U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

SESSION 1-1

REFRESHER ON PRA METHODOLOGY

Donnie Harrison

U.S. Nuclear Regulatory Commission

Donnie.Harrison@nrc.gov

301.415.2470

RISK-INFORMED REGULATION SEMINAR
Mexico City, Mexico August 27-31, 2012

Topics

- General Introduction on risk
- Probabilistic Risk Assessment (PRA) modeling
- What can we learn from PRA results?

Terminology and Overview

- USA refers to Probabilistic Risk Assessment (PRA)
- Internationally referred to as Probabilistic Safety Analysis (PSA)
- PRA ≡ PSA

What is Risk?

- **Arises from a "Danger" or "Hazard"**
- **Always associated with undesired event**
- **Involves both:**
  - likelihood of undesired event
  - severity (magnitude) of the consequences

What is Risk?

- **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)?

How is risk used in the traditional regulatory framework?

- **Traditional engineering or "design basis" approaches**
  - Implicit consideration of risk (which accidents, systems, etc. are important?)
  - Engineering judgment in determining a set of **"credible" accident categories** that require prevention/mitigation capabilities
    - You'll hear this called **"deterministic"** analysis
  - Reliance on **worst case analyses**, single failure criterion, defense-in-depth, and safety margins

How is risk used in the risk-informed regulatory framework?

- **Risk-informed approaches**
  - Explicit consideration of risk
  - "Full picture" – scope includes **all potential accident initiators and mitigation failures** (including multiple failures)
  - Address the **possibility of releases** greater than regulatory limits

What tool is 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*

Why is risk information used?

- **Commission's policy statement on the use of PRA* included four main statements:**

1. **Increase use of PRA** to the extent supported by the state-of-the-art and in a way that **complements** traditional engineering approaches
2. Use PRA both to **reduce unnecessary conservatism** in current requirements and to support proposals for **additional regulatory requirements**
3. Be as **realistic** as practicable
4. Consider **uncertainties** appropriately when using the Commission's safety goals and subsidiary numerical objectives

**** 8/16/95***

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Probabilistic Risk Assessment (PRA) Modeling

RISK-INFORMED REGULATION SEMINAR
Mexico City, Mexico August 27-31, 2012

What is a PRA?

PRA is a structured, analytical process for identifying potential weaknesses and strengths of a plant design in an **integrated** fashion

- **PRAs 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 the technical basis for the PRA model?

- **The PRA model is constructed to model the as-built, as-operated plant**
- **Multiple sources of information from the traditional engineering disciplines, including:**
  - Plant design information
  - Thermal hydraulic analyses of plant response
  - System drawings and performance criteria
  - Operating experience data
  - Emergency, abnormal, and system operating procedures
  - Maintenance practices and procedures

What is the technical basis for the PRA model?

- **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 is the technical basis for the PRA model?

- **This understanding is used to establish success criteria (based on engineering analyses)**
  - Definition of end states:
    - Establish the acceptance criteria for prevention of core damage, e.g., collapsed level greater than 1/3 core height
    - Establish containment capability
  - Determination of system success criteria for a given scenario:
    - Time at which system is required to prevent damage
    - Required system performance, e.g., two out of three pumps

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)

- **Outputs may include**
  - **Core damage** frequency ("Level 1" PRA)
  - **Release** frequencies ("Level 2")
  - **Radiological consequences** to public ("Level 3")

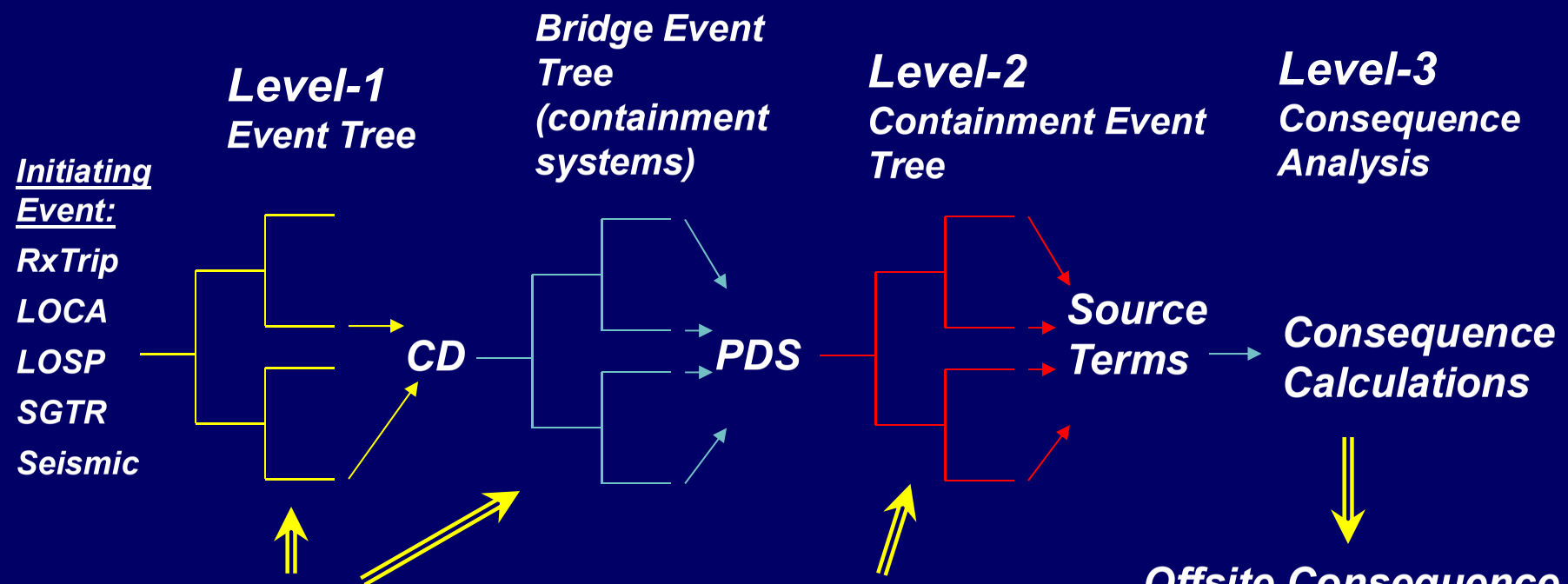
What are the end states of a PRA?

