# PRA BASICS FOR REGULATORY APPLICATIONS P-105

May 2016

United States
Nuclear Regulatory Commission

Idaho National Laboratory

# DISCLAIMER NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability of responsibility for any third party’s use, or the results of such use, or any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Idaho National Laboratory

# PRA Basics for Regulatory Applications P-105

## Course Presented by

***Michael Calley, INL***

***Michael.Calley@inl.gov***
***208-526-9230***

***Jim Knudsen, INL***

***James.Knudsen@inl.gov***
***208-526-6432***

*May 3 - 5, 2016*
*NRC Professional Development Center*
*Rockville, MD*

# PRA Basics for Regulatory Applications P-105

# Course Introduction – Overview

- This course is designed to provide an overview of probabilistic risk assessment (PRA) methodology and how this method is applied to the nuclear industry.
- This course will introduce how PRA is used by the NRC for risk informed regulation, and PRAs role in the NRC's reactor oversight process with specific applications such as SDP, MSPI, and etc.
- Other courses are available to provide additional details with specific topics such as Bayesian Inference (P-102 and P-502), System Modeling Technique (P-200), Human Reliability Analysis (P-203), External Events (P-204), etc.

# Course Overview

- Separated into two sections
  - Section I - PRA methodology
    - First 11 modules of Section I
    - Overview of basic terms and concepts
    - Designed to provide information about the development of a probabilistic risk assessment model (all of the pieces)
    - Provide background information on different types of PRAs (external events, low power/ shutdown, Level 2 & 3)

# Course Overview (continued)

- Section II - PRA applications
  - Last 6 modules of Section II
  - Risk Informed Regulation and Risk Informed Decision-Making
  - NRC uses of PRA
    - Configuration risk management
    - Significance Determination
    - Mitigating System Performance Indicator

# Section I. PRA Methodology

# 1. Risk Assessment Concepts & PRA

# Risk Assessment Concepts & PRA

- **Purpose: Students will be introduced to the fundamental concepts which underlie risk assessment. Will include discussion of the definition of risk, approaches to risk assessment besides PRA, basic terminology used in risk analysis, and the objectives and limitations of PRA.**
- **Objectives: At the conclusion of this section, students will be able to:**
  - **understand basic terms used in risk assessment**
  - **identify types of information generated by PRA & example uses**
  - **enumerate the basic questions answered by PRA (i.e., risk triplet)**
  - **list several strengths and limitations of PRA**
- **References:**
  - **NUREG/CR-2300, *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants***
  - **NUREG-1489, *A Review of NRC Staff Uses of Probabilistic Risk Assessment***

# What is Risk?

- Arises from a “Danger” or “Hazard”
  - Hazard → A deviation from normal conditions (e.g., flood) or a “physically harmful” condition (e.g., fission products)
- Always associated with undesired event
- Involves both:
  - likelihood of undesired event
  - severity (magnitude) of the consequences

# Risk Definition

*Traditional definition of risk*

- **Risk – the frequency with which a given consequence occurs**
- **Frequency, or rate, is the number of occurrences of some event of interest in some defined interval of time**
- **Risk then represented by a *scalar* quantity**
  - **Overall risk represented by a single point**
  - **Each accident scenario represented by a point on a scale (i.e., most risk significant accident scenario has largest product of frequency and consequence)**

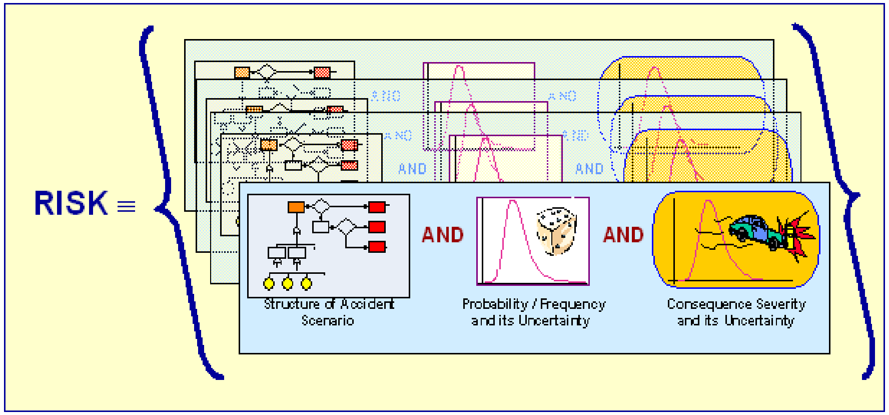
# An Operational Definition for Risk

- Risk is a set of triplets <Si, Pi, Ci> that answer the questions :
  - What can go wrong? (scenarios, Si)
  - How likely is it? (probabilities, Pi)
  - What are the consequences? (adverse effects, Ci)

$$R = \text{RISK} = \{\langle S_i, P_i, C_i \rangle\}$$

  - Kaplan & Garrick, Risk Analysis, 1981

| Scenario | Probability | Consequence |
|---|---|---|
| $S_1$ | $p_1$ | $C_1$ |
| $S_2$ | $p_2$ | $C_2$ |
| $S_3$ | $p_3$ | $C_3$ |
| ⋮ | ⋮ | ⋮ |
| $S_N$ | $p_N$ | $C_N$ |


RISK ≡
AND
AND
Structure of Accident Scenario
Probability / Frequency and its Uncertainty
Consequence Severity and its Uncertainty

# Several Example Approaches for Assessing Risk

- **Maximum Credible Accident**
- **Design Basis Accident**
- **Actuarial Analysis**
- **PRA/PSA**

DILBERT, YOU HAVE BEEN CHOSEN TO DESIGN THE WORLD'S SAFEST NUCLEAR POWER PLANT.
THIS IS THE GREATEST ASSIGNMENT THAT ANY ENGINEER COULD HOPE FOR. I'M FLATTERED BY THE TRUST YOU HAVE IN ME.
BY "SAFE" I MEAN "NOT NEAR MY HOUSE."
www.dilbert.com scottadams@aol.com
2/18/02 © 2002 United Feature Syndicate, Inc.

# Maximum Credible Accident

- Requires worst-case, credible accident to be postulated
- Consequences of accident are estimated
- Example:
  - WASH-740, Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants: A Study of Possible Consequences if Certain Assumed Accidents, Theoretically Possible but Highly Improbable, Were to Occur in Large Nuclear Power Plants, WASH-740, U.S. Atomic Energy Commission, Washington, D.C., March 1957.
    - Estimated offsite consequences of maximum credible accident for commercial U.S. LWR
    - Established concept of engineered containment building

# Maximum Credible Accident

*DRAWBACKS*

- How to define “credible”
- Specification of worst-case accident is subjective
  - Loss of offsite power and failure of backup emergency power (SBO scenario)
  - Reactor breach (LOCA)
- May lead to overly conservative design or inappropriate focus, regulation
- Likelihood of worst-case accident not quantified
- Implication that “worst case” is bounding for all situations might not be true

# Design Basis Accident

- **Definition (NRC)**
  - A postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to ensure public health and safety.
- **Traditional, deterministic approach to nuclear safety**
- **Plant designed to cope with specified set of accidents**
  - Only single, active component failures typically considered in DBA approach
  - Gives limited consideration of operator actions
- **TMI-2 and Fukushima accidents highlighted problems of this approach**

# Actuarial Analysis

- Estimates frequencies of accidents from statistical databases
- Used widely by insurance industry
- Requires large empirical database (which fortunately the commercial nuclear power industry does not have)

# Probabilistic Risk Assessment (PRA)

- An analytical tool to……….
  - Identify accident scenarios
  - Estimate likelihood of each accident scenario
  - Estimate consequences of each accident scenario

# PRA is a Technical Analysis that systematically answers:

- **Three questions which are commonly referred to as the risk triplet (see article by Kaplan and Garrick in the Bibliography)**
  - **What can go wrong?**
    - **(accident scenario)**
  - **How likely is it to occur?**
    - **(frequency, probability)**
  - **What will be the outcome?**
    - **(consequences)**
- **A fourth question, reflecting the importance of uncertainty, has also been addressed in recent PRAs**
  - **How confident are we in our answers to these three questions?**

# Strengths of PRA

- Quantifies risks associated with performance measures
  - PRA metrics are integral risk metrics
- Captures dependences and other relationships between sub-systems
- Works within a scenario-based concept of risk that best informs decision-making
  - Identifies contributing elements (initiating events, pivotal events, basic events)
  - Quantifies the risk significance of contributing elements, helping focus on where improvements will be effective
  - Provides a means of re-allocating analytical priorities according to where the dominant risk contributors appear to be coming from
  - Provides a framework for a monitoring / trending program to detect risk-significant adverse trends in performance

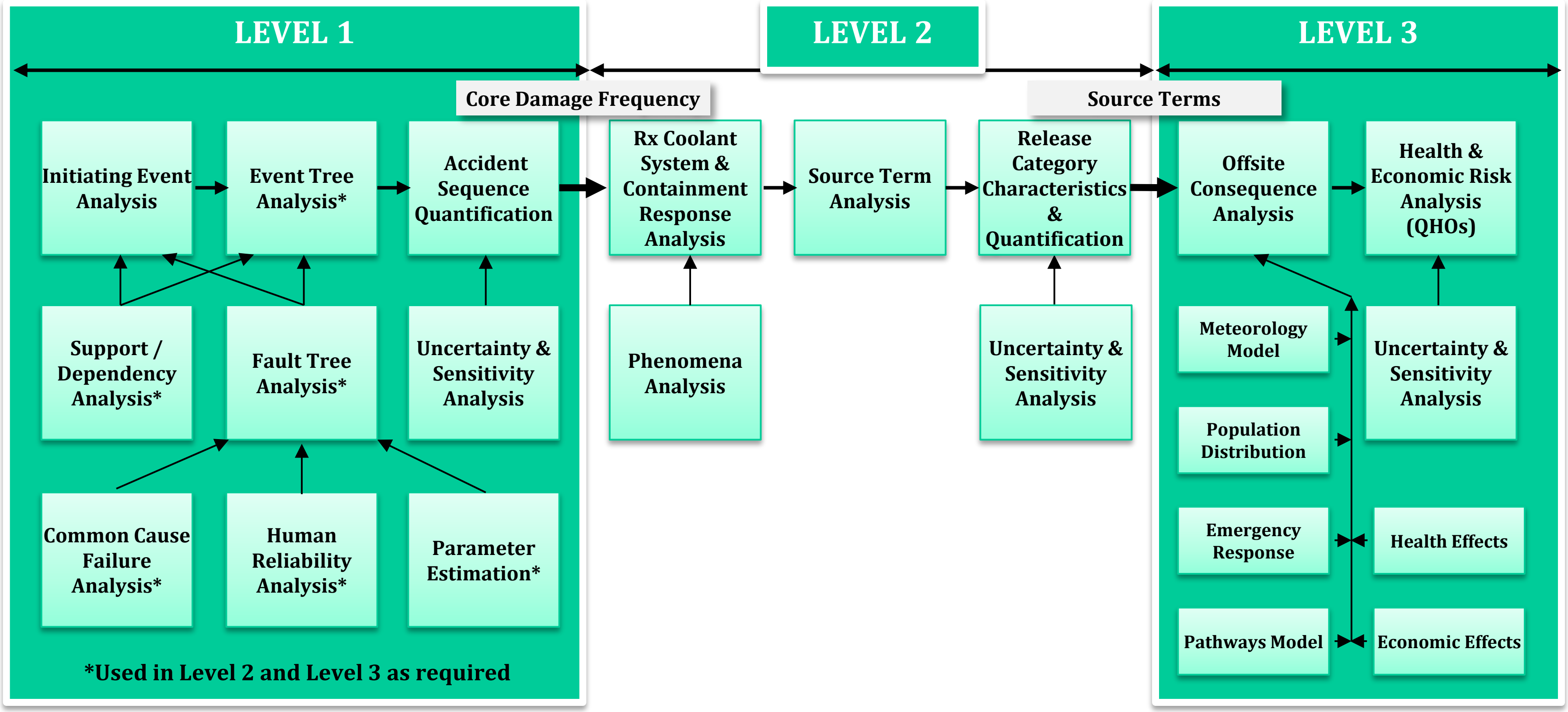
# Strengths of PRA (cont.)

- Rigorous, systematic analysis tool
- Information integration (multidisciplinary)
- Allows consideration of complex interactions
- Develops qualitative design insights
- Develops quantitative measures for decision making
- Provides a structure for sensitivity studies
- Provides a structure for uncertainty analysis of input parameter values

# Limitations of PRA

- Sparseness of available data
  - Less of a limitation now than in the past, at least for existing nuclear plants
- Lack of understanding of physical processes
- High sensitivity of some results to assumptions
- Constraints on modeling effort (limited resources)
  - Simplifying assumptions
  - Truncation of results during quantification
    - Less of a limitation now than in the past
- Lack of completeness (e.g., human errors of commission typically not considered)
- PRA is typically a snapshot in time
  - This limitation may be addressed by having a “living” PRA
    - Plant changes (e.g., hardware, procedures and operating practices) reflected in PRA model
    - Temporary system configuration changes (e.g., out of service for maintenance) reflected in PRA model
    - Living PRA required for new reactor designs

# Principal Steps in PRA



LEVEL 1

LEVEL 2

LEVEL 3

Core Damage Frequency

Source Terms

Initiating Event Analysis

Event Tree Analysis*

Accident Sequence Quantification

Rx Coolant System & Containment Response Analysis

Source Term Analysis

Release Category Characteristics & Quantification

Offsite Consequence Analysis

Health & Economic Risk Analysis (QHOs)

Support / Dependency Analysis*

Fault Tree Analysis*

Uncertainty & Sensitivity Analysis

Phenomena Analysis

Uncertainty & Sensitivity Analysis

Meteorology Model

Uncertainty & Sensitivity Analysis

Population Distribution

Common Cause Failure Analysis*

Human Reliability Analysis*

Parameter Estimation*

Emergency Response

Health Effects

Pathways Model

Economic Effects

*Used in Level 2 and Level 3 as required

Idaho National Laboratory

# Risk Units

- **Risk - the frequency with which a given consequence occurs**

$$\text{Risk}\left[\frac{\text{Consequence Magnitude}}{\text{Unit of Time}}\right] =$$

$$\text{Frequency}\left[\frac{\text{Events}}{\text{Unit of Time}}\right] \text{ x Consequences}\left[\frac{\text{Magnitude}}{\text{Events}}\right]$$

Note that the frequency can be replaced by a probability

# Quantitative Health Objectives- Death Due to Accidents(Example)

- Societal Risk = 130,557 Accidental-Deaths/year
- Average Individual Risk

  = (130,557 Accidental-Deaths/Year)/316,128,180 Est. U.S. Pop.

  = 4.1E-04 Accidental-Deaths/Person-Year

  ≈ 1/2,421 Accidental-Deaths/Person-Year
- In any given year, approximately 1 out of every 2,421 people in the entire U.S. population will die from an accidental death
  - Note: Figures presented above are based on the National Vital Statistics Reports, Deaths: Final Data for 2013, February 16, 2016, Volume 64, Number 2, at www.cdc.gov which is the Centers for Disease Control and Prevention (CDC) National Center for Health Statistics (NCHS) for the United States.
  - Unintentional injuries is the preferred term to accidental deaths in the public health community.
  - Average individual risk for accidental deaths in the 1980s was approximately 5.0E-04 Deaths/Person-year.

# Quantitative Health Objectives- Death Due to Cancer (Example)

- Societal Risk = 584,881 Cancer-Deaths/year
- Average Individual Risk

  = (584,881 Cancer-Deaths/Year)/316,128,180 Est. U.S. Pop.

  = 1.9E-03 Cancer-Deaths/Person-Year

  ≈ 1/540 Cancer-Deaths/Person-Year
- In any given year, approximately 1 out of every 540 people in the entire U.S. population will die from cancer
  - Note: Figures presented above are based on the National Vital Statistics Reports, Deaths: Final Data for 2013, February 16, 2016, Volume 64, Number 2, at www.cdc.gov which is the Centers for Disease Control and Prevention (CDC) National Center for Health Statistics (NCHS) for the United States.
  - Malignant neoplasms is the preferred term to cancer deaths in the public health community.
  - Average individual risk for cancer deaths in the 1980s was approximately 2.0E-03 Deaths/Person-year.

# Commission’s Safety Goals

- Qualitative Safety Goals
  - No significant additional risk to life and health to individual members of public from nuclear power
  - Comparable or less than risks from other energy generation technologies to society.

- From the goals, the Commission determined objectives (“lines in the sand”)
  - Quantitative Health Objectives (Originally known as the Probabilistic Safety Goals)
  - Subsidiary Objectives

Reference – Policy Statement, 8/21/86 (51 FR 30028)

# NRC Quantitative Health Objectives (QHOs)

- Originally known as the Probabilistic Safety Goals
  - NRC adopted two probabilistic safety goals on August 21, 1986
- High-level goal: incremental risk from nuclear power plant operation < 0.1% of all risks
  - Average individual (within 1 mile of plant) early fatality (accident) risk

    < 5E-7/year
  - Average individual (within 10 miles of plant) latent fatality (cancer) risk

    < 2E-6/year
  - The “0.1%” was a subjective factor determined after much deliberation and consideration

# Subsidiary Objectives

- Lower level subsidiary goals were derived from the high-level QHOs
  - Frequency of significant core damage (CDF) < 1E-4/year
    - Surrogate for latent cancer fatalities
  - Frequency of large early release of fission products from containment (LERF) < 1E-5/year
    - Surrogate for prompt fatalities
- Metrics for new reactors (Staff Requirements Memo, SRM, on SECY-10-0121, 09/14/2010)
  - CDF < 1E-4/year
  - Large release frequency (LRF) < 1E-6/year
  - Conditional containment failure probability (CCFP) < 0.1

# Review of Risk Assessment Concepts & PRA

**Key Points of Section:**

- Risk involves both the likelihood of the undesired event and the severity (or magnitude) of the consequences.

  *Risk = Frequency* X *Consequence*

- Risk Triplet – Three basic questions answered by PRA
  - What can go wrong? (i.e., accident scenario)
  - How likely is it to occur? (i.e., frequency, probability)
  - What is the outcome? (i.e., consequences)
- Three Levels of PRA
  - Level 1 – analysis of initiating events and response with output being core damage frequency
  - Level 2 – analysis of reactor and containment response to core damage sequences with output being release category characteristics
  - Level 3 – analysis of release categories characteristics with output being offsite health and/or economic consequences
- Strengths and limitations of PRA
  - Strengths: systematic analysis tool, qualitative insights, a means for *quantitative* measures for decision making, allows for consideration of uncertainty
  - Limitations: sparseness of available data, constraints on modeling effort, lack of completeness

Page Intentionally Left Blank

# 2. Basic PRA Techniques

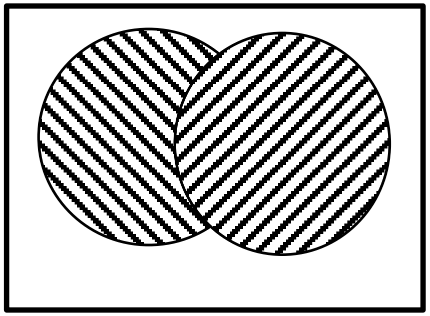
# Basic PRA Techniques

- **Purpose: Introduce/review elementary probability concepts, with focus on PRA relevant items**
- **Objectives: At the conclusion of this section, students will understand:**
  - **Basic probability operations**
  - **Difference between frequency and probability**
  - **How to calculate probability from frequency**
  - **Cut sets**
- **Reference:**
  - **NUREG-0492, *Fault Tree Handbook***

# Basic Probability Concepts Used in PRAs

*A or B*

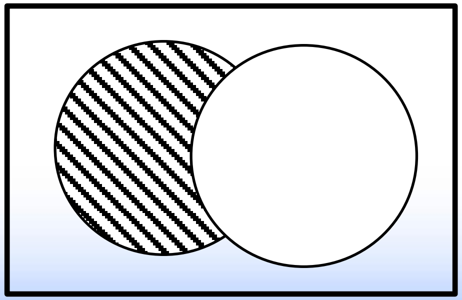
*A + B*



**Venn Diagram**

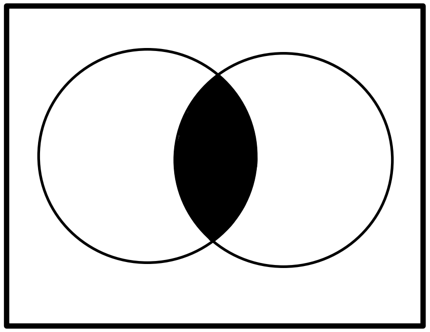
*A and /B*

*A * /B*



*A and B*

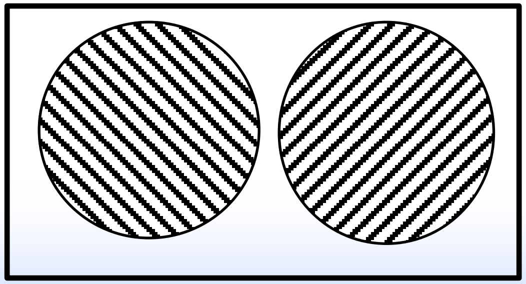
*A * B*



*A or B*

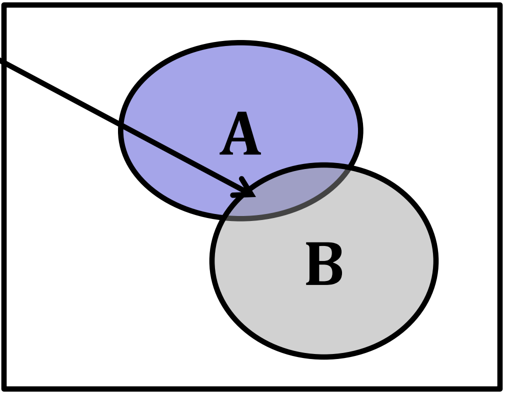
*A + B*

*with the two events mutually exclusive*



# Rules for Manipulating Probabilities – OR (Union)

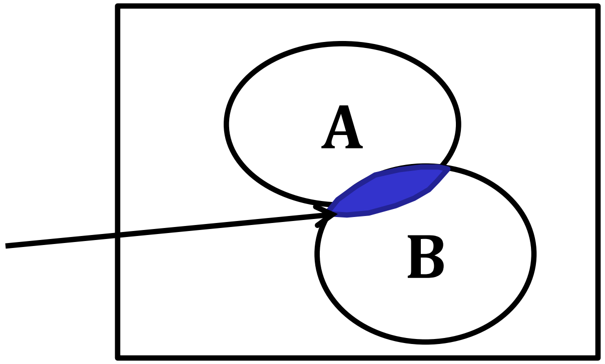
- The OR (or union) operation
  - A **OR** B = combined event containing everything in A or in B
  - Also written A ∪ B
- Rules for the OR Operation
  - In general, if A, B are not disjoint (*not mutually exclusive*)
    - Pr(A or B) = Pr(A) + Pr(B) - Pr(A AND B)
    - Can extend to three or more events
  - If A, B are disjoint (*mutually exclusive*)
    - Pr(A or B) = Pr(A) + Pr(B)
    - Example:
      with a die, Pr(1 or 2) = Pr(1) + Pr(2)
      because outcomes are disjoint



Venn Diagram

# Rules for Manipulating Probabilities – AND (Intersection)

- The AND (or intersection) operation
  - A AND B = combined event containing everything that is both in A and in B
  - Also written A ∩ B
- Rules for the AND operation
  - If A, B are independent
    - Pr(A AND B) = Pr(A) • Pr(B) (definition)



  - If A, B are not independent (i.e., dependent)
    - Pr(A AND B) = Pr(A) • Pr(B|A) = Pr(B) • Pr(A|B)
      - Pr(B|A) read as “probability of B occurring, given that A occurs,” or more simply, “probability of B, given A”
      - The “|” is statistical shorthand for “given that”

# Definition of “Conditional Probability”

- Conditional probability definition
  - We said that in general
    - Pr(A AND B) = Pr(A) • Pr(B | A)
  - The conditional probability is last term, Pr(B | A), so
    - Pr(B | A) = Pr(A AND B) / Pr(A), Pr(A) $\neq$ 0
    - Pr(A | B) = Pr(A AND B) / Pr(B), Pr(B) $\neq$ 0
  - These last equations define “conditional probability”.

# Basic Probability Concepts

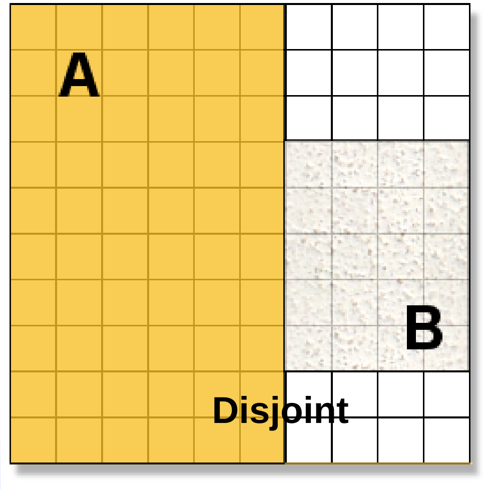
- Independent
  - Means that the occurrence (or non-occurrence) of an event (such as A) has no influence on the subsequent occurrence (or non-occurrence) of another event (such as B) and vice versa
  - If a fair coin is tossed randomly, the occurrence of Heads on the first toss should not influence the probability of Tails on the second toss.
  - This property allows us to write:
    - If A and B are two independent events, then Pr(A and B) = Pr(A) * Pr(B).
    - Example: Pr(H and T | two tosses) = Pr(H) * Pr(T)
- Mutually Exclusive
  - Means that events (such as A and B) cannot both happen on a single trial of an experiment
  - With the toss of a fair coin, either a Head or a Tail is the expected outcome, cannot possibly get both a Head and a Tail as an outcome on a single toss
  - This property allows us to write:
    - If A and B are two mutually exclusive events, the Pr(A or B) = Pr(A) + Pr(B)
    - If Mutually Exclusive, Pr(A and B) = Pr(A)*Pr(B|A) = Pr(B)*Pr(A|B) = 0
    - Example: Pr(H or T | one toss) = Pr(H) + Pr(T) ∴ Pr(H and T | one toss) = 0

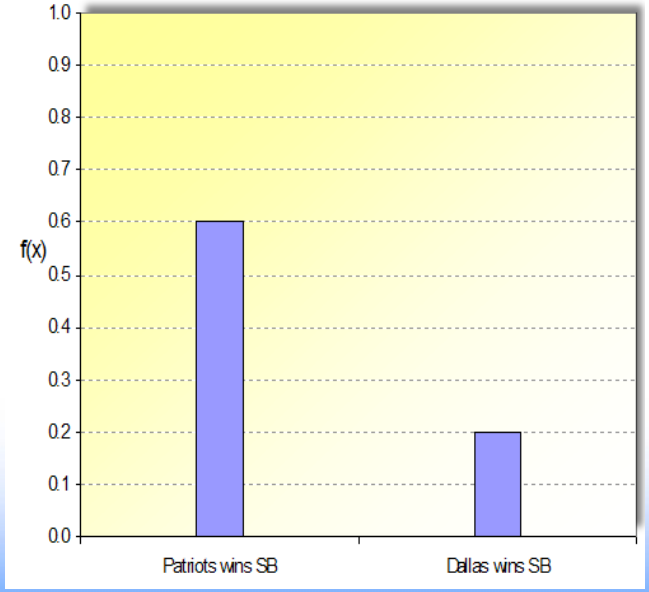
# Basic Probability Concepts (cont.)

