Overview of Risk-Informed Regulation of Operating Nuclear Reactors

Presented to the Joint Meeting of the
Boston and Hartford Actuaries Clubs
November 17, 2011

Steven A. Laur
Sr. Technical Advisor – Risk-Informed Initiatives
Division of Risk Assessment
USNRC Office of Nuclear Reactor Regulation

Topics

- Risk-Informed Regulation
  - Commission's Safety Goal Policy Statement
  - Reactor Risk Metrics
  - Key Principles
- Probabilistic Risk Assessment (PRA)
  - Description and Bases of Nuclear Plant PRA
  - PRA Building Blocks
  - Solving the PRA Model
- Example Applications
  - Rules
  - Licensing and Certification
  - Oversight
- Conclusion

What do risk and risk-informed regulation mean?

What is risk?

- In everyday usage, "risk" is often used synonymously with the probability of a loss.
- In the context of evaluating risk from a nuclear power plant, risk is commonly expressed as the "risk triplet":
  1. What can go wrong (accident scenario)?
  2. How likely is it (frequency on a reactor year basis)?
  3. What are the consequences (impact on the plant or on people)?
- We characterize risk in terms of its effect on people
  - What is the likelihood of a nuclear accident
    - Causing near-term death? (prompt fatality)
    - Causing death from cancer? (latent fatality)

Commission's Safety Goal Policy

- Safety Goal Policy
  - Intent
    - Addresses risks to public from nuclear power plant operations with the objective of "establishing goals that broadly define an acceptable level of radiological risk that might be imposed on the public as a result of nuclear power plant operation"
    - Establish "how safe is safe enough"
  - Approach
    - Qualitative goals
    - Quantitative objectives

August 21, 1986 (51 FR 30028)

Commission's Safety Goal Policy

- Qualitative goals
  - "Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health."
  - "Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks."

Commission's Safety Goal Policy

- Quantitative objectives
  - Risk of prompt fatality to an average individual in vicinity of a nuclear power plant that might result from reactor accidents
    - < 1/10 of 1% of the sum of prompt fatality risks from other accidents
    - Numerically – 5×10^{-7} per year
  - Risk of cancer fatalities to population in area near a nuclear power plant that might result from operation
    - < 1/10 of 1% of sum of cancer fatality risks
    - Numerically – 2×10^{-6} per year

How do we characterize risk?

- Subsidiary objectives
  - Core damage frequency (CDF) no more than about **once every 10,000 years (1E-4/year)** per plant
    - Surrogate for latent cancer fatalities
  - Large early release frequency (LERF) no more than about **once every 100,000 years (1E-5/year)** per plant
    - Surrogate for prompt fatalities

What tools are available to evaluate risk?

- Probabilistic Risk Assessment (PRA) Methods
  - PRA is a structured, analytical process for identifying potential weaknesses and strengths of a plant design in an **integrated** fashion
  - **One way** of analyzing risk in the nuclear industry
  - PRA provides a framework for explicitly addressing and presenting uncertainties (vs. making conservative assumptions to deal with uncertainty)

- Alternate methods include:
  - Qualitative arguments
  - Bounding analyses
  - Screening tools

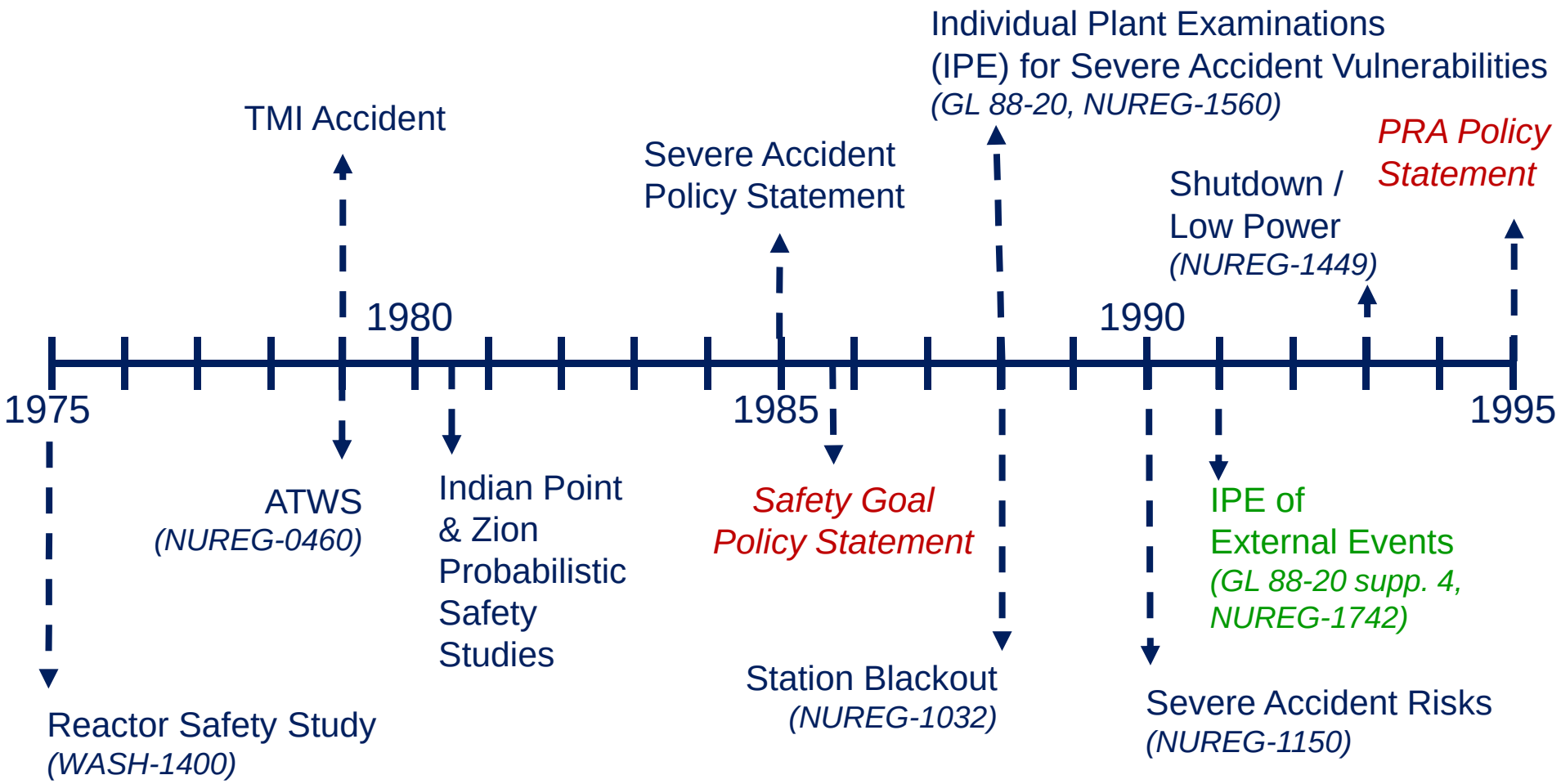
Why are risk-informed approaches used?

