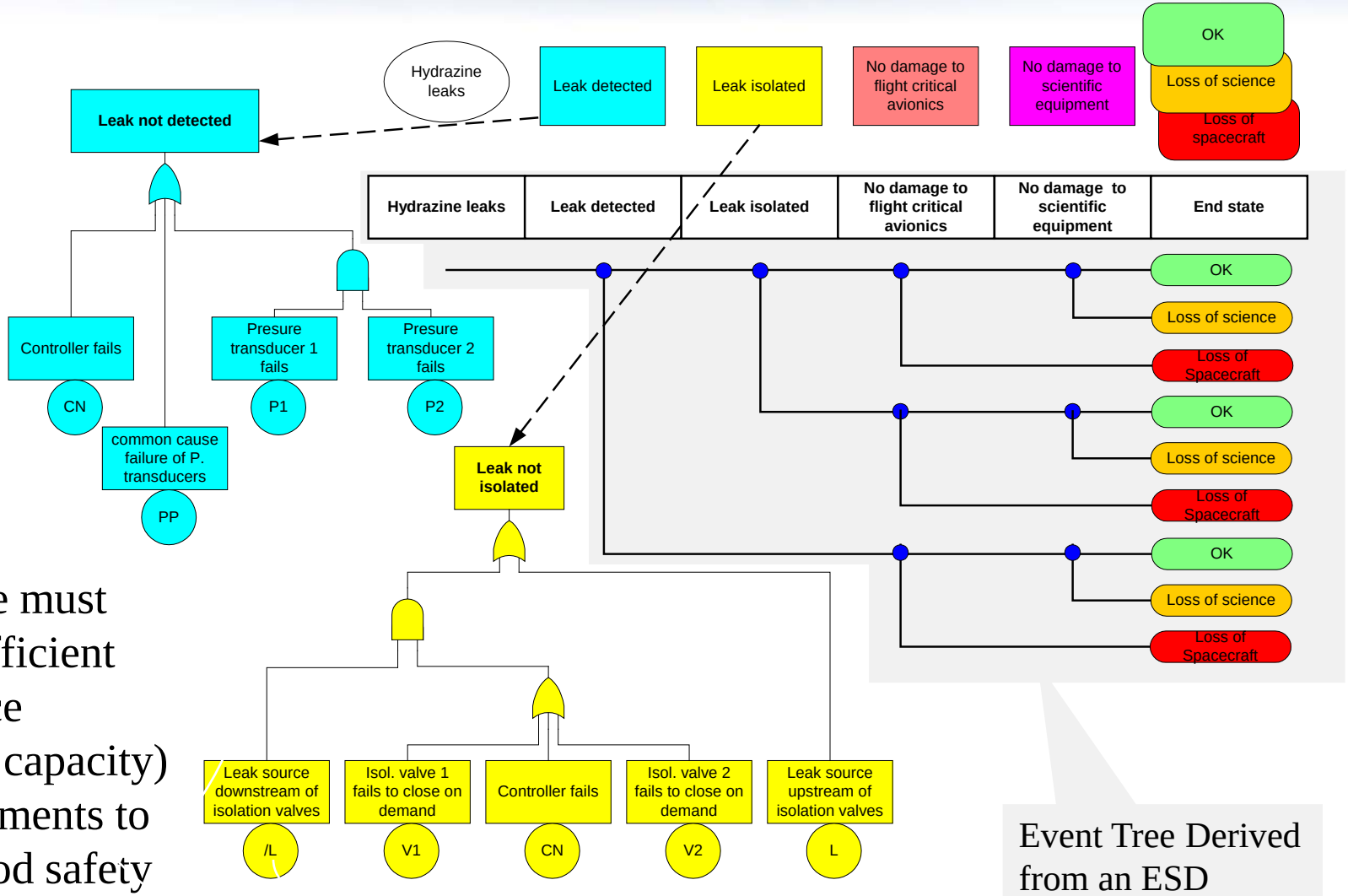
Graded Approach to Analysis



Risk Assessment / Risk Management Tools
(not an exhaustive set)



Each Pivotal Event May Require Detailed Analysis



Safety Case must allocate sufficient performance (reliability, capacity) to these elements to achieve good safety outcome

Event Tree Derived from an ESD

Source: NASA PRA Procedures Guide

Scope of System Safety Modeling (NASA NPR 8715.3C)