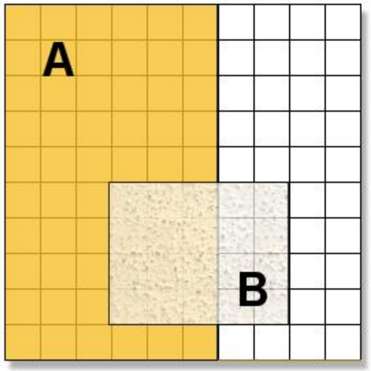
- **Dependent**
  - **Means that the occurrence (or non-occurrence) of an event (such as A) has an influence on the subsequent occurrence (or non-occurrence) of another event (such as B) and vice versa**
  - **For example, if a resistor overheats in an electronic circuit, it may very well change the failure probability of a nearby transistor or related circuitry.**
  - **This property allows us to write**
    - **If A and B are two mutually interdependent events, then Pr(A and B) = Pr(A) * Pr(B|A) = Pr(B) * Pr(A|B)**
    - **Term Pr(B|A) represents the probability of B given that A has happened**
  - **Note: if they are independent then Pr(B|A) = Pr(B) and Pr(A|B) = Pr(A)**
- **Complement (or “not”)**
  - **Means the probability is “1 -” the probability of event**
    - **Pr(not A) = 1 – Pr(A)**

# Independent vs Disjoint (mutually exclusive)

- An example using disjoint events
  - If two events A and B are disjoint (mutually exclusive)
    - Pr(A AND B ) = 0
    - If Pr(A) = 0.6 while Pr(B) = 0.2 then the “Venn” diagram is



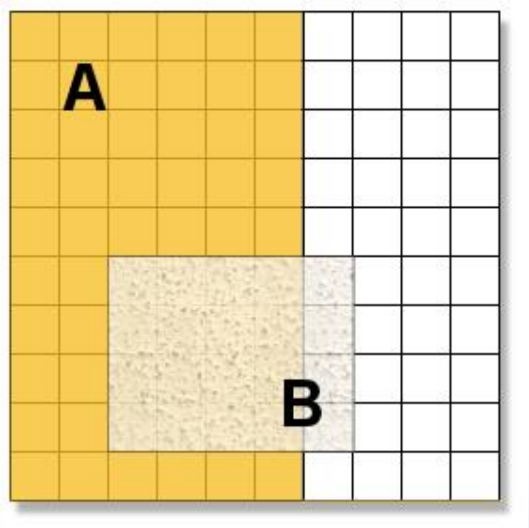




**Pr(A AND B) = 0.12**
**if A, B were independent…**

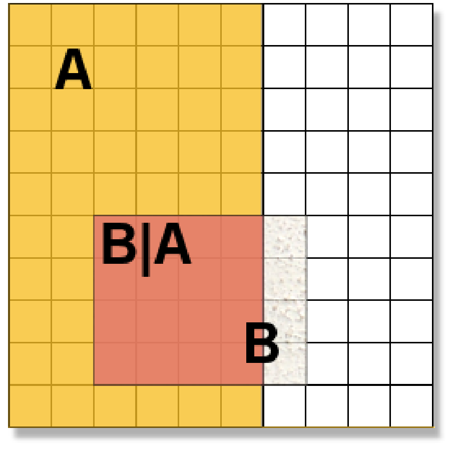
# Independent versus Dependent

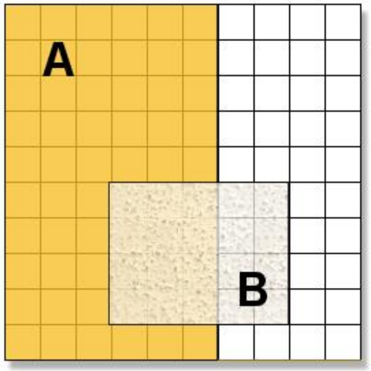
- An example using dependent events
  - If Pr(A) = 0.6, Pr(B) = 0.2, and Pr(A AND B) = 0.16, then
    - Pr(B|A) = Pr(A AND B)/Pr(A) = 0.16/0.6 = 0.2667
      - since Pr(A AND B) = Pr(A) • Pr(B|A)
    - Pr(A|B) = Pr(A AND B)/Pr(B) = 0.16/0.2 = 0.80
      - since Pr(A AND B) = Pr(B) • Pr(A|B)



A and B are dependent

Where is Pr(B|A) on the Venn diagram?
16 blocks/60 blocks = 0.26667

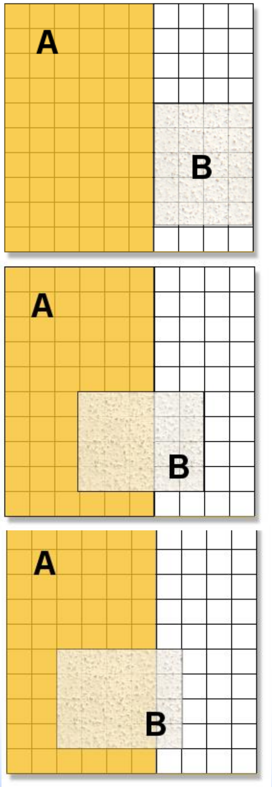




Pr(A AND B) = 0.12
if A, B were independent…

# Disjoint, Independent, Dependent Summary

- **Table below summarized the probability rules**



| Case | Operation | Rule |
|---|---|---|
| Disjoint | OR | p(A OR B) = p(A)+p(B) |
| | AND | p(A AND B) = 0 |
| Independent | OR | p(A OR B) = p(A)+p(B) - p(A AND B) |
| | AND | p(A AND B) = p(A)p(B) |
| Dependent | OR | p(A OR B) = p(A)+p(B) - p(A AND B) |
| | AND | p(A AND B) = p(A)p(B \| A)<br>= p(B)p(A \| B) |

# Some Events have an Associated Frequency which is used to Calculate a Probability

- Frequency
  - Frequency can be any positive value (i.e., can be greater than one)
  - Events per unit of time
  - Typically used for initiating events and failure rates
    - For example, failure rate of operating pump (X per hour)
- Probability
  - Value between 0 and 1
  - Internal measure of certainty about the truth of a proposition
    - For example, the probability of a valve opening is Y
  - Always conditional
  - Unitless
  - Used for all events in a PRA except the initiating event
- Different concepts; sometimes numerically equal

# Common Probability Models

- **Bernoulli processes → Binomial model**
  - Tossing a coin
  - Starting a pump
  - Opening a closed valve
  - Turning on a light
  - Launching a rocket
- **Poisson processes → Poisson model**
  - Counting radioactive particles
  - Number of (lit) lights failing
  - Operation of (running) pump
  - Earthquakes
  - Initiating events

# Common Probability Models

- **Binomial (used for failures on demand)**
  - **P[r failures in N trials |p] =** $\binom{N}{r} p^r (1-p)^{N-r}$
    - **Recall:** $\binom{N}{r} = \frac{N!}{r!(N-r)!}$
    - **Probability of failure for a single demand**

$$\text{P[1 failure \ in 1 trial | p]} = \frac{N!}{r!(N-r)!} p^r (1-p)^{N-r} = \frac{1!}{1!(1-1)!} p^1 (1-p)^{1-1} = (1)\, p^1 (1) = p$$

- **Binomial Example:**
  - **Pump data failing to start on demand p = 0.001**
  - **Probability of 1 failure to start in 1 demand?**

$$\text{P[1 failure \ in 1 trial} \,|\, 0.001] = \frac{1!}{1!(1-1)!} 0.001^1 (1-0.001)^{1-1} = \frac{1!}{1!(0)!} 0.001^1 (0.999)^0 = (1)(0.001)(1) = 0.001$$

# Common Probability Models (cont.)

- **Poisson (used for failures/events in time)**
  - **P[r failures in (0,t) | $\lambda$ ] =** $\dfrac{(\lambda t)^r e^{-\lambda t}}{r!}$
  - **Probability of one or more failures**
    - **P[$T_f$ < t | $\lambda$ ] = 1 - $e^{-\lambda t} \approx \lambda t$ (for small $\lambda t$; when $\lambda t < 0.1$)**
      - **Example: estimate of product $\lambda t$ versus exact of 1 - $e^{-\lambda t}$**

|  |  |  |
|---|---|---|
| 0.5 | vs | 0.39 |
| 0.1 | vs | 0.095 |
| 0.05 | vs | 0.04877 |
| 0.01 | vs | 0.00995 |
| 0.005 | vs | 0.0049875 |

- **Poisson Example:**
  - **Pump data failing to run $\lambda$ = 1E-4 failures per operating hour**
  - **Probability of failure to run for 24 hours?**
    - **P[$T_f$ < 24 hours | 1E-4 failures/hour]**

**= 1 - $e^{-(\text{1E-4failures/hour})(\text{24 hours})}$ = 1 - $e^{-(\text{2.4E-3})}$ = 1 – (0.997602878) = 0.002397122**

**$\approx$ 2.4E-3 [i.e., product of $\lambda t$ = (1E-4)(24)]**

# Probability of Core Damage

- **Assume 100 plants, each with CDF = $10^{-4}$/yr**
- **Assume operation over 40 years**
- **What is probability of at least one core damage accident during that time?**

**P($\geq$ 1 core damage|CDF = $10^{-4}$/yr)**

**= 1 – exp[-($10^{-4}$/plant-yr)(40 yr)(100 plants)]**

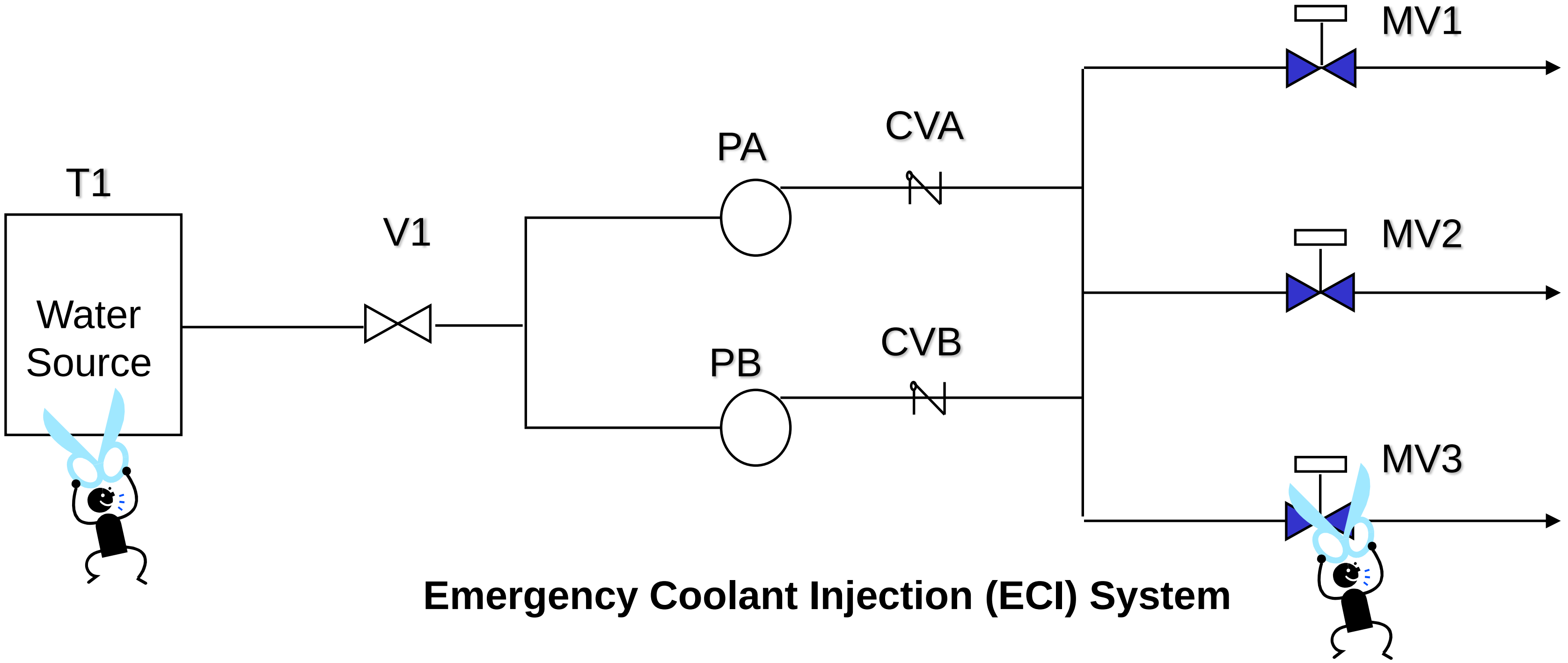
**= 1 – exp[-($10^{-4}$/plant-year)(4,000 plant-years)]**

**= 0.33**

# Cut Sets

- **Combinations of events that result in a particular outcome**
- **Minimal Cut Sets are those combinations that are both *necessary* and *sufficient* to produce the particular outcome**
  - **i.e., minimal combination**
- **Each cut set represents a failure scenario that must be "ORed" together with all other cut sets for the top event when calculating the total probability of the top event**
- **Boolean algebra (discussed later) used for processing cut sets**

# Cut Set Example



Emergency Coolant Injection (ECI) System

**Success if there is flow from the tank through any one pump train through any one motor-operated valve.  ECI components include:**

**T# - tank**
**V# - manual valve, normally open**
**P# - pump**
**CV# - check valve**
**MV# - motor-operated valve, normally closed**

# Cut Sets for ECI

By inspection of the ECI piping and instrumentation diagram (P&ID):

ECI-System-Failure =
T1 +
V1 +
PA * PB +
PA * CVB +
PB * CVA +
CVA * CVB +
MV1 * MV2 * MV3

# Quantifying Cut Sets

- Three different quantification methods to quantify the probability of cut sets:
  1. Exact Solution
  2. Rare Event Approximation
  3. Minimal Cut Set Upper Bound Approximation

# Exact Solution

- **Exact Solution for Cut Sets = A OR B**
  - **P(Exact Solution for Cut Sets) = P(A + B) = P(A) + P(B) - P(AB)**

- **Cross terms become unwieldy for large lists of cut sets.**
  - **E.g., if Cut Sets = A OR B OR C, then:**
  - **P(Exact Solution for Cut Sets) =**

$$\underbrace{P(A)+P(B)+P(C)}_{\text{Add the Singles}} - \underbrace{[P(AB)+P(AC)+P(BC)]}_{\text{Subtract the Doubles}} + \underbrace{P(ABC)}_{\text{Add the Triples}} \quad \ldots$$

# Rare Event Approximation

- **Rare Event Approximation for Cut Sets = A OR B**
  - **P(Union of Cut Sets) ≈ sum of the probabilities of each individual cut set**
  - **P(Union of Cut Sets) ≈** $\sum_{k=1}^{K} P(Cutset_k)$
    - **K = total # of cut sets**
  - **P(A AND B) judged to be sufficiently small (rare) and thus can be ignored (i.e., cross-terms are simply dropped)**

- **In general,**
  - **P{*Exact* Solution for Cut Sets} ≤** $\sum_{k=1}^{K} P(Cutset_k)$

# Minimal Cut Set Upper Bound

- **Minimal Cut Set Upper Bound (“min cut”) Approximation for Cut Sets = A OR B**
  - **P(Minimal Cut Set Upper Bound for Cut Sets) ≈ 1.0 minus the product of each individual cut set NOT occurring**
    - **Failure = 1 - Success**
  - **P(MCSUB for Cut Sets) ≈** $1-\prod_{k=1}^{K}[1-P(Cut\ Set_k)]$
  - **P(MCSUB for Cut Sets) ≈** $1-\left[(1-P(A))*(1-P(B))\right]$
  - **This is exact when cut sets are independent (i.e., no shared basic events in individual cut sets)**
- **In general,**
  - **P{*Exact* Solution for Cut Sets} ≤ P(MCSUB for Cut Sets) ≤ P(Rare Event for Cut Sets)**

# Examples of Cut Set Quantification Methods for P(A+B)

| | Cut Sets A & B independent; individual cut set values low | Cut Sets A & B independent; individual cut set values high | Cut Sets A & B are not independent (they have shared basic events); individual cut set values low |
|---|---|---|---|
| Cut-Sets<br>= A + B | P(A) = 0.01<br>P(B) = 0.03 | P(A) = 0.4<br>P(B) = 0.6 | Cut Set A = BE1 * BE2<br>Cut Set B = BE2 * BE3<br>P(BE1) = 0.1<br>P(BE2) = 0.1<br>P(BE3) = 0.3 |
| Exact | = 0.01 + 0.03 - (0.01 * 0.03)<br>= 0.04 – 0.0003<br>= 0.0397 | = 0.4 + 0.6 - (0.4 * 0.6)<br>= 1.0 - (0.24)<br>= 0.76 | = (BE1*BE2) + (BE2*BE3) – (BE1*BE2)*(BE2*BE3)<br>= (BE1*BE2) + (BE2*BE3) – (BE1*BE2*BE3)<br>= 0.01 + 0.03 – 0.003<br>= 0.04 – 0.003<br>= 0.037 |
| Rare Event | = 0.01 + 0.03<br>= 0.04 | = 0.4 + 0.6<br>= 1.0 | = 0.01 + 0.03<br>= 0.04 |
| MinCut UB | = 1 - [(1-0.01) * (1-0.03)]<br>= 1 - [(0.99) * (0.97)]<br>= 1 - [0.9603]<br>= 0.0397 | = 1 - [(1-0.4) * (1-0.6)]<br>= 1 - [(0.6) * (0.4)]<br>= 1 - [0.24]<br>= 0.76 | = 1 - [(1-0.01) * (1-0.03)]<br>= 1 - [(0.99) * (0.97)]<br>= 1 - [0.9603]<br>= 0.0397 |

# Review Basic PRA Techniques

**Key Points of Section:**

- Two major probability operations:
  - AND
  - OR
- Frequency and probability are different!
- Probability calculated from a frequency based on a specified mission
- Cut sets:
  - Combination of events leading to an outcome of interest
  - Minimal cuts sets are those combinations that are necessary and sufficient to produce the outcome
  - Each cut set represents a failure scenario
- Cut set quantification methods:
  - Exact Solution (intractable for real problems)
  - Rare Event Approximation
    - Can be overly conservative
  - Minimal Cut Set Upper Bound Approximation
    - Less conservative than rare event approximation
    - Default method in SAPHIRE and most PRA software

# WORKSHOP - Probability and Frequency Questions – (question 1 of 3)

- **1. An event occurs with a frequency of 0.02 per year.**
  - **1.1. What is the probability that at least one event will occur within a given year?**
  - **1.2. What is the probability that at least one event will occur within 50 years?**

# WORKSHOP - Probability and Frequency Questions – (question 2 of 3)

- 2. Event A occurs with a frequency of 0.1 per year. Event B occurs with a frequency of 0.3 per year.
  - 2.1. What is the probability that at least one event (either A or B) will occur within a given year?
  - 2.2. What is the probability that at least one event (either A or B) will occur within 5 years?

# WORKSHOP - Probability and Frequency Questions – (question 3 of 3)

- 3. An experiment has a probability of 0.1 of producing a failure.
  - 3.1. What is the probability of observing exactly one failure if the experiment is repeated 4 times?
  - 3.2. What is the probability of observing at least one failure if the experiment is repeated 4 times?

# 3. Event Tree Analysis

# Event Tree Analysis

- **Purpose: Students will learn purposes & techniques of event tree analysis. Students will learn how event tree analysis is related to the identification and quantification of accident sequences.**
- **Objectives:**
  - **Understand purposes of event tree analysis**
  - **Understand currently accepted techniques and notation for event tree construction**
  - **Understand purposes and techniques of dominant accident sequence identification**
- **References:**
  - **NUREG/CR-2300, *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants***
  - **NUREG-1489, *A Review of NRC Staff Uses of Probabilistic Risk Assessment***

# Event Trees

- Typically used to model the response to an initiating event
- Features:
  - One event tree for each initiating event
  - Related to systems/functions/operations
  - Identifies relationships in event occurrence
  - Identifies relative timing of event occurrence
  - Event sequence progression
  - End-to-end traceability of accident sequences
- Primary use
  - Identification of accident sequences which result in some outcome of interest
    - Usually core damage (Level 1) or containment failure (Level 2)
  - Forms the basis for accident sequence quantification

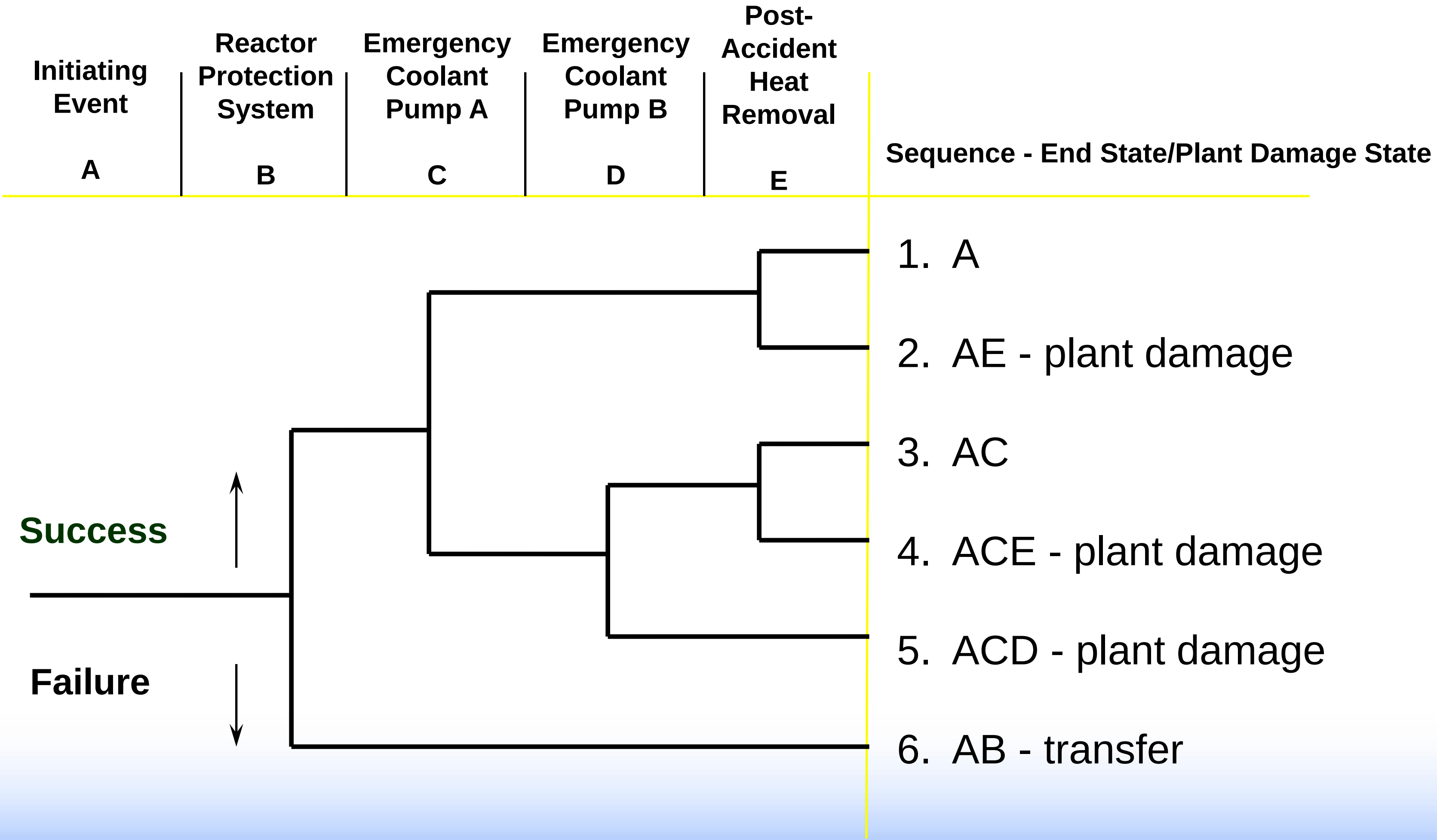
# Initiating Events

- Traditional U.S. reactor PRA categorization:
  - Internal Initiating Events
    - Loss-of-coolant accident (LOCA)
      - Involves breach of primary coolant boundary (pipe break or open valve)
    - Transient
      - Event requiring reactor shutdown, but without primary breach
  - External Initiating Events
    - Typically originates outside plant systems
    - Requires special analysis techniques, so treated separately
    - Examples: earthquake, fire, flood

# Identification of Initiating Events

- Past operating experience, including similar stations
- Review of other PRAs
- Failure Modes and Effects Analysis (FMEA)
- Feedback from system modeling
- Master logic diagram (special type of fault tree)
- Expert elicitation

# Simple Event Tree



Initiating Event

A

Reactor Protection System

B

Emergency Coolant Pump A

C

Emergency Coolant Pump B

D

Post-Accident Heat Removal

E

Sequence - End State/Plant Damage State

1. A
2. AE - plant damage
3. AC
4. ACE - plant damage
5. ACD - plant damage
6. AB - transfer

Success

Failure

# Principal Steps in Event Tree Development

- Determine boundaries of analysis
  - E.g., small leak might be defined as leaks up to a certain size
- Define critical plant safety functions available to mitigate each initiating event
- Determine systems available to perform each critical plant safety function
- Determine success criteria for each system for performing each critical plant safety function
- Event tree heading - order & development
- Sequence delineation

# Determining Boundaries

- Mission time
  - How long do specific systems/functions/components need to operate?
- Dependencies among safety functions or systems
- Sequence end states - undesired outcome
  - Core vulnerable
  - Containment vulnerable
  - Core damage
- Extent of operator actions explicitly modeled in event tree

# Success Criteria

- Start with functional event tree
  - Define the functions that are needed to respond to the initiating event
  - Those fundamental safety functions that will be challenged or required to mitigate the accident initiator
- Six fundamental safety functions for core & containment
  1. Reactor subcriticality
  2. Core heat removal
  3. Core inventory makeup
  4. Containment pressure suppression
  5. Containment heat removal
  6. Containment integrity

# Success Criteria

- Identify systems which can perform each of the required fundamental safety function
- Identify the minimum required equipment necessary to perform function
  - This is often based on thermal/hydraulic calculations
  - This may be a source of uncertainty (difference in the scenario may result in different success criteria)
  - Calculations often best-estimate, rather than conservative, since this assumption goes into the PRA
- May credit non-safety-related equipment where feasible

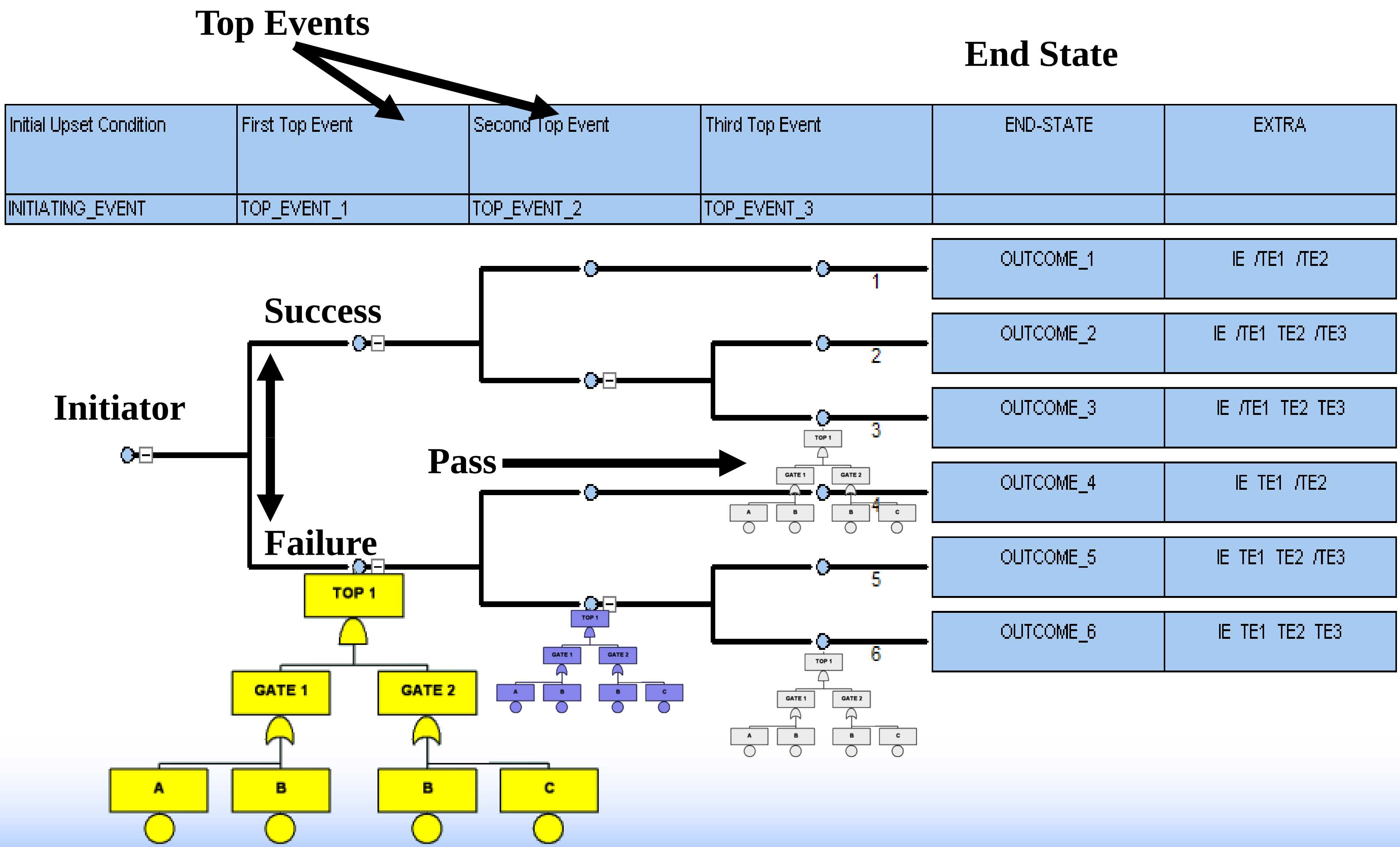
# Event Tree Development

- **An event tree consists of**
  - **An initiating event (one per tree) followed by a number of headings (or top events)**
  - **Event tree structure (success/failure) branching for the top events**
- **The top events represent systems, components, and/or operations identified by success criteria**
- **To the extent possible, the top events are ordered in the time-related sequence in which they would occur**
  - **Selection of top events and their ordering reflects the emergency operating procedures (EOPs)**
- **Each node (or branch point) below a top event represents the success or failure of the respective top event**
  - **Logic typically binary**
    - **Down branch → failure of top event**
    - **Up branch → success of top event**
  - **Logic can have more than binary branch, with each branch representing a specific status of the respective top event**

# Event Tree Development (Continued)

- Branches can be pruned logically (branch points for specific nodes removed) to remove unnecessary combinations of system success requirements
  - This minimizes the total number of sequences that will be generated and eliminates illogical sequences
- Each path of an event tree represents a potential scenario
- Each potential scenario results in either plant success or core damage (or a particular end state of interest)

# Traditional Event Tree Format



| Initial Upset Condition | First Top Event | Second Top Event | Third Top Event | END-STATE | EXTRA |
|---|---|---|---|---|---|
| INITIATING_EVENT | TOP_EVENT_1 | TOP_EVENT_2 | TOP_EVENT_3 | | |

| | | |
|---|---|---|
| 1 | OUTCOME_1 | IE /TE1 /TE2 |
| 2 | OUTCOME_2 | IE /TE1 TE2 /TE3 |
| 3 | OUTCOME_3 | IE /TE1 TE2 TE3 |
| 4 | OUTCOME_4 | IE TE1 /TE2 |
| 5 | OUTCOME_5 | IE TE1 TE2 /TE3 |
| 6 | OUTCOME_6 | IE TE1 TE2 TE3 |

# Plant Damage States (PDS)

- Also called "Accident Classes" or "End States"
- Can use "indicators" to relate a core damage accident sequence to the status of plant safety function such as
  - The reactor coolant system at onset of core damage (breached or closed)
  - Various systems' operability (e.g., AC power)
  - Water inventories (e.g., injection into RPV)
  - The containment (e.g., pressure, integrity)
  - Timing of the onset of core damage (early/late)
- Plant damage states are used to
  - Group accident sequences with similar outcomes for core damage
  - Simplify subsequent use in Level 2/3 analysis

# Example Category Definitions for PDS Indicators

1. Status of RCS at onset of Core Damage

| | |
|---|---|
| T | no break (transient) |
| A | large LOCA (6” to 29”) |
| S1 | medium LOCA (2” to 6”) |
| S2 | small LOCA (1/2” to 2”) |
| S3 | very small LOCA (less than 1/2”) |
| G | steam generator tube rupture with SG integrity |
| H | steam generator tube rupture without SG integrity |
| V | interfacing LOCA |

2. Status of ECCS

| | |
|---|---|
| I | operated in injection only |
| B | operated in injection, now operating in recirculation |
| R | not operating, but recoverable |
| N | not operating and not recoverable |
| L | LPI available in injection and recirculation of RCS pressure reduced |

3. Status of Containment Heat Removal Capability

| | |
|---|---|
| Y | operating or operable if/when needed |
| R | not operating, but recoverable |
| N | never operated, not recoverable |

# Review of Event Tree Analysis

## Key Points of Section:

- Event trees model the response to an initiating event. They identify accident sequences which result in some outcome.
- Event trees consist of: an initiating event, top events (system mitigators), branching, and end states.
- Accident sequences are obtained by moving across the event tree from left to right, keeping track of successes and failures for each system top event until a specific end state is reached. These sequences can then be quantified to obtain the "dominant accident sequences".

# WORKSHOP – Event Tree Example

- Develop an event tree to identify the different scenarios (accident sequences) of not making it to work on time and what will be the consequences (end states [not making it at all, 10 minutes late, etc.]) where the initiating event is you need to go to work.