- Reactor Safety Study (WASH-1400)* assessed reactor risk using PRA
  - Revealed actual risk significant areas and interactions that were very different from the design basis events
    - Ex: **small loss of coolant accidents (LOCAs)** are significant risk contributors
  - Demonstrated the value of an **integrated** view of risk

- Other risk studies followed to expand on these early findings

** NUREG-75/014, 10/75*

Early History – Risk Studies



Risk-Informed Regulation

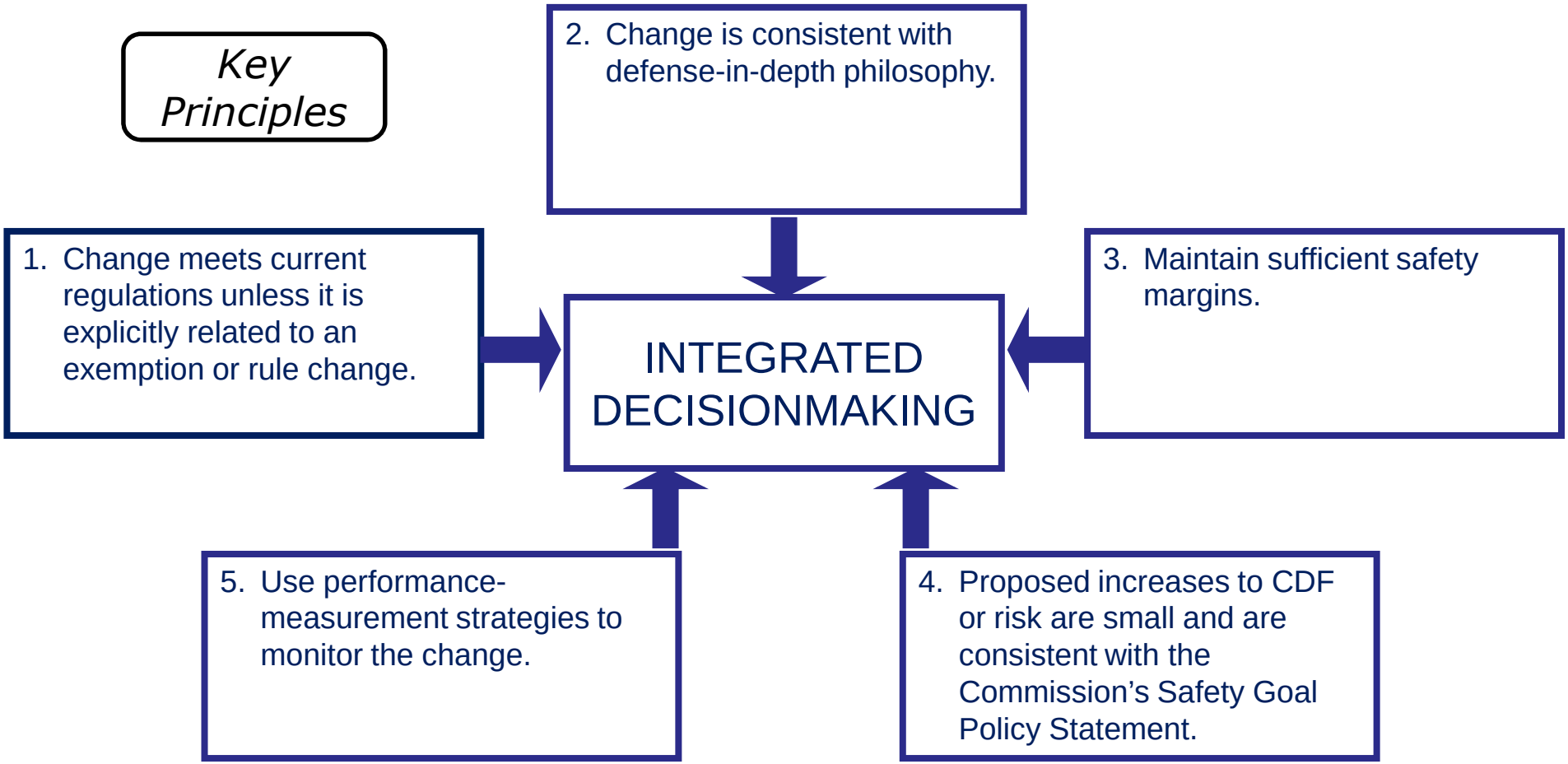
- A philosophy whereby risk insights are considered together with other factors* to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to health and safety.

- NRC approach is not "*risk-based*"

* e.g., traditional engineering approaches

(Source: SRM on SECY-98-144, 3/1/99)

Principles of Risk-Informed Regulation



(Source: RG 1.174, 11/02)

How do we build PRA models?

What is a PRA?

- Risk assessments include identification and analysis of…
  - Initiating events
    - Circumstances that put a nuclear plant in an **off-normal condition**
  - Safety functions
    - Functions designed to **mitigate the initiating event**
  - Accident sequences
    - Combination of **safety function successes and failures** that describe the accident after an initiator
- Successful response is that the plant transitions to safe, stable end-state for specified period of time
- We use a PRA model to look at the frequency and consequences of NOT achieving a safe, stable end-state

What is an Initiating Event?

- Understanding the plant perturbation – "initiating event"
  - Transient (loss of feedwater, condenser vacuum, instrument air, etc.)
  - Loss of offsite power
  - Loss of coolant accident
- Understanding how the plant responds to the perturbation
  - **Physical responses**
    - Neutronic
    - Thermal-hydraulic (e.g., vessel and containment pressure, temperature, water level)

  Automatic responses
    - Reactor trip/turbine trip
    - Mitigating equipment actuates

  Operator responses (per procedures)
    - Manual reactor trip
    - Manual switchover to sump recirculation