- **Core damage occurs when**
  - **Safety functions** are not met
    - Such as removal of decay heat, control of reactivity, or control of inventory
  - Engineering models show that core parameters exceed certain pre-determined limits

- **Large early release occurs when**
  - Core damage with **containment challenge**, leading to significant, **unmitigated releases prior to effective evacuation** of the close-in population

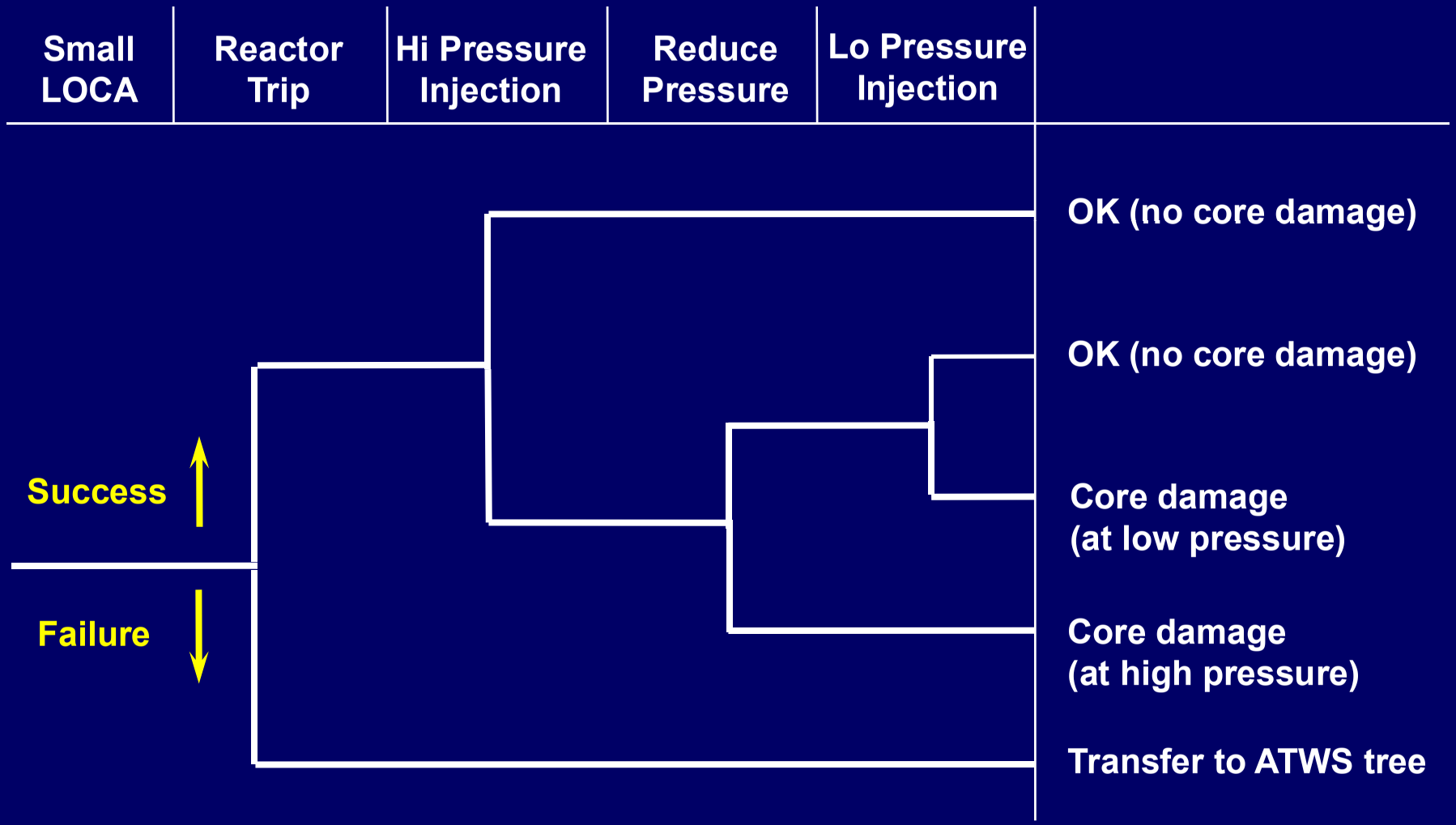
- **A limited Level 2 PRA provides insights related to core damage and large early release.**

3 Levels of PRA/PSA

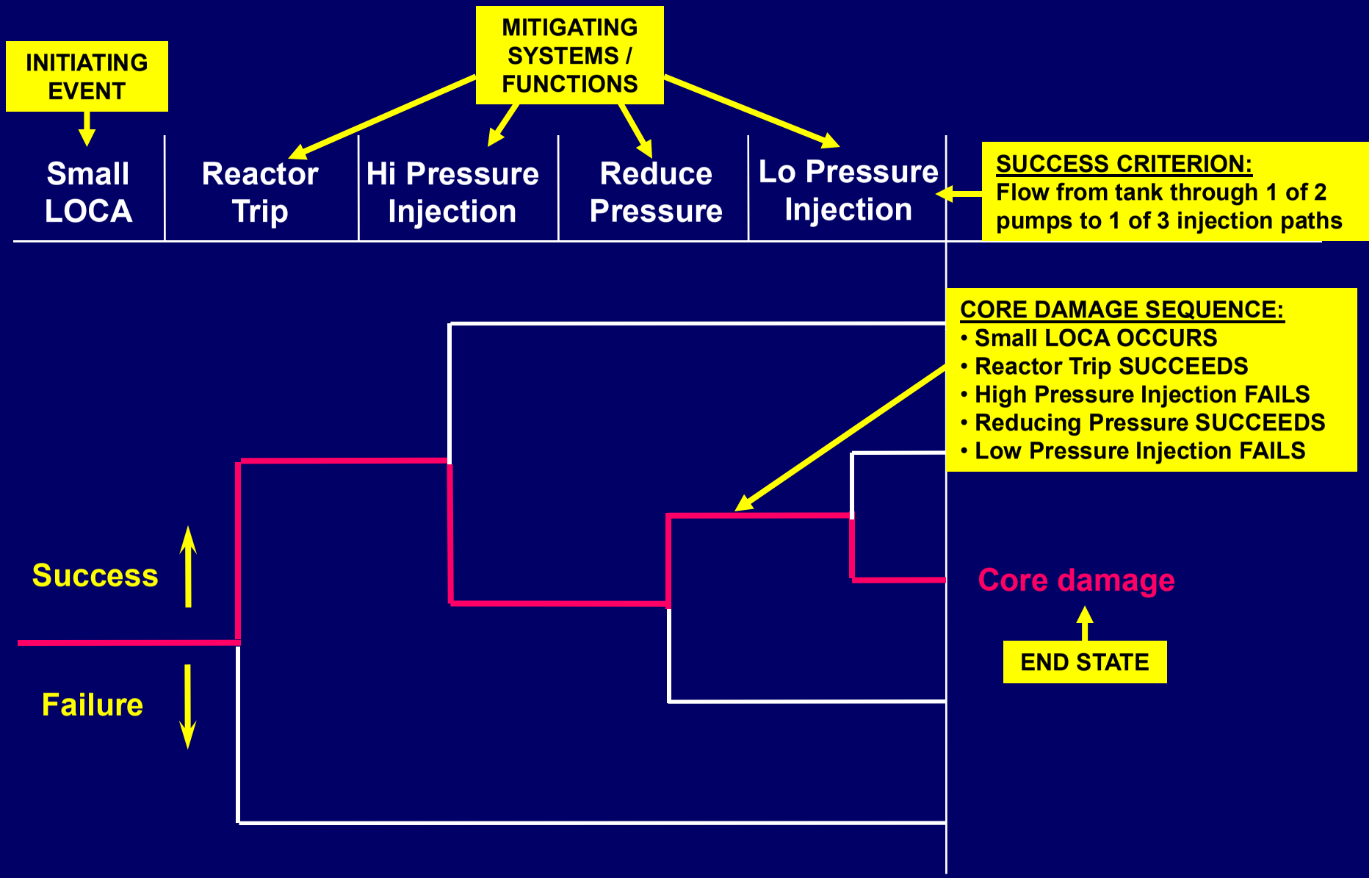


What is an event tree?