# WORKSHOP – workspace

# 4. Fault Tree Analysis

# Fault Tree Analysis

- **Purpose:** **Students will learn purposes & techniques of fault tree analysis. Students will learn how appropriate level of detail for a fault tree analysis is established. Students will become familiar with terminology, notation, and symbology employed in fault tree analysis. In addition, a discussion of applicable component failure modes relative to the postulation of fault events will be presented.**
- **Objectives:**
  - **Demonstrate working knowledge of terminology, notation, and symbology of fault tree analysis**
  - **Demonstrate knowledge of purposes & methods of fault tree analysis and reduction to minimal cut sets**
- **References:**
  - **NUREG-0492, *Fault Tree Handbook***
  - **NUREG/CR-2300, *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants***
  - **NUREG-1489, *A Review of NRC Staff Uses of Probabilistic Risk Assessment***

# Fault Tree Analysis Definition

*"An analytical technique, whereby an* ***undesired state*** *of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed* ***in the context of its environment and operation*** *to find all* ***credible*** *ways in which the undesired event can occur."*

***NUREG-0492, Fault Tree Handbook***

# Fault Trees

- Deductive analysis (event trees are inductive)
- Top down approach starting with undesired event (top event) definition
  - This “top” definition frequently comes from the event tree model
- Explicitly models multiple failures
  - As many things as it takes to case the top event to occur
- Provides event relationships (i.e., combinations of events leading to undesired event)
- Used to estimate top event unreliability
  - probability top event fails to perform intended function

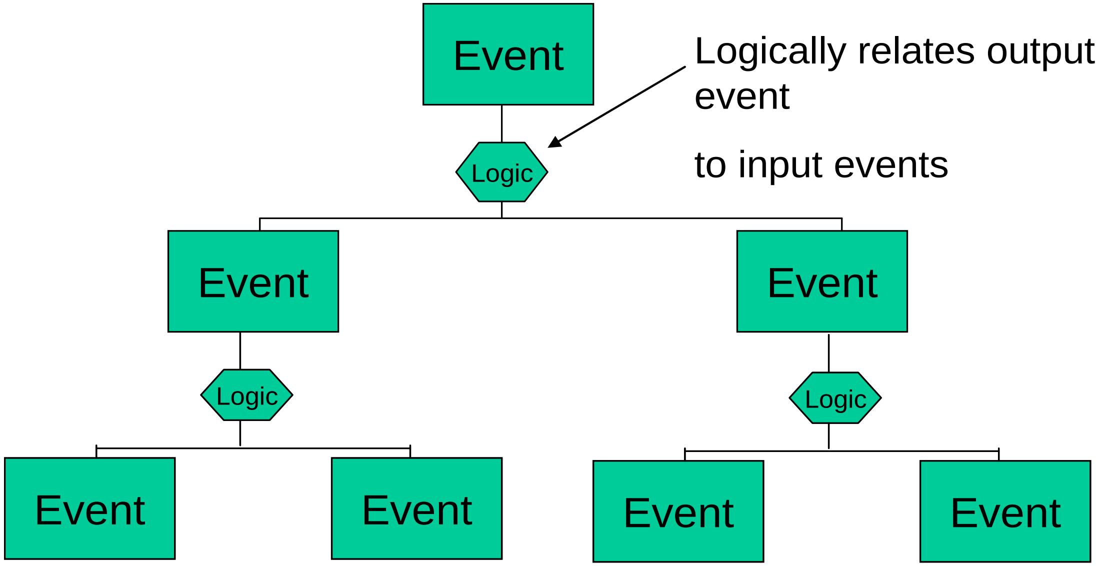
# Purpose of Fault Tree Analysis

- Fault trees can be used to identify the ways in which a system, component, function, or operation can fail.
- Fault tree models can be used to determine:
  - Interrelationships between fault events, failure combinations producing undesired event
  - System "weaknesses"
    - Qualitative
    - Quantitative
  - System unreliability (system failure probability)
  - Sometimes used for initiating events (e.g., loss of service water)

# FTA Decomposes System Failures into Basic Events

- **A fault tree is a common model to resolve the system failure into basic events**
- **Basic Events involve:**
  - **Component failures (pump fails to _______)**
  - **Human errors (operator fails to _______)**
  - **Phenomenological events**
  - **Etc.**
- **The fault tree logic mirrors the operational logic of the system, accounting for redundancies and interfaces**
- **The fault tree is used to express the system failure in terms of combinations of necessary basic events**

# General Characteristics of FTs



Logically relates output event

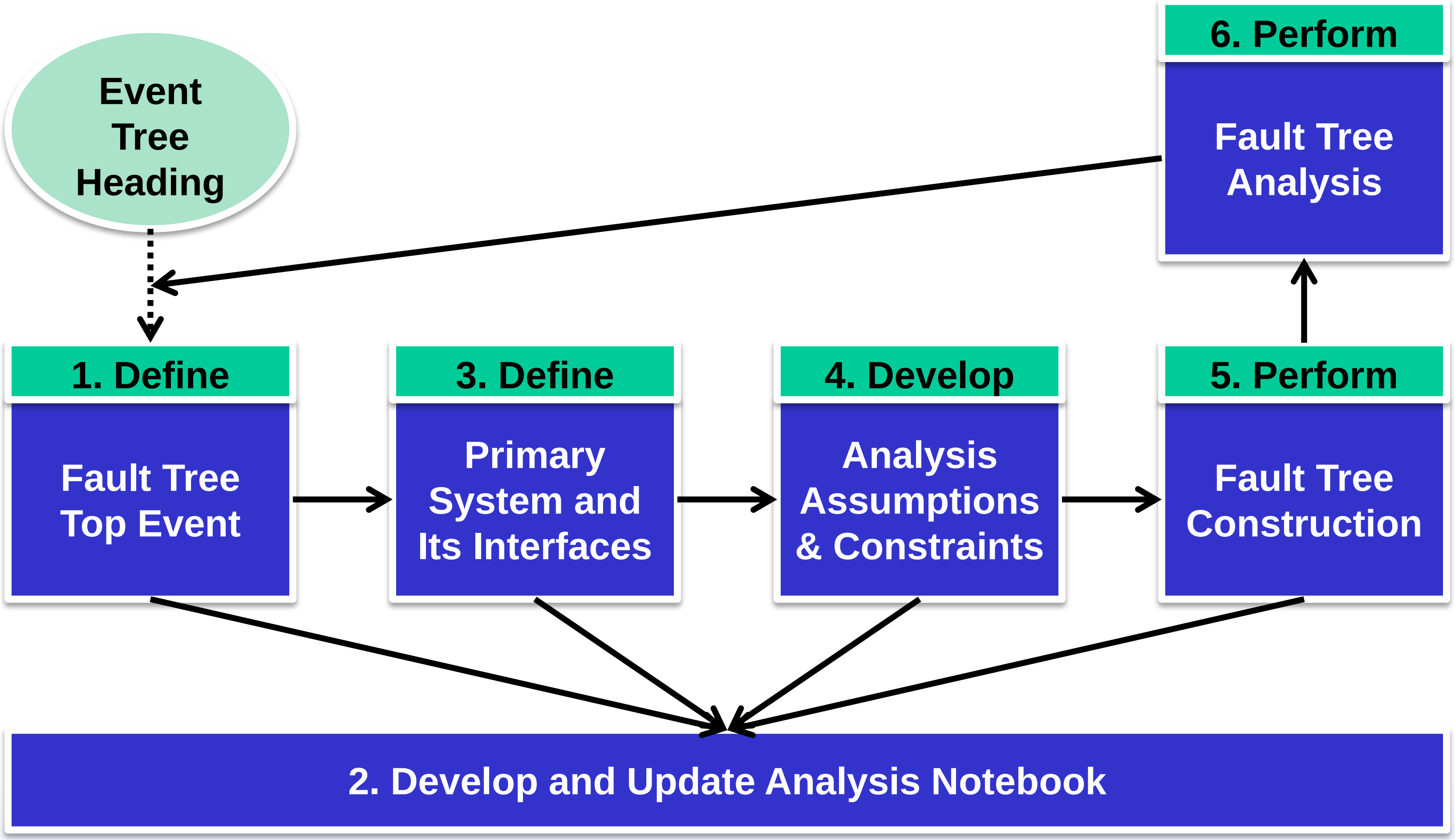
to input events

**LOGIC**
**AND or OR**

**AND Gate occurs if**
**all its inputs occur**

**OR Gate occurs if**
**any one of its inputs occur**

# Fault Tree Development and Analysis Process



# 1. Define Top Event

- Undesired event or state of system
  - Often corresponds to a top event on an event tree
  - Based on success criterion for system
    - Typically initiating-event-dependent (e.g., HPI would have different success criteria for small LOCA vs. medium LOCA)
    - Success criteria determined from thermal/hydraulic calculations
      - E.g., computer code runs made to determine how much injection is needed to keep core covered given particular IE
  - Success criterion used to determine failure criterion
    - Fault tree top event
  - Will often have multiple versions of system failure fault tree
    - For different sequences of an event tree or for different IEs

# 2. Develop & Maintain Analysis Notebook

- Scope of analysis and system definition
- Notebook should include;
  - system design and operation information
  - technical specifications
  - test and maintenance data
  - pertinent analytical assumptions
- Notebook reflects the iterative nature of fault tree analysis.

# 3. Define Primary System & Interfaces

- “A collection of discrete elements which interact to perform, in total or in part, a function or set of functions”
- System boundary definition depends on:
  - information required from analysis
  - the basic event level (i.e., the level of resolution of available data)
  - function of the system being modeled
- Identify shared components with other systems.
- Clear documentation of system boundary definition is essential

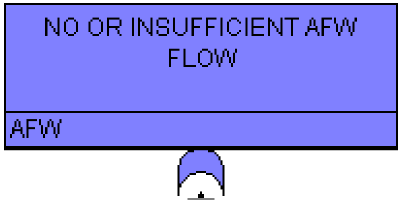
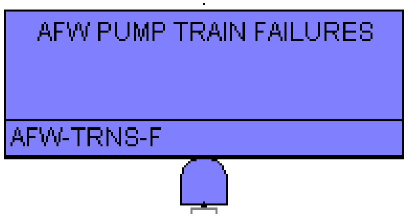
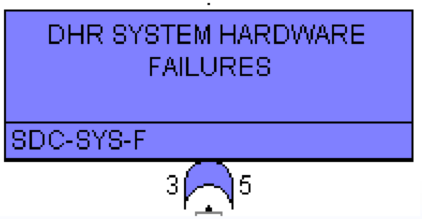
# 4. Develop Analysis Assumptions & Constraints

- Analytical assumptions must be developed to compensate for incomplete knowledge of:
  - Plant response
  - System response and operation
  - Failure modes and mechanisms, and
  - Potential recovery actions
- Rationale for assumptions should be specified and, wherever possible, supported by engineering analysis
- Time and/or budget constraints, as well as the tools available for performing the analysis, can often contribute to defining the scope of the analysis.

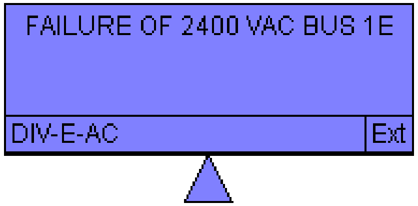
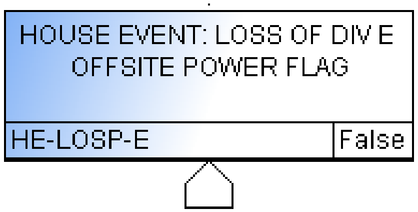
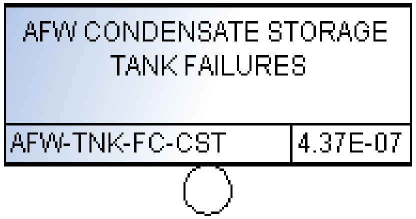
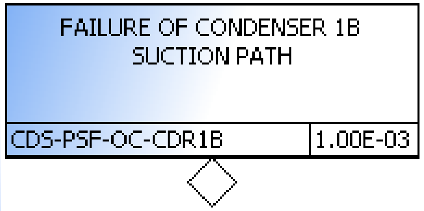
# 5. Fault Tree Construction

- Fault tree construction requires the step-by-step postulation of system faults, starting at the top event and working down to the basic events whose failures contribute to the top event failure.
- Standard symbol to represent the logic
- Postulation consistent with level of resolution of the data and the analytical assumptions.
- Iterative process requiring feedback from other PRA processes and other steps in fault tree development
- Can employ different strategies for construction
  - Output-to-input
  - Functional blocks
  - Resulting fault trees may appear different

# Fault Tree Symbols used during FT Construction

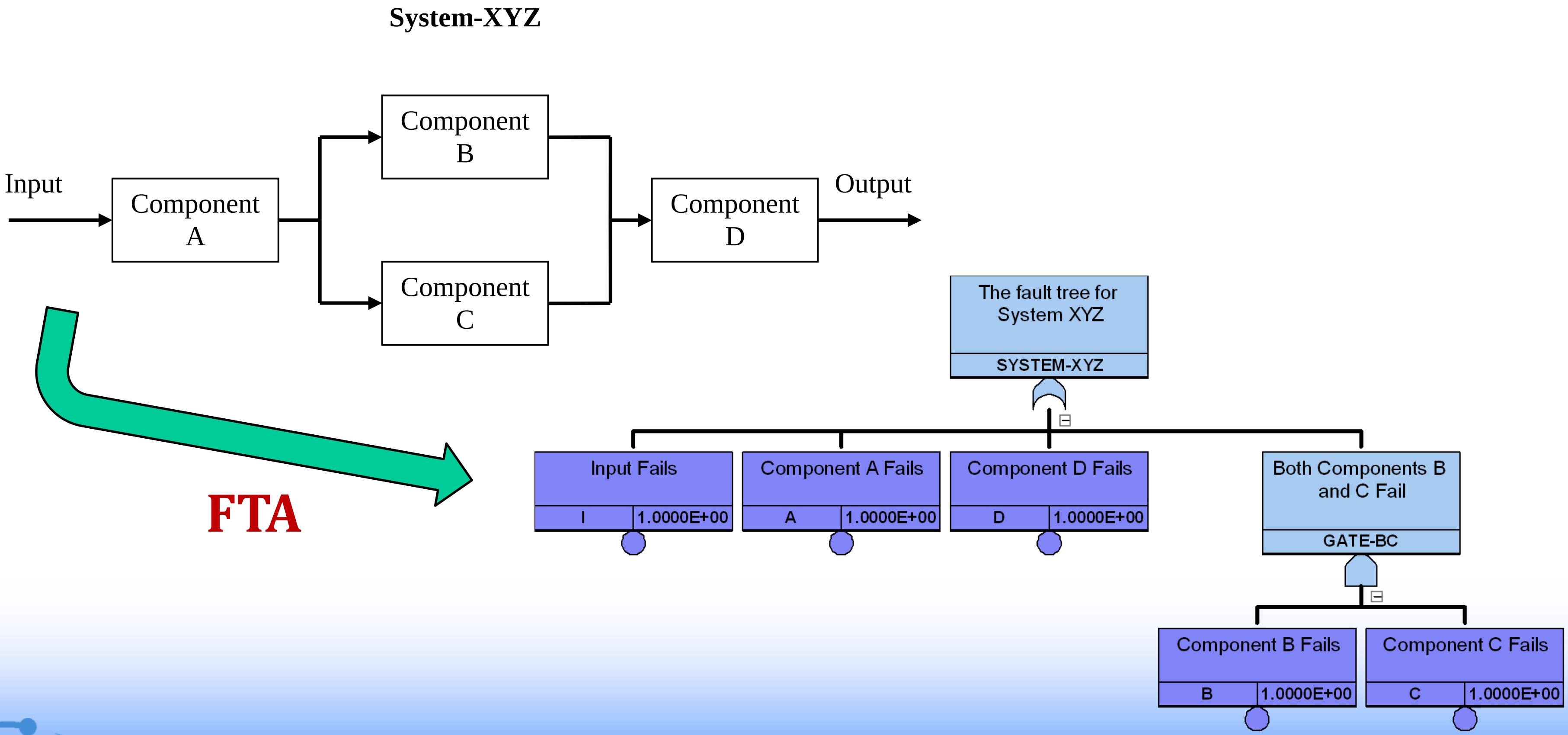
| Symbol | | Description |
|---|---|---|
|  | “OR” Gate | Logic gate providing a representation of the Boolean union of input events. The output will occur if at least one of the inputs occur. |
|  | “AND” Gate | Logic gate providing a representation of the Boolean intersection of input events.  The output will occur if all of the inputs occur. |
|  | N-of-M | Logic gate providing a representation of the Boolean union of input events. The output will occur if at least N of the M number of the inputs occur. |

# Fault Tree Symbols (cont.)

| Symbol | | Description |
|---|---|---|
|  | Transfer Gate | A transfer symbol to connect various parts of the fault tree |
|  HOUSE EVENT: LOSS OF DIV E OFFSITE POWER FLAG<br>HE-LOSP-E<br>False | House Event | Used as a trigger event for logic structure changes within the fault tree. Used to impose boundary conditions on FT. Used to model changes in plant system status. |
|  AFW CONDENSATE STORAGE TANK FAILURES<br>AFW-TNK-FC-CST<br>4.37E-07 | Basic Event | A basic component fault which requires no further development. Consistent with level of resolution in databases of component faults. |
|  FAILURE OF CONDENSER 1B SUCTION PATH<br>CDS-PSF-OC-CDR1B<br>1.00E-03 | Undeveloped Event | A fault event whose development is limited due to insufficient consequence or lack of additional detailed information |

# Example of FTA

- **FTA works to translate a system into its associated fault tree**



System-XYZ

Input

Component A

Component B

Component C

Component D

Output

FTA

The fault tree for System XYZ

SYSTEM-XYZ

Input Fails

I 1.0000E+00

Component A Fails

A 1.0000E+00

Component D Fails

D 1.0000E+00

Both Components B and C Fail

GATE-BC

Component B Fails

B 1.0000E+00

Component C Fails

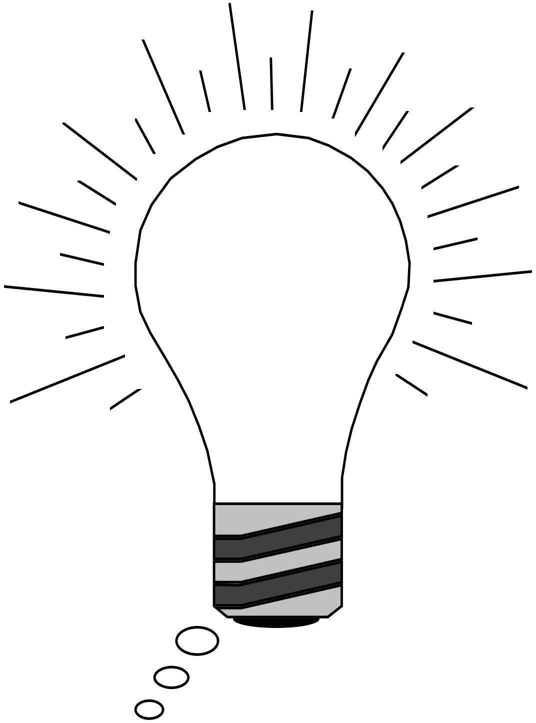
C 1.0000E+00

# 6. Fault Tree Solution

- Due to the complexity of most fault trees, computers are used to generate results.
  - This produces a list of the various combinations of basic event failures that cause the top event to occur.
- Fault tree results – the list of various combinations are called Minimal Cut Sets.
- Solution relies on rules of Boolean algebra.
- Because typical models are very large, solution most often approximated by performing minimal cut set truncation.
  - Truncation typically based upon frequency (or probability) value → solve down to a user-defined numerical level

# Minimal Cut Set

A group of basic event failures (component failures and/or human errors) that are ***collectively necessary*** and ***sufficient*** to cause the TOP event to occur.

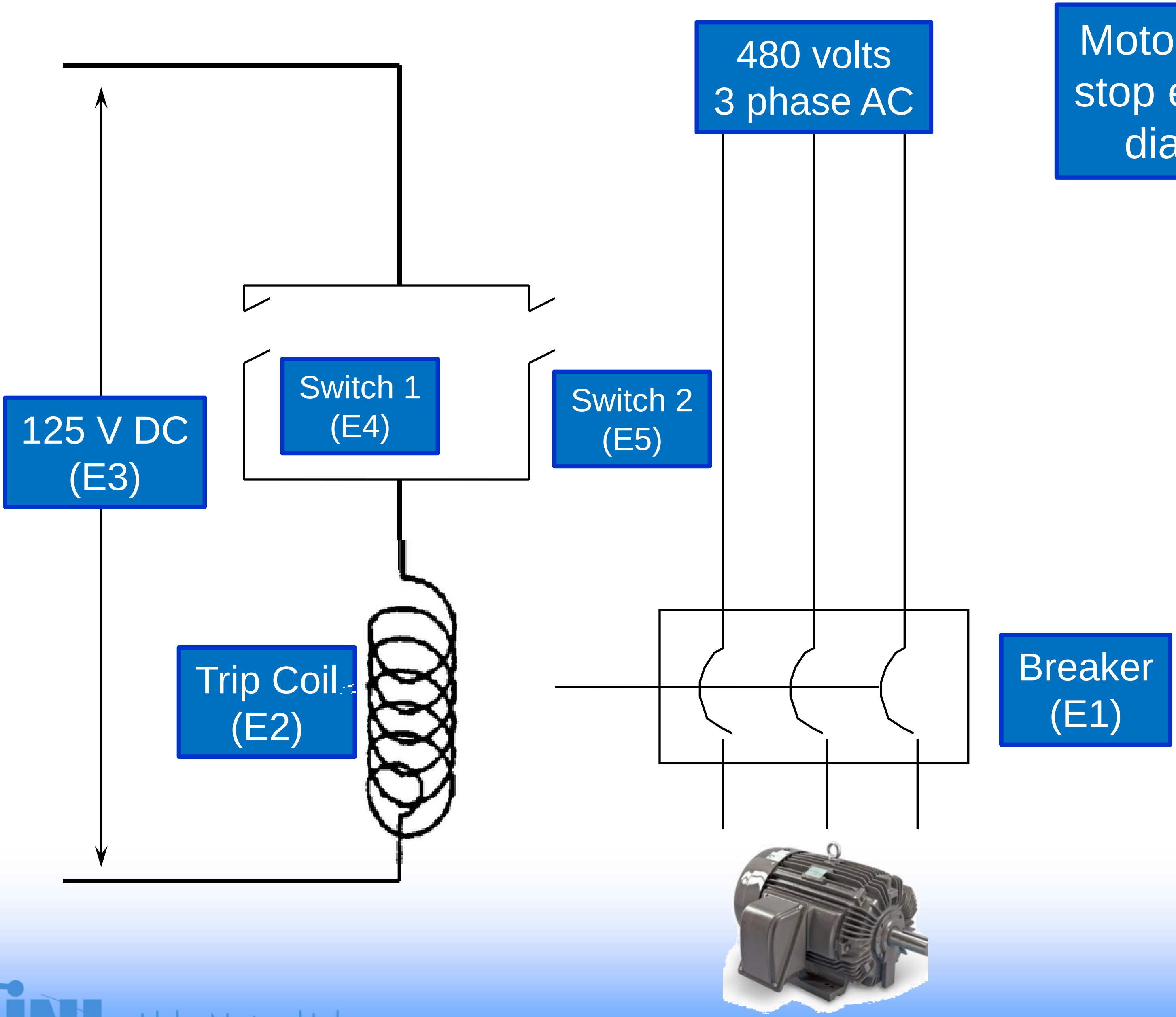


Understanding the concept of minimal cut sets is one of the most important steps in understanding PRA (results)

# Demonstration of the Fault Tree Construction & Solution Process

- **Build fault tree for the schematic provided (next page)**
- **Assumptions:**
  - **Ignore wire faults**
  - **Do not model details of 125V dc power supply**
- **Will solve fault tree and discuss "meaning" of the solution process**

# Motor fails to stop example diagram



480 volts
3 phase AC

125 V DC
(E3)

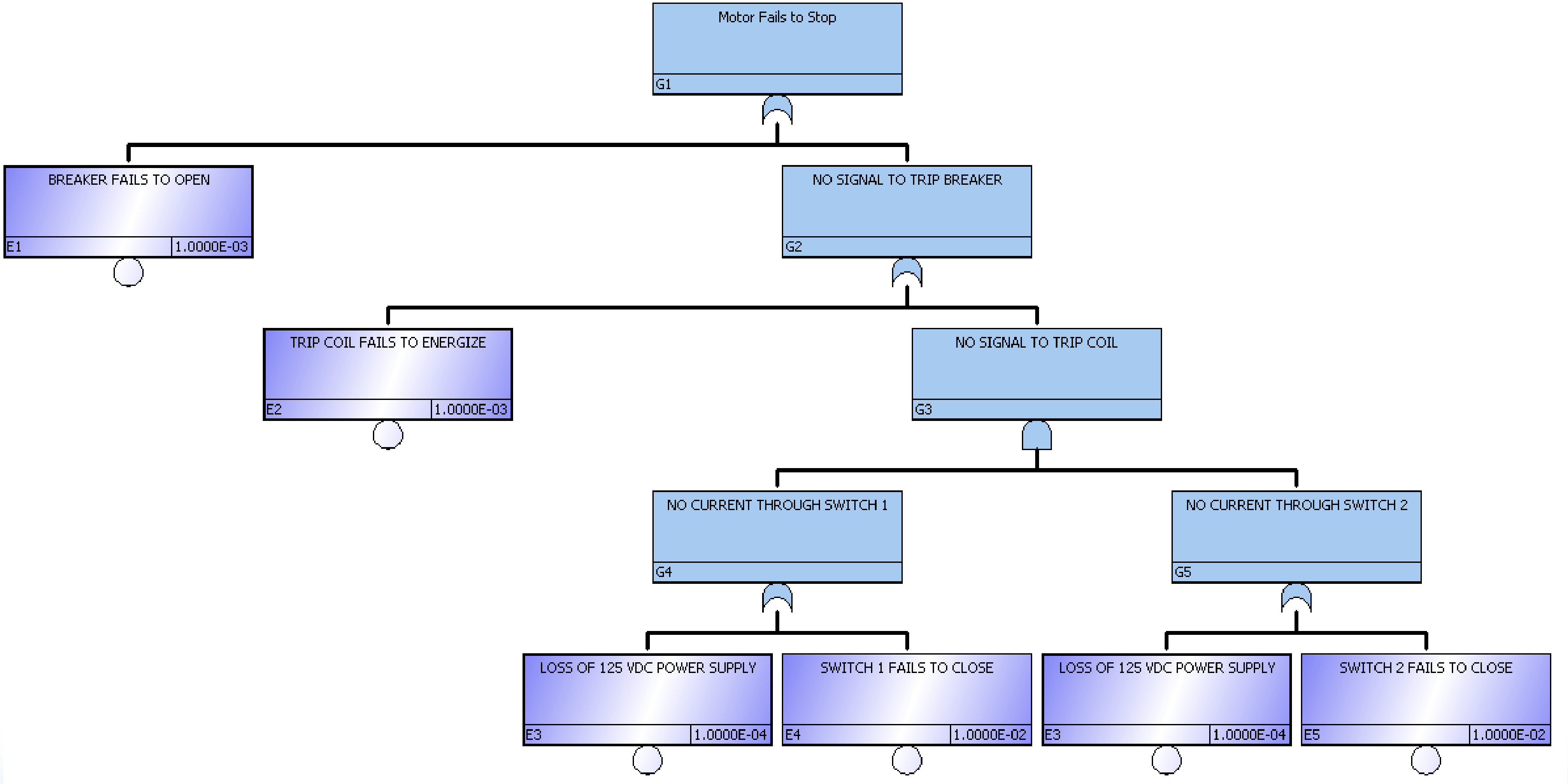
Switch 1
(E4)

Switch 2
(E5)

Trip Coil
(E2)

Breaker
(E1)

# The Corresponding Fault Tree



# Boolean Fault Tree Reduction

1. Express fault tree logic as Boolean equation
2. Apply rules of Boolean algebra to reduce terms
   - This process results in a reduced form of the Boolean equation
     - Minimal cut sets appear in this reduced Boolean equation, separated by OR (+) operator

- Boolean reduction is typically done automatically by the fault tree software during the solving process
  - SAPHIRE is the NRC tool for solving logic models

# Rules of Boolean Algebra

| Mathematical Symbolism | Engineering Symbolism | Designation |
|---|---|---|
| (1a) $X \cap Y = Y \cap X$ | $X * Y = Y * X$ | Commutative Law |
| (1b) $X \cup Y = Y \cup X$ | $X + Y = Y + X$ | |
| (2a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ | $X * (Y * Z) = (X * Y) * Z$ | Associative Law |
| (2b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$ | $X + (Y + Z) = (X + Y) + Z$ | |
| (3a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ | $X * (Y+Z) = (X * Y) + (X * Z)$ | Distributive Law |
| (3b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ | $X + (Y * Z) = (X + Y) * (X + Z)$ | |
| (4a) $X \cap X = X$ | $X * X = X$ | Idempotent Law |
| (4b) $X \cup X = X$ | $X + X = X$ | |
| (5a) $X \cap (X \cup Y) = X$ | $X * (X + Y) = X$ | Law of Absorption |
| (5b) $X \cup (X \cap Y) = X$ | $X + (X * Y) = X$ | |

# Reduction of Example Fault Tree

- **Top down logic equations (+ = “OR”, $*$ = “AND”)**

  **$G1 = E1 + G2$**

  **$G2 = E2 + G3$**

  **$G3 = G4 * G5$**

  **$G4 = E3 + E4$**

  **$G5 = E3 + E5$**

- **Back-substitute**

  **$G3 = (E3 + E4) * (E3 + E5)$**

  **$G2 = E2 + [(E3 + E4) * (E3 + E5)]$**

  **$G1 = E1 + E2 + [(E3 + E4) * (E3 + E5)]$**

# Reduction of Example Fault Tree

- Expand parentheses

  G1 = E2 + E3*E3 + E3*E5 + E4*E3 + E4*E5 + E1

- Reduce terms using rules of Boolean algebra
  - Idempotent Law applies to E3 ∗ E3 = E3

  G1 = E2 + [E3*E3] + E3*E5 + E4*E3 + E4*E5 + E1

  G1 = E2 + [E3] + E3*E5 + E4*E3 + E4*E5 + E1

  Law of Absorption applies to E3 + (E3*“XX") = E3

  G1 = E2 + [E3 + (E3*E5)] + E4*E3 + E4*E5 + E1

  G1 = E2 + [E3] + E4*E3 + E4*E5 + E1

  G1 = E2 + [E3 + (E4*E3)] + E4*E5 + E1

  G1 = E2 + [E3] + E4*E5 + E1

- Reduced equation is list of minimal cut sets, each minimal cut set separated by “+”

  G1 = E1 + E2 + E3 + E4∗E5

- Quantify the minimal cut sets to calculate probability

  Pr(G1) ≈ Pr(E1) + Pr(E2) + Pr(E3) + [Pr(E4) ∗ Pr(E5)]

# Review of Fault Tree Analysis

## Key Points of Section:

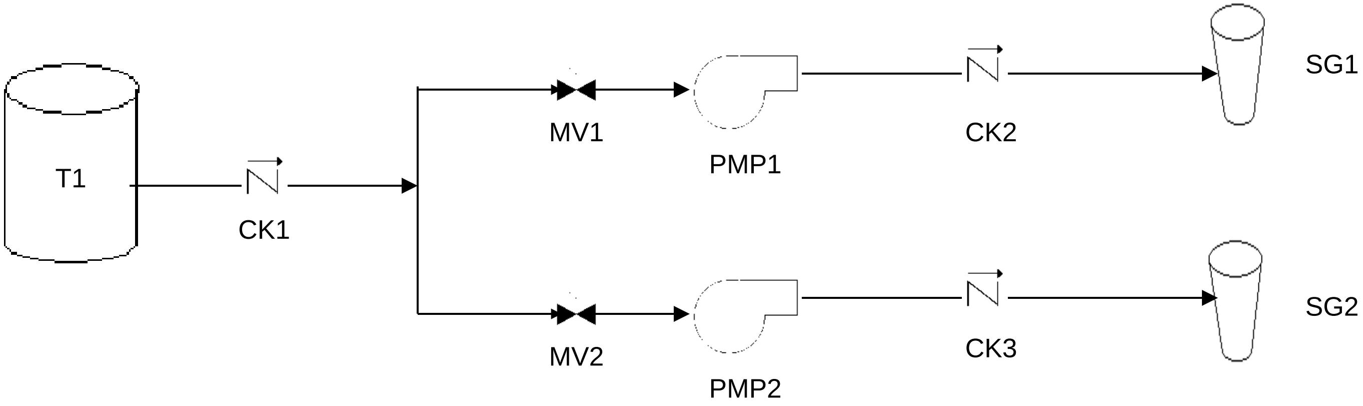
- Fault trees start with an undesired event definition and are used to estimate system unreliability
- Models multiple failures and system interdependencies
- Fault Tree Development Process: 1) Define top event, 2) Develop analysis notebook, 3) Define primary system and interfaces (boundary conditions), 4) Develop analysis assumptions, 5) Construct fault tree using logic symbols.
- Boolean algebra is implemented (by software) for fault tree reduction and produces minimal cut sets

**For more information on event tree and fault tree analysis, see P-200 course**

**For information on SAPHIRE software, see P-201 and P-202 courses**

# Fault Tree Workshop

- Create a fault tree for the simplified Auxiliary Feedwater (AFW) system shown below. AFW system success achieved if there is flow from the tank (T1) to any one of the two steam generators (SG1 or SG2).
- Level of resolution down to the components as listed (i.e., T1, CK1, MV1, PMP1, etc.).
- Generate AFW system minimal cut sets by using Boolean equation to express the fault tree and then reduce by applying Boolean Algebra rules.
- Verify minimal cut sets against AFW system diagram and success criteria.