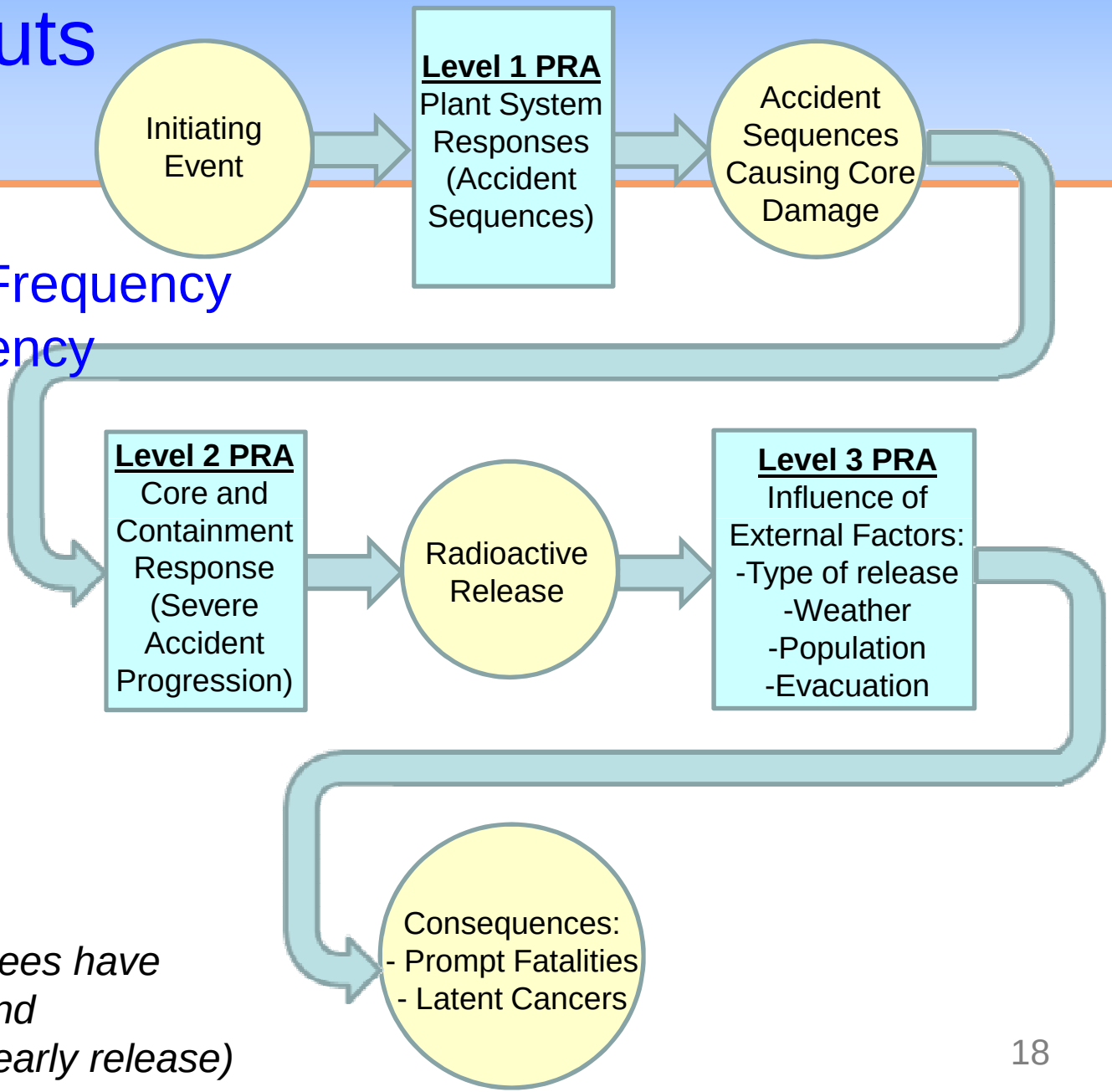
What are typical safety functions? Accident sequences?

- Safety functions include
  - Maintaining the core sub-critical
  - Maintaining coolant inventory
  - Removing fission-product decay heat
- Accident sequences are:
  - An initiating event, plus
  - Failures of equipment relied upon to fulfill safety functions, such that
  - A safe, stable end state is not achieved

PRA Outputs

"Levels"

1. Core Damage Frequency
2. Release Frequency
3. Consequences



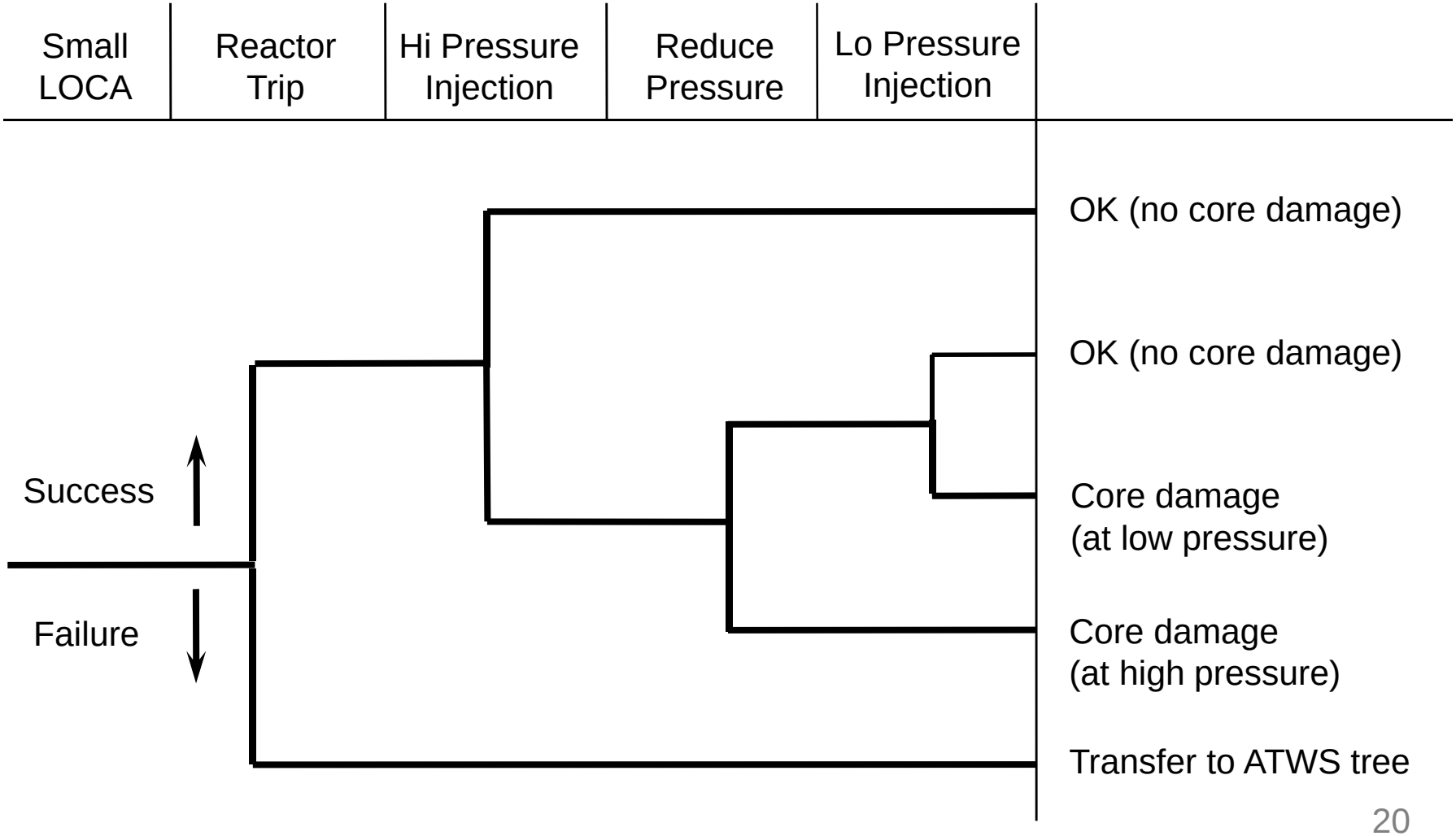
Most nuclear plant licensees have Level 1 (core damage) and simplified Level 2 (large-early release)

What are the basic components of a PRA?