Table 2.1. Criteria for Determining the Project Priority

CONSEQUENCE CATEGORY	CRITERIA / SPECIFICS		Project Priority Ranking
Human Safety and Health	Public Safety and Health	Planetary Protection Program Requirement	I
		White House Approval (PD/NSC-25)	
		Space Missions with Flight Termination Systems	
	Human Space Flight		
Mission Success (for non-human rated missions)	High Strategic Importance Projects		
	Limited Window		
	High Cost (See NPR 7120.5)		
	Medium Cost (See NPR 7120.5)		II
	Low Cost (See NPR 7120.5)		III

Table 2.2: Graded Approach to System Safety Modeling

Priority Ranking	Scope (The level of rigor and details are commensurate with the level of design maturity
I	Probabilistic Risk Assessment (per NPR 8705.5) supported by qualitative system safety analysis
II	Qualitative system safety analysis supplemented by probabilistic risk assessment where appropriate
III	Qualitative system safety analysis

Methods in use at the NRC

- Initially, and still today: demonstration of safety performance through analysis of design-basis events (originally, the “maximum credible accident”)
- First large-scale probabilistic risk analysis (PRA): WASH-1400 (“Reactor Safety Study,” aka “The Rasmussen Report”)
  - Done for two plant types to show how safe operating plants were
  - Used fault-tree / event-tree methodology
- Based in part on PRA application, many requirements were changed after WASH-1400, especially after the Three Mile Island accident
  - Some rules added, Some requirements relaxed
- Nowadays:
  - PRA is required for design certification
  - PRA is a key tool for “Risk-Informed Regulation” and, especially, application in the Reactor Oversight Process

Reactors

Non-reactors

- Probabilistic performance modeling of geologic repository
- Equivalent of hazard-analysis-based methods in regulation of byproduct materials systems

5. USES OF PRAs IN DOE NUCLEAR SAFETY APPLICATIONS

DOE P 420.1 allows the use of PRA when employed to supplement DOE's qualitative/ deterministic processes* and supported by industry practices and availability of risk data.

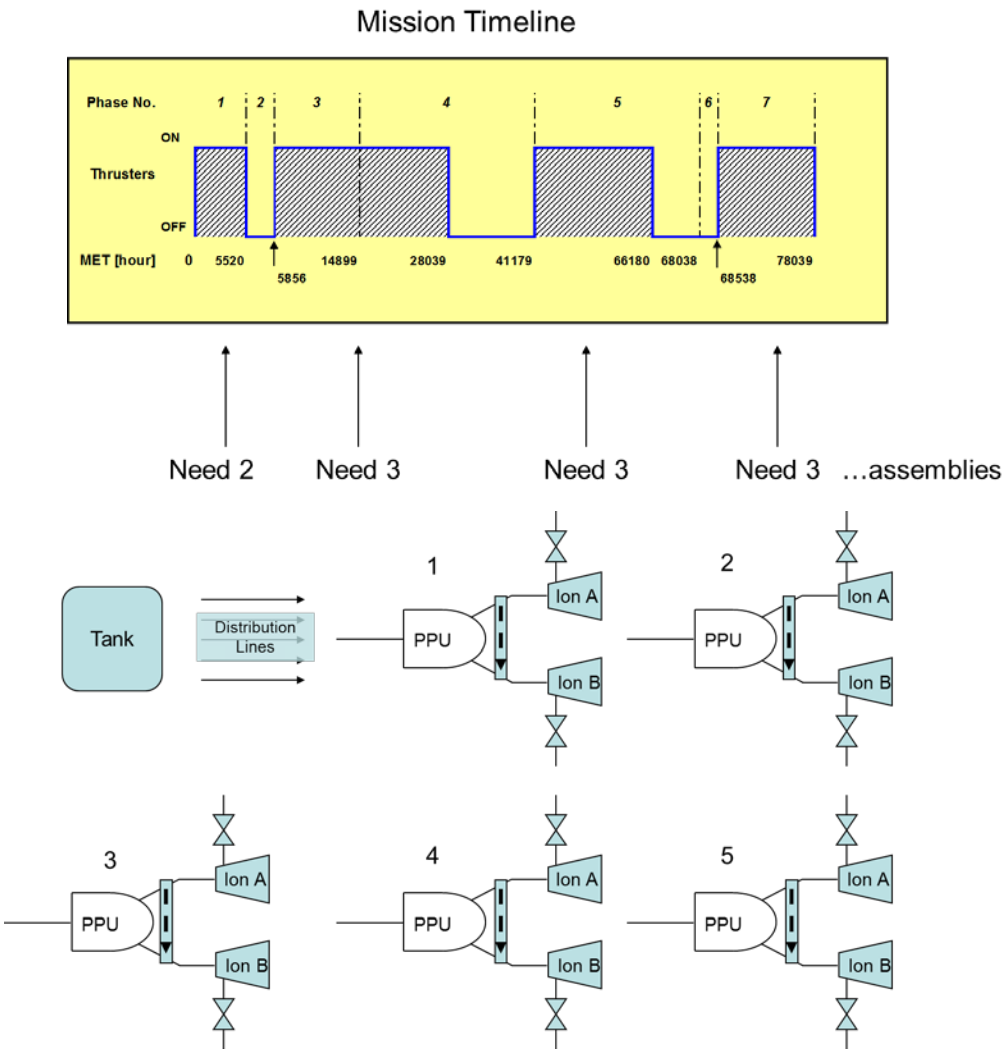
In determining whether a facility-specific PRA should be pursued, the following are relevant considerations:

- Purpose for the PRA (risk-informed decisions, complex accident phenomena and progression, …
- Complexity of facility processes (number and complexity of SSCs, scope of facility functions and operations), and relevant phenomena (such as fires);
- Magnitude of unmitigated dose consequences; and,
- Programmatic importance of the facility (mission critical), and facility design life-cycle stage (new, existing, major modifications).

DOE has determined that PRA insights may be used to supplement traditional analytic approaches; examples are provided below.

*Such as analysis of evaluation-basis events

Simulation-based risk analysis vs. Conventional Fault-Tree / Event-Tree Models

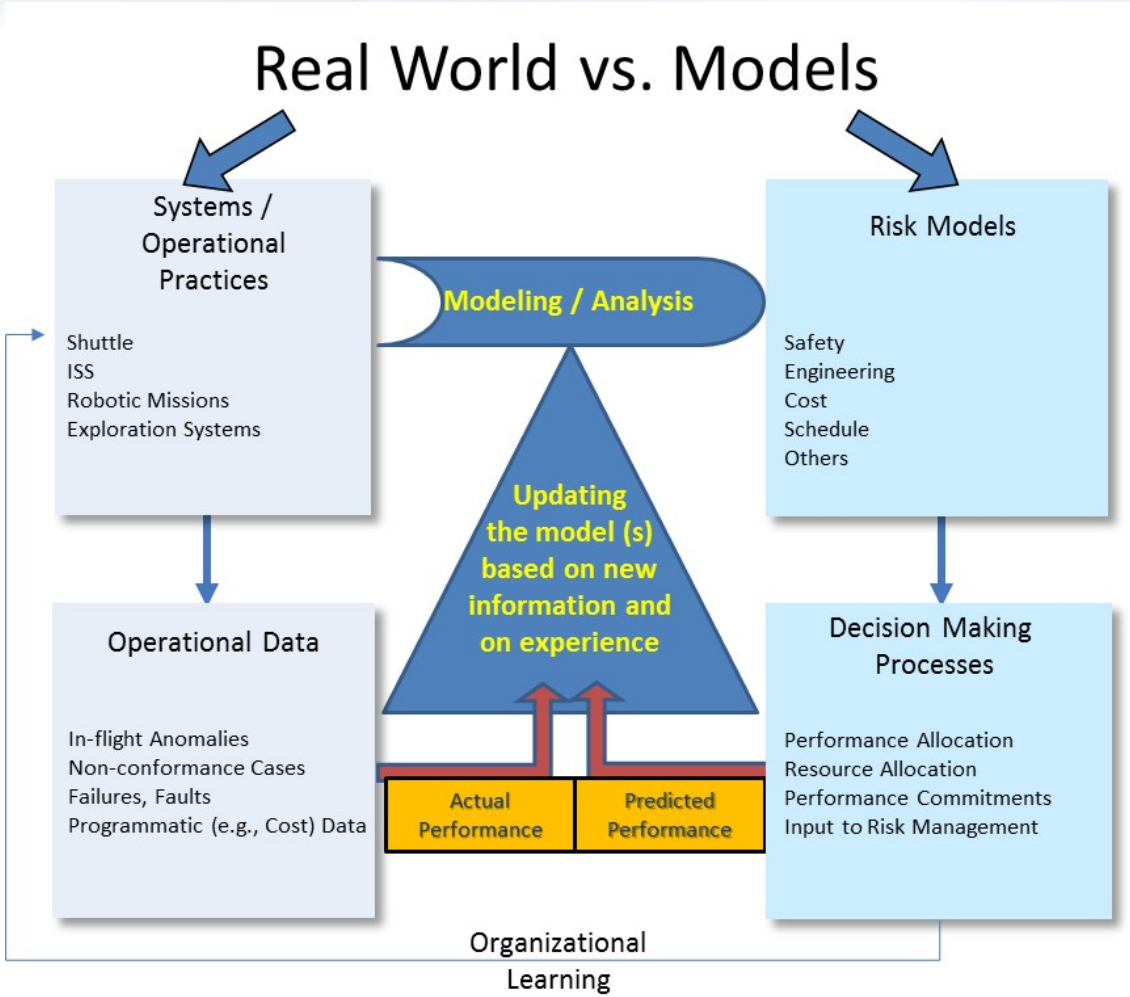


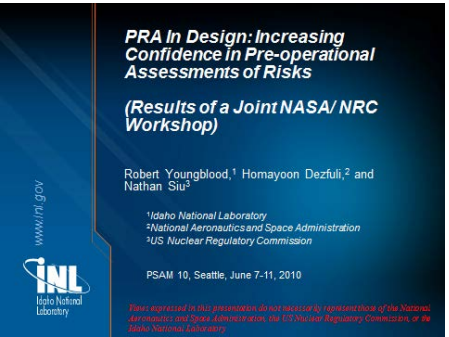
- Space craft 10-year mission with a lot of switching propulsion on & off
- Timing issues, varying amount of propulsion needed, …

Trying to model this system in a FT / ET framework was
(a) Beyond difficult, and
(b) Unnecessary,
given that a simple rule-based simulation could do the job perfectly well.

Real World vs. Models

Models (not just 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 "model"





Completeness <= Learning from precursors

Summary

- In safety oversight of high-hazard systems, there is arguably broad consensus on the following needs:
  - To analyze hazards and controls in a fundamentally scenario-based way
    - Too much is missed through over-reliance on analysis of surrogate events
  - To match analysis rigor to the decision being made
    - Uncertainties have to be understood well enough to plan the analysis intelligently within a graded approach
  - To match safety system performance requirements …
    - capability (including safety margin), reliability (including redundancy and diversity), availability

    … and operating practices and oversight (inspection, …) …

    … to the situation
    - frequency of system challenges, consequences of safety system failure
- Integrated PRA modeling is not the sole basis for safety oversight [where it is used at all], but many complex, high-stakes situations call for some form of it

Summary (2)

- In general, it's necessary to think very carefully about the interpretation and applicability of "data"
    - Can't just look them up in "data bases"
    - Your failure probability number depends on the causal mechanisms that operate in your application