# WORKSHOP - workspace

# 5. Component Failure Data

# Component Failure Data

- Purpose: Students will be introduced to sources of hardware data and equipment failure modes, including common cause failure, that are modeled in PRAs.
- Objectives: Students will be able to:
  - Understand failure modes typically modeled in PRA and how each failure mode is quantified.
  - Understand what is meant by the terms
    - Generic data
    - Plant-specific data
    - Bayesian updating
  - Describe what is meant by common-cause failure, why it is important, and how it is included in PRA
- References:
  - NUREG/CR-2300, PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants
  - NUREG-1489, (App. C), A Review of NRC Staff Uses of Probabilistic Risk Assessment
  - NUREG/CR-5485, Guidelines on modeling Common-Cause failures in PRA
  - NUREG/CR-5497, Common-Cause Failure Parameter Estimations
  - NUREG/CR-6268, Common-Cause Failure Database and Analysis System: Event Definition and Classification
  - N. Siu and D. Kelly, “Bayesian Parameter Estimation in PRA,” tutorial paper in Reliability Engineering and System Safety 62 (1998) 89-116.

# Component Failure Type Dictates the Basic Event Model

- **Demand based (binomial)**
  - **Normally in standby**
  - **Required to perform one (or more) times**
    - **E.g., actuation systems, relief valves, state change of component**
- **Time based (Poisson)**
  - **Either in standby or normally operating**
  - **Required to operate for some length of time, which affects unreliability**
    - **E.g., power system coolant flow, thermal control**

# Definition of Terms

- Q = Failure probability (unreliability or unavailability)
- p = Demand failure probability
- $\lambda_s$ = Failure rate (per hour) standby
- $\lambda_h$ = Failure rate (per hour) operating
- $t_m$ = mission time
- $t_i$ = surveillance test interval
- $\lambda_m$ = maintenance frequency
- $d_m$ = maintenance duration
- $t_{OOS}$ = total time out of service
- $t_{total}$ = total time

# Component Failure Modes

- **Demand failure**
  - $Q_d = p$
  - Need number of failures and valid demands to estimate p (p = # of failures/total # of demands)
- **Mission time failure (failure to run)**
  - $Q_r = 1 – e^{-\lambda_h t_m}$
  - $Q_r \approx \lambda_h t_m$ (for small $\lambda t$; when $\lambda_h t_m < 0.1$)
  - Need number of failures and run time to estimate $\lambda_h$ ($\lambda_h$ = # of failures/total run hours)
- **Test and maintenance unavailability**
  - $Q_m = \lambda_m d_m = t_{OOS}/t_{total}$
  - Need either
    - Maintenance frequency ($\lambda_m$) and duration ($d_m$)
    - Out-of-Service (OOS) time ($t_{OOS}$) and total time ($t_{total}$)
- **Standby failure (alternative to demand failure model)**
  - $Q_s \approx \lambda_s t_i/2$
  - Need number of failures and time in standby to estimate $\lambda_s$ ($\lambda_s$ = # of failures/total time in standby)

# Data Sources for Parameter Estimation

- **Generic data**
- **Plant-specific data**
- **Bayesian updated data**
  - **Prior distribution**
  - **Updated estimate**

# Typical Generic Data Sources

- **Older data sources**
  - **WASH-1400 (pre-1975)**
  - **NUREG-1150 supporting documents (NUREG/CR-4550 series, pre-1987)**
  - **IEEE Standard 500 (1990)**
  - **NUREG/CR-3862 for initiating events (pre-1986)**
  - **NUREG/CR-5750 for initiating events (1987-1995)**
  - **NUREG-1032 for loss of offsite power(pre-1988)**
  - **NUREG/CR-5496 loss of offsite power (1980-1996)**
  - **NUREG/CR-6890 loss of offsite power (1986-2004)**
- **New data sources**
  - **NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, February 2007**
  - **Main data sources kept at**

    **NRCOE.INEL.GOV**

# Typical Generic Data Sources

- **SECY 04-0060 Loss-of-Coolant Accident Break Frequencies for the Option III Risk-Informed Reevaluation of 10 CFR 50.46, Appendix K to 10 CFR Part 50, and General Design Criteria (GDC) 35 (April 2004)**
- **NUREG-1829 Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process (June 2005)**
- **Institute of Nuclear Power Operations Nuclear Plant Reliability Data System (NPRDS) – archival only (no longer maintained)**
- **Institute of Nuclear Power Operations Equipment Performance Information Exchange (EPIX) – replaced NPRDS**

# Plant-Specific Data Sources

- Licensee Event Reports (LERs)
  - Can also be source of generic data
- Maintenance reports and work orders
- System engineer files
- Control room logs

# Plant-Specific Data Issues

- Combining data from different sources can result in:
  - Double counting of the same failure events
  - Inconsistent component boundaries
  - Inconsistent definition of “failure”
- Plant-specific data is sometimes limited
  - Small statistical sample size leads to large uncertainty in estimate
- Inaccuracy and non-uniformity of reporting
  - LER reporting rule changes
- Difficulty in interpreting “raw” failure data
  - Administratively declared inoperable, does not necessarily equate to a “PRA” failure
- Completeness and uncertainty issues with the data base

# Bayes' Theorem is Basis for Bayesian Updating of Data

- Typical use: sparse plant-specific data combined with generic data using Bayes' Theorem:

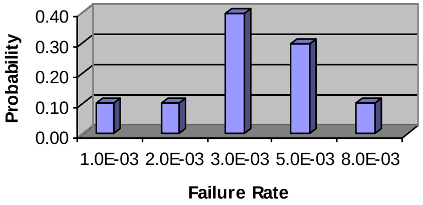
This goes into the PRA basic event

$$\boxed{\pi_1(\theta | E)} = \frac{L(E | \theta)\pi_0(\theta)}{\int L(E | \theta)\pi_0(\theta)\, d\theta}$$

- Where:
  - $\theta$ is parameter of interest
  - $\pi_o(\theta)$ is prior distribution (generic data)
  - $L(E|\theta)$ is likelihood function (plant-specific data)
    - "E" is evidence (observations)
  - $\pi_1(\theta|E)$ is posterior distribution (updated estimate)

# Bayesian Updating

$$\pi_0(\lambda)$$



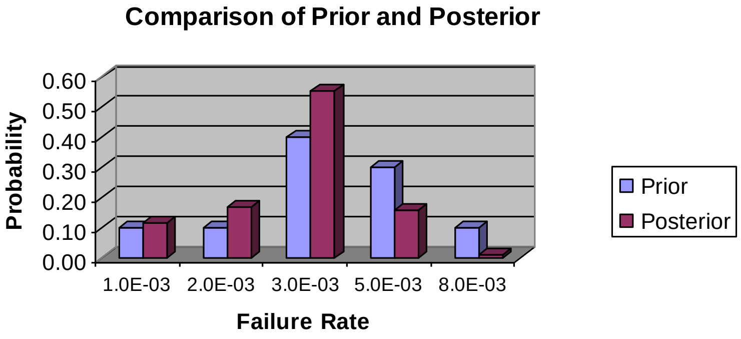
$$L(E|\lambda) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

**Model: Poisson**
**Evidence: K failures in t hours of operation**
**K=2; t=1000 hours**

Our prior knowledge about the failure rate

$$\pi_1(\lambda|E) = \frac{\pi_0(\lambda)\bullet L(E|\lambda)}{k}$$

Our model and observed data (evidence E)

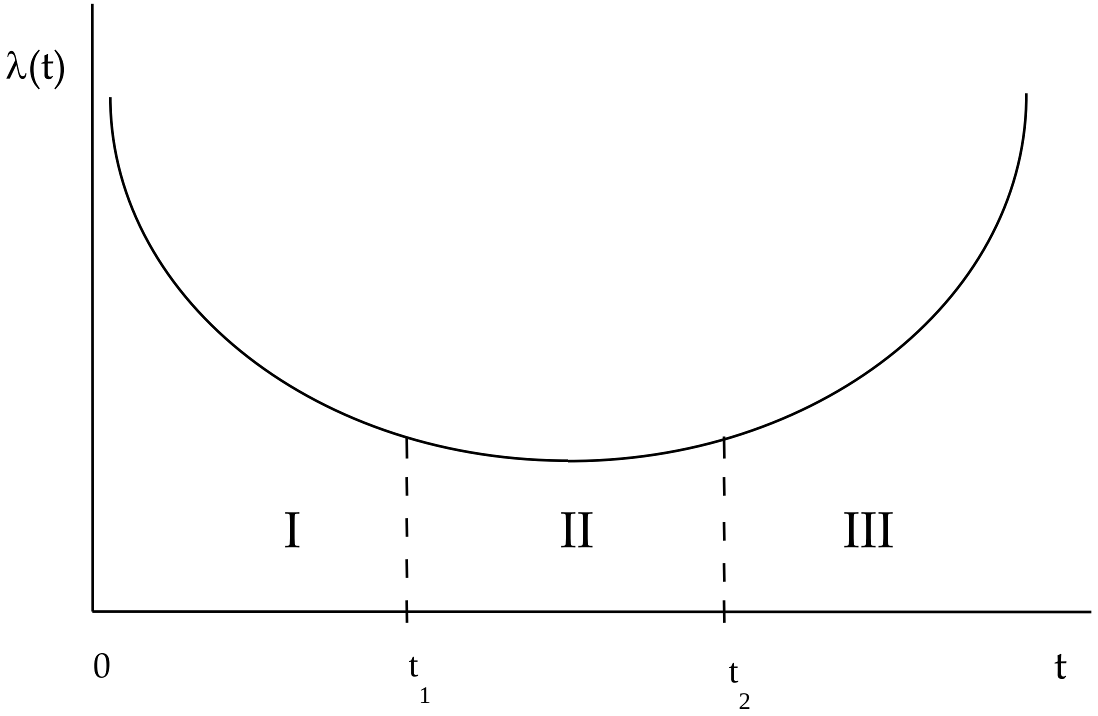


Use Bayes' Theorem to combine our prior knowledge and our evidence

# Component Data Not Truly Time Independent

- PRAs typically assume time-independence of component failure rates
  - One of the assumptions for a Poisson process (i.e., failures in time)
- However, experience has shown failure rates can change with time
  - Improved maintenance can cause $\lambda$ or p to decrease over time
  - Aging can cause $\lambda$ or p to increase
  - These ideas lead to the concept of the “Bathtub” curve representing changes in a failure rate over time

# The “Bathtub” Curve



| | |
|---|---|
| I: | Burn-in (Infant Mortality) |
| II: | Maturity (Useful Life) |
| III: | Wear-out (Aging) |

# The “Bathtub” Curve

- Most PRAs assume failure rates are a constant in “flat” portion of bathtub curve
  - May not be all that bad of an assumption considering
    - Quality level of equipment
    - Extensive maintenance performed
    - Testing requirements imposed
  - However, this assumption does imply that aging (increasing failure rate) may not be modeled in the PRA
    - Models for aging are available, but not typically used

# Definition of Dependent Failures

- Three general types of dependent failures:
  1. Certain initiating events (e.g., fires, floods, earthquakes, service water loss)
  2. Inter-system dependencies including:
     - Functional dependencies (e.g., dependence on AC power)
     - Shared-equipment dependencies (e.g., HPCI and RCIC share common suction valve from CST)
     - Human interaction dependencies (e.g., maintenance error that disables separate systems such as leaving a manual valve closed in the common suction header from the RWST to multiple ECCS system trains)
  3. Inter-component dependencies (e.g., design defect exists in multiple similar valves)
- The first two types are captured by event tree and fault tree modeling; the third type is known as common cause failure (CCF)
  - Represents complex dependencies not explicitly modeled
  - Quantified with parametric CCF models

# Common Cause Failures (CCF)

- **Conditions which may result in failure of more than one component, subsystem, or system**
- **Concerns:**
  - **Defeats redundancy and/or diversity**
  - **Data suggest high probability of occurrence relative to multiple independent failures**
- **CCF Mechanisms**
  - **Environment**
    - **Radioactivity**
    - **Temperature**
    - **Corrosive environment**
  - **Design deficiency**
  - **Manufacturing error**
  - **Test or Maintenance error**
  - **Operational error**

# CCF Modeling in PRA

- Three parametric models used
  - Beta factor (original CCF model)
  - Multiple Greek Letter (MGL) model (expanded on beta-factor)
  - Alpha factor model (addressed uncertainty concerns in MGL)
    - Used in NRC SPAR models
- Apply to components containing same failure mode within the same system and perform the same operation
  - Diesel generators
  - Valves
    - MOVs, AOVs, PORVs, SRVs
  - Pump
  - Batteries

# CCF Modeling in PRA

| Model | Parameters | General Form for Multiple Component Failure |
|---|---|---|
| Beta Factor | $Q_t$, β<br>where:<br>• $Q_t$ is the total probability of each component failing due to all independent and common cause events.<br>• β is a constant fraction of the component failure probability that can be associated with common cause events shared by other components in a common cause component group. | $Q_{k}^{(m)} = \begin{cases} (1-\beta)Q_t, & k=1 \\ 0, & m>k>1 \\ \beta Q_t, & k=m \end{cases}$ |
| Multiple Greek Letters (MGL) | $Q_t$, β, γ, …<br>where:<br>• $Q_t$ is the total probability of each component failing due to all independent and common cause events.<br>• β is the conditional probability that the cause of a component failure will be shared by one or more additional components, given that a specific component has failed.<br>• γ is the conditional probability that the cause of a component failure that is shared by one or more components will be shared by two or more components, given that two specific components have failed. | $Q_{k}^{(m)} = \frac{1}{\binom{m-1}{k-1}} \prod_{i=1}^{k} \rho_i (1-\rho_{k-1}) Q_t$<br>$\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \ldots, \rho_{m+1} = 0$ |
| Alpha Factor | $Q_t$, $\alpha_1$, $\alpha_2$, $\alpha_3$, …, $\alpha_m$<br>where:<br>• $Q_t$ is the total probability of each component failing due to all independent and common cause events.<br>• $\alpha_k$ is the probability that when a common cause basic event occurs in a common cause group of size m, it involves the failure of k components.. | Non-staggered testing (all components tested simultaneously):<br>$Q_{k}^{(m)} = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \qquad k = 1, \ldots, m$<br>Staggered testing (components tested sequentially):<br>$Q_{k}^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t \qquad k = 1, \ldots, m$<br>where:<br>$\alpha_t = \sum_{k=1}^{m} k\, \alpha_k$<br>$\binom{m-1}{k-1} = \frac{(m-1)!}{(m-k)!\,(k-1)!}$ |

# Beta Factor Example

- **Basic events for example (HPI-MDP-FS-A, HPI-MDP-FS-B)**

  **Data - 47 failures to start in approximately 15,667 demands**

  **(47 failures)/(15,667 demands) ≈ 3.0E-3**

- **Common Cause Failure (Beta Factor)**

  **10 common cause failures out of the 47 total failures**

$$\beta \approx \frac{\text{Number of common cause failures}}{\text{Total number of failures}}$$

$$\beta \approx \frac{\text{10 CCF failures}}{\text{47 total failures}} \approx \text{2.1E-1}$$

**HPI-MDP-CCF-CCFAB ≈ (2.1E-1*3.0E-3) = 6.3E-4**

- **Total fails to start for the redundant system**

  **HPI-MDP-FS-A * HPI-MDP-FS-B + HPI-MDP-CF-CCFAB**

  **(3.0E-3)*(3.0E-3) + 6.3E-4 ≈ 6.39E-4**

# Review Component Failure Data

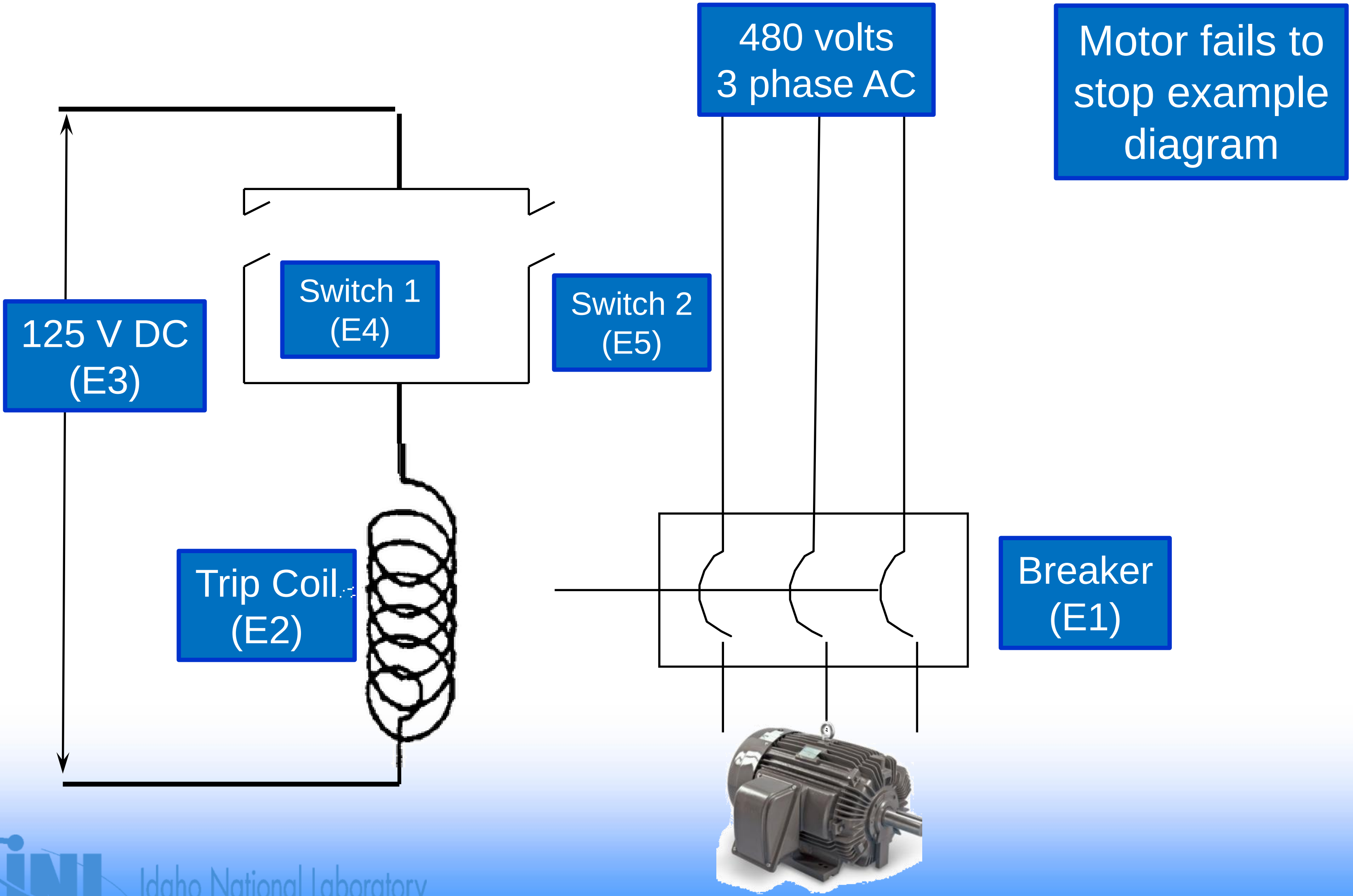
**Key Points of Section:**

- Failure modes
  - Demand failure (fail to start, fail to open, etc.)
  - Mission time failure (fail to run, fail to remain open, etc.)
  - Test & maintenance
  - Standby failure
- Data sources for PRAs include: Generic data, plant-specific data, and Bayesian updating
- Dependent failures are those failures that depend on something to instigate the failure (i.e. time, temperature, human interaction, etc.) This dependent nature may result in multiple component failures called Common Cause Failures
- Common Cause Failures defeat redundancy and/or diversity

**For more information on Parameter estimation and Bayesian analysis, see P-102 course**

**For more information on common cause failure modeling and parameter estimation, see P-200 and P-302 courses**

# CCF Workshop - Question 1 of 2



480 volts
3 phase AC

Motor fails to stop example diagram

125 V DC
(E3)

Switch 1
(E4)

Switch 2
(E5)

Trip Coil
(E2)

Breaker
(E1)

# CCF Workshop - Question 1 of 2 (cont.)

- **Using the Motor Fails to Stop diagram, minimal cut sets, and probability values listed below;**

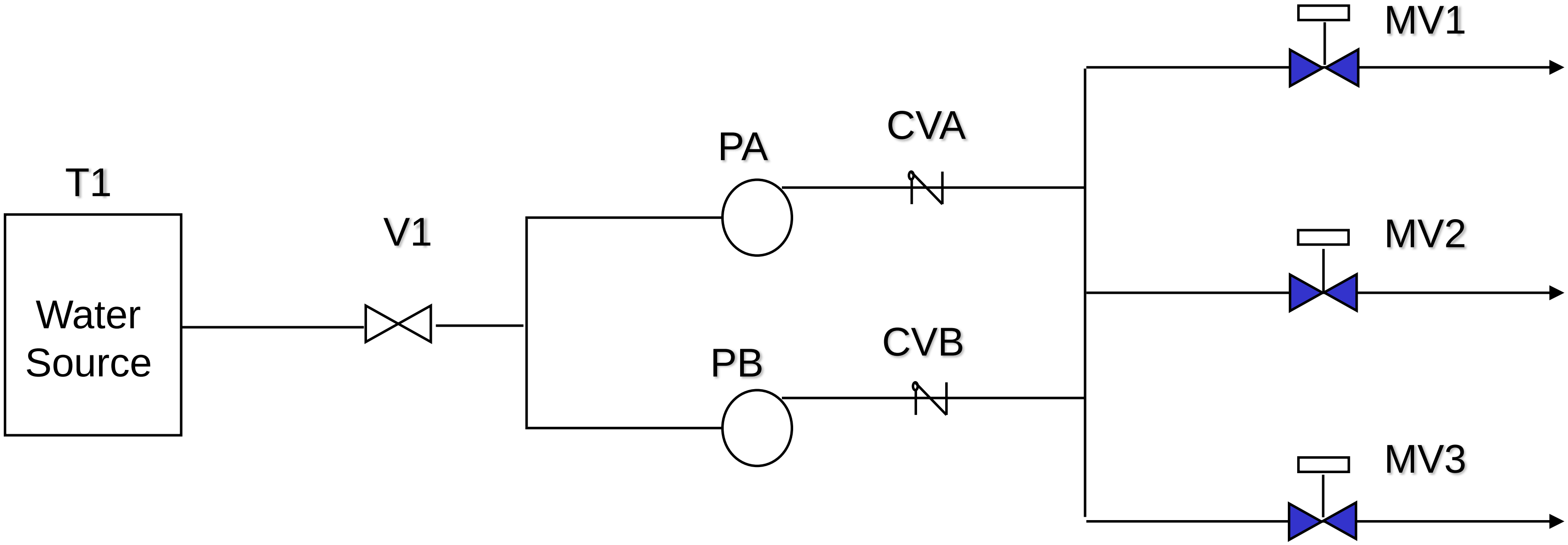
  **G1 = E1 + E2 + E3 + E4∗E5**

  **Basic Event Values:**

  **E1 = Breaker fail to open = 1E-3**
  **E2 = Trip coil fails to energize = 1E-3**
  **E3 = 125 VDC power supply fails = 1E-4**
  **E4 = E5 = Switch fails to close = 1E-2**

  - **Calculate the probability that the Motor Fails to Stop [assuming no CCF event(s)]**
  - **What CCF event(s) should be considered?**
  - **What would each CCF event value be assuming any β = 0.1?**
  - **Calculate the probability that the Motor Fails to Stop taking into consideration CCF contribution**

# CCF Workshop - Question 2 of 2



*Emergency Coolant Injection (ECI) System: ECI system success if there is flow from the tank through any one pump train through any one motor-operated valve. ECI system components include;*

*T# - tank*
*V# - manual valve, normally open*
*P# - pump*
*CV# - check valve*
*MV# - motor-operated valve, normally closed*

# CCF Workshop - Question 2 of 2 (cont.)

- Using the ECI system diagram, minimal cut sets, and probability values listed below;

  *ECI-System-Failure = T1 + V1 + PA * PB + PA * CVB + PB * CVA + CVA * CVB + MV1 * MV2 * MV3*

  Basic Event Values:

  T1 = 1E--6
  V1 = 5E-5
  PA = PB = 1E-2
  CVA = CVB = 1E-4
  MV1 = MV2 = MV3 = 3E-3

  – Calculate the probability that the ECI system fails [assuming no CCF event(s)]

  – What CCF event(s) should be considered?

  – What would each CCF event value be assuming any $\beta = 0.1$?

  – Calculate the probability that the ECI system fails taking into consideration CCF contribution

# WORKSHOP – workspace

# 6. Human Reliability Analysis

# Human Reliability Analysis

- Purpose: To expose the student to how human actions are treated in a PRA.
- Objectives - the student will be able to:
  - Explain the role of HRA within the overall context of PRA
  - Describe common error classification schemes used in HRA
  - Describe how human interactions are incorporated into system models
  - Identify strengths and limitations of HRA
- References:
  - The SPAR-H Human Reliability Model (NUREG/CR-6883)
  - NUREG-1792, HRA Good Practices, 2005
  - NUREG-1842, Review of HRA Methods Against Good Practices, 2006
  - NUREG/CR-1278, Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Application (“Swain & Guttman”)
  - Gertman, D.I. and Blackman, Harold S., Human Reliability & Safety Analysis Data Handbook (1994)
  - IEEE Std. 1082-1997

# Human Error Contribution to Risk Can Be Large

- Human error has been shown to be a significant contributor to overall plant risk:
  - Past studies have indicated that operator error may contribute a large percentage of total nuclear plant risk
  - Human errors may have significantly higher probabilities than hardware failures
  - Humans can circumvent the system design (e.g., shutting off safety injection during an accident)

# Human Reliability Analysis (HRA)

- **Starts with the basic premise that the humans are, in effect, part of the system.**
  - **Thus, nuclear power plants and systems which comprise them are "human-machine systems"**
- **Identifies and quantifies the ways in which human actions contribute to the**
  - **Initiation,**
  - **Propagation**
  - **Termination of accident sequences**

# “Human Reliability” is the probability that a person will:

- **Correctly perform some system-required activity, and**
- **Perform no extraneous activity that can degrade the system.**

# Categories Of Human Error

- **Errors can occur throughout the accident sequence**
  - **Pre-initiator errors (latent errors that may occur in or out of the main control room)**
    - **Failure to restore**
    - **Miscalibration**
    - **Sometimes captured in equipment failure data**
  - **As a contribution or cause to initiating events**
    - **Usually implicitly included in data used to quantify initiating event frequencies**

# Categories Of Human Error

- Errors can occur throughout the accident sequence
  - Post-initiator errors
    - Operation of components from the control room or locally
    - Operation of components that have failed to operate automatically
    - “Sequence level” errors modeled in the event trees (e.g., failure to depressurize the RCS in accordance with the EOPs)
    - Recovery actions (consideration of actions that may be taken to recover from a fault depending upon actions required and amount of time available)

# Types Of Human Error

- Generally, two types of human errors are defined:
  - Errors of omission
    - Failure to perform a required action or step, e.g., failure to monitor makeup tank level
  - Errors of commission
    - Action performed incorrectly or wrong action performed, e.g., opening the wrong valve, turning off SI
- Normally only errors of omission and very simple errors of commission (slips) are modeled due to
  - Uncertainty in being able to identify errors of commission
  - Lack of modeling and quantification methods to address such errors

# HRA Process

- Identify Human Failure Events to be considered in plant models:
  - Normal Plant Ops
    - Identify potential errors involving miscalibration or failure to restore equipment by observing test and maintenance
  - Upset Conditions
    - Determine potential errors in manipulating equipment in response to various accident situations
      - Review emergency operating procedures to identify potential human errors
      - List human actions that could affect course of events

# HRA Process

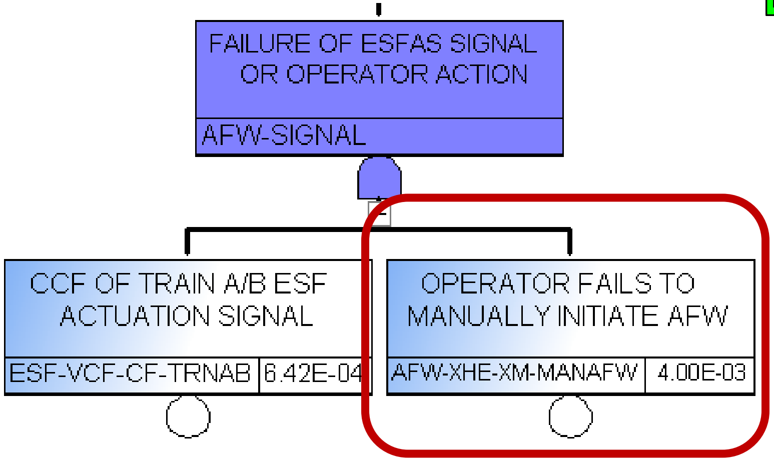
- Perform screening analysis
  - – Uses deliberately conservative estimates of human error probability
    - Solve model and evaluate human failure events that become dominant
    - Screening methods include ASEP
  - – Leaves smaller set of human failure events for more detailed analysis

# HRA Process

- **Detailed analysis of events that survive screening**
  - **Conduct Human Reliability Task Analyses**
    - **Breakdown required actions (tasks) into each of the physical or mental steps to be performed**
    - **Develop and quantify HRA model of event**
      - **Assign nominal human error estimates**
      - **Determine plant-specific adjustments to nominal human error estimates**
      - **Account for dependence between tasks**