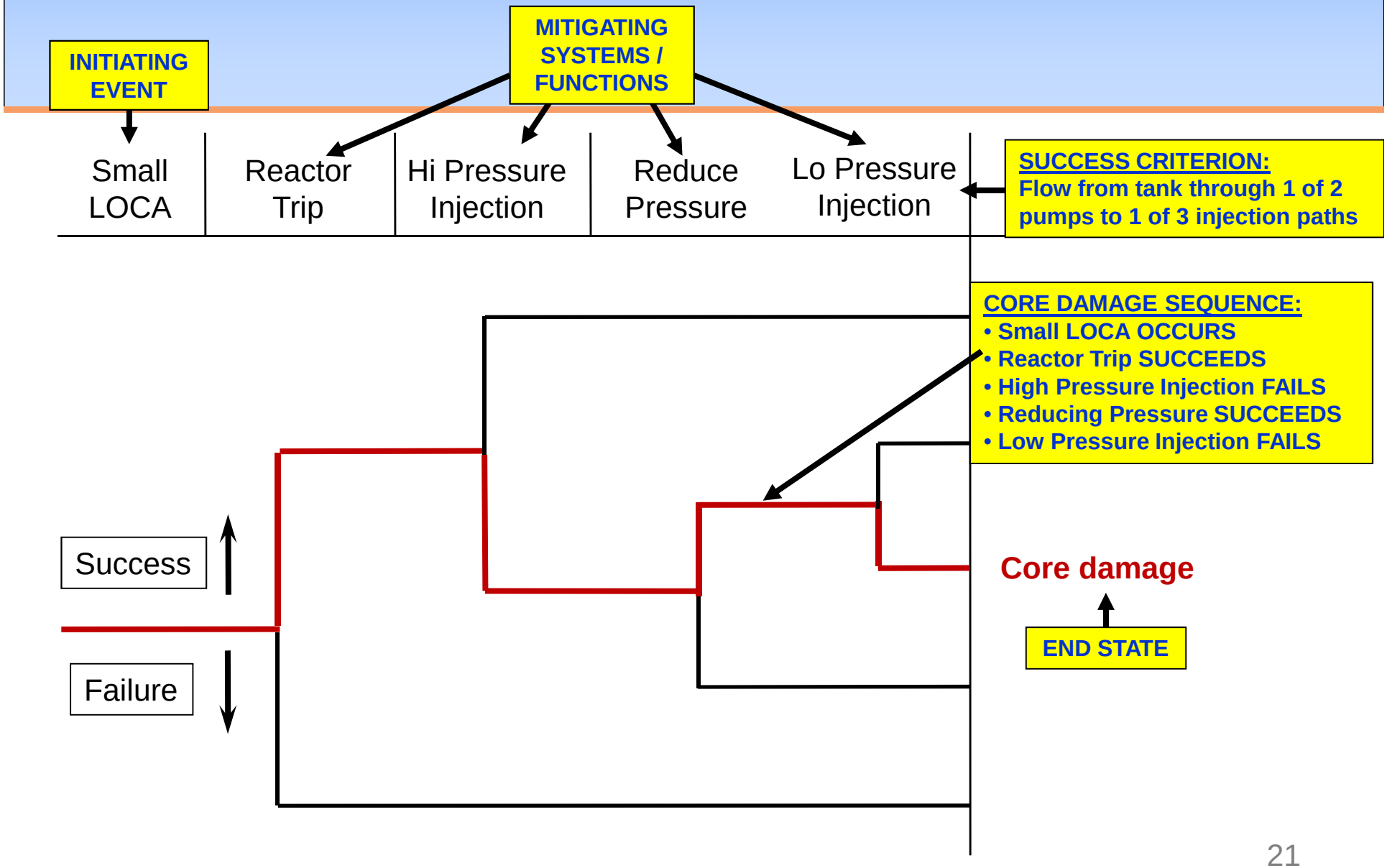
- PRA models use
  - **Event trees** to model the sequence of events from an initiating event to an end state
  - **Fault trees** to model failure of mitigating functions, including equipment dependencies to function as required
  - **Frequency** and **probability** estimates for model elements (e.g., initiating events, component failures)

What is an event tree?

A graphical depiction of a sequence of events



What is an event tree?



What is an event tree?

- Event tree "top events" may represent:
  - Functions or systems to **mitigate** core damage
  - Key **operator actions**
  - **Containment** support systems
- Event tree also used for Level 2
  - Use tree to model **core melt and severe accident phenomenology** that challenges containment integrity

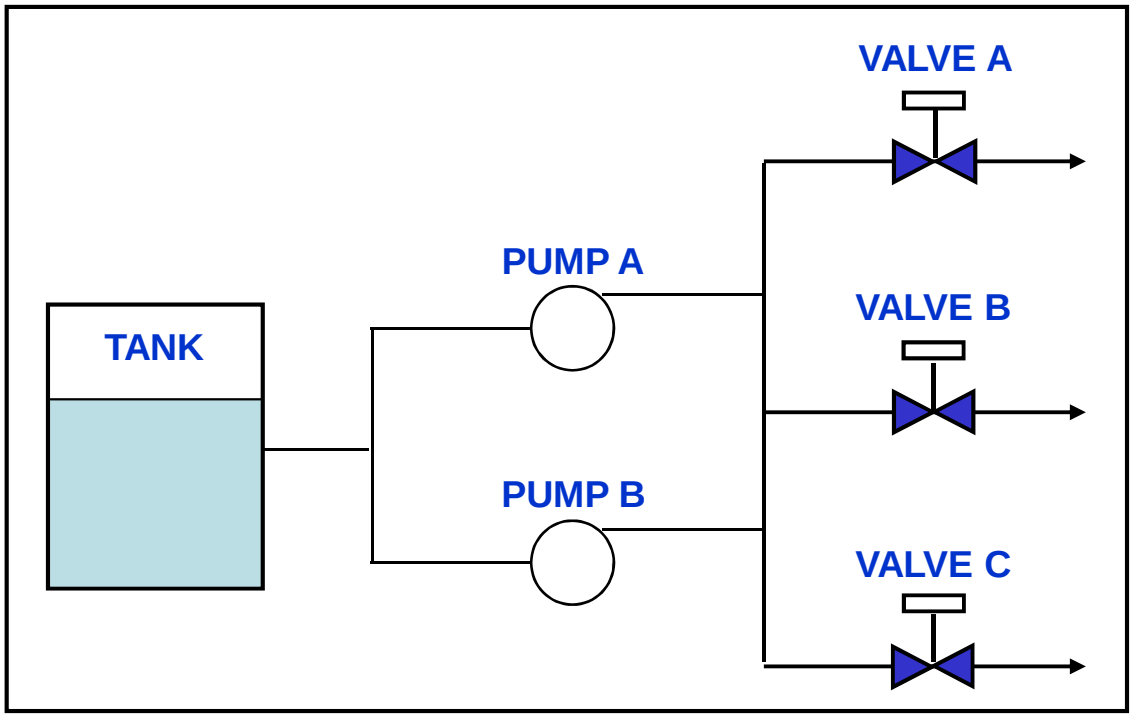
    LERF is a subset of Level 2 – specific tree end states

What is a fault tree?