- In regulatory applications especially, it's important to think carefully about how to interpret the numbers
    - If a regulated entity is using risk analysis in a dialogue with the regulator, then some of the numbers arguably represent investment decisions
        - "We commit to achieving the quoted level of reliability …"
    - Monitoring of performance in those areas may be an appropriate performance-based approach to ongoing confirmation of satisfactory safety performance
        - As in the case of NRC's Reactor Oversight Process for operating nuclear power plants
            - Reliability and availability of key systems are trended and the results are used (along with other inputs) to direct regulatory attention to possible performance issues

Summary (3)

- Model results are typically conditional on assumptions about operating environment, component quality, inspection, monitoring, etc., and it's important to be sure that the reality of these things is consistent with those assumptions
- Therefore, commit to continuous review of experience in order to:
  - Pick up on previously unappreciated accident causes, and
  - Improve the quantitative basis for decision-making

References

1. Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, WASH-1400 (1975).
2. S. Kaplan and B.J. Garrick, “On the Quantitative Definition of Risk,” **Risk Analysis 1**, 11-27(1981).
3. “Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners,” NASA SP-2011-3421, Second Edition (National Aeronautics and Space Administration, 2011).
4. NPR 8000.4A, “Agency Risk Management Procedural Requirements” (National Aeronautics and Space Administration, December 16, 2008).
5. NASA/SP-2010-576, “NASA Risk-Informed Decision Making Handbook” (National Aeronautics and Space Administration, April, 2010).
6. U.S. Department of Defense Draft Military Standard (MIL-STD-882E) Standard Practice for System Safety
7. **Engineering a Safer World**, N. G. Leveson
8. SAPHIRE.INL.GOV (Fault tree / event tree software)
9. NASA General Safety Program Requirements, NPR 8715.3C
10. NASA Accident Precursor Analysis Handbook, NASA/SP-2011-3423.
11. Space Propulstion System Phased-Mission Probability Analysis Using Conventional PRA Methods, J. Knudsen and C. Smith, Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management, May 14-18, 2006, New Orleans, Louisiana, USA (ASMe, 2006).