# Incorporating HEPs Into a PRA Model:

Basic events on fault trees



FAILURE OF ESFAS SIGNAL OR OPERATOR ACTION

AFW-SIGNAL

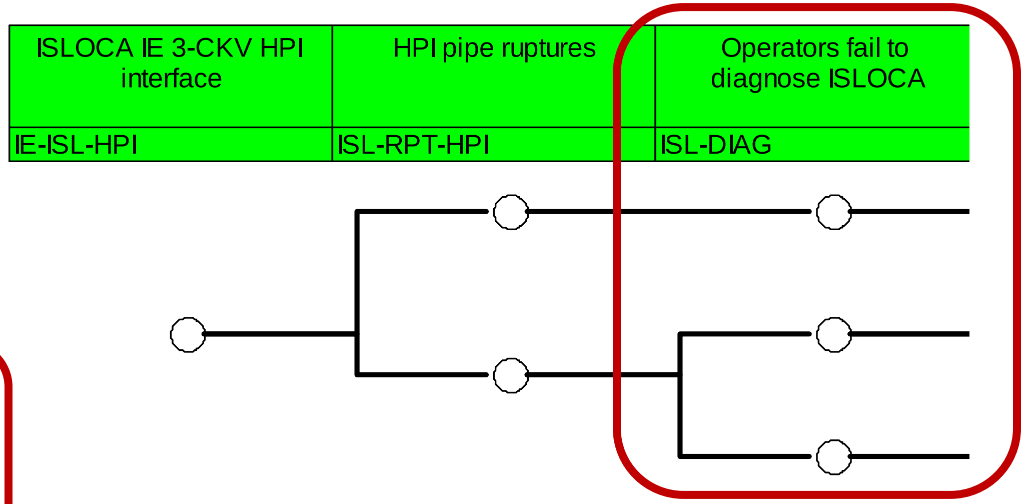
CCF OF TRAIN A/B ESF ACTUATION SIGNAL

ESF-VCF-CF-TRNAB 6.42E-04

OPERATOR FAILS TO MANUALLY INITIATE AFW

AFW-XHE-XM-MANAFW 4.00E-03

Top events on event trees



ISLOCA IE 3-CKV HPI interface

IE-ISL-HPI

HPI pipe ruptures

ISL-RPT-HPI

Operators fail to diagnose ISLOCA

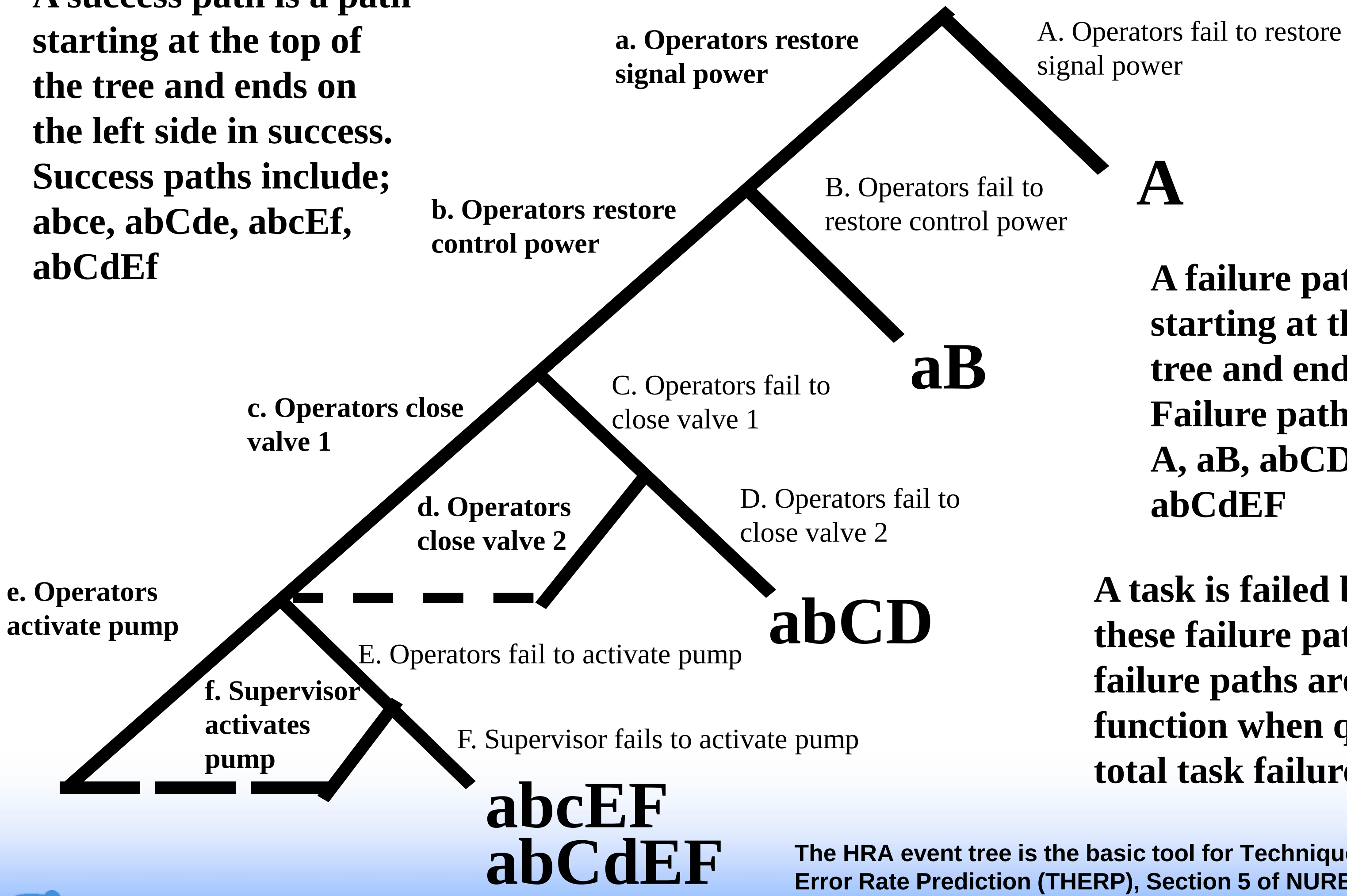
ISL-DIAG

Recovery actions added by applying post-processing rules to minimal cut set

```
If EPS-DGN-FS-A * EPS-DGN-FS-B then
    RECOVERY = OP-DOESNOT-RECOVER-DGNS;
endif
```

# Sample HRA Event Tree

**A success path is a path starting at the top of the tree and ends on the left side in success. Success paths include; abce, abCde, abcEf, abCdEf**



**a. Operators restore signal power**

A. Operators fail to restore signal power

**A**

**b. Operators restore control power**

B. Operators fail to restore control power

**aB**

**c. Operators close valve 1**

C. Operators fail to close valve 1

**d. Operators close valve 2**

D. Operators fail to close valve 2

**abCD**

**e. Operators activate pump**

E. Operators fail to activate pump

**f. Supervisor activates pump**

F. Supervisor fails to activate pump

**abcEF**
**abCdEF**

**A failure path is a path starting at the top of the tree and ends in failure. Failure paths include; A, aB, abCD, abcEF, abCdEF**

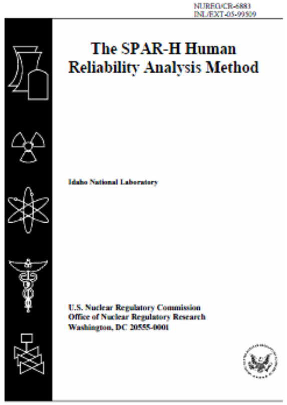
**A task is failed by any of these failure paths. The failure paths are an OR function when quantifying total task failure.**

**The HRA event tree is the basic tool for Technique for Human Error Rate Prediction (THERP), Section 5 of NUREG/CR-1278**

# Performance Shaping Factors (PSFs)

- Are people-, task-, environmental-centered influences which serve to alter nominal error rates
- Most HRA modeling techniques allow the analyst to account for PSFs during their quantification procedure
- PSFs can *Positively* or *Negatively* impact human error probabilities
- PSFs are identified in human reliability task analysis

# SPAR-H (NUREG/CR-6883)



NUREG/CR-6883
INL/EXT-05-99509

The SPAR-H Human Reliability Analysis Method

Idaho National Laboratory

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

- The SPAR HRA, or SPAR-H, method was developed at the INL to support the NRC
- The current Standardized Plant Analysis Risk (SPAR) models evolved from the early NRC PRAs
  - Now exist in full-power models for each nuclear plant
  - Being applied to low power and shut down models
- SPAR-H is a simplified approach based on THERP
  - HEPs in SPAR-H derived from THERP
  - Approach uses performance shaping factors (PSFs) instead of sample scenarios, making it easier to generalize

# SPAR-H Quantification

- **SPAR-H Worksheets are used to quantify HEPs by considering factors that may increase/decrease likelihood of error**
  - **Available time**
  - **Complexity**
  - **Procedures**
  - **Fitness for duty**
  - **Stress/stressors**
  - **Experience/training**
  - **Ergonomics/HMI**
  - **Work processes**

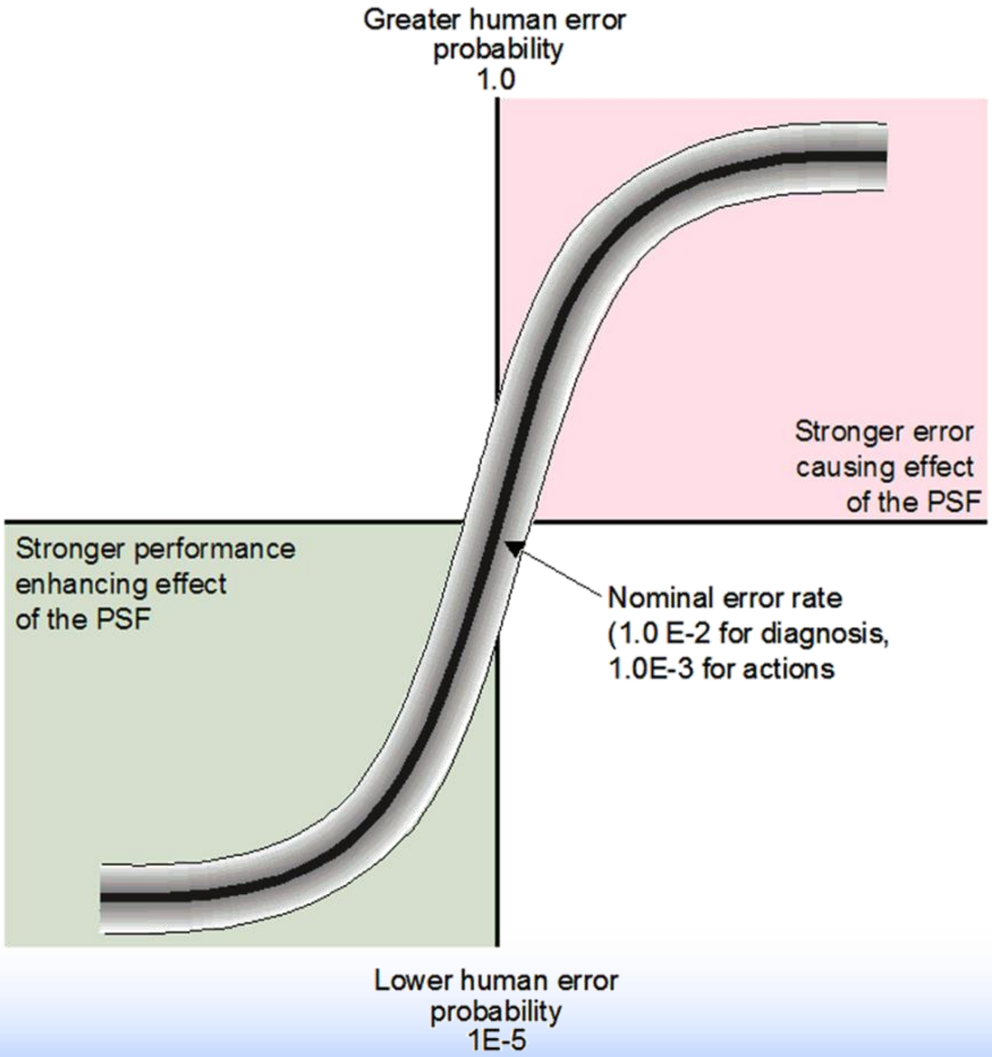
- **In SPAR-H, these influences are specifically called PSFs**

**Example: Available Time**

- ***inadequate time* → *p(failure)* = 1.0**
- ***barely adequate time* → *p(failure)* = HEP x 10**
- ***nominal time* → *p(failure)* = HEP x 1**
- ***extra time* → *p(failure)* = HEP x 0.1**
- ***expansive time* → *p(failure)* = HEP x 0.01**

# PSFs Shown Graphically

- PSFs influence performance, which determines likelihood of human error probability

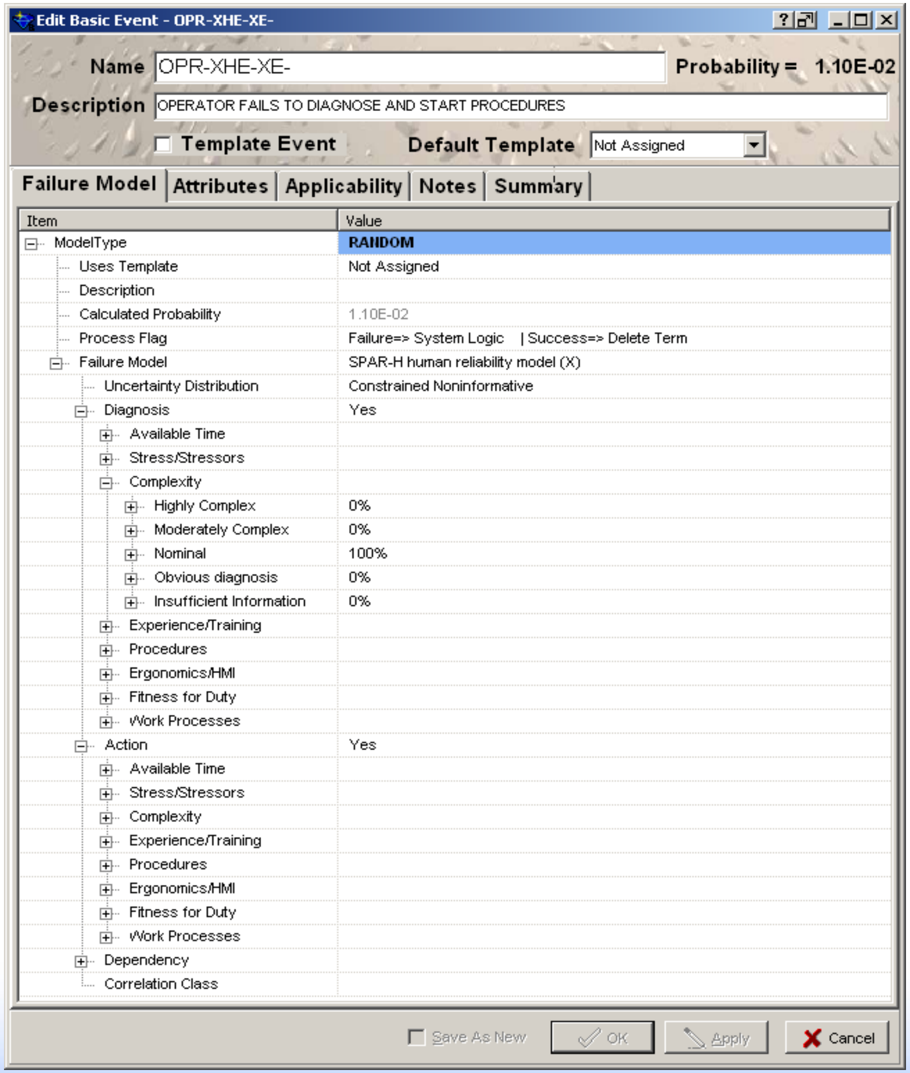

Greater human error probability 1.0
Stronger error causing effect of the PSF
Stronger performance enhancing effect of the PSF
Nominal error rate (1.0 E-2 for diagnosis, 1.0E-3 for actions
Lower human error probability 1E-5

# Typical PSFs Considered in HRA

- Stress
  - Knowledge of consequences of act performed improperly, insufficient time, etc.
- Training
  - How frequent does it cover the task being evaluated
- Skill level
  - What is time in grade (master tech)
- Motivation, morale
  - Untidy facility, lack of procedures, noncompliance, high absenteeism
- Procedures
  - Labels which don’t exist, steps which are incomplete or confusing, placement and clarity of caution statements
- Interface
  - Indicator and control switch design and layout
- Noise
  - Evaluate in terms of Db

# Incorporating Performance Shaping Factors

- **SAPHIRE SPAR-H Human Error Basic Event Example**
  - **Diagnosis:**
    - **Nominal Value 1.0E-2**
  - **Action:**
    - **Nominal Value 1.0E-3**
  - **Influences on the PSFs**
    1. **Available time**
    2. **Stress/stressors**
    3. **Complexity**
    4. **Experience/training**
    5. **Procedures**
    6. **Ergonomics/HMI**
    7. **Fitness for Duty**
    8. **Work processes**
  - **Dependency**



Edit Basic Event - OPR-XHE-XE-

Name: OPR-XHE-XE-   Probability = 1.10E-02

Description: OPERATOR FAILS TO DIAGNOSE AND START PROCEDURES

□ Template Event   Default Template: Not Assigned

| Item | Value |
|---|---|
| ModelType | RANDOM |
| Uses Template | Not Assigned |
| Description | |
| Calculated Probability | 1.10E-02 |
| Process Flag | Failure=> System Logic \| Success=> Delete Term |
| Failure Model | SPAR-H human reliability model (X) |
| Uncertainty Distribution | Constrained Noninformative |
| Diagnosis | Yes |
| Available Time | |
| Stress/Stressors | |
| Complexity | |
| Highly Complex | 0% |
| Moderately Complex | 0% |
| Nominal | 100% |
| Obvious diagnosis | 0% |
| Insufficient Information | 0% |
| Experience/Training | |
| Procedures | |
| Ergonomics/HMI | |
| Fitness for Duty | |
| Work Processes | |
| Action | Yes |
| Available Time | |
| Stress/Stressors | |
| Complexity | |
| Experience/Training | |
| Procedures | |
| Ergonomics/HMI | |
| Fitness for Duty | |
| Work Processes | |
| Dependency | |
| Correlation Class | |

# Sources of HRA Data

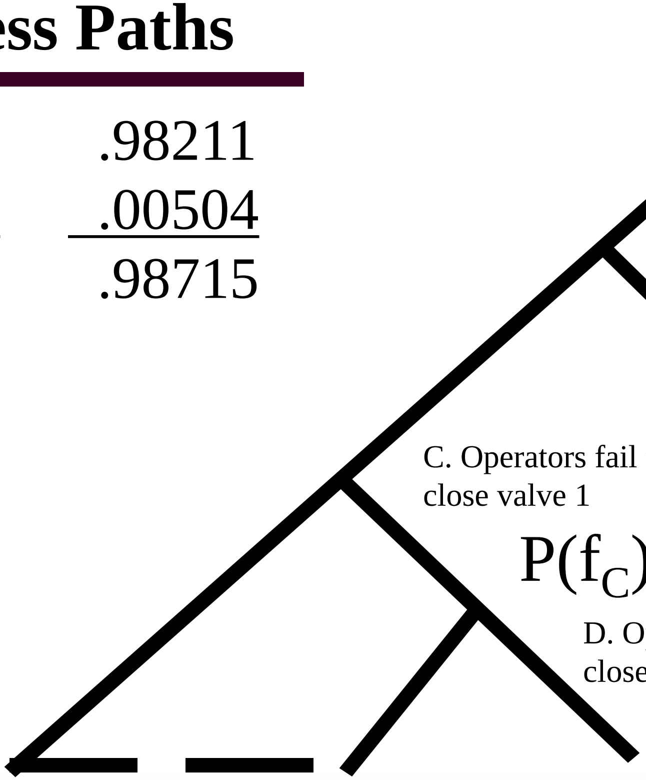
- Nuclear and allied industries
- Military
- Nuclear plant simulators
- Expert elicitation

# HRA Event Tree Quantification

Plug HEP data into the model and calculate paths and total HEP

**Success Paths**

| | |
|---|---|
| abc | .98211 |
| abCd | .00504 |
| Total | .98715 |


A. Operators fail to restore signal power

$P(f_A)=.006$

B. Operators fail to restore control power

$P(f_B)=.006$

C. Operators fail to close valve 1

$P(f_C)=.006$

D. Operators fail to close valve 2

$P(f_D)=.15$

**Failure Paths**

| | |
|---|---|
| A | .006 |
| aB | .00596 |
| abCD | .00089 |
| Total | .01285 |

# HRA Strengths and Limitations

- **Major Strength:**
  - HRA identifies areas where improvements may be made in training, procedures, and equipment to reduce risk
- **Limitations:**
  - Lack of consensus as to which modeling and quantification approach to use (many exist)
  - Lack of data on human performance forces reliance on subjective judgment
  - Skill and knowledge of those performing the HRA
- **These limitations result in a wide variability in human error probability estimates and make human contribution to risk a principal source of uncertainty**

# Review of Human Reliability Analysis

**Key Points of Section:**

- Human error has been shown to be a significant contributor to plant risk, that is why we include it in PRA
- HRA identifies and quantifies the mechanisms where human actions contribute to the initiation, propagation, or termination of an accident sequences.
- Categories of human error:
  - Pre-initiator errors
  - As a contribution or cause to an initiating event
  - Post-initiator errors
- Types of human error:
  - Errors of omission
  - Errors of commission
- HRA process:
  - Identify Human Errors, both Normal plant operations and upset conditions operations
  - Perform screening analysis
  - Conduct human reliability task analysis using performance shaping factors
- HRA strength:
  - Identifies areas where improvements may be made
- HRA limitations:
  - Lack of consensus as to which modeling and quantification approach to use
  - Lack of data on human performance
  - Inadequate skill and knowledge of those performing HRA

**For more information on HRA, see P-203 course and P-406 course for NMSS applications**

# WORKSHOP – Human Error Probability

In this workshop, determine the human error probability for the task of assembling a BBQ for a get together at your place that will begin in 4 hours.  According to the manufacturer, the estimated time to assemble the standard design BBQ (3ft x 2ft lower grill and a 3ft x 1ft upper grill) is 3 hours.  Tests by the manufacture have shown the nominal failure rate for this task is 1 out of 200 people or 5E-3.

Use your own experience and known mechanical skills and other “performance shaping factors” to obtain your new human error probability in not satisfying the success criteria.  Use the HEP worksheet and make any necessary updates to the worksheet to obtain your new personalized HEP result.

Nominal HEP = 5E-3

New HEP = 5E-3 * __ * __ * __ * __ * __ * __ * __ * __ * __ = _____

| Performance Shaping Factor | PSF Level | Multiplier | Notes & Assumptions |
|---|---|---|---|
| Available Time | Inadequate | 2 | |
| | Nominal | 1 | |
| | Extra | 0.1 | |
| Stress | High | 5 | |
| | Nominal | 1 | |
| | Low | 0.1 | |
| Complexity | High | 2 | |
| | Nominal | 1 | |
| | Low | 0.5 | |
| Ergonomics | Poor | 2 | |
| | Nominal | 1 | |
| Fitness for Duty | Unfit | 2 | |
| | Nominal | 1 | |
| | Excellent | 0.5 | |
| Experience/Training | Poor | 2 | |
| | Nominal | 1 | |
| | Excellent | 0.1 | |
| Procedures | Incomplete | 5 | |
| | Nominal | 1 | |
| | Well written, color coded, etc. | 0.1 | |
| Additional Help | Ineffective help | 2 | |
| | Nominal | 1 | |
| | Effective help | 0.1 | |
| Any Other PSFs | | | |

# 7. Sequence Quantification

# Sequence Quantification

- **Purpose: This topic will provide students with an understanding of the quantitative basis of PRA. Elements of accident sequence quantification and importance analysis will be presented.**
- **Objectives: At the conclusion, students will be able to:**
  - **Describe the major processes for accident sequence quantification**
  - **Explain the concepts of importance analysis**
- **References:**
  - **NUREG/CR-2300, *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants***
  - **NUREG-1489, (App. C), A *Review of NRC Staff Uses of Probabilistic Risk Assessment***

# Quantification Inputs

- Initiating events and frequencies
- Event trees to define accident sequences
- Fault trees and Boolean expressions for all systems (front line and support)
- Data (component failures and human errors)

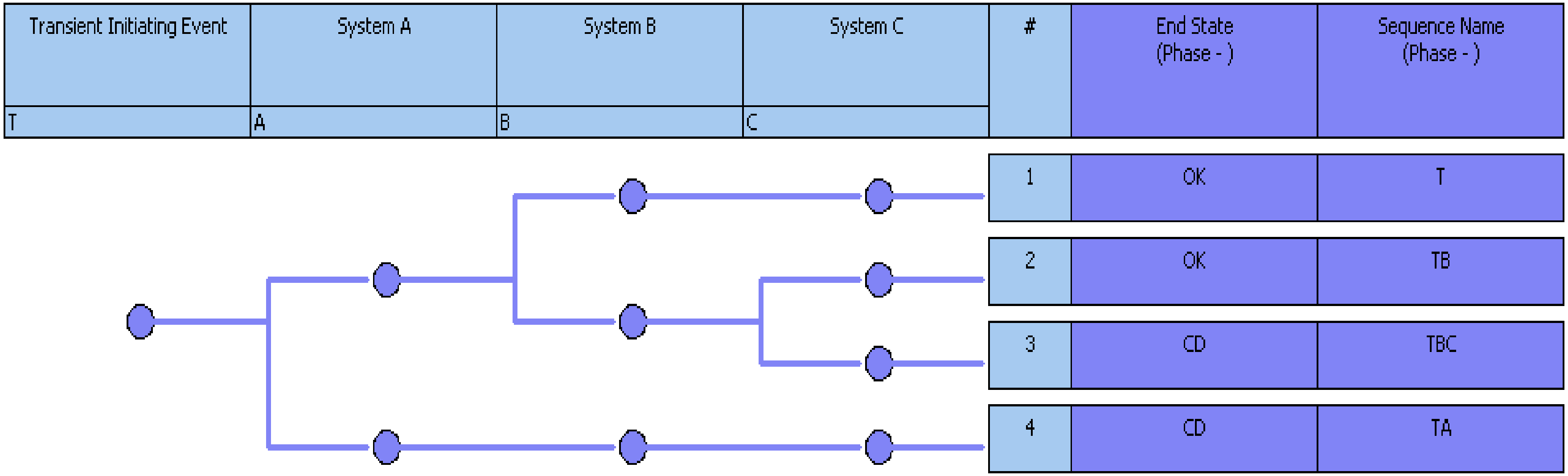
# Parameter Inputs for Sequence Quantification

- Initiating event frequencies
  - $\lambda_{IE}$
- Demand failures
  - $Q_d = p$
- Standby failures
  - $Q_s \approx \lambda_s t_i/2$
- Mission time failures (failure to run)
  - $Q_r \approx \lambda_h t_m$
- Test and maintenance unavailability
  - $Q_m = \lambda_m d_m$
- Common-cause parameters
  - $\beta$
- Human error probabilities (HEPs) from HRA

# Fault-Tree Linking Approach to Accident Sequence Quantification

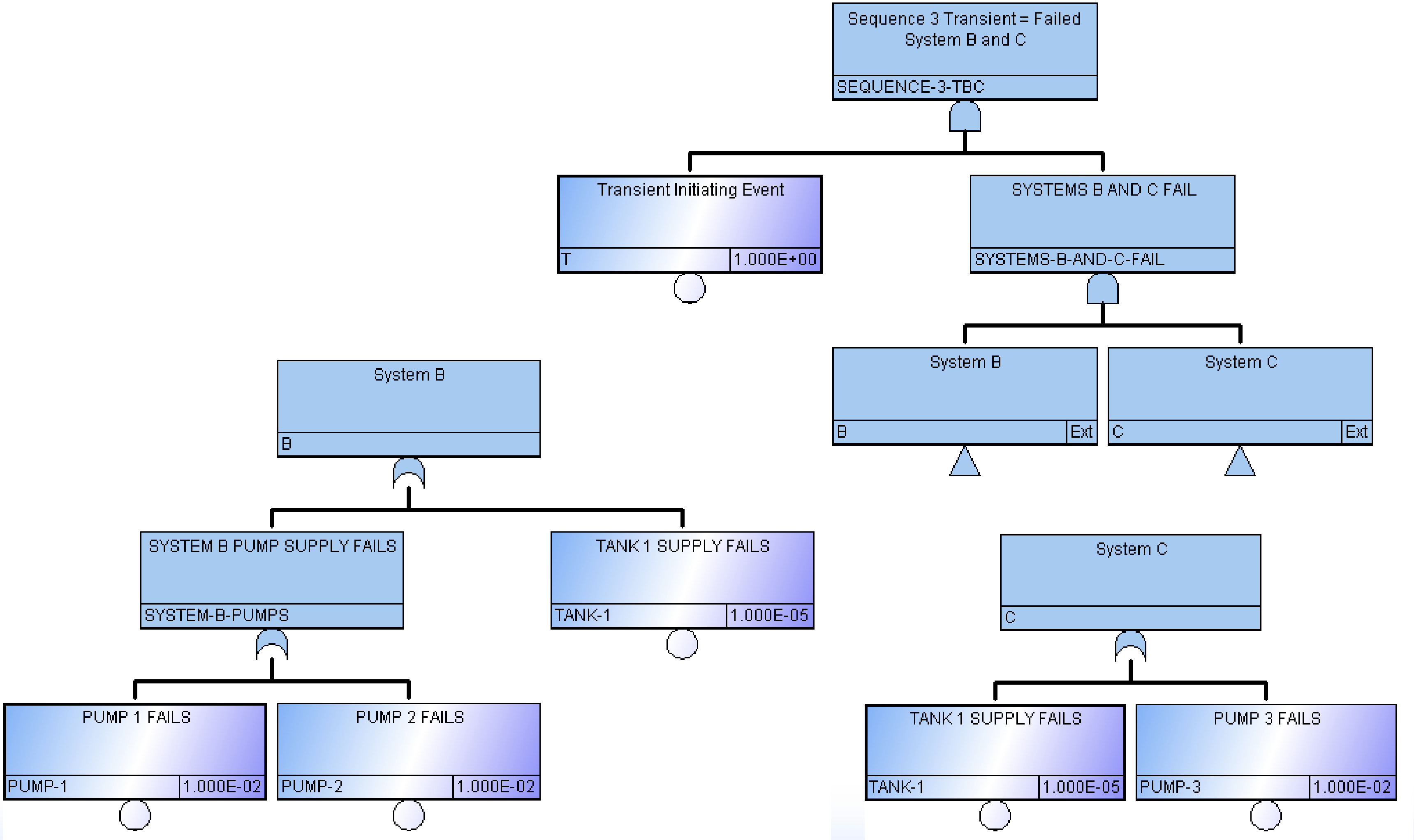
- Link fault tree models on sequence level using event trees
- Evaluate each sequence for minimal cut sets (Boolean reduction)
- Make sure operator recovery actions and common cause failures have been addressed in the event trees, fault trees, or recovery rules applied to minimal cut sets
- Quantify sequence minimal cut sets with data
- Determine dominant accident sequences
- Perform sensitivity, importance, and uncertainty analysis

# Quantification Process – Sequence 3 TBC



| Transient Initiating Event<br>T | System A<br>A | System B<br>B | System C<br>C | # | End State<br>(Phase - ) | Sequence Name<br>(Phase - ) |
|---|---|---|---|---|---|---|
| | | | | 1 | OK | T |
| | | | | 2 | OK | TB |
| | | | | 3 | CD | TBC |
| | | | | 4 | CD | TA |