A graphical depiction of how a system can fail

SUCCESS CRITERION:
Flow from tank through 1 of 2 pumps to 1 of 3 injection paths

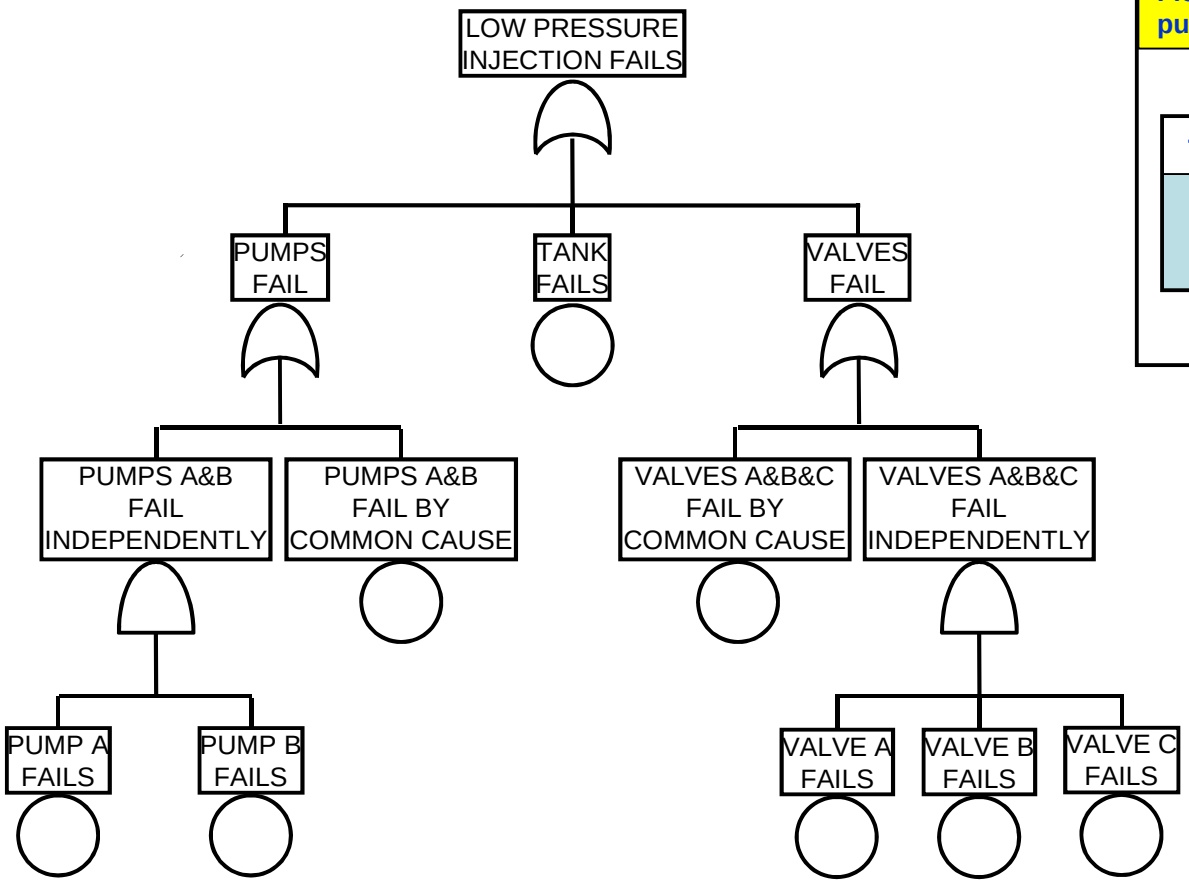
FAILURE OCCURS WHEN:
No flow from tank
OR
No flow from pumps
OR
No flow through injection paths

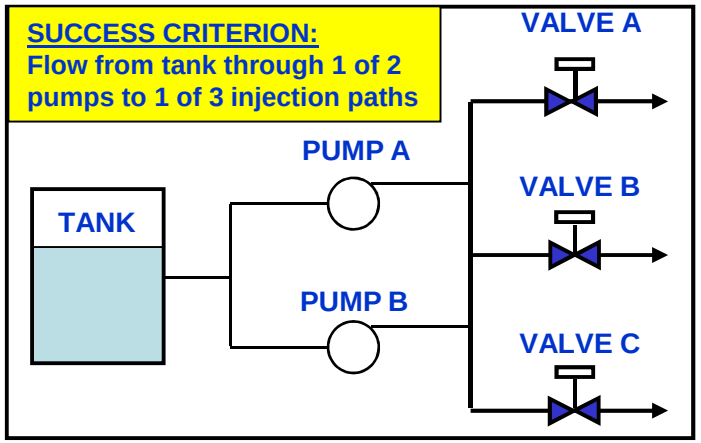


What is a fault tree?

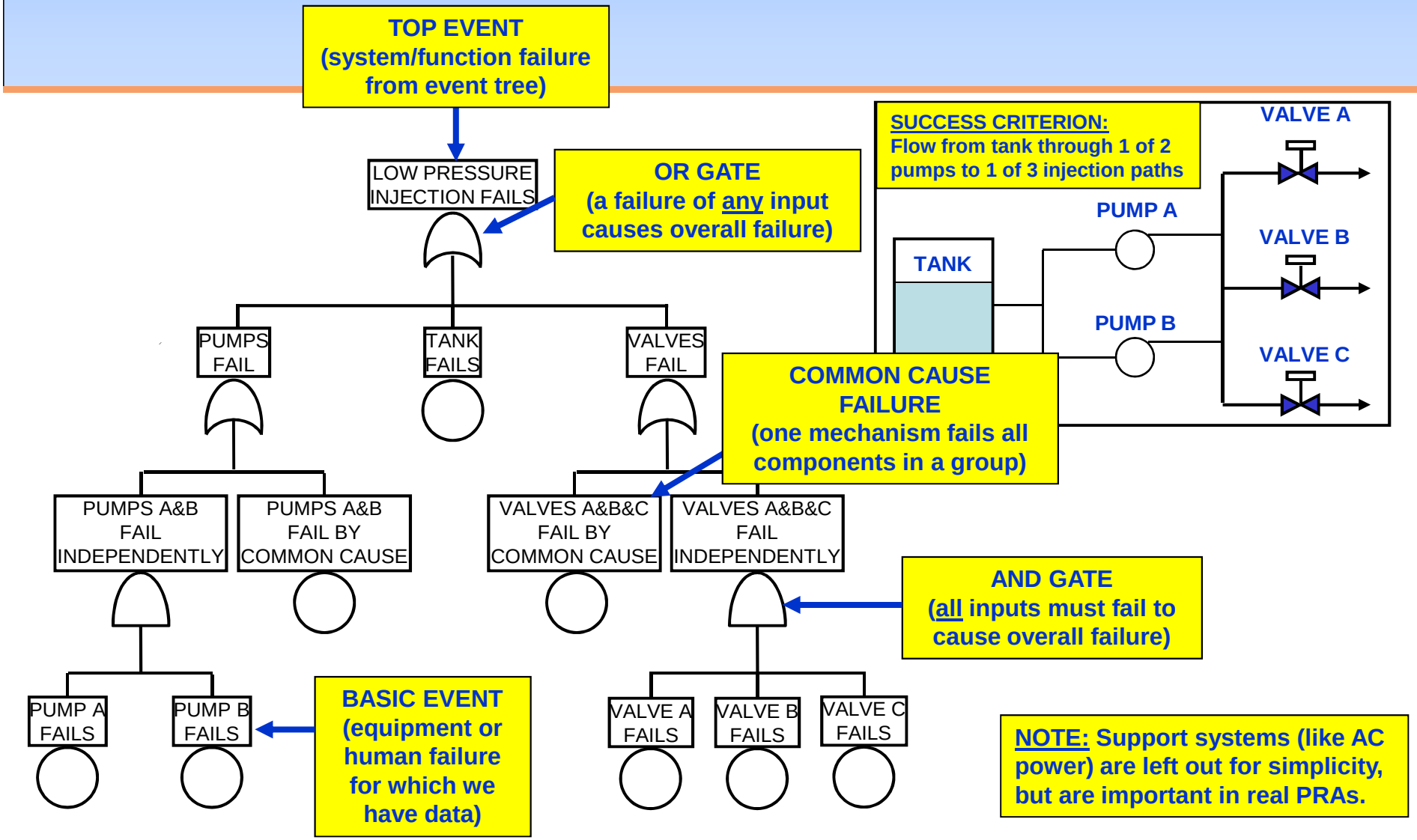
- Developing fault trees
  - Need for fault tree usually arises from the event tree
    - What equipment can provide the function?
    - What operator actions must take place?
  - Define **success criteria**, e.g.
    - How much flow is needed to remove decay heat?
    - How much flow is necessary to restore inventory?
    - How many valves must close to isolate containment?
  - Determine the **failure modes** to include in the tree
  - Determine supporting systems; e.g., electric power, room cooling, seal and cooling water, control power, etc.
  - Continue modeling to **basic event level**

What is a fault tree?