A graphical depiction of a sequence of events



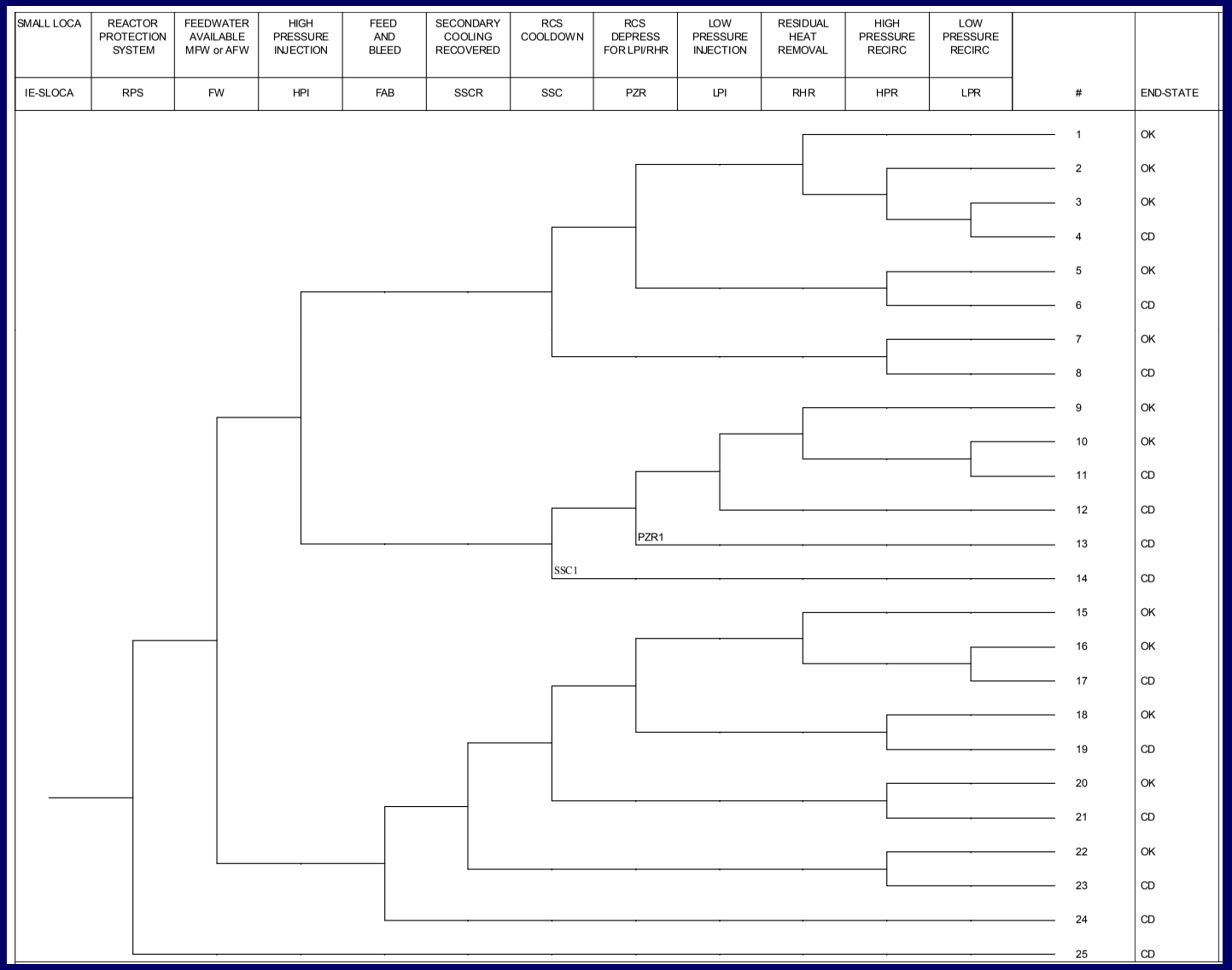
What is an event tree?



What is an event tree?

- **Event tree "top events" may represent:**
  - Functions or systems to **mitigate** core damage
  - Key **operator actions**
  - **Containment** support systems
    - Fan coolers, sprays
    - Isolation
- **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

More Complex Event Tree

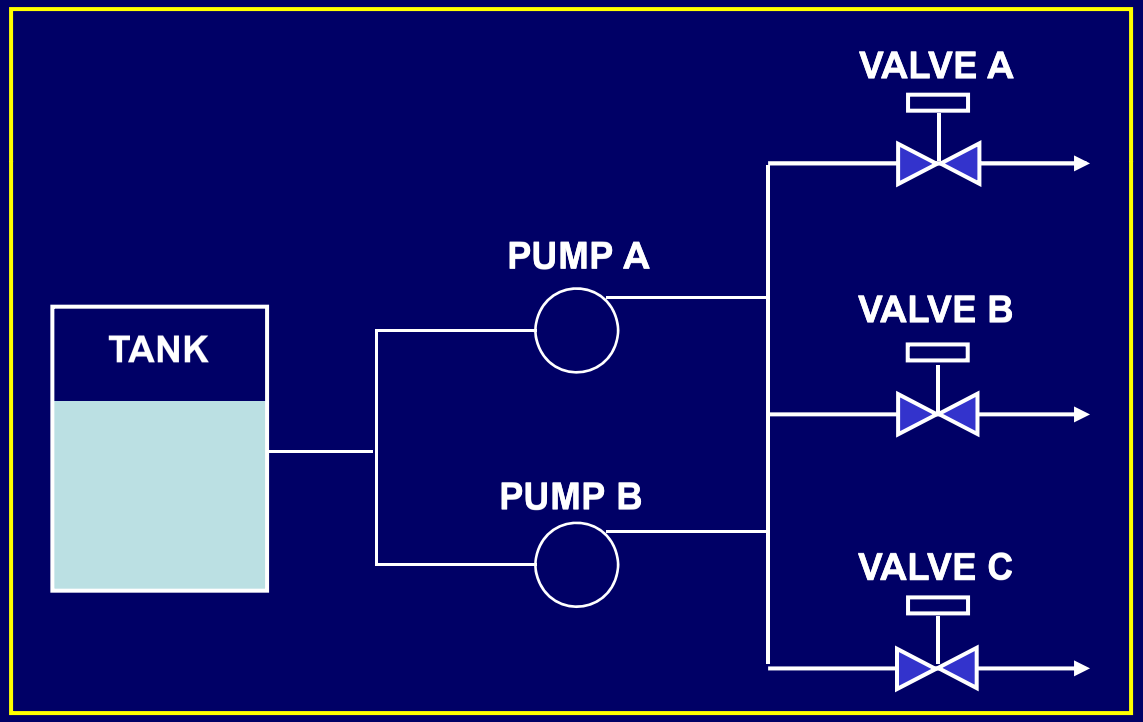


What is a fault tree?