# Quantification Process



Sequence 3 Transient = Failed System B and C

SEQUENCE-3-TBC

Transient Initiating Event

T 1.000E+00

SYSTEMS B AND C FAIL

SYSTEMS-B-AND-C-FAIL

System B

B Ext

System C

C Ext

System B

B

SYSTEM B PUMP SUPPLY FAILS

SYSTEM-B-PUMPS

TANK 1 SUPPLY FAILS

TANK-1 1.000E-05

PUMP 1 FAILS

PUMP-1 1.000E-02

PUMP 2 FAILS

PUMP-2 1.000E-02

System C

C

TANK 1 SUPPLY FAILS

TANK-1 1.000E-05

PUMP 3 FAILS

PUMP-3 1.000E-02

# Quantification Process

SEQUENCE-3-TBC = Transient * System B Fails * System C Fails

= T * [B * C]

= T * [(TANK-1 + PUMP-1 + PUMP-2) * (TANK-1 + PUMP-3)]

= T * [(TANK-1 * TANK-1) + (TANK-1 *PUMP-3) + (PUMP-1 * TANK-1) + (PUMP-1 * PUMP-3) + (PUMP-2 * TANK-1) + (PUMP-2 * PUMP-3)]

= T * [**(TANK-1 * TANK-1)** + **(TANK-1 *PUMP-3)** + **(PUMP-1 * TANK-1)** + (PUMP-1 * PUMP-3) + **(PUMP-2 * TANK-1)** + (PUMP-2 * PUMP-3)]

= T * [(TANK-1) + (PUMP-1 * PUMP-3) + (PUMP-2 * PUMP-3)]

= 10/YR [(1E-5) + (1E-2 * 1E-2) + (1E-2 * 1E-2)]

= 10/YR [(1E-5) + (1E-4) + (1E-4)]

= 10/YR [2.1E-4]

= 2.1E-3/YR

# Recovery Analysis

- Analysis on accident sequence level
  - Examination of contributors to failure
  - Identification of potential for recovery
- Recovery factors
  - Critical time for recovery (e.g., time to uncover core)
  - Action required
  - Time required to perform action
  - Probability of recovery versus time available
- Final accident sequence frequency includes recovery

# Recovery Analysis (cont.)

- Recovery events are evaluated and appended to events that can be recovered within sequence cut sets.
- For example, using the cut sets from sequence 3, it is assumed that there is a potential to recover pump-1 (for illustration only).
- Recovery event is based on procedures, timing to get the component operating, etc.
  - A recovery event is created and its probability is based on failing to perform this operation (nonrecovery probability)
  - Assume a probability of 0.5

# Recovery Analysis (cont.)

- **The resultant cut sets and final result after recovery is:**

= T * [(TANK-1) + {(PUMP-1 * PUMP-3) * **XHE-REC**}+ (PUMP-2 * PUMP-3)]

= 10/YR [(1E-5) + (1E-2 * 1E-2 * 0.5) + (1E-2 * 1E-2)]

= 10/YR [(1E-5) + (5E-5) + (1E-4)]

= 10/YR [1.6E-4]

= 1.6E-3/YR

# Importance Measures

- **Provide quantitative perspective on dominant contributors to risk and sensitivity of risk to changes in input values**
- **Usually calculated at core damage frequency level**
- **Common importance measures include;**
  - **Fussell-Vesely**
  - **Risk Reduction**
  - **Risk Increase or Risk Achievement**
  - **Birnbaum**

# Fussell-Vesely (FV)

- Measures the overall percent contribution of cut sets containing a basic event of interest to the total risk
- Calculated by finding the value of cut sets that contain the basic event of interest ($x_i$) and dividing by the value of all cut sets representing the total risk (baseline risk)

  $FV_{xi} = F(i) / F(x)$

  where,

  F(i) is risk from just those cut sets that contain event $x_i$

  F(x) is the total risk from all cut sets
- The FV range is from 0 to 1 (0% to 100%)

# Fussell-Vesely Importance Example

- **Consider these minimal cut sets:**

T * [(TANK-1) + (PUMP-1 * PUMP-3) + (PUMP-2 * PUMP-3)]

10/YR * [(1E-5) + (1E-2 * 1E-2) + (1E-2 * 1E-2)]

1E-4/YR + 1E-3/YR + 1E-3/YR

F(x) = 2.1E-3/YR

- **Fussell-Vesely Importance**

$FV_{T}$ = 2.1E-3/2.1E-3 = 1.000

$FV_{PUMP\text{-}1}$ = 1.0E-3/2.1E-3 = 0.476

$FV_{PUMP\text{-}2}$ = 1.0E-3/2.1E-3 = 0.476

$FV_{PUMP\text{-}3}$ = 2.0E-3/2.1E-3 = 0.952

$FV_{TANK\text{-}1}$ = 1.0E-4/2.1E-3 = 0.048

# Risk Reduction Importance (Risk Reduction Worth)

- Measures the amount that the total risk would decrease if a basic event's failure probability were 0 (i.e., never fails)
- Calculated as either ratio or difference between the value of all cut sets representing the total risk (baseline risk) and the value of the total risk with the failure probability for the basic event of interest ($x_i$) set to 0

  Ratio: $RRR_{xi} = RRW_{xi} = F(x) / F(0)$

  Difference (or Interval): $RRI_{xi} = F(x) - F(0)$

  where,

  F(x) is the total risk from all cut sets and all basic events are at their nominal failure probability

  F(0) is the total risk with basic event $x_i$ probability set to 0
- The Risk Reduction Ratio range is from 1 to ∞
- Risk Reduction gives the same ranking as Fussell-Vesely
- For Maintenance Rule (10 CFR 50.65), NUMARC Guide 93-01 (endorsed by NRC) uses a RRR significance criterion of 1.005
  - Equivalent to Fussell-Vesely importance of 0.005

# Risk Reduction Importance Example

- **Consider these minimal cut sets:**

  T * [(TANK-1) + (PUMP-1 * PUMP-3) + (PUMP-2 * PUMP-3)]

  10/YR * [(1E-5) + (1E-2 * 1E-2) + (1E-2 * 1E-2)]

  1E-4/YR + 1E-3/YR + 1E-3/YR

  F(x) = 2.1E-3/YR

- **Risk Reduction Ratio = F(x)/F(0)**

  $RRR_{T}$ = 2.1E-3/0 = ∞

  $RRR_{PUMP\text{-}1}$ = 2.1E-3/1.1E-3 = 1.909

  $RRR_{PUMP\text{-}2}$ = 2.1E-3/1.1E-3 = 1.909

  $RRR_{PUMP\text{-}3}$ = 2.1E-3/1.0E-4 = 21.000

  $RRR_{TANK\text{-}1}$ = 2.1E-3/2.0E-3 = 1.050

# Risk Increase Importance (Risk Achievement Worth)

- Measures the amount that the total risk would increase if a basic event's failure probability were 1 (e.g., component taken out of service or is failed)
- Calculated as either ratio or difference between the value of the total risk with the failure probability for the basic event of interest ($x_i$) set to 1 and the total risk (baseline risk)

  Ratio: $RIR_{xi}$ or $RAW_{xi}$ = F(1) / F(x)
  Difference (or Interval): $RII_{xi}$ = F(1) - F(x)

  where,

  F(x) is the total risk from all cut sets and all basic events are at their nominal failure probability

  F(1) is the total risk with basic event $x_i$ probability set to 1
- Ratio measure referred to as Risk Achievement Worth (RAW)
- The RAW range is $\geq 1$
  - Caution when interpreting RAW for initiating events, recall initiating events input as a frequency
- For Maintenance Rule (10 CFR 50.65), NUMARC Guide 93-01 (endorsed by NRC) uses a RAW significance criterion of 2

# Risk Increase Importance Example

- **Consider these minimal cut sets:**

  T * [(TANK-1) + (PUMP-1 * PUMP-3) + (PUMP-2 * PUMP-3)]

  10/YR * [(1E-5) + (1E-2 * 1E-2) + (1E-2 * 1E-2)]

  1E-4/YR + 1E-3/YR + 1E-3/YR

  F(x) = 2.1E-3/YR

- **Risk Achievement Worth = F(1)/F(x)**

  $RAW_{T}$ = 2.100E-4/2.1E-3 = 0.100

  (caution when interpreting RAW for initiating events, recall initiating events input as a frequency)

  $RAW_{PUMP-1}$ = 1.011E-1/2.1E-3 = 48.143

  $RAW_{PUMP-2}$ = 1.011E-1/2.1E-3 = 48.143

  $RAW_{PUMP-3}$ = 2.001E-1/2.1E-3 = 95.286

  $RAW_{TANK-1}$ = 1.000E+1/2.1E-3 = 4,761.905

# Birnbaum (B)

- Measures the rate of *change* in total risk as a result of changes to the probability of an individual basic event
- Ranks events according to the effect they produce on the risk level when they are modified from their nominal values

$$B_x = \partial F(x) / \partial x$$

where,

F(x) is the total risk from all cut sets and all basic events are at their nominal failure probability

$\partial / \partial x$ is the first derivative of the risk expression with respect to the basic event of interest ($x_i$)

- When the risk expression has a linear form

$$B_{xi} = F(1) - F(0)$$

- The Bi range is between 0 and the cumulative initiating event frequency
  - That is, a Bi = 0 indicates little risk sensitivity and a Bi = cumulative initiating event frequency indicates large risk sensitivity

# Birnbaum Importance Example

- **Consider these minimal cut sets:**

  T * [(TANK-1) + (PUMP-1 * PUMP-3) + (PUMP-2 * PUMP-3)]

  10/YR * [(1E-5) + (1E-2 * 1E-2) + (1E-2 * 1E-2)]

  1E-4/YR + 1E-3/YR + 1E-3/YR

  F(x) = 2.1E-3/YR

- **Birnbaum = F(1) - F(0)**

  $B_{T}$ = (2.100E-4) – (0) = 2.100E-4

  $B_{PUMP-1}$ = (1.011E-1) – (1.1E-3) = 1.000E-1

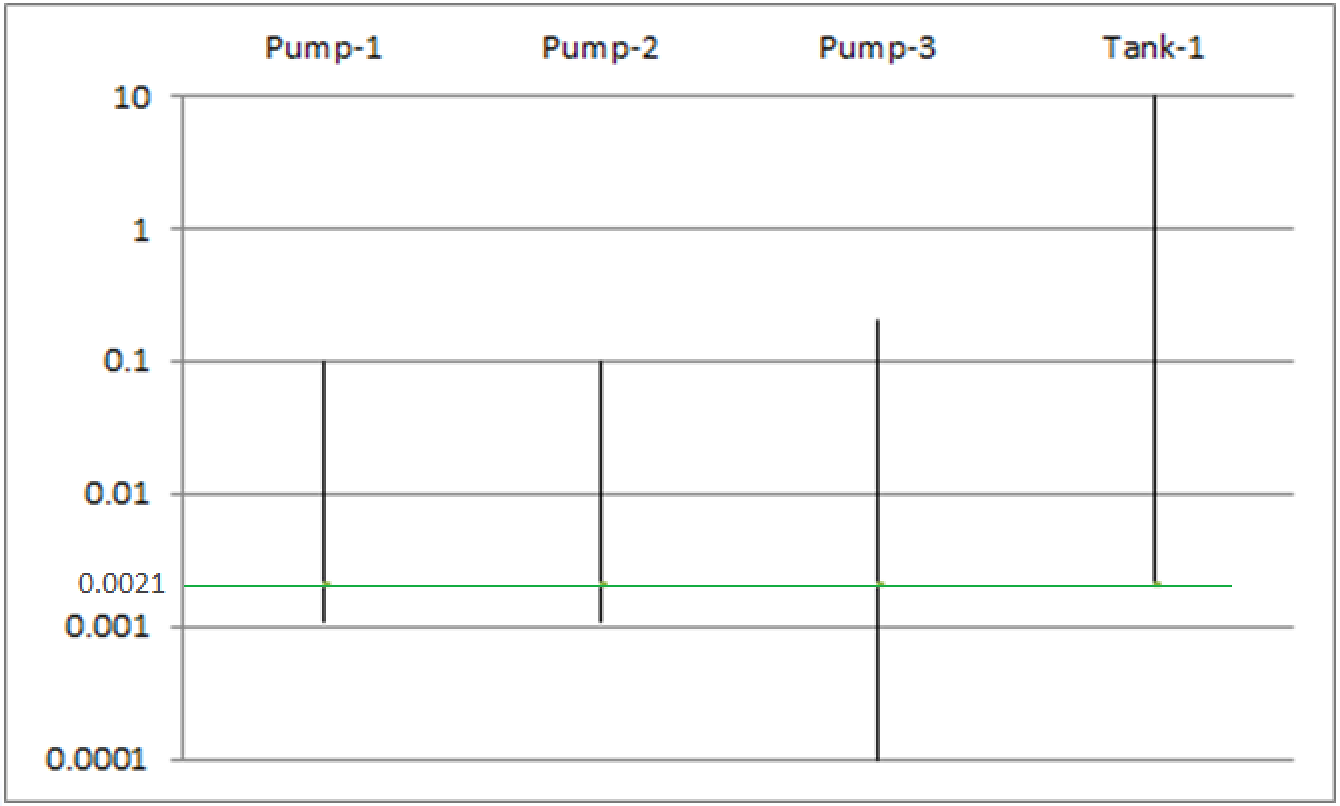
  $B_{PUMP-2}$ = (1.011E-1) – (1.1E-3) = 1.000E-1

  $B_{PUMP-3}$ = (2.001E-1) – (1.0E-4) = 2.000E-1

  $B_{TANK-1}$ = (1.000E+1) – (2.0E-3) = 9.998E+0

# Birnbaum Importance Example

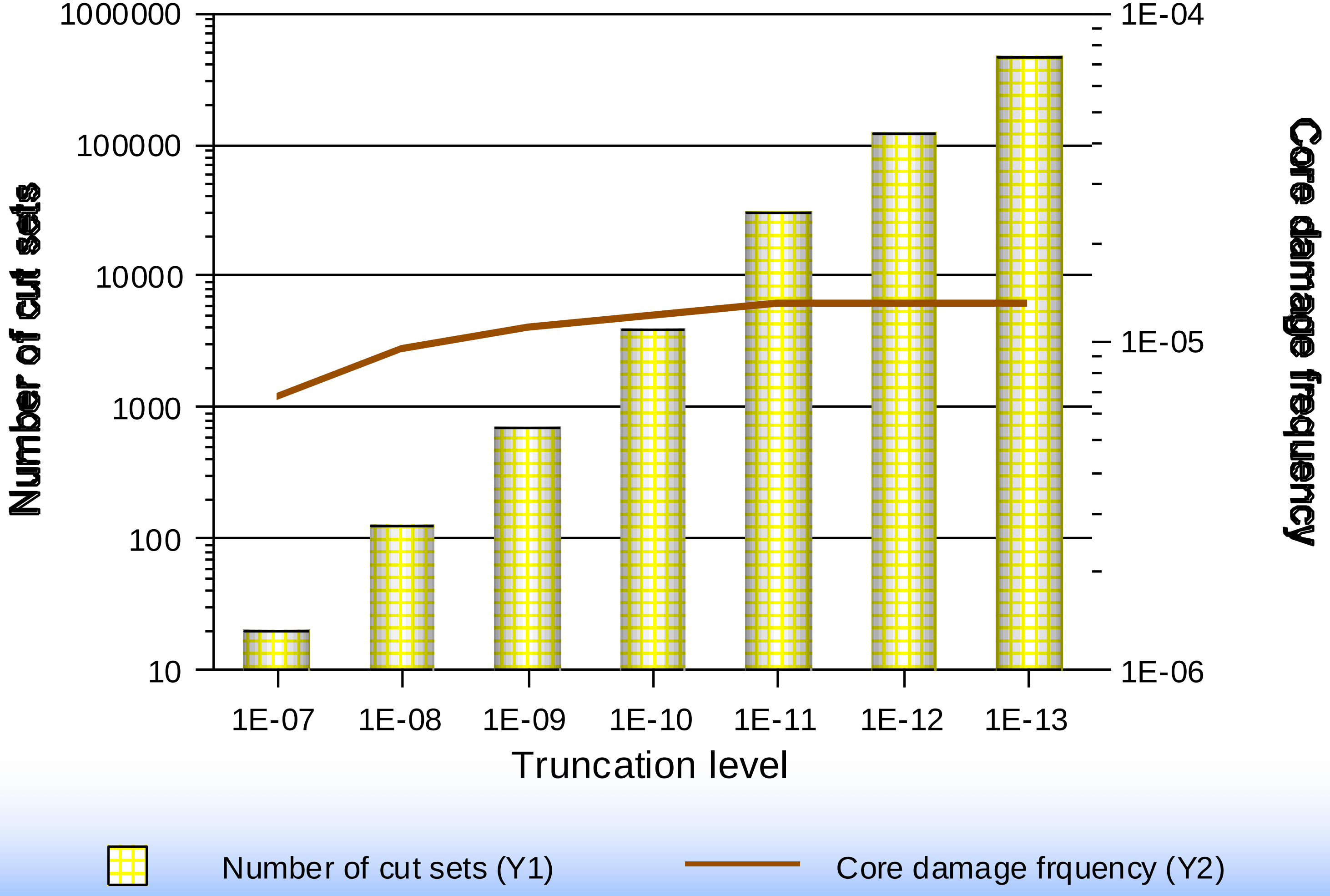
## Plot of component's Birnbaums



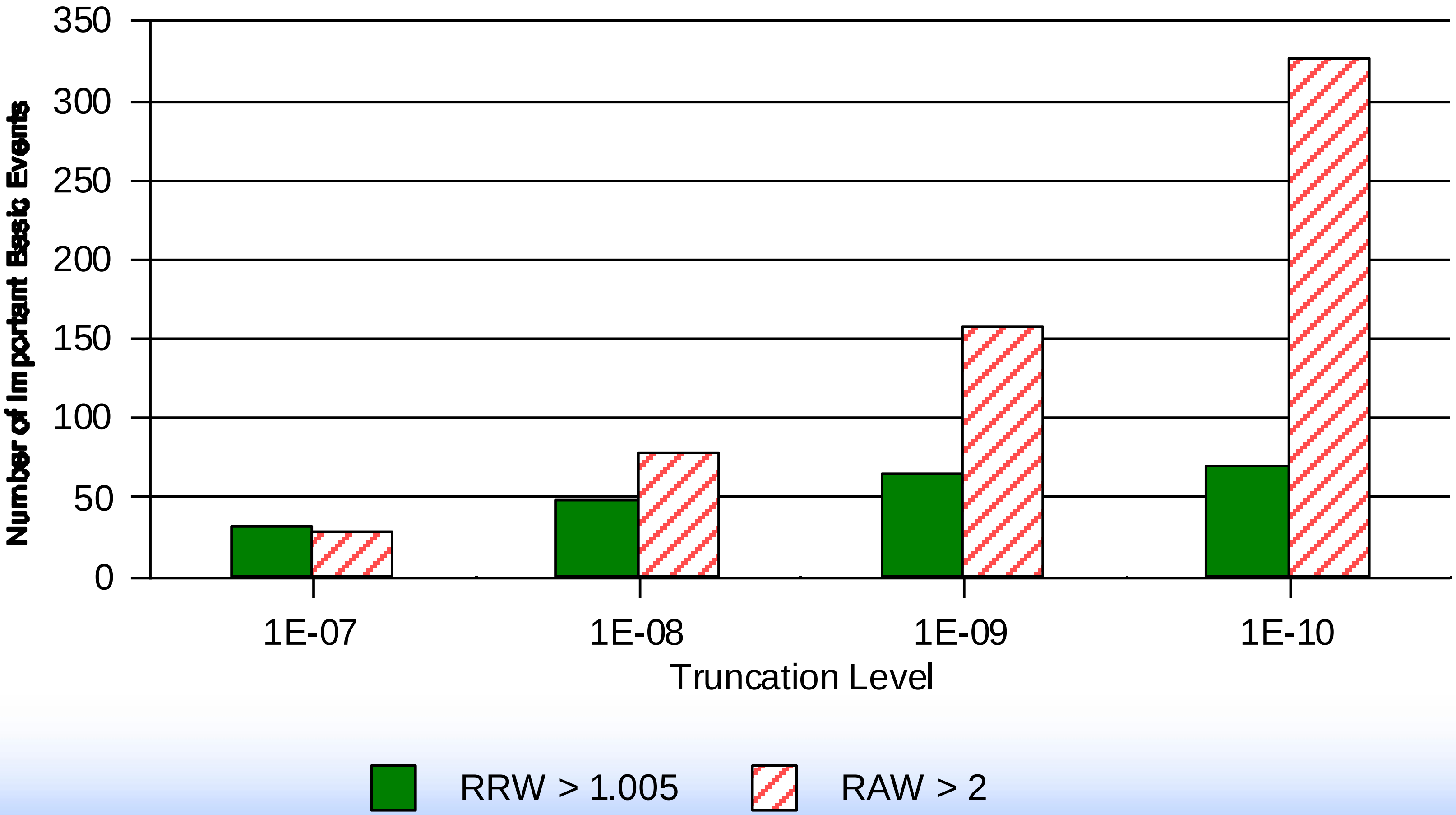
# Limitations of Risk Importance Measures

- Numerical values can be affected by:
  - Exclusion of equipment from PRA model
  - Parameter values used for other events in model
  - Present configuration of plant (equipment that is already out for test/maintenance)
  - Model truncation during quantification

# Core Damage Frequency and Number of Cut Sets Sensitive to Truncation Limits



# Truncation Limits Affect Importance Rankings



# Limitations of Risk Importance Measures

- Risk rankings are not always well-understood in terms of their issues and engineering interpretations
  - That is, high importance does not necessarily mean dominant contributor to CDF
- RAW provides indication of risk impact of taking equipment out of service but full impact may not be captured
  - That is, taking component out of service for test and maintenance may increase likelihood of initiating event due to human error

# Other Considerations When Using Importance Measures

- F-V and RAW rankings can differ significantly when using different risk metrics
  - Such as, core damage frequency due to internal events versus external events, shutdown risk, etc.
- Individual F-V or RAW measures cannot be combined to obtain risk importance for combinations of events
  - Critical combinations can be extremely important due to failure of redundant components
    - Individual components in one train may have low rankings (i.e., importance measure values do not add)

# Review of Sequence Quantification

## Key Points of Section:

- Accident Sequence Quantification:
  - Accident sequences are generated by “linking” fault tree models to event trees
  - Quantify sequence minimal cut sets with data
  - Add any “recovery actions”
  - Determine dominant accident sequences
  - Perform sensitivity, importance and uncertainty analysis
- Types of importance measures:
  - Fussell-Vesely
  - Risk Reduction
  - Risk Increase Ratio (or Risk Achievement)
  - Birnbaum
- Risk importance measures do have limitations such as quantification truncation and plant configuration can effect the values.  In addition, F-V and RAW rankings can differ significantly  when using different risk metrics.

# Importance Measure Workshop

**Using the Motor Fails to Stop and the ECI System Failure examples, calculate the importance measures for basic events appearing in the minimal cut sets.**

# Importance Measure Workshop – Question 1 of 4

- Using the Motor Fails to Stop minimal cut sets, probability values listed below, and results;

  G1 = E1 + E2 + E3 + E4 * E5

  Basic Event Values:

  E1 = Breaker fail to open = 1E-3
  E2 = Trip coil fails to energize = 1E-3
  E3 = 125 VDC power supply fails = 1E-4
  E4 = E5 = Switch fails to close = 1E-2

  G1 = E1 + E2 + E3 + E4 * E5
  G1 = 1E-3 + 1E-3 + 1E-4 + (1E-2) * (1E-2)
  G1 = 1E-3 + 1E-3 + 1E-4 + 1E-4
  G1 = 2.199E-3

  – What would the Fussell-Vesely be for basic event E2 for the Motor Fails to Stop cut sets where CCF event(s) are not included?

  – What would the RRR be for basic event E2 for the Motor Fails to Stop cut sets where CCF event(s) are not included?

  – What would the RAW be for basic event E2 for the Motor Fails to Stop cut sets where CCF event(s) are not included?

  – What would the Birnbaum be for basic event E2 for the Motor Fails to Stop cut sets where CCF event(s) are not included?

# Importance Measure Workshop – Question 2 of 4

- Using the Motor Fails to Stop minimal cut sets with CCF event(s) included, probability values listed below, and results;

  G1 = E1 + E2 + E3 + E4 * E5 + E45-CCF

  Basic Event Values:
  E1 = Breaker fail to open = 1E-3
  E2 = Trip coil fails to energize = 1E-3
  E3 = 125 VDC power supply fails = 1E-4
  E4 = E5 = Switch fails to close = 1E-2
  $\beta$ = 0.1

  G1 = E1 + E2 + E3 + E4 * E5
  G1 = 1E-3 + 1E-3 + 1E-4 + (1E-2) * (1E-2) + [(0.1) *(1E-2)]
  G1 = 1E-3 + 1E-3 + 1E-4 + 1E-4 +1E-3
  G1 = 3.196E-3

  – What would the Fussell-Vesely be for basic event E2 for the Motor Fails to Stop cut sets where CCF event(s) are included?

  – What would the RRR be for basic event E2 for the Motor Fails to Stop cut sets where CCF event(s) are included?

  – What would the RAW be for basic event E2 for the Motor Fails to Stop cut sets where CCF event(s) are included?

  – What would the Birnbaum be for basic event E2 for the Motor Fails to Stop cut sets where CCF event(s) are included?

# Importance Measure Workshop – Question 3 of 4 (Optional)

- Using the ECI system minimal cut sets, probability values listed below, and results;

  *ECI = T1 + V1 + PA * PB + PA * CVB + PB * CVA + CVA * CVB + MV1 * MV2 * MV3*

  Basic Event Values:

  T1 = 1E-6<br>
  V1 = 5E-5<br>
  PA = PB = 1E-2<br>
  CVA = CVB = 1E-4<br>
  MV1 = MV2 = MV3 = 3E-3

  *ECI = T1 + V1 + PA * PB + PA * CVB + PB * CVA + CVA * CVB + MV1 * MV2 * MV3*
  *ECI = (1E-6) + (5E-5) + (1E-2) * (1E-2) + (1E-2) * (1E-4) + (1E-2) * (1E-4) + (1E-4) * (1E-4) + (3E-3) * (3E-3) * (3E-3)*
  *ECI = (1E-6) + (5E-5) + (1E-4) + (1E-6) + (1E-6) + (1E-8) + (2.7E-8)*
  *ECI* = 1.530E-4

  – What would the Fussell-Vesely be for basic event PA for the ECI-System cut sets where CCF event(s) are not included?

  – What would the RRR be for basic event PA for the ECI-System cut sets where CCF event(s) are not included?

  – What would the RAW be for basic event PA for the ECI-System cut sets where CCF event(s) are not included?

  – What would the Birnbaum be for basic event PA for the ECI-System cut sets where CCF event(s) are not included?

# Importance Measure Workshop – Question 4 of 4 (Optional)

- Using the ECI system minimal cut sets with CCF event(s) included, probability values listed below, and results;

_ECI = T1 + V1 + PA * PB + PA * CVB + PB * CVA + CVA * CVB + MV1 * MV2 * MV3_ + PAB-CCF + CVAB-CCF + MV123-CCF

Basic Event Values:

T1 = 1E-6
V1 = 5E-5
PA = PB = 1E-2
CVA = CVB = 1E-4
MV1 = MV2 = MV3 = 3E-3
$\beta$ = 0.1

_ECI = T1 + V1 + PA * PB + PA * CVB + PB * CVA + CVA * CVB + MV1 * MV2 * MV3_ + PAB-CCF + CVAB-CCF + MV123-CCF
_ECI = (1E-6)+(5E-5)+(1E-2)*(1E-2)+(1E-2)*(1E-4)+(1E-2)*(1E-4)+(1E-4)*(1E-4)+(3E-3)*(3E-3)*(3E-3)+[_(0.1)*(1E-2)]+[(0.1)*(1E-4)]+[(0.1)*(3E-3)]
_ECI = (1E-6) + (5E-5) + (1E-4) + (1E-6) + (1E-6) + (1E-8) + (2.7E-8)_ + (1E-3) + (1E-5) + (3E-4)
_ECI_ = 1.463E-3

- What would the Fussell-Vesely be for basic event PA for the ECI-System cut sets where CCF event(s) are included?
- What would the RRR be for basic event PA for the ECI-System cut sets where CCF event(s) are included?
- What would the RAW be for basic event PA for the ECI-System cut sets where CCF event(s) are included?
- What would the Birnbaum be for basic event PA for the ECI-System cut sets where CCF event(s) are included?

# 8. Uncertainties in PRA

# Uncertainties in PRA

- **Purpose: To acquaint students with how PRA treats uncertainty, including the identification of two types of uncertainty, aleatory and epistemic, and the characterization of one type of epistemic uncertainty with probability distributions.**
- **Objectives: Students will be able to identify the two types of uncertainty, along with their sources, and interpret probability distributions as an expression of epistemic uncertainty.**
- **References:**
  - **G. Apostolakis, "The Concept of Probability in Safety Assessments of Technological Systems," Science, 250, 1990.**
  - **NUREG-1489, *A Review of NRC Staff Uses of Probabilistic Risk Assessment***
  - **G. Parry, "The Characterization of Uncertainty in Probabilistic Risk Assessments of Complex Systems," Reliability Engineering and System Safety, 54 (1996), 119-126.**
  - **R. Winkler, "Uncertainty in Probabilistic Risk Assessment," Reliability Engineering and System Safety, 54 (1996), 127-132.**
  - **N. Siu and D. Kelly, "Bayesian Parameter Estimation in PRA," tutorial paper published in Reliability Engineering and System Safety 62 (1998).**

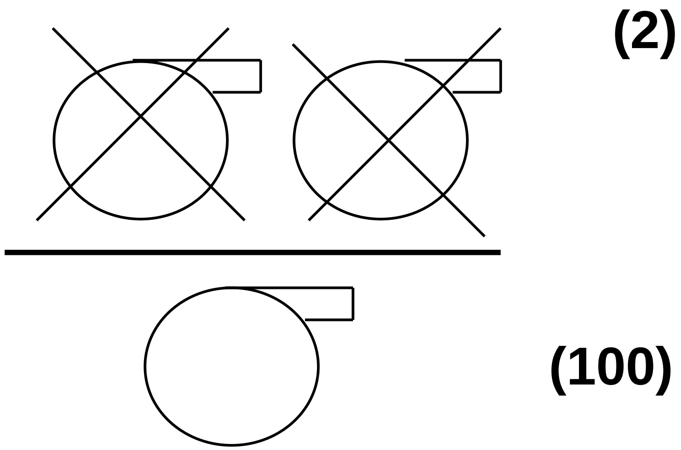
# Uncertainty Arises From Many Sources

- Inability to specify initial and boundary conditions precisely
  - Cannot specify result with deterministic model
  - Instead, use probabilistic models (e.g., tossing a coin)
- Sparse data on initiating events, component failures, and human errors
- Lack of understanding of phenomena
- Modeling assumptions (e.g., success criteria)
- Modeling limitations (e.g., inability to model errors of commission)
- Incompleteness (e.g., failure to identify system failure mode)

# Key Terminology:
# Frequentist Interpretation of Probability

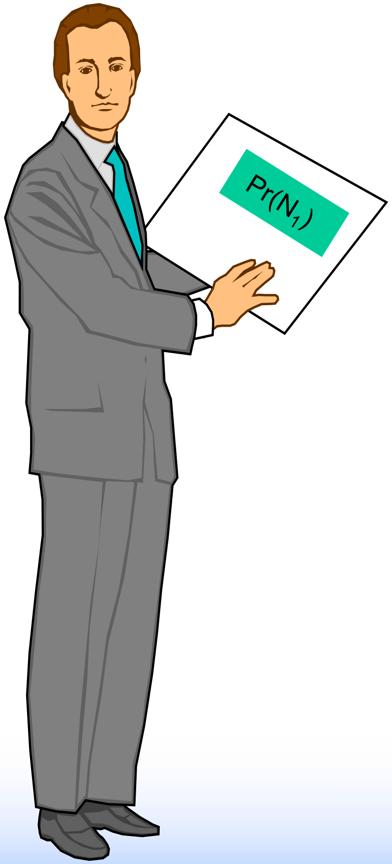
$$\Pr(N_1) = \lim_{N \to \infty} N_1 \;/\; N$$

$\hat{p} =$



= 1/50
= 0.02
= 2E-2

# Key Terminology: Subjectivist (Bayesian) Interpretation of Probability



- Pr($N_1$) is the degree of belief the analyst holds about the likelihood of event $N_1$ occurring, based on current information.