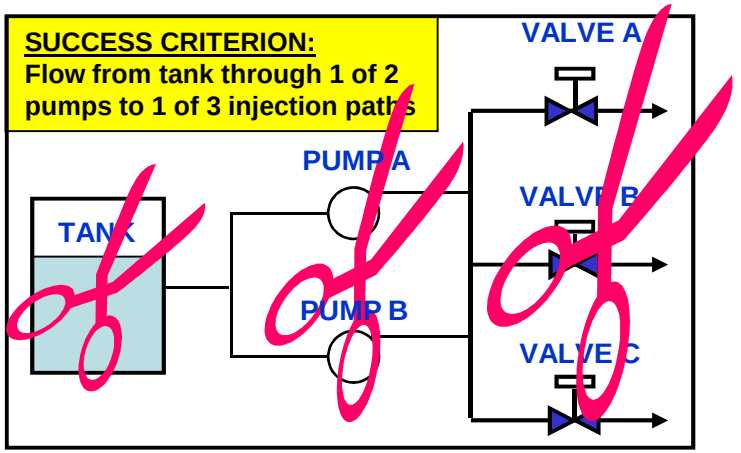


What is a fault tree?



How do we solve fault trees?

- Reducing the logic in a fault tree gives:
  - **Cutsets**, sets of failures that result in overall failure
    - PUMP A FAILS and PUMP B FAILS
      - Independently or by common cause
    - VALVE A FAILS and VALVE B FAILS and VALVE C FAILS
      - Independently or by common cause
    - TANK FAILS
  - **Probability that the function will fail**, derived from the cutsets and the failure probabilities of the basic events therein

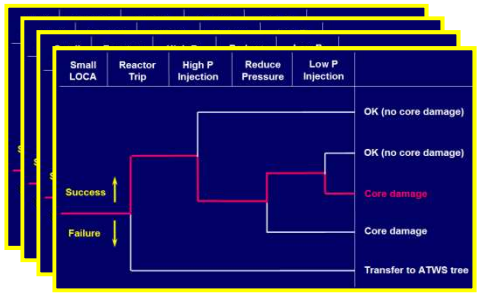


Where do we get the numbers?

- Operating experience data for:
  - Frequency of many initiating events
  - Failure rates of plant equipment
  - Average availability of plant equipment
  - Probabilities of repair and recovery (e.g., restoration of offsite power)
- Special methods:
  - **Expert elicitation** for rare events (e.g., large LOCA frequency)
  - **Human reliability analysis** (e.g., operator fails to switch to recirculation)

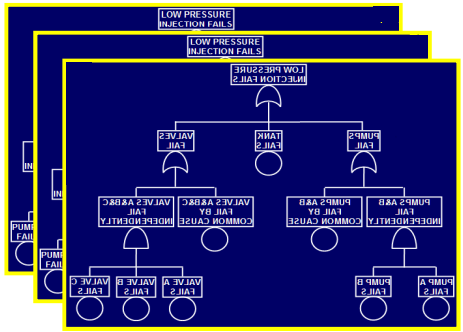
  Common cause failure modeling

How do we “solve” the PRA model?



CORE DAMAGE SEQUENCES:

- **Small LOCA OCCURS & Reactor Trip SUCCEEDS & High Pressure Injection FAILS & Reducing Pressure SUCCEEDS & Low Pressure Injection FAILS**
- **… (may be several on each tree!)**

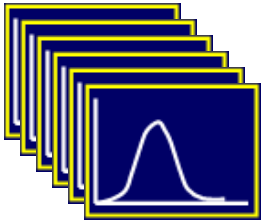


SYSTEM CUTSETS:

- **PUMP A FAILS & PUMP B FAILS**
- **TANK FAILS**
- **… (may be several for each tree!)**

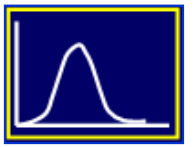
CORE DAMAGE CUTSETS:

- **SMALL LOCA & HPI TANK FAILS & LPI PUMP A FAILS & LPI PUMP B FAILS**
- **SMALL LOCA & HPI PUMP A FAILS & HPI PUMP B FAILS & LPI TANK FAILS**
- **… (many combinations per sequence!)**



FAILURE PROBABILITIES & INITIATING EVENT FREQUENCIES

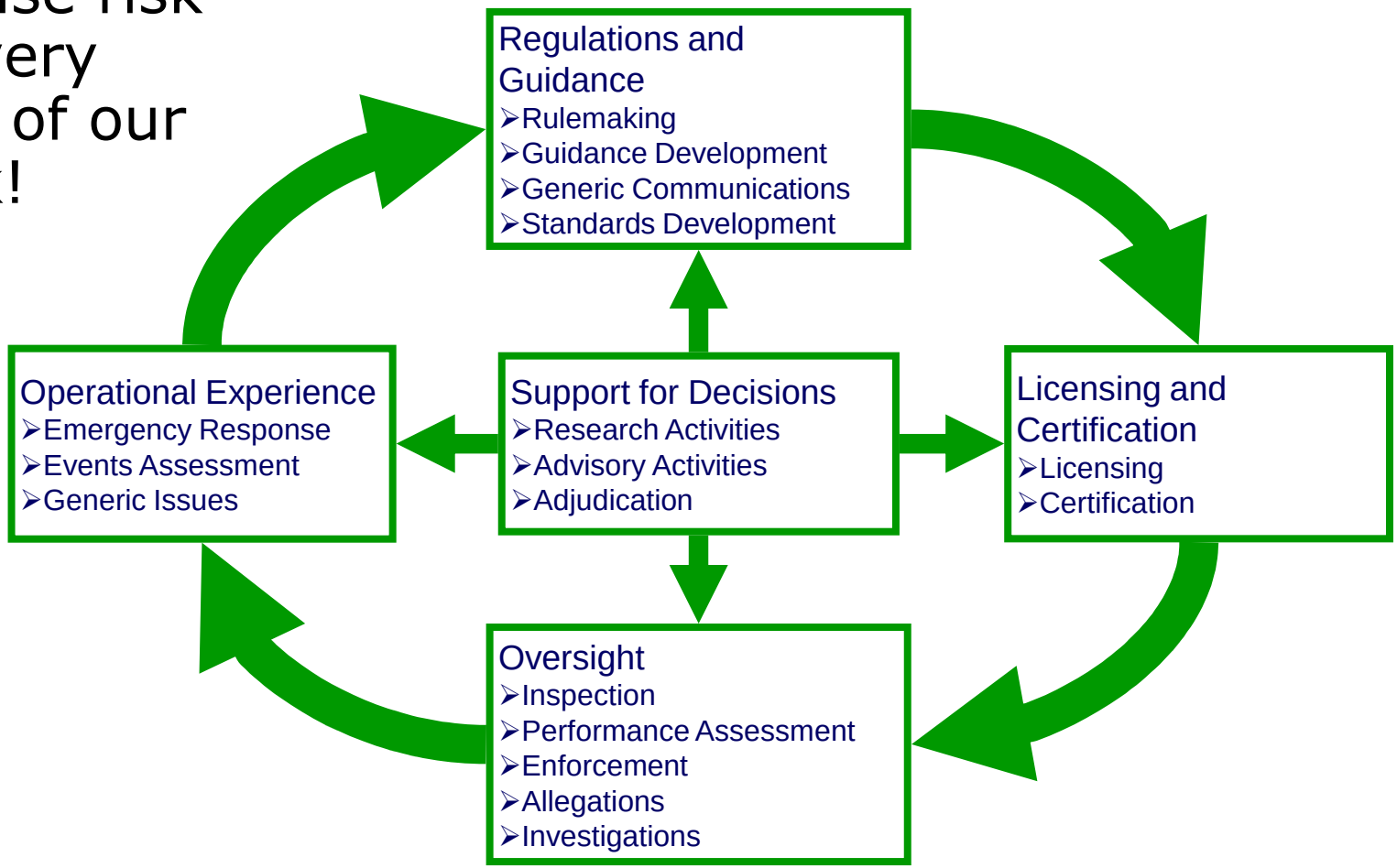
- **CORE DAMAGE FREQUENCY**
- **UNCERTAINTY ANALYSIS**
- **IMPORTANCE MEASURES**
- **SENSITIVITY STUDIES**
- **RISK INSIGHTS**