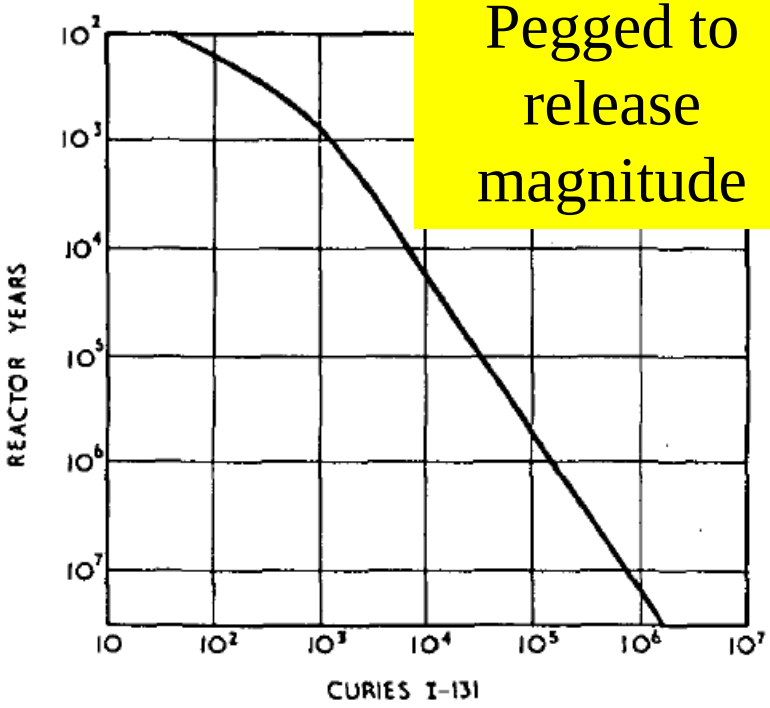
PARKING LOT

SITING CRITERIA - A NEW APPROACH
F. R. FARMER

The development of siting philosophies and criteria during the past decade is reviewed. Experience in applying the criteria is described and the problems arising from their qualitative nature are examined. A new quantitative approach developed by the United Kingdom Atomic Energy Authority and currently being applied to problems of reactor siting is described. It is shown how this approach can facilitate assessment and lead to a quantitative criterion of acceptability.

Proceedings of a Symposium
Vienna, 3-7 April **1967**
Containment and Siting of Nuclear Power Plants