# PRAs Identify Two Types of Uncertainty

- Distinction between aleatory and epistemic uncertainty:
  - “Aleatory” from the Latin Alea (dice), of or relating to random or stochastic phenomena.
    - Also called “random uncertainty or variability”
  - “Epistemic” of, relating to, or involving knowledge; cognitive, from Greek episteme, knowledge
    - Also called “state-of-knowledge uncertainty”

# Aleatory Uncertainty

- Variability in or lack of precise knowledge about underlying conditions makes events unpredictable.
- Aleatory models represent randomness in the outcome of a process
  - For example, flipping a coin is “random” process
    - Often modeled by a binomial distribution
    - Characterize # of heads (or tails) seen for given # of flips
    - When flipping a coin, the “random,” but observable, quantity is number of heads/tails
    - Probabilities are not observable
- These are the same models we described as “probabilistic”
  - Examples → Poisson and binomial

# Epistemic Uncertainty

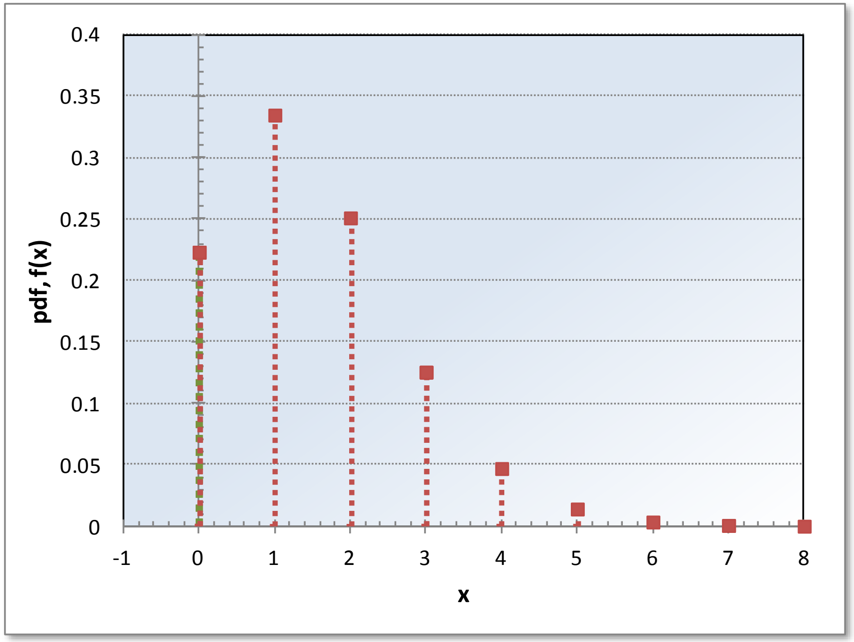
- In the Poisson model, the parameter λ is not known precisely
- Could we model uncertainty in estimate of λ using statistical confidence interval
  - Cannot propagate confidence intervals through PRA models
  - Cannot interpret confidence intervals as probability statements about value of λ
  - Cannot include non-empirical information available
- PRAs represent lack of knowledge about value of λ by assigning a probability distribution to λ
  - Probability distribution for λ can be generated using Bayesian methods

# Epistemic Uncertainty

- Advantages to Bayesian Approach
  - Allows uncertainties to be propagated easily through PRA models
    - We describe all of our “results” as probability distributions
  - Allows probability statements to be made concerning $\lambda$ and outputs that depend upon $\lambda$
  - Provides unified, consistent framework for parameter estimation
    - Allows inclusion of non-empirical information
    - Does not have problems with cases like zero failures in 50 demands

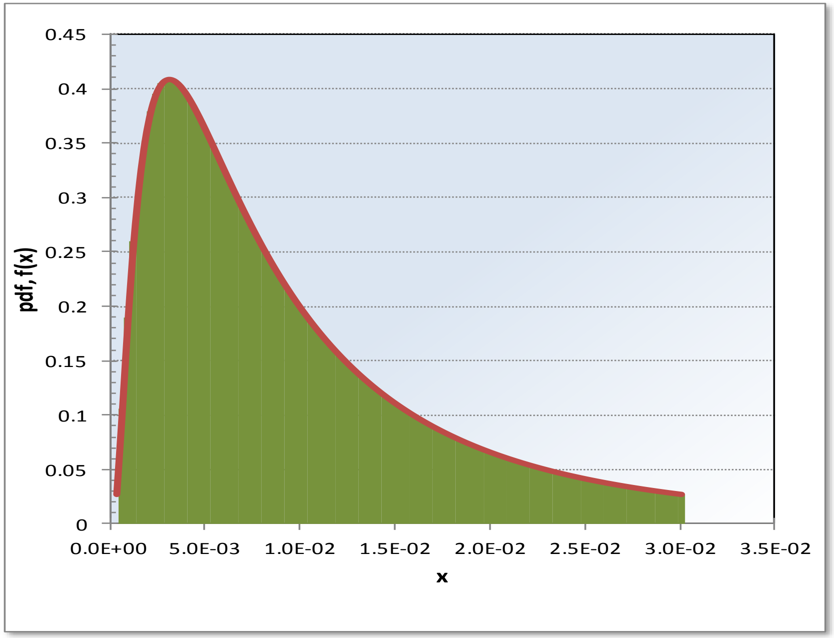
# Uncertainty as Probability Distribution

- We have discrete and continuous distributions



**Discrete Distribution**

**(Poisson with a mean of 1.5)**

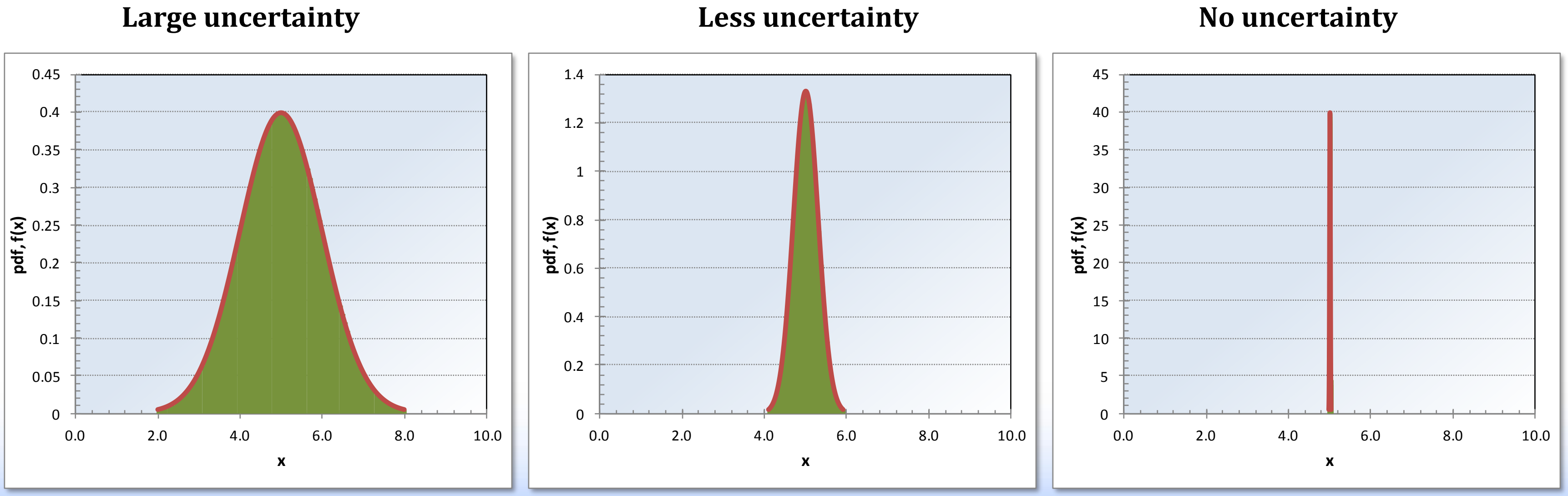


**Continuous Distribution**

**(Lognormal with mean of 0.005)**

# Probability Distributions Represent Uncertainty

- Usually used to represent state of knowledge of parameter values
  - Model assumptions typically addressed via sensitivity studies
- Probability distribution π(λ) represents analyst’s uncertainty about unknown value of λ
  - Note that λ may *not* be observable (for example, if a failure rate)

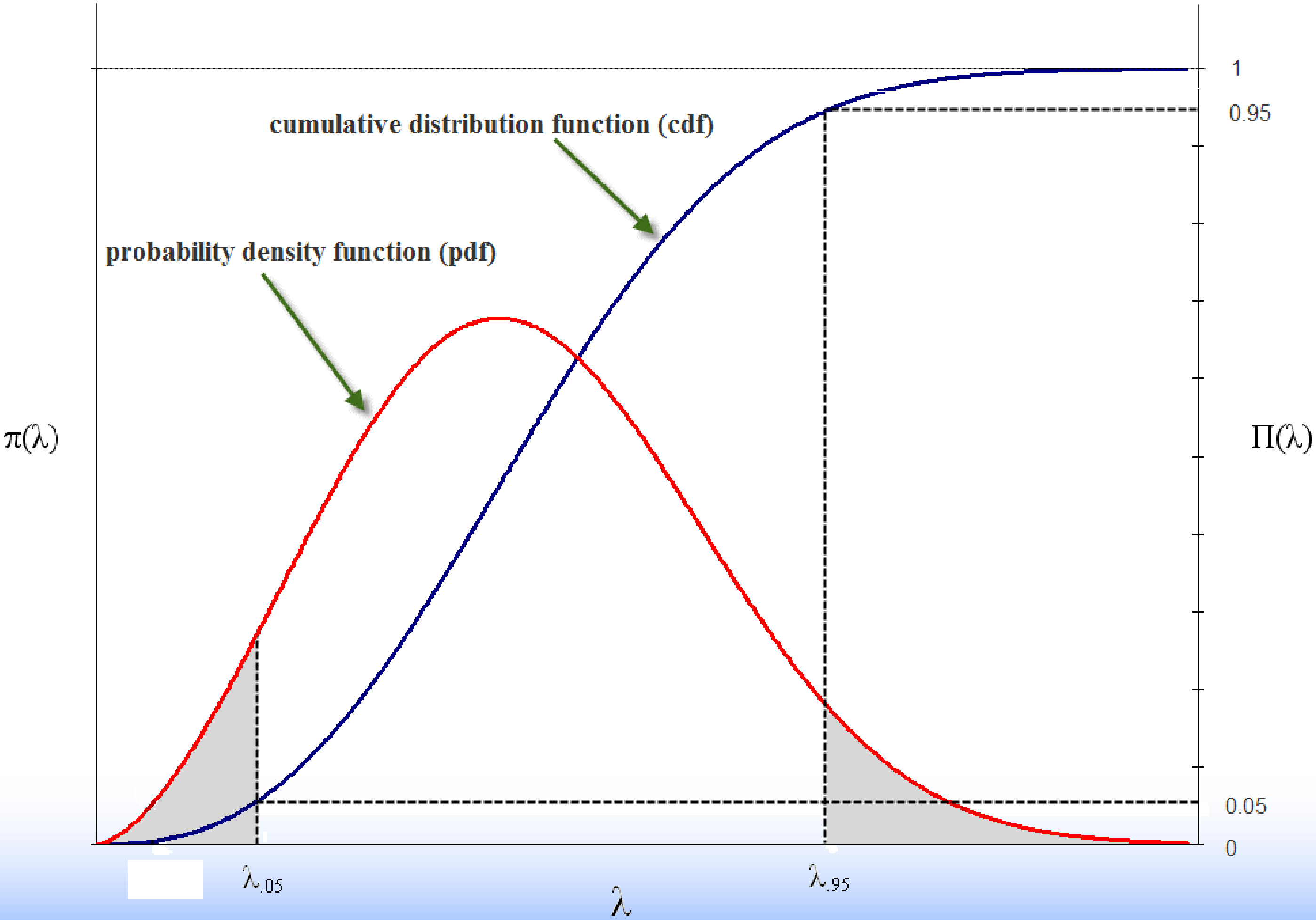


Large uncertainty

Less uncertainty

No uncertainty

# Uncertainty in λ Expressed as Probability Distribution

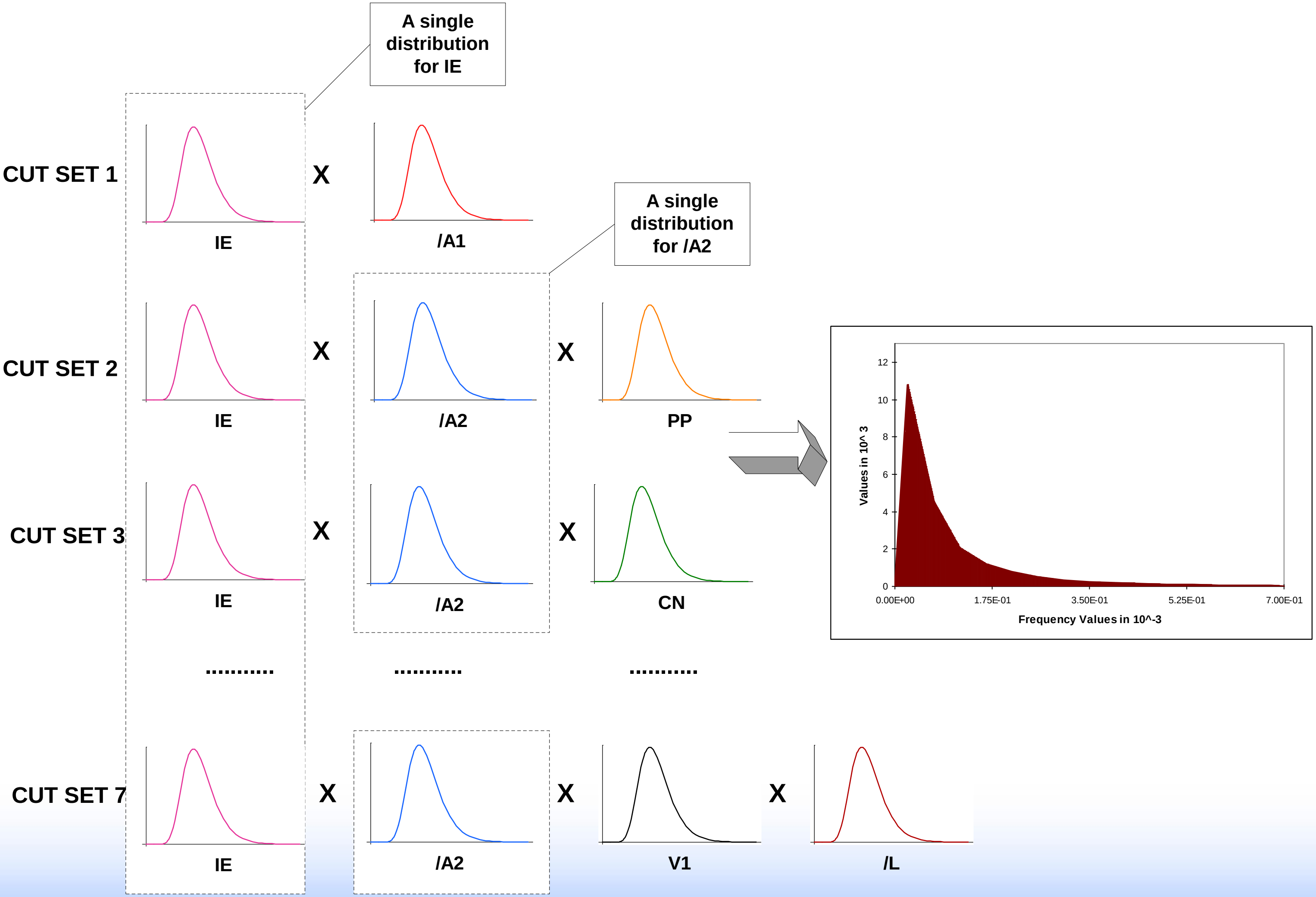


# Uncertainty Propagation

- Uncertainties propagated via Monte Carlo sampling
- In this approach, output probability distribution is generated empirically by repeated sampling from input parameter distributions

TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
NINE NINE NINE NINE NINE NINE
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.

# Uncertainty Propagation through Model



A single distribution for IE

A single distribution for /A2

CUT SET 1: IE X /A1

CUT SET 2: IE X /A2 X PP

CUT SET 3: IE X /A2 X CN

...........

CUT SET 7: IE X /A2 X V1 X /L

# Other Epistemic Uncertainties in PRA

- **Modeling uncertainty**
  - **System success criteria**
  - **Accident progression phenomenology**
  - **Health effects models (linear versus nonlinear, threshold versus nonthreshold dose-response model)**

# Other Epistemic Uncertainties in PRA

- Completeness
  - Complex errors of commission
  - Design and construction errors
  - Unexpected failure modes and system interactions
  - All modes of operation not modeled
- Errors in analysis
  - Failure to model all trains of a system
  - Data input errors
  - Analysis errors

# Addressing Other Epistemic Uncertainties

- Modeling uncertainty usually addressed through sensitivity studies
- Completeness addressed through comparison with other studies and peer review
  - Some issues (e.g., design errors) are simply acknowledged as limitations
  - Other issues (e.g., errors of commission) are topics of ongoing research
- Analysis errors may be difficult to catch; addressed through peer review and validation process

# Review of Uncertainties in PRA

Key Points of Section:

- Sources of Uncertainty: Inability to precisely specify initial and boundary conditions, sparse data, lack of phenomena understanding, modeling assumptions and limitations, and incompleteness.
- Two Types of Uncertainty:
    - Aleatory Uncertainty- Variability in or lack of precise knowledge about underlying conditions.
    - Epistemic Uncertainty- “State of Knowledge Uncertainty.”

For more information on uncertainty and propagation of uncertainty, see P-102 course

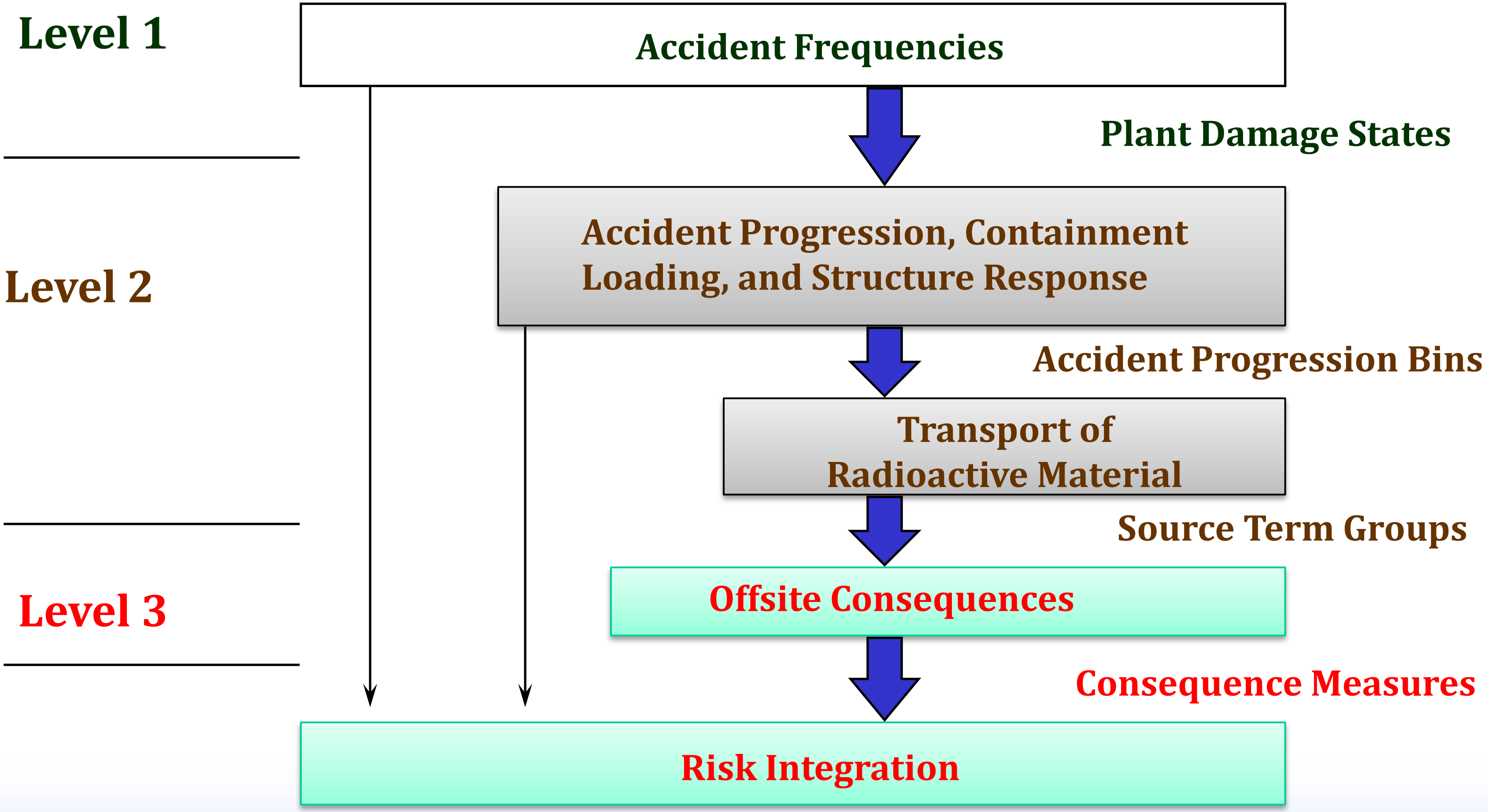
For more information on uncertainty, see a new course added FY-06 titled *Assessing the Adequacy of Models for Risk-Informed Decisions*

# 9. Accident Progression & Consequence Analysis

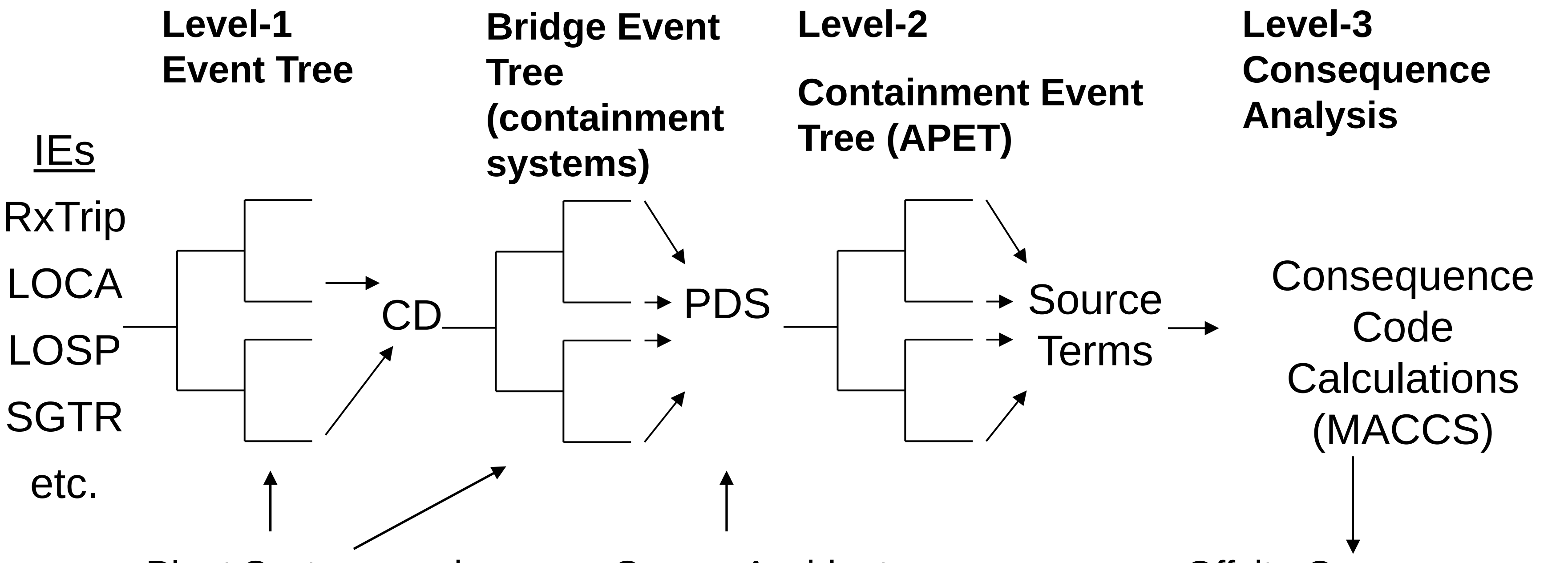
# Accident Progression Analysis, Containment Response, Fission Product Transport, and Consequence Analysis

- **Purpose: Students receive a brief introduction to accident progression (Level 2 PRA) and consequence analysis (Level 3 PRA).**
- **Objectives: At the conclusion of this topic, students will be able to:**
  - **List primary elements which comprise accident phenomenology**
  - **Explain how accident progression analysis is related to full PRA**
  - **Explain general factors involved in containment response**
  - **Explain general factors involved in fission product transport & consequences**
  - **Name the major computer codes used in accident process and consequence analysis**
- **Reference:**
  - **NUREG/CR-2300, *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants***
  - **NUREG/CR-6042, *Perspectives on Reactor Safety***

# Principal Steps in PRA Process



# Overview of Level-1/2/3 PRA



**Level-1 Event Tree**

**Bridge Event Tree (containment systems)**

**Level-2**

**Containment Event Tree (APET)**

**Level-3 Consequence Analysis**

IEs

RxTrip

LOCA

LOSP

SGTR

etc.