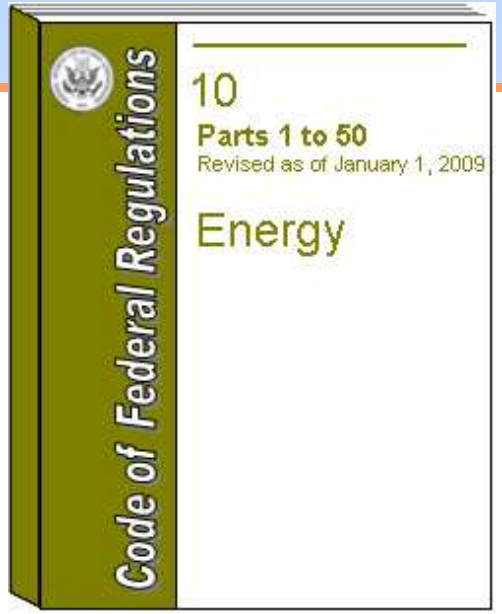
Where do we use risk-informed approaches?

Where do we use risk-informed approaches?

- We use risk in every area of our work!



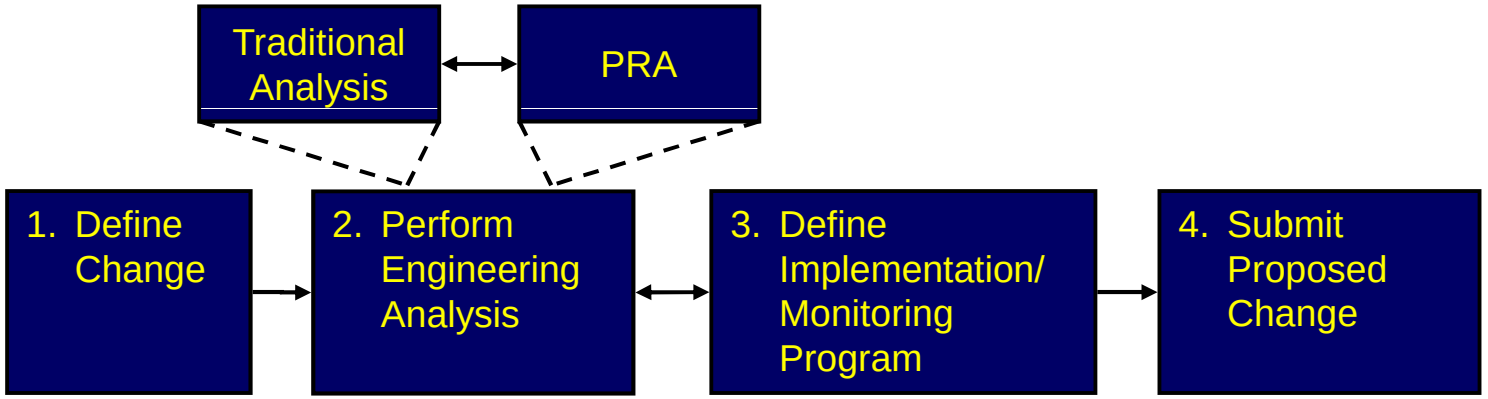
Regulations and Guidance



- Risk-informed requirement reductions
  - Combustible Gas Control (50.44)
- Risk-informed requirement additions
  - ATWS (50.62)
  - SBO (50.63)
  - Maintenance Rule (50.65)
  - PRA Requirements for New Reactors (50.71(h); 52.47)
- Risk-informed alternatives
  - Fire Protection (50.48(c))
  - Special Treatment (50.69)
  - Pressurized Thermal Shock (50.61a)
  - Alternative ECCS Acceptance Criteria (50.46a) (Pending)

Licensing and Certification

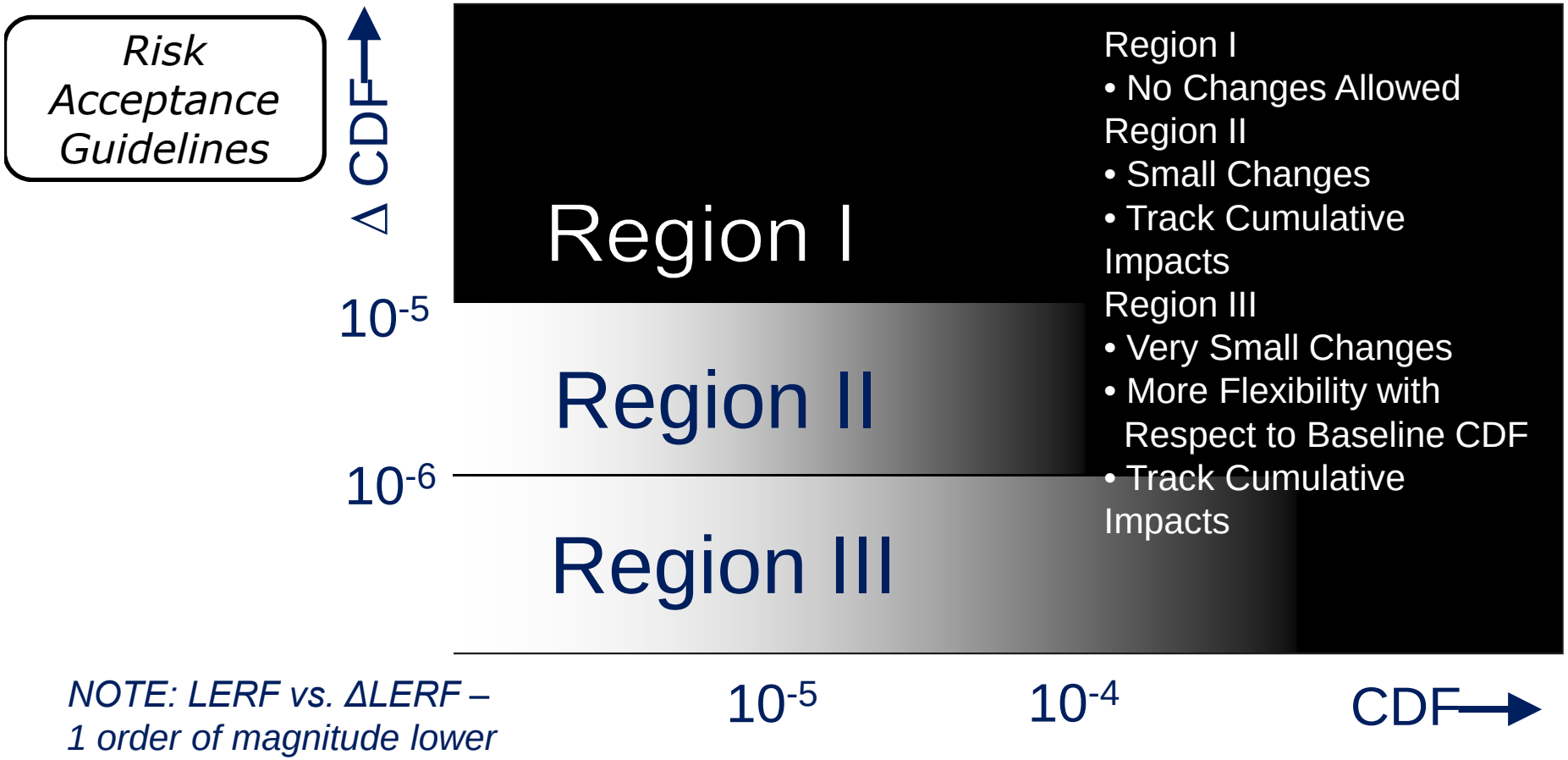
- e.g., risk-informed license amendments per Regulatory Guide (RG) 1.174*
  - Process