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

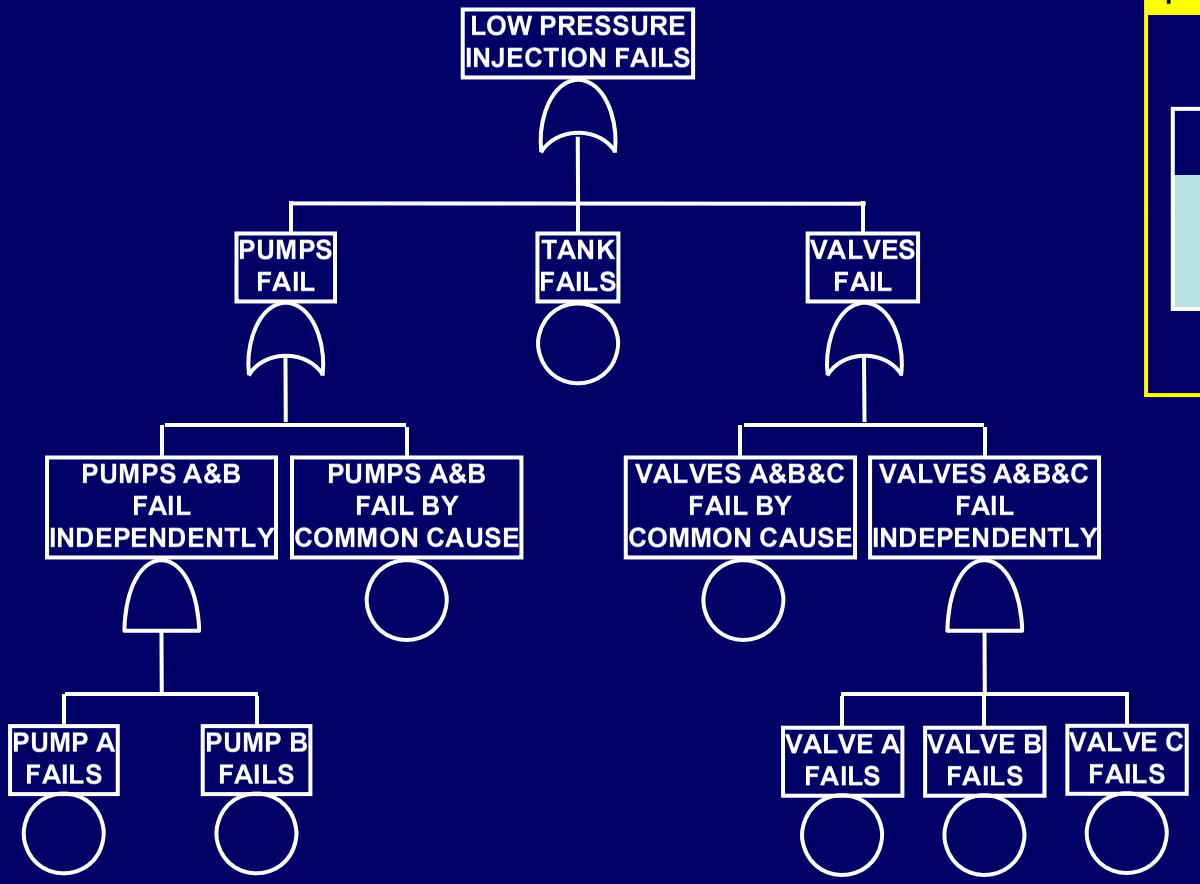
FAILURE OCCURS WHEN:
No flow from tank
OR
No flow from pumps
OR
No flow through injection paths

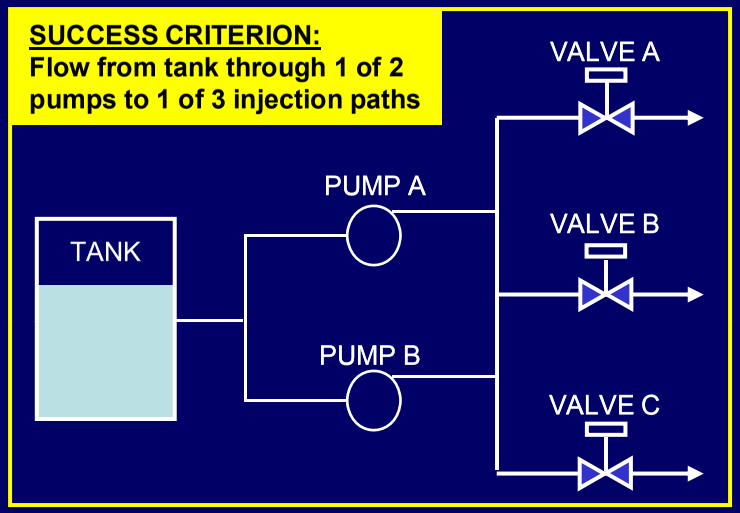


What is a fault tree?

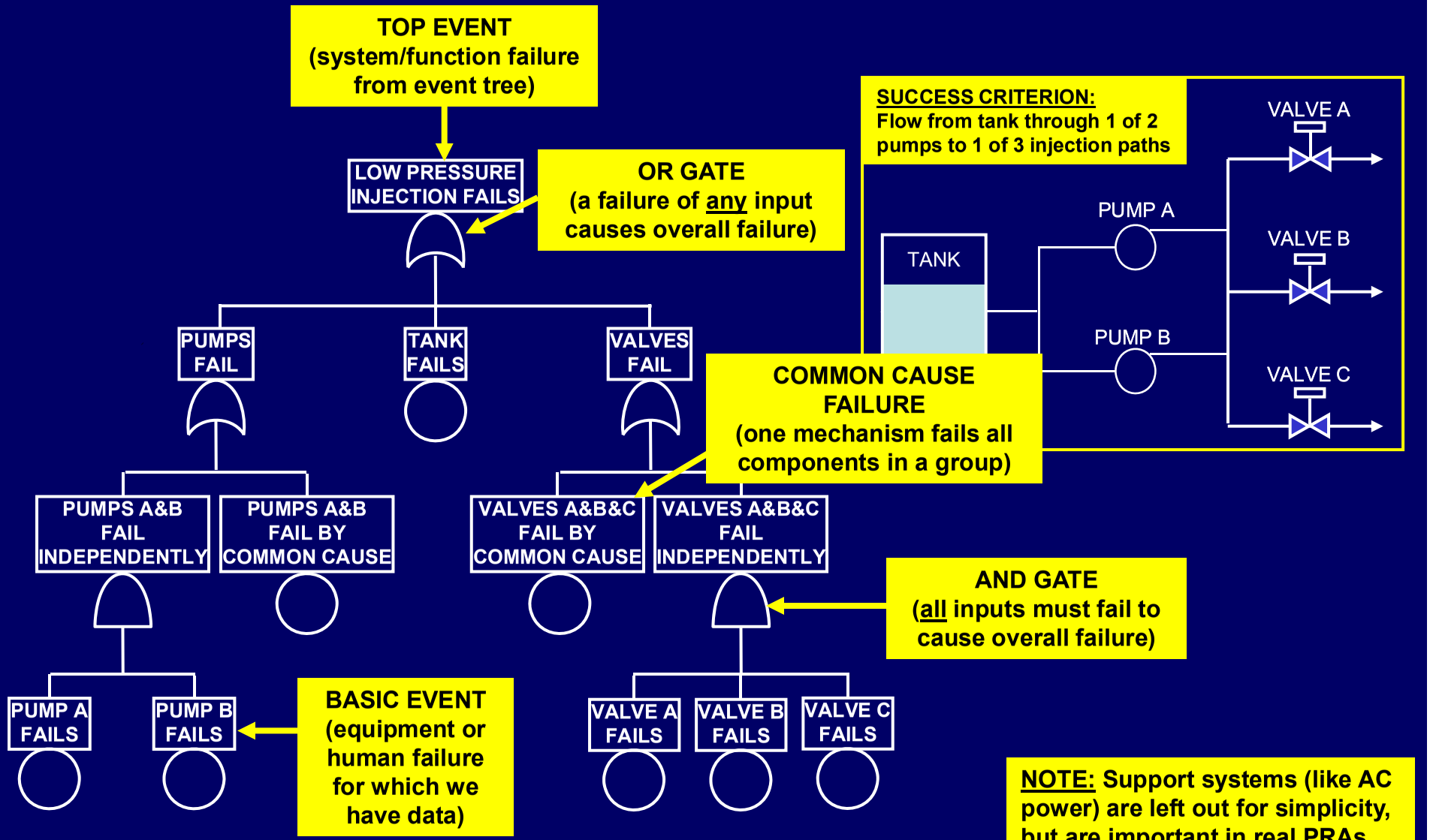
- **Developing fault trees**
  - Need for fault tree usually arises from the event tree
    - What equipment can provide the function?
    - What operator actions must take place?
  - Define **success criteria**, e.g.
    - How much flow is needed to remove decay heat?
    - How much flow is necessary 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?