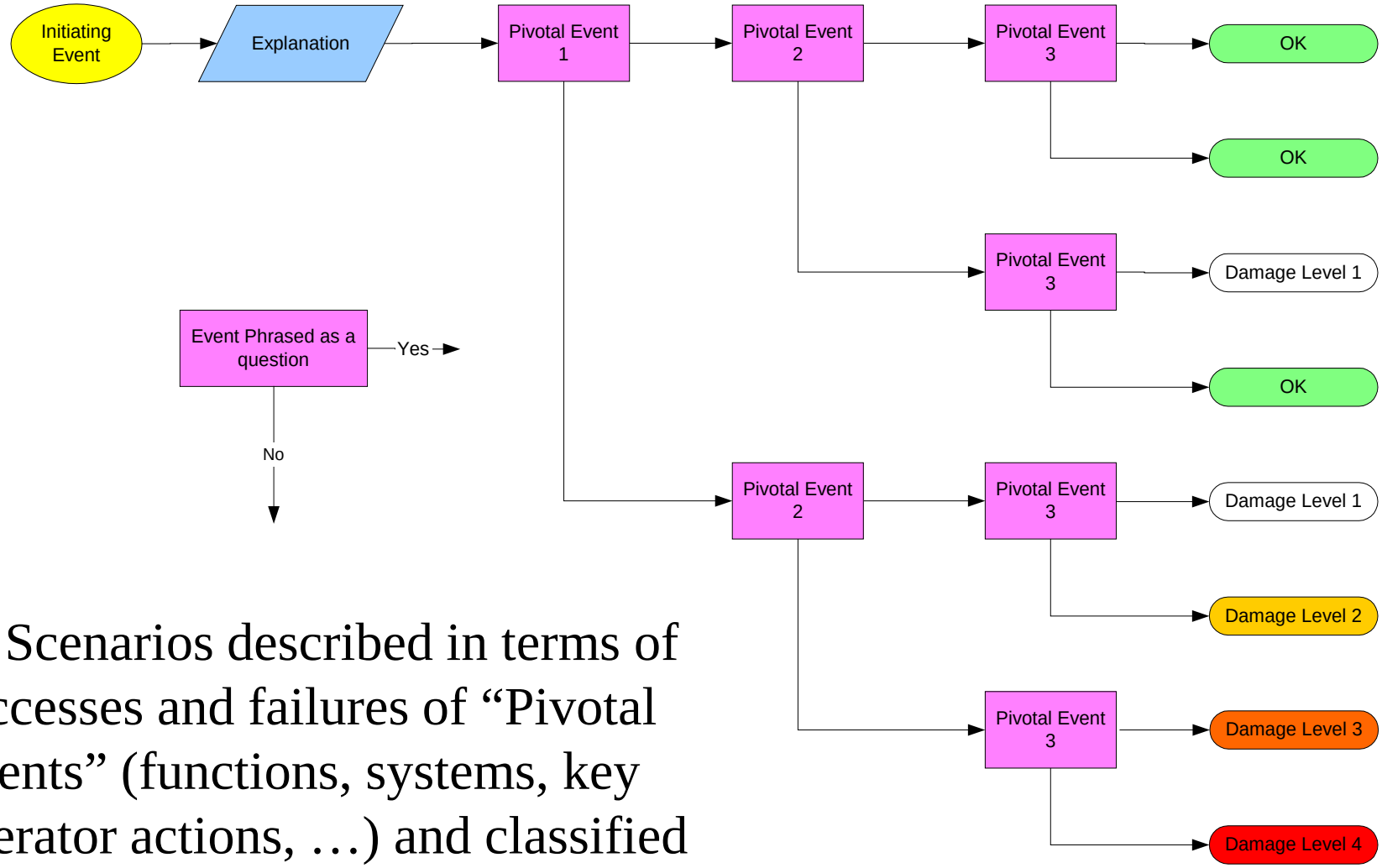
SM-89/34



Pegged to release magnitude

FIG. 12. Proposed release criterion

Scenario modeling may start with "Event Sequence Diagrams" (ESDs)



… Scenarios described in terms of successes and failures of "Pivotal Events" (functions, systems, key operator actions, …) and classified by outcome severity

Meaning of "PRA"

- Some assume that PRA should furnish risk metric results to the decision maker, who then uses these results (along with uncertainty information) in his/her own way to formulate expectations regarding the performance of decision alternatives.
- This purely prognostic view of PRA is too narrow:
  - The PRA should be understood not just as an unconditional (albeit uncertain) prediction of performance, but more importantly as a mapping from presumed (or perhaps "committed") performance levels of components and subsystems to top-level risk metrics.
  - The design-stage PRA should be seen as a tool for **allocation**.
    - Its output is not prognostic, but only ***conditionally*** prognostic: its results can apply only if certain input levels of performance are attained in practice.
- This attitude towards the numbers arguably applies to any model-based assessment of a decision alternative

➢ **So a key part of risk management is establishing whether those input levels are, in fact, coming true**

  - **What about component aging? Maintenance effectiveness? …**

Completeness

- All synthetic methods* (arguably, **all methods**) are challenged by the completeness issue
  - Have we thought of everything?
  - It is arguably possible to write down a complete set of classes of functional scenarios that will lead to adverse consequences, but it is difficult to argue the completeness of the set of *causes* of those scenarios
- It is found that many serious accidents have been presaged by precursor events, or at least by indications of impending failure
- This suggests monitoring and trending operational experience, including a careful review of experience to identify previously unappreciated near misses

➢ **So there are multiple reasons to keep trying to reconcile the model with reality:**
  - **Are the numbers coming true?**
  - **Did we leave anything out?**

* Methods in which we model aggregate risk as a combination of contributions from scenarios that we explicitly identify *a priori*