  - Uses the 5 key principles (discussed in part 1)
  - Risk acceptance guidelines (next slide)

* RG 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis"

Risk Acceptance Guidelines



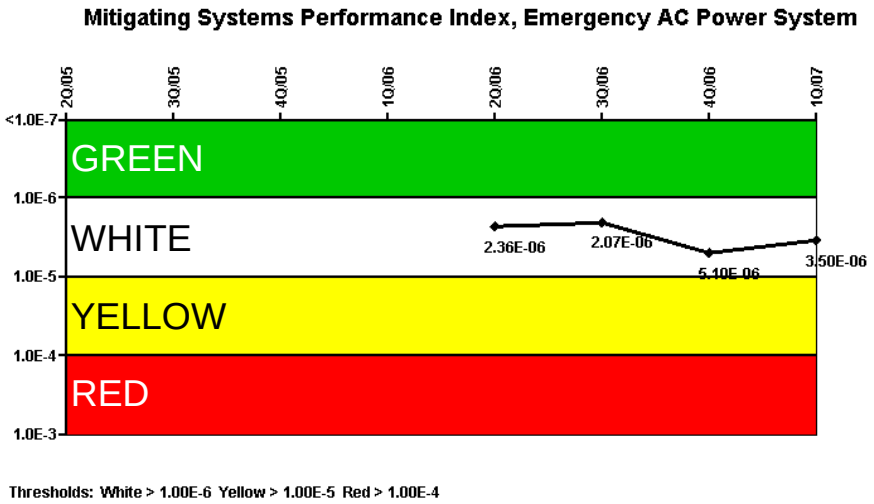
NOTE: LERF vs. ΔLERF – 1 order of magnitude lower

(Source: RG 1.174, 11/02)

Oversight

- Notice of Enforcement Discretion (NOED)*
  - Non-compliance with a technical specification or license condition
  - Risk argument for avoiding unnecessary plant transient, inappropriate test/inspection, or unjustified delay in startup

- Reactor Oversight Process
  - Risk-informed performance indicators
    - Mitigating System Performance Index (MSPI)**
  - Risk-informed baseline inspections
  - Significance Determination Process for inspection findings

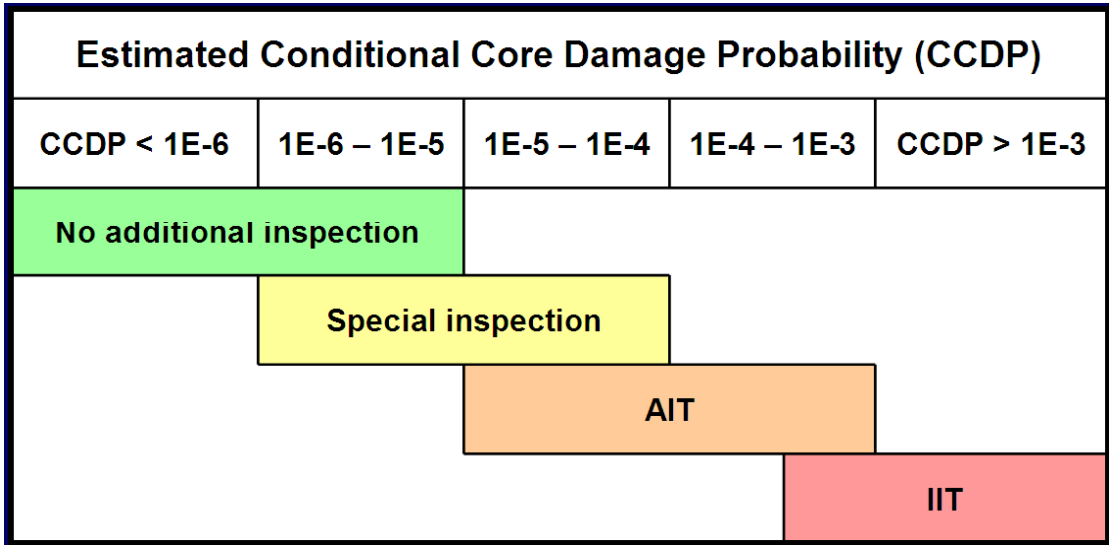


** Inspection Manual Chapter Part 9900*

*** http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/mspi.html*

Operational Experience

- Incident response
  - Follow-up inspections based on event significance*
- Event assessment
  - Risk-informed decision-making**
  - Accident Sequence Precursor (ASP) program reported to Congress



** Management Directive 8.3*
*** NRR Office Instruction LIC-504*

Conclusion

- NRC uses risk information to supplement traditional engineering approaches – "risk-informed regulation"
- PRA models provide quantitative measures of the risk of nuclear power plant operation, in terms of, e.g., "core damage frequency"
- Risk insights are used in the rulemaking, licensing, oversight, and operating experience arenas

QUESTIONS?

References

Selected sources of information on nuclear plant risk assessment:

- Hickman, J.W., "PRA Procedures Guide," NUREG/CR-2300, US Nuclear Regulatory Commission, January 1983.
- NUREG-1855, "Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making," Volume 1, March 2009.
- Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," U.S. Nuclear Regulatory Commission, Washington, DC.
- U.S. NRC, 1975, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), October 1975.
- U.S. NRC, 1981, Fault Tree Handbook, NUREG-0492, January 1981.
- U.S. NRC, 1990, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, Vol. 1-3.
- W.T. Pratt et al., "An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events," NUREG/CR-6595, Revision 1, October 2004.