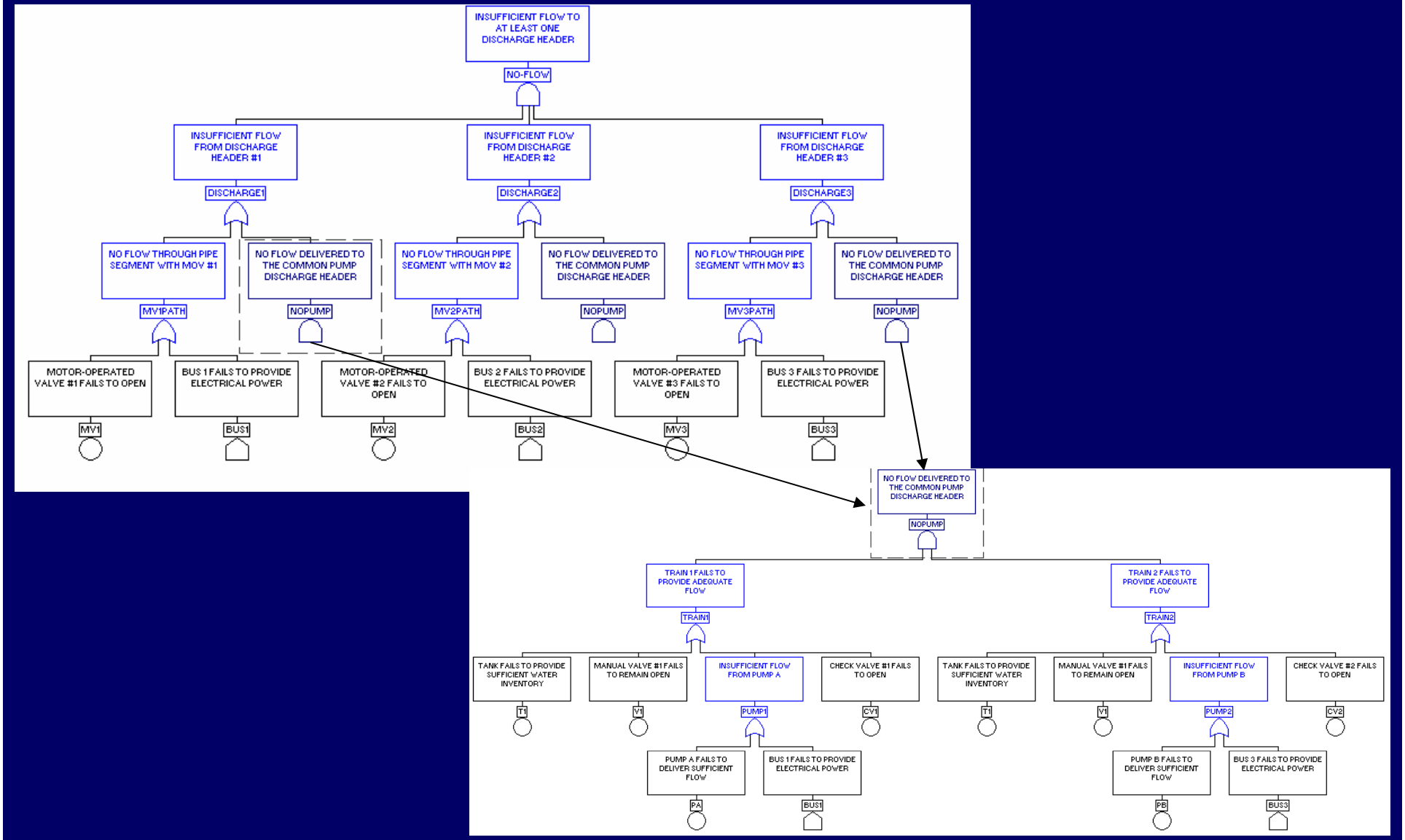


What is a fault tree?



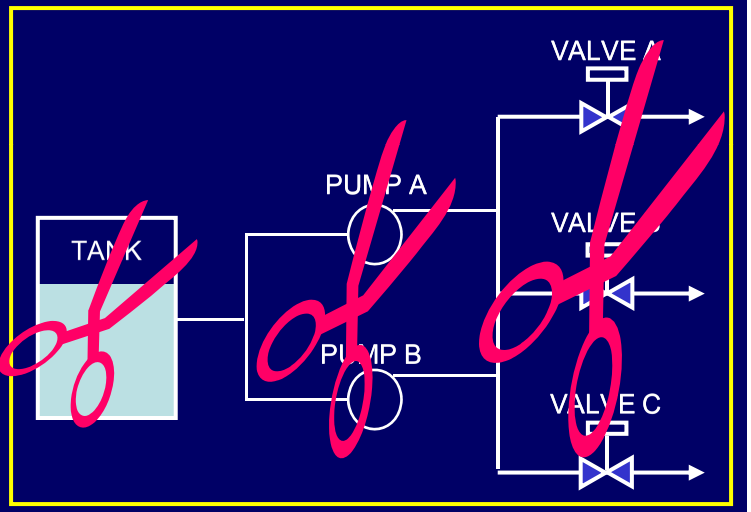
NOTE: Support systems (like AC power) are left out for simplicity, but are important in real PRAs.

More Complex Fault Tree



How do we solve fault trees?

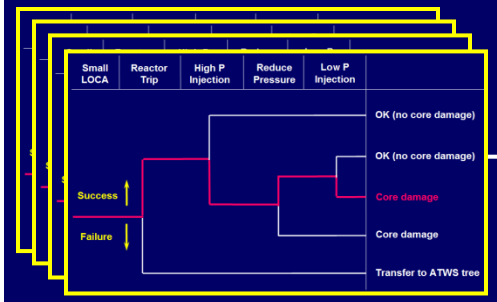
- **Reducing the logic in a fault tree gives:**
  - **Cutsets**, sets of failures that result in overall failure
    - PUMP A FAILS and PUMP B FAILS
      - Independently or by common cause
    - VALVE A FAILS and VALVE B FAILS and VALVE C FAILS
      - Independently or by common cause
    - TANK FAILS
  - **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?

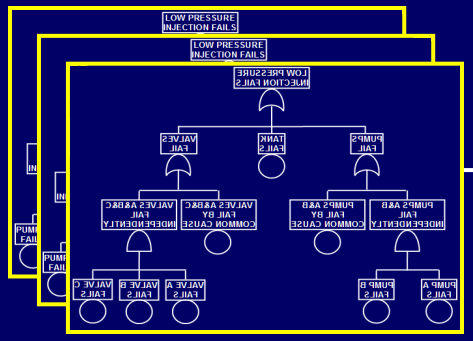
- **Operating experience data for:**
  - Frequency of many initiating events
  - Failure rates of plant equipment
  - Average availability of plant equipment
  - Probabilities of repair and recovery (e.g., restoration of offsite power)
- **Special methods:**
  - **Expert elicitation** for rare events (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!)

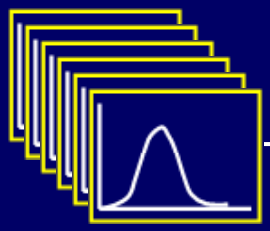


SYSTEM CUTSETS:

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

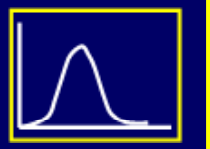
CORE DAMAGE CUTSETS:

- 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



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

What can we learn from PRA results?

RISK-INFORMED REGULATION SEMINAR
Mexico City, Mexico August 27-31, 2012

What can we learn from PRA results?

- **A quantitative assessment of risk impact**
- **The significant contributors to the risk measures being used, in terms of, for example:**
  - Accident sequences
  - Cutsets
  - Significant basic events
- **A number of tools are available to extract these results and characterize their significance and the confidence we can have in them:**
  - Importance analyses
  - Uncertainty analysis
  - Sensitivity analyses
- **Qualitative insights about plant vulnerabilities**

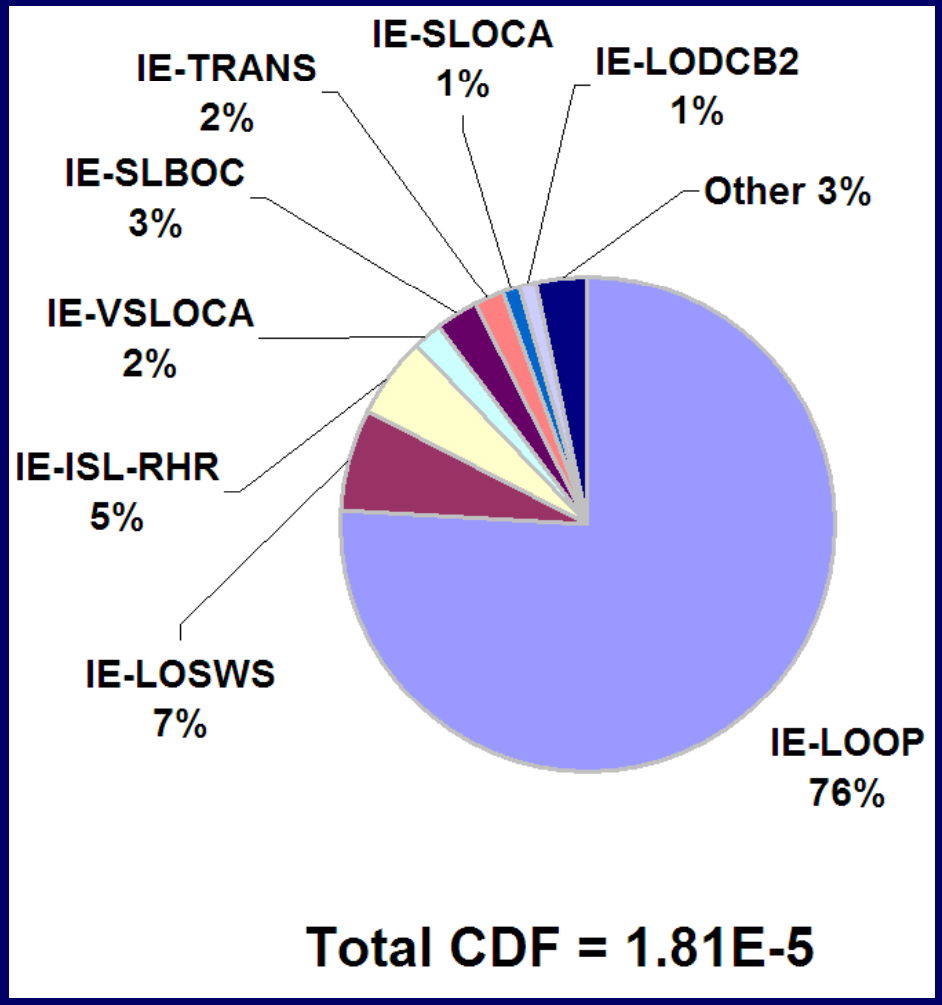
Quantitative PRA Results: Core Damage

- **Core Damage Frequency (CDF)**
  - What is the **frequency** (on a per-year basis) that an **initiating event** and subsequent **mitigating system failures** that lead to **core damage** will occur?
- **Change in CDF (ΔCDF)**
  - Given a component **failure or longer maintenance** time that **increases the probability of a mitigating system failure**, how much does the **overall CDF** increase?
- **Core Damage Probability (CDP)**
  - What is the probability that core damage will occur during a **given period**?
- **Conditional Core Damage Probability (CCDP)**
  - Given that an **initiating event occurs**, what is the probability that a combination of system **failures leading to core damage** will occur?
  - Given a component **failure or maintenance** that lasts a certain duration, what is the probability that **both an initiating event and subsequent mitigating system failures that lead to core damage** will occur during that time period?
- **Incremental Conditional Core Damage Probability (ICCDP)**
  - How much higher is the **CCDP during a component failure or maintenance** compared to the **average CDP** over the same time period?

Quantitative PRA Results: Large Early Release Frequency

- **Large Early Release Frequency (LERF)**
  - What is the **frequency** (on a per-year basis) that a core damage accident with a **large radioactive release before there is time to evacuate** will occur?
- **Change in LERF (ΔLERF)**
  - Given a component **failure or longer maintenance** time that **increases the probability of a mitigating system failure**, how much does the **overall LERF** increase?
- **Large Early Release Probability (LERP)**
  - What is the probability that core damage and large early release will occur during a **given period**?
- **Conditional Large Early Release Probability (CLERP)**
  - Given that an **initiating event occurs**, what is the probability that a combination of system **failures leading to large early release** will occur?
  - Given a component **failure or maintenance** that lasts a certain duration, what is the probability that **an initiating event and subsequent mitigating system failures leading to large early release** will occur during that period?
- **Incremental Conditional Large Early Release Probability (ICLERP)**
  - How much higher is the **CLERP during a component failure or maintenance** compared to the **average CLERP** over the same time period?

Core Damage Contribution by Initiating Event*



LOOP:	Loss of Offsite Power
LOSWS:	Loss of Service Water
ISL-RHR:	Intersystem LOCA - RHR
VSLOCA:	Very Small LOCA
SLBOC:	Steam Line Break
TRANS:	General Transient
SLOCA:	Small LOCA
LODCB2:	Loss of DC Bus 1EB2
Other:	All Other Initiating Events

** Comanche Peak SPAR version 3.31*

Importance Measures

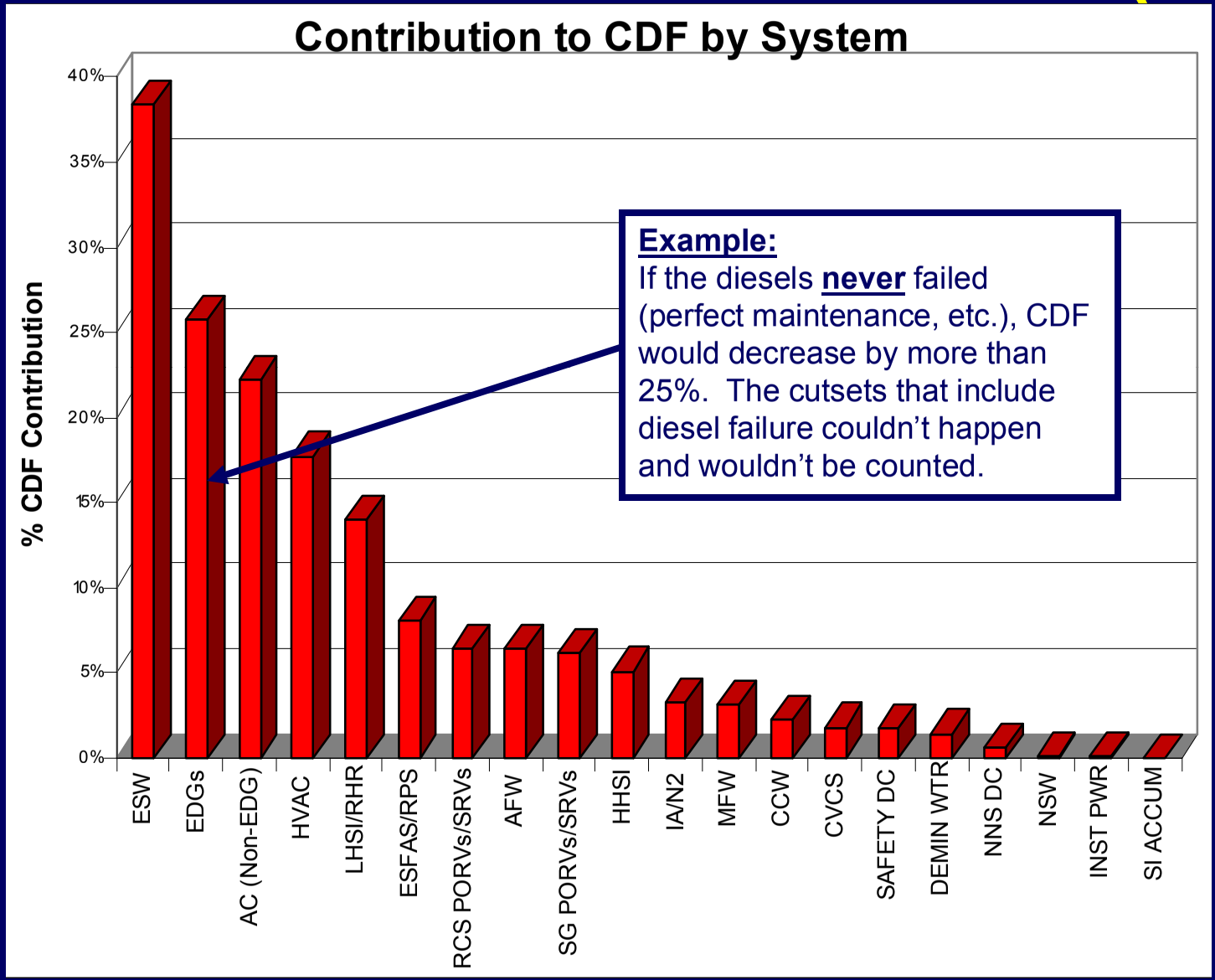
- **Provide insight into impact of basic events on overall risk**
- **Generally two types:**

1. Risk decrease measures
   - How much the overall **risk would decrease** if the associated SSC were **less likely to fail**
   - Fussell-Vesely (FV)
2. Risk increase measures
   - How much the overall **risk would increase** if the associated SSC were **certain to fail**
   - Risk Achievement Worth (RAW)

Fussell-Vesely (FV)

- **Answers the questions:**
  - What is driving **current risk**?
  - What **fraction of the total risk comes from cutsets that include a particular component**?
  - If a component were **less likely to fail** (better maintenance, etc.), would that **decrease risk a lot or a little**? (i.e., is it worth the effort?)
- **We use it to:**
  - Focus on **key initiating events, equipment, operator actions, and procedures**
  - Help decide what to inspect
- **A component needs more attention when:**
  - FV is greater than **0.005** (i.e., that event appears in cutsets that contribute to ½% of the risk)

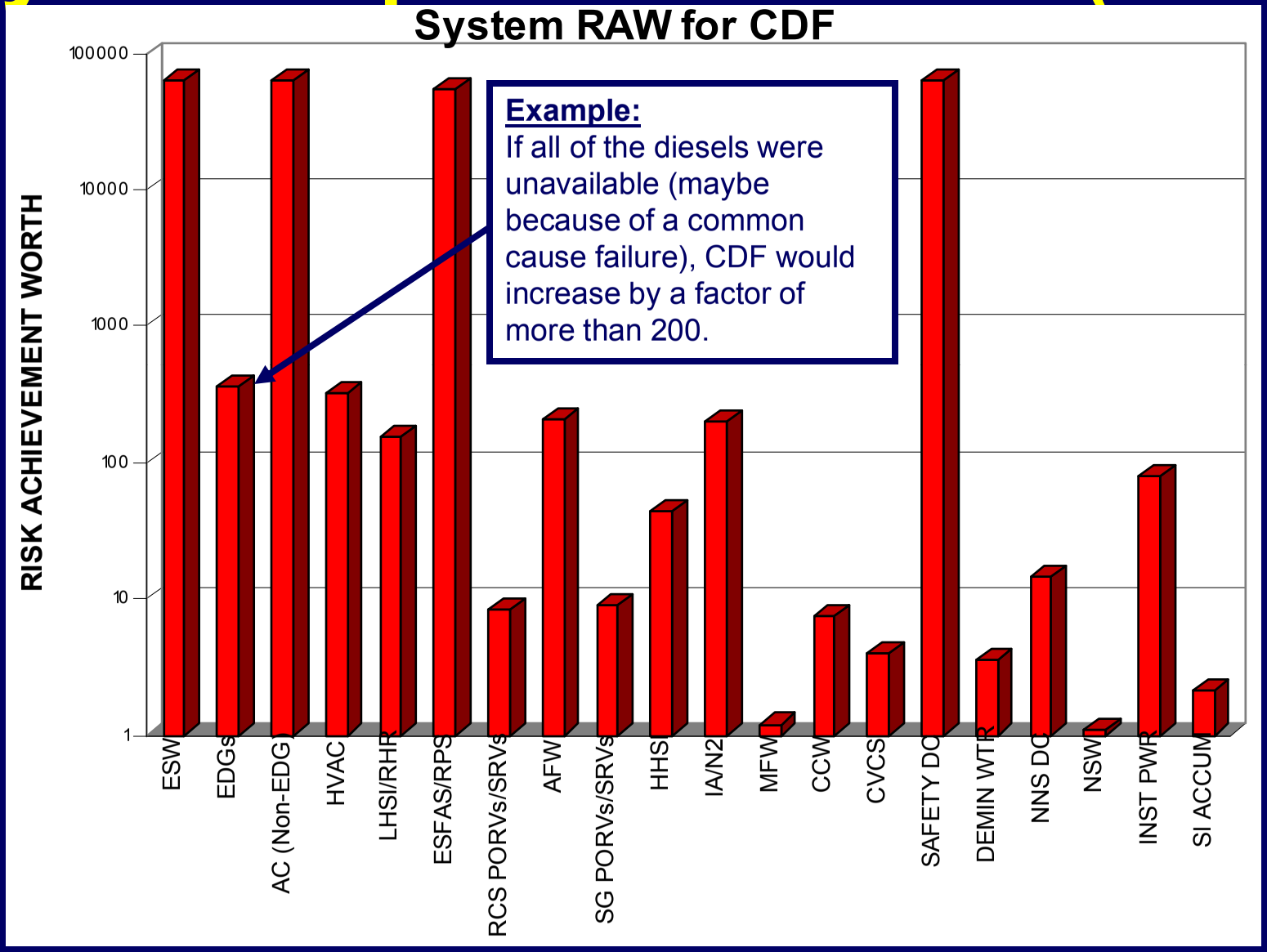
System Contribution to CDF (FV)



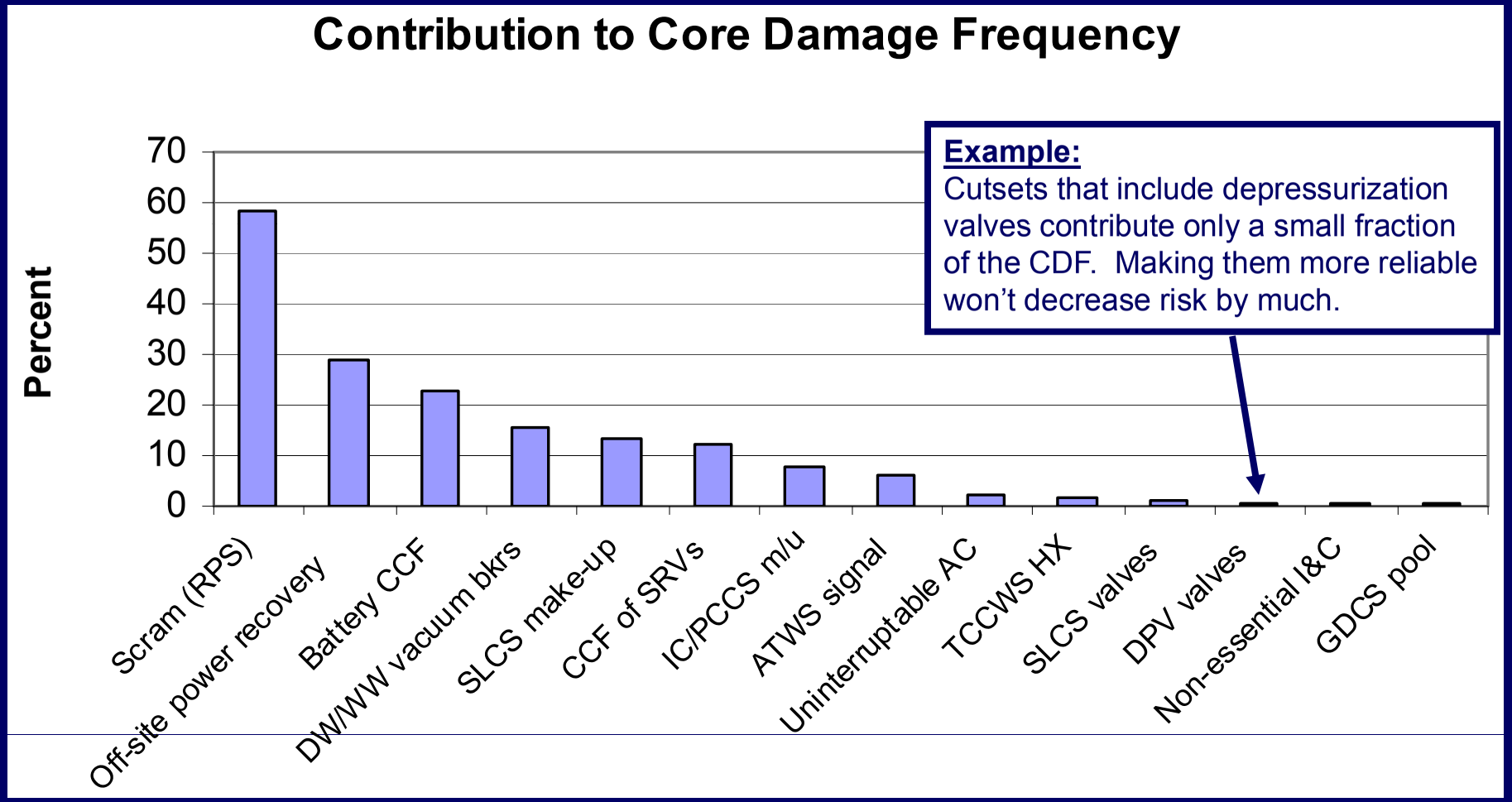
Risk Achievement Worth (RAW)

- **Answers the questions:**
  - If this **component were broken or unavailable**, would that **increase risk a lot or a little**?
  - How important is a component to **maintaining the current level of risk**?
- **We use it to:**
  - Help determine the **significance of inspection findings**
  - **Prioritize systems** to review
  - Identify equipment that needs **special controls** to keep it operational
- **A component is treated differently when:**
  - RAW is greater than **2** (i.e., risk doubles without that component)

System Importance to CDF (RAW)



System Contribution to CDF (Fussell-Vesely)



System Importance to CDF (RAW)

Plant Vulnerabilities

- Key operator action or procedure appearing in many core damage sequences
- Safety function that needs a single piece of equipment or support system for success
- Degradation that could fail redundant components
- Unexpected and adverse system interactions

Plant Vulnerabilities

- Key operator action or procedure appearing in many core damage sequences
- Safety function that needs a single piece of equipment or support system for success
- Degradation that could fail redundant components
- Unexpected and adverse system interactions

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

The End

Questions & Answers…..