CD

PDS

Source Terms

Consequence Code Calculations (MACCS)

Plant Systems and Human Action Models (Fault Trees and Human Reliability Analyses)

Severe Accident Progression Analyses (Experimental and Computer Code Results)

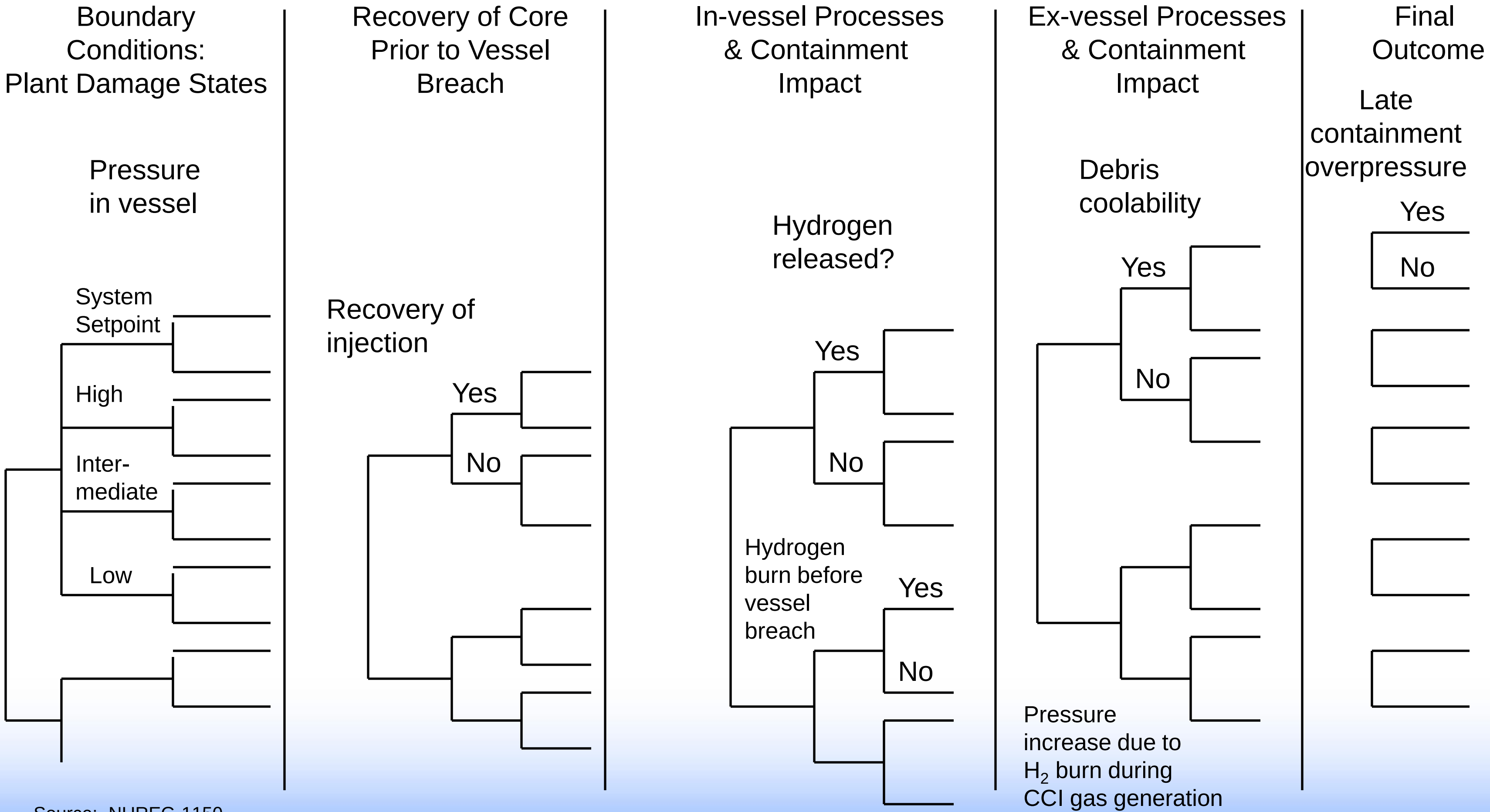
Offsite Consequences Risk:

- Early Fatalities/year
- Latent Cancers/year
- Offsite Cost ($)/year
- Population Dose (person-Sv/year)

# Accident Progression Analysis

- There are 4 major steps in Accident Progression Analysis
  - 1. Develop the Accident Progression Event Trees (APETs)
  - 2. Perform structural analysis of containment
  - 3. Quantify APET issues
  - 4. Group APET sequences into accident progression bins

# Schematic of Accident Progression Event Tree

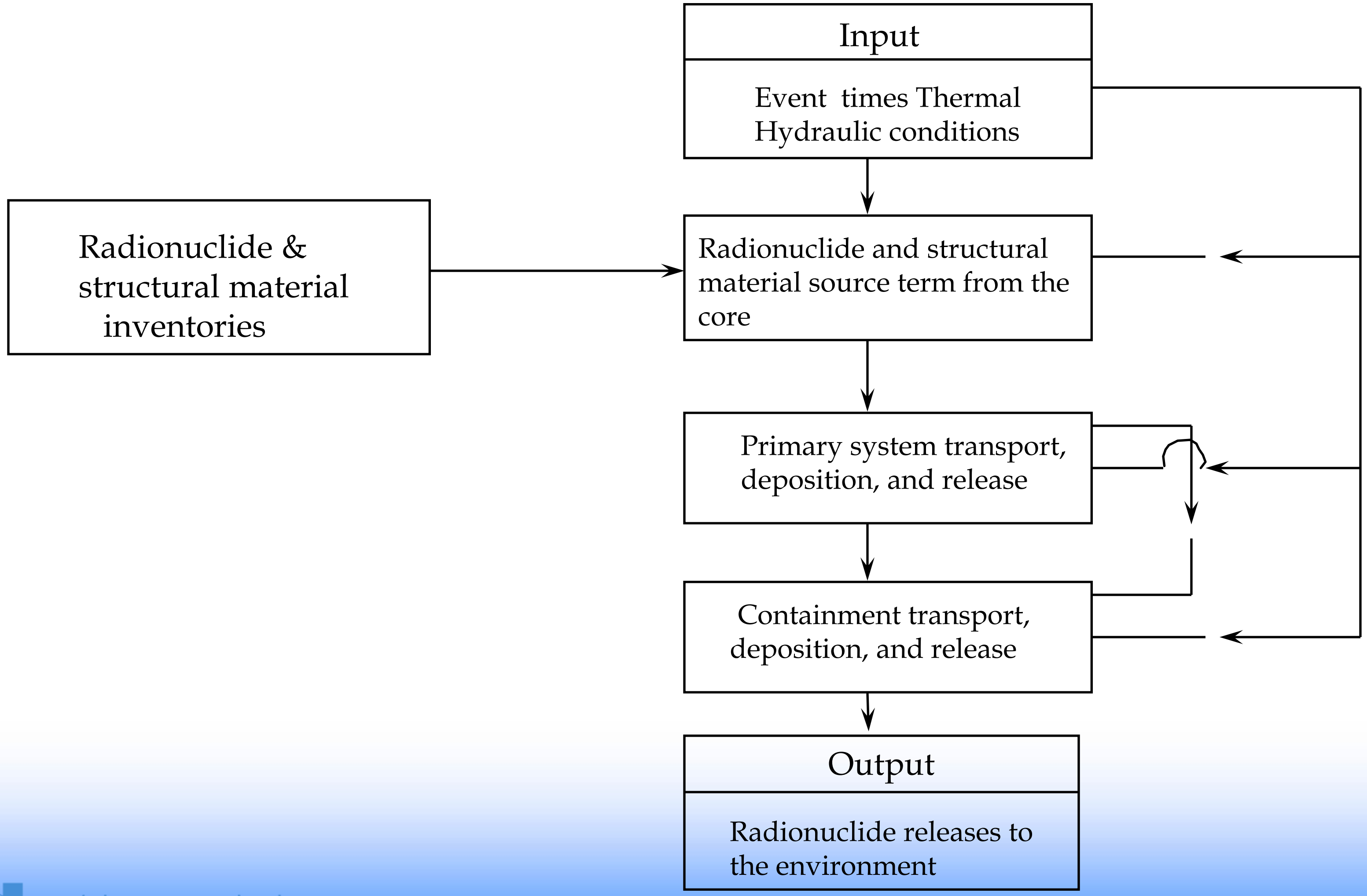

Boundary Conditions: Plant Damage States
Recovery of Core Prior to Vessel Breach
In-vessel Processes & Containment Impact
Ex-vessel Processes & Containment Impact
Final Outcome
Pressure in vessel
System Setpoint
High
Inter-mediate
Low
Recovery of injection
Yes
No
Hydrogen released?
Yes
No
Hydrogen burn before vessel breach
Yes
No
Debris coolability
Yes
No
Pressure increase due to $H_2$ burn during CCI gas generation
Late containment overpressure
Yes
No

Source: NUREG-1150

# Containment Response

- How does the containment system deal with physical conditions resulting from the accident?
  - Pressure
  - Heat sources
  - Fission products
  - Steam and water
  - Hydrogen
  - Other noncondensables

# Elements in the Analysis of Radionuclide Behavior in the Reactor



Input

Event times Thermal Hydraulic conditions

Radionuclide & structural material inventories

Radionuclide and structural material source term from the core

Primary system transport, deposition, and release

Containment transport, deposition, and release

Output

Radionuclide releases to the environment

# Computer codes used to model Accident Progression & Fission Product Behavior

- **RELAP5/SCDAP - in-vessel behavior**
- **CONTAIN - containment behavior**
- **VICTORIA - fission product behavior**
- **Integrated, comprehensive codes**
  - **MAAP - industry code**
  - **MELCOR - NRC code**

# Fission Product Source Term Outcomes of Interest

- **Fractions Released Outside Containment**
  - Noble Gases
  - Iodine
  - Cesium - Rubidium
  - Tellurium - Antimony
  - Barium - Strontium
  - Ruthenium - Molybdenum - Rhenium - Technetium - Cobalt
  - Lanthanum and other rare earth metals

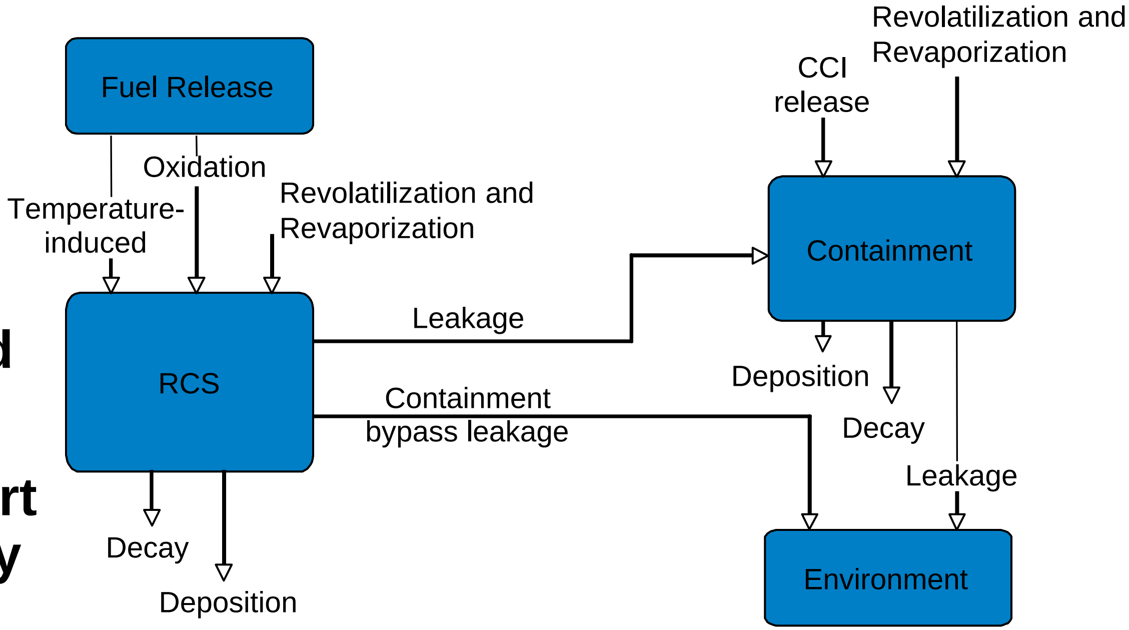
- **Parameters for Consequence Model**
  - Time of release
  - Duration of release
  - Warning time for evacuation
  - Elevation of release
  - Energy of release

# Source Term Calculation Models

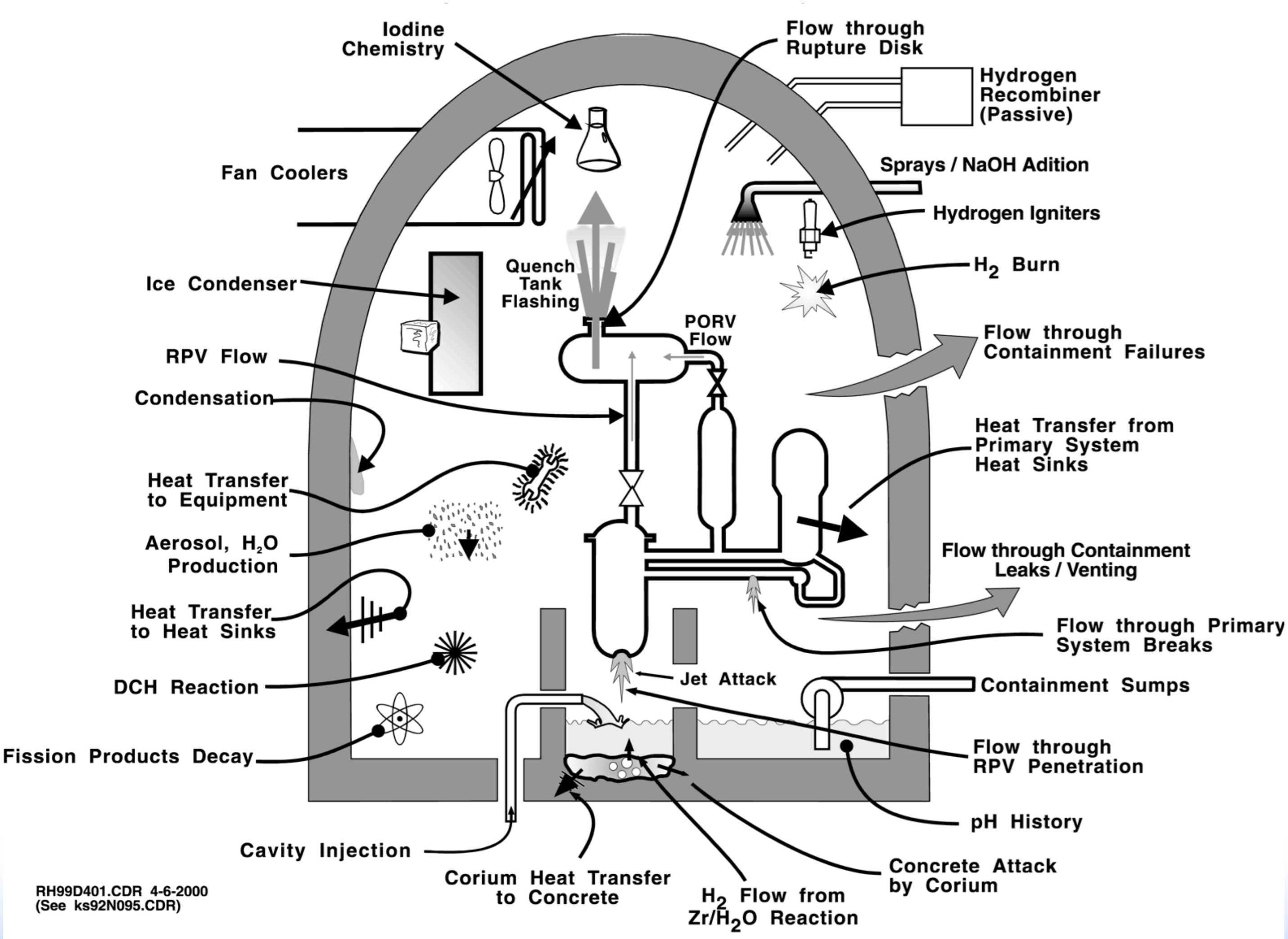
- Integrated Deterministic Code (MELCOR)
  - Point estimate radionuclide release calculations for scenarios important to risk
  - Selected sensitivity calculations to explore uncertainties that can be modeled by the code
- Parametric Source Term Code
  - Point estimate radionuclide release calculations for scenarios less important to risk (simulation of source code package)
  - Extensive sensitivity calculations to explore uncertainties that cannot be modeled by code package

# Source Terms Estimated Parametrically

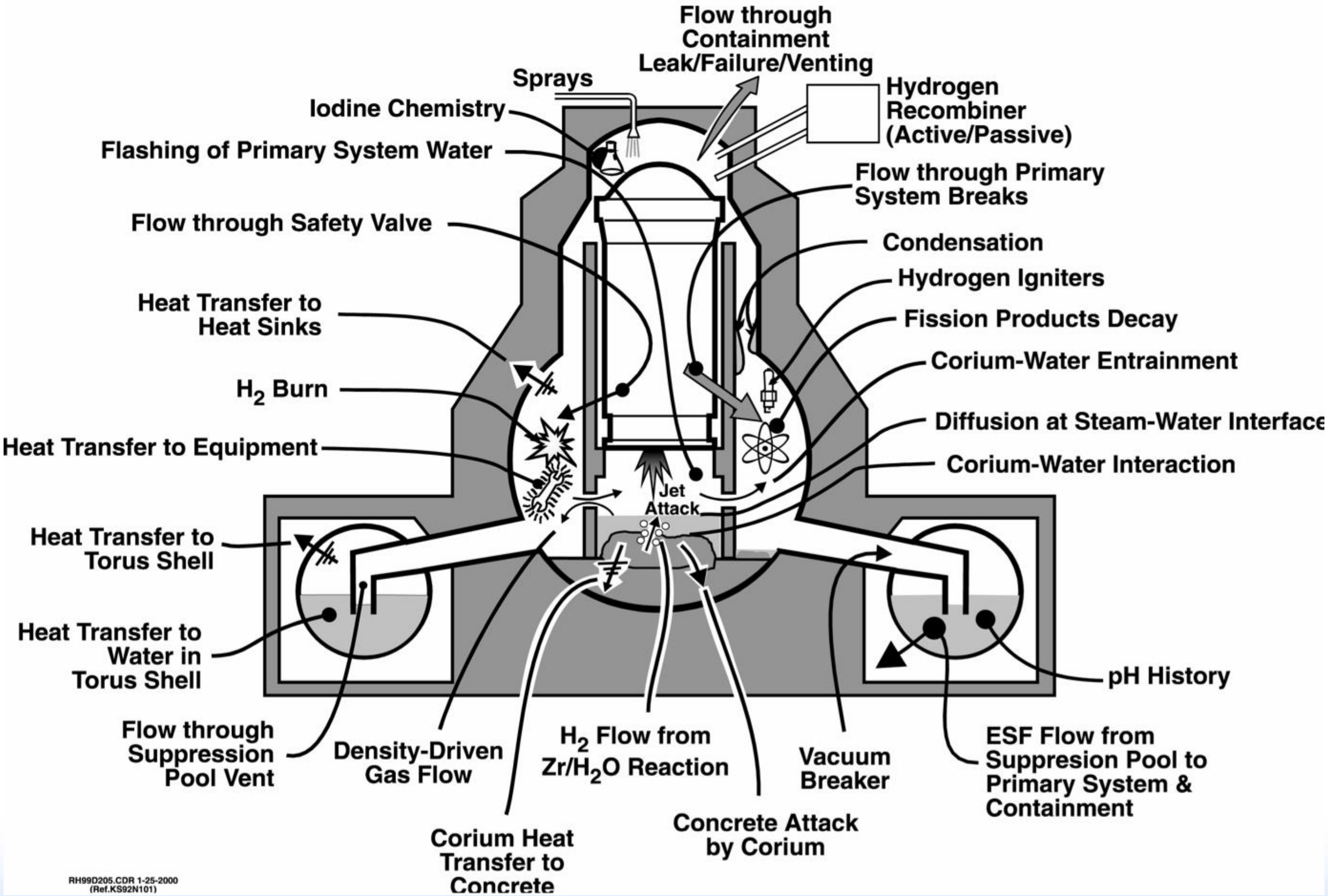
- **Models activity transport between volumes.**
- **User specifies connections between volumes**
- **General transport equation applied to each volume**
- **Considers physics and time-dependence**
- **Code results and expert review used to quantify lower level, input parameters.**



# MAAP Modeled PWR Phenomena


Iodine Chemistry
Flow through Rupture Disk
Hydrogen Recombiner (Passive)
Fan Coolers
Sprays / NaOH Adition
Hydrogen Igniters
Ice Condenser
Quench Tank Flashing
$H_2$ Burn
PORV Flow
Flow through Containment Failures
RPV Flow
Condensation
Heat Transfer from Primary System Heat Sinks
Heat Transfer to Equipment
Aerosol, $H_2O$ Production
Flow through Containment Leaks / Venting
Heat Transfer to Heat Sinks
Flow through Primary System Breaks
DCH Reaction
Jet Attack
Containment Sumps
Fission Products Decay
Flow through RPV Penetration
pH History
Cavity Injection
Concrete Attack by Corium
Corium Heat Transfer to Concrete
$H_2$ Flow from $Zr/H_2O$ Reaction
RH99D401.CDR 4-6-2000
(See ks92N095.CDR)

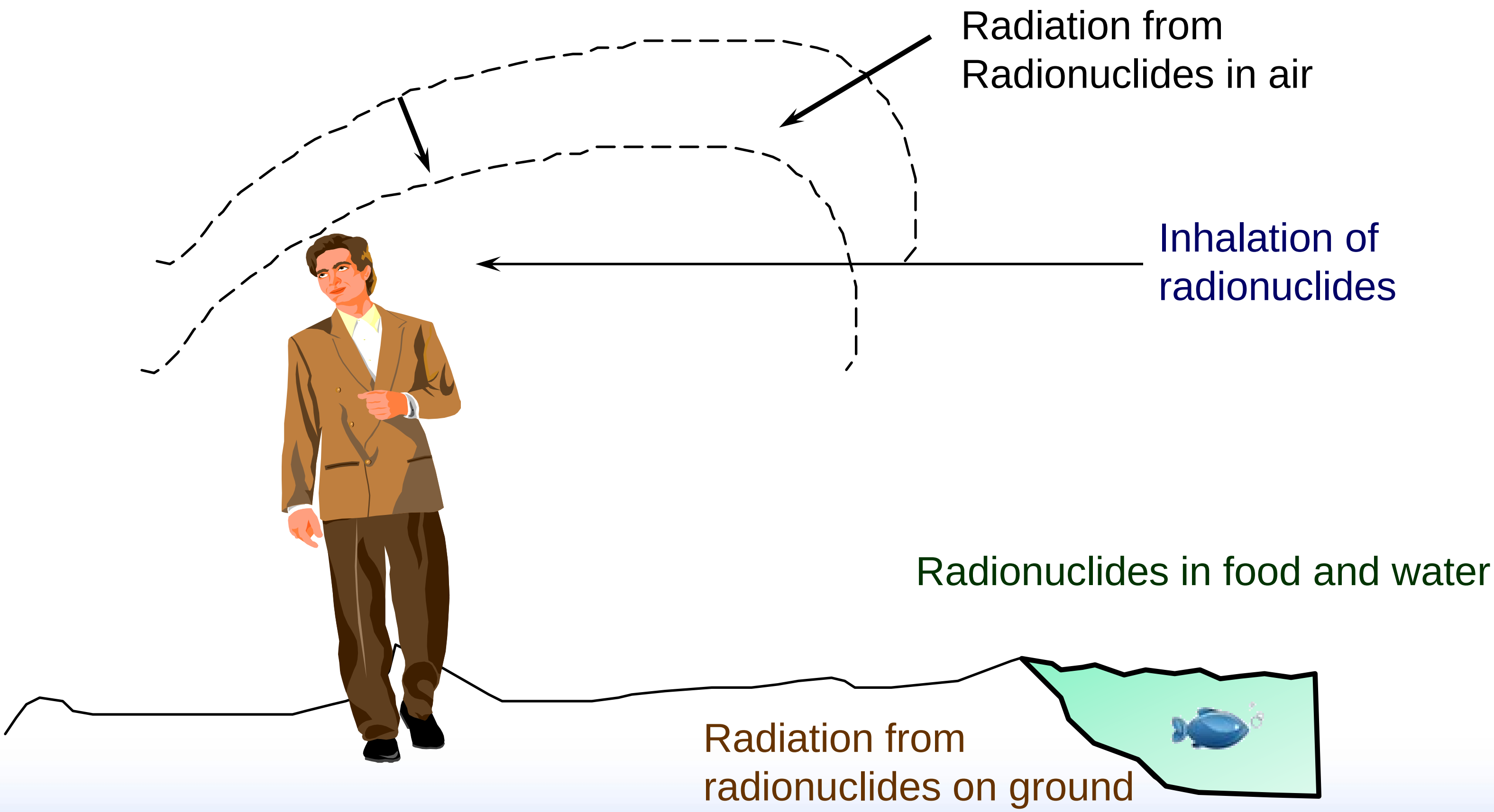
# MAAP Modeled BWR Phenomena


Flow through Containment Leak/Failure/Venting
Sprays
Iodine Chemistry
Hydrogen Recombiner (Active/Passive)
Flashing of Primary System Water
Flow through Primary System Breaks
Flow through Safety Valve
Condensation
Hydrogen Igniters
Heat Transfer to Heat Sinks
Fission Products Decay
Corium-Water Entrainment
$H_2$ Burn
Diffusion at Steam-Water Interface
Heat Transfer to Equipment
Corium-Water Interaction
Jet Attack
Heat Transfer to Torus Shell
Heat Transfer to Water in Torus Shell
pH History
Flow through Suppression Pool Vent
Density-Driven Gas Flow
$H_2$ Flow from Zr/$H_2O$ Reaction
Vacuum Breaker
ESF Flow from Suppression Pool to Primary System & Containment
Corium Heat Transfer to Concrete
Concrete Attack by Corium
RH99D205.CDR 1-25-2000
(Ref.KS92N101)

# Components of a Consequence Model

- Atmospheric transport and diffusion model
- Pathways models
- Dosimetry models
- Health effects model
- Other models:
  - Evacuation
  - Interdiction
  - Decontamination
  - Economic effects

# Pathways to People



Radiation from Radionuclides in air

Inhalation of radionuclides

Radionuclides in food and water

Radiation from radionuclides on ground

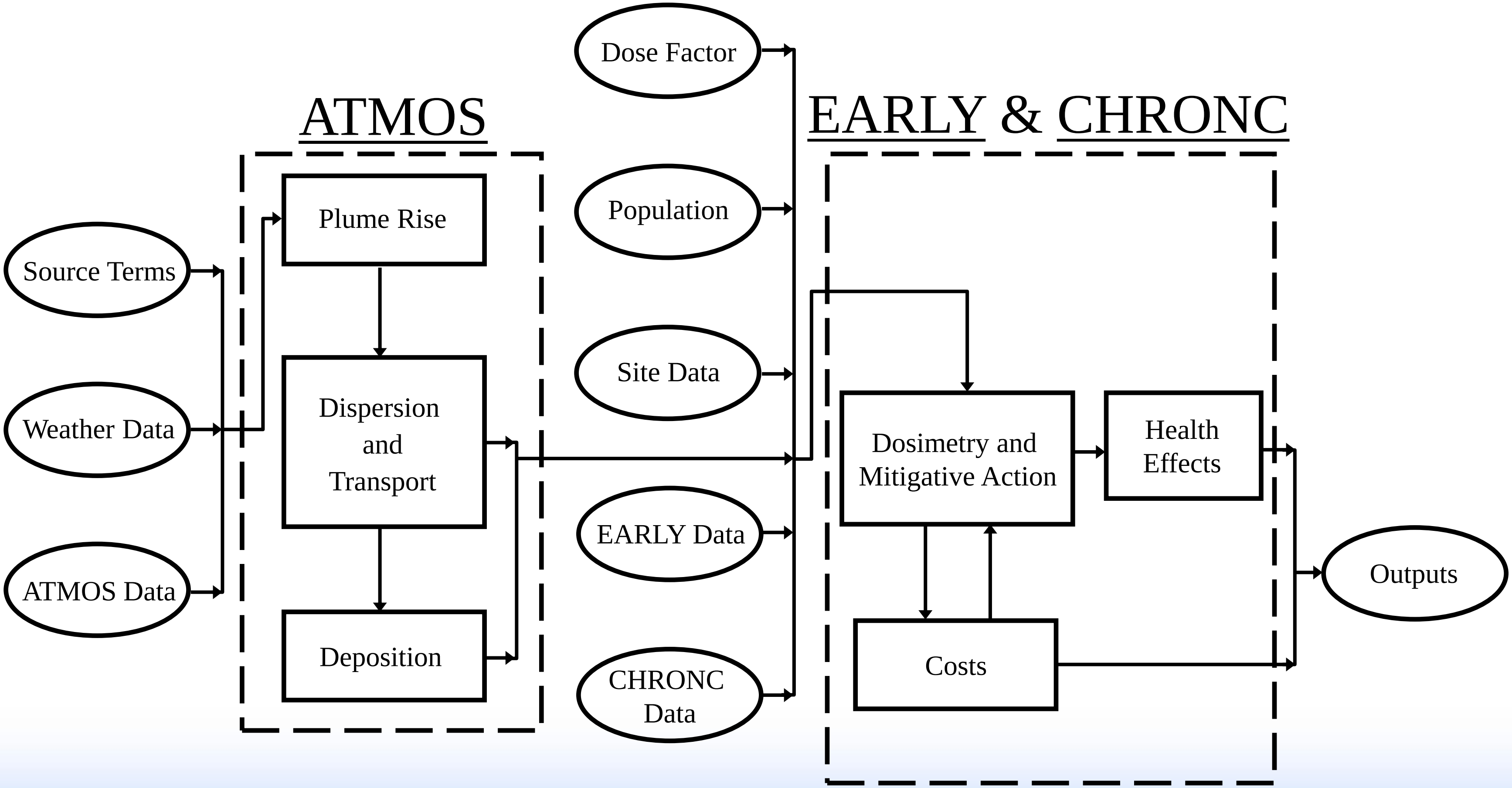
# Consequences

- Population dose
- Acute effects
  - Number of fatalities, injuries, and illnesses occurring within one year due to initial exposure to radioactivity; nonlinear with dose equivalent
- Latent effects
  - Number of delayed effects and time of appearance as functions of dose for various organs; linear, no-threshold model typically used

# Consequence Evaluation Models

- MACCS (MELCOR Accident Consequence Code System)
  - MACCS2 is now available
  - Successor to CRAC/CRAC2
- Improved environmental transport, dosimetry, health effects, and economic cost models
- Improved wet deposition model for rainout
- Dependence of dry deposition velocity on particle size
- Multi-plume dispersion model including multi-step crosswind concentration profile
- Improved code architecture

# MACCS Modeling Diagram



# Dominant Risk Contributors Sometimes Not Dominant With Respect to CDF

- For PWRs, SGTR and bypass sequences (e.g., ISLOCA) dominate LERF and therefore early fatalities
- SGTR and bypass not dominant contributors to core damage frequency
  - If SGTR or bypass occur, consequences are large
  - Remember: risk = frequency × consequence

# Review of Accident Progression & Consequence Analysis

**Key Points of Section:**

- Three levels of PRA:
  - Level 1: Accident frequency
  - Level 2: Accident progression, containment response
  - Level 3: Offsite consequences
- Four steps to Accident Progression Analysis:
  - Develop APETs
  - Perform structural analysis of containment
  - Quantify APET issues
  - Group sequences into accident progression bins
- Several factors are involved in containment response such as pressure, heat, fission products, steam and water, hydrogen
- Components of a consequence model include: atmospheric transport, pathway models, dosimetry models, health effects model (acute and latent effects), economic effects, evacuation, etc.

For more information on accident progression analysis, see P-300 course

For more information on accident consequence analysis, see P-301 course

For more information on accident phenomenology, see R-800 course

Page Intentionally Left Blank

# 10. External Events

# External Events

- **Purpose: This topic will acquaint students with the definition of external events and the IPEEEs.**
- **Objectives:**
  - **Define external events and understand how they differ from internal events**
  - **List several of the more significant external events, including those analyzed in the IPEEEs**
  - **Know acceptable approaches for seismic events and fires to meet objectives of the IPEEE**
  - **Explain the ways in which external events may be evaluated and how this evaluation is related to the overall PRA task flow.**
- **References:**
  - **ANSI/ANS Std. 58.21-2007 (External Events PRA Standard)**
  - **NUREG/CR-6850 (fire PRA methodology)**

# Overview of External Events Analysis

- External Events (EE) refers to those events that are external to system being analyzed
  - Examples: fires, floods, earthquakes
    - Includes on-site events such as flooding of various rooms within plant
- EE are important and of concern due to their dependent nature, that is EE can both:
  - Initiate potential core damage accident; and
  - Fail or compromise the safety systems and/or procedures used to prevent or mitigate core damage accidents and consequences
- General approach
  - Identify hazard and its intensity
  - Estimate conditional failure probability of plant structure, systems, and components (SSCs)
  - Assess overall plant response to event

# NPP External Events Risk (first analyzed 1979)

- **1979 - Oyster Creek (first seismic PRA)**
- **1979 - HTGR (first fire PRA)**
- **1981 - Big Rock Point**
- **1982 - Zion/Indian Point**
- **1983 - NUREG/CR-2300, *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants* (includes external events)**
- **1988 - GL 88-20 (IPEs to include internal floods)**
- **1989 - NUREG-1150 (fire and seismic)**
- **1991 - GL-88-20, Supplement 4 (IPEEE, revised in 1995 with supplement 5, which revised seismic requirements)**

# Initial List of Potential External Event Hazards (1 of 2)

- Aircraft
- Avalanche
- *Earthquake
- *Fire in plant
- Fire outside plant but on site
- Fire off site
- Flammable fluid release
- Fog
- *Flooding, external (including seiche, storm surge, dam failure, and tsunami)
- **Flooding, internal
- *High winds (including tornadoes)
- Hurricane
- Ice
- Industrial or military accident offsite
- Landslide

*** Included in IPE*

** Included in IPEEE*

# Initial List of Potential External Event Hazards (2 of 2)

- Lightning
- Meteorite impact
- Pipeline accident
- Sabotage
- Ship impact
- Toxic gas release
- Transportation accident
- Turbine missile
- Volcanic activity
- Blizzard/Snow
- Drought
- Erosion
- Hail
- Heavy rain
- High temperature
- Low Temperature
- River diversion or change in lake level
- War

# Most Hazards Excluded for Various Reasons

- **IPEEE required analysis of hazards believed to dominate external event risk**
  - Seismic
  - Internal fires
  - High winds and tornadoes
  - External floods (internal flood analysis required in IPE)
  - Transportation and nearby facility accidents
  - Any known plant-unique hazards

# External Events Analyses Performed at Various Levels of Detail

- Seismic
  - Seismic PRA
    - Required for high-seismicity sites
  - Seismic margin assessment (calculates HCLPF - high confidence of low probability of failure)
- Fire
  - Fire PRA
  - Fire-Induced Vulnerability Evaluation (FIVE)
- Other
  - External Event PRA
  - Screening analysis

# Seismic Hazard PRA - 3 Basic Steps

- Hazard analysis (frequency-magnitude relationship for earthquakes)
  - Location-specific hazard curves produced by NRC (LLNL) and EPRI
  - New curves related by USGS in 2014
- Fragility analysis ("strength" of component)
  - Conditional probability of failure given a specific earthquake severity
- Accident sequence analysis

*Analysis process briefly looked at in following slides*

# Four Steps in Seismic Hazard Curve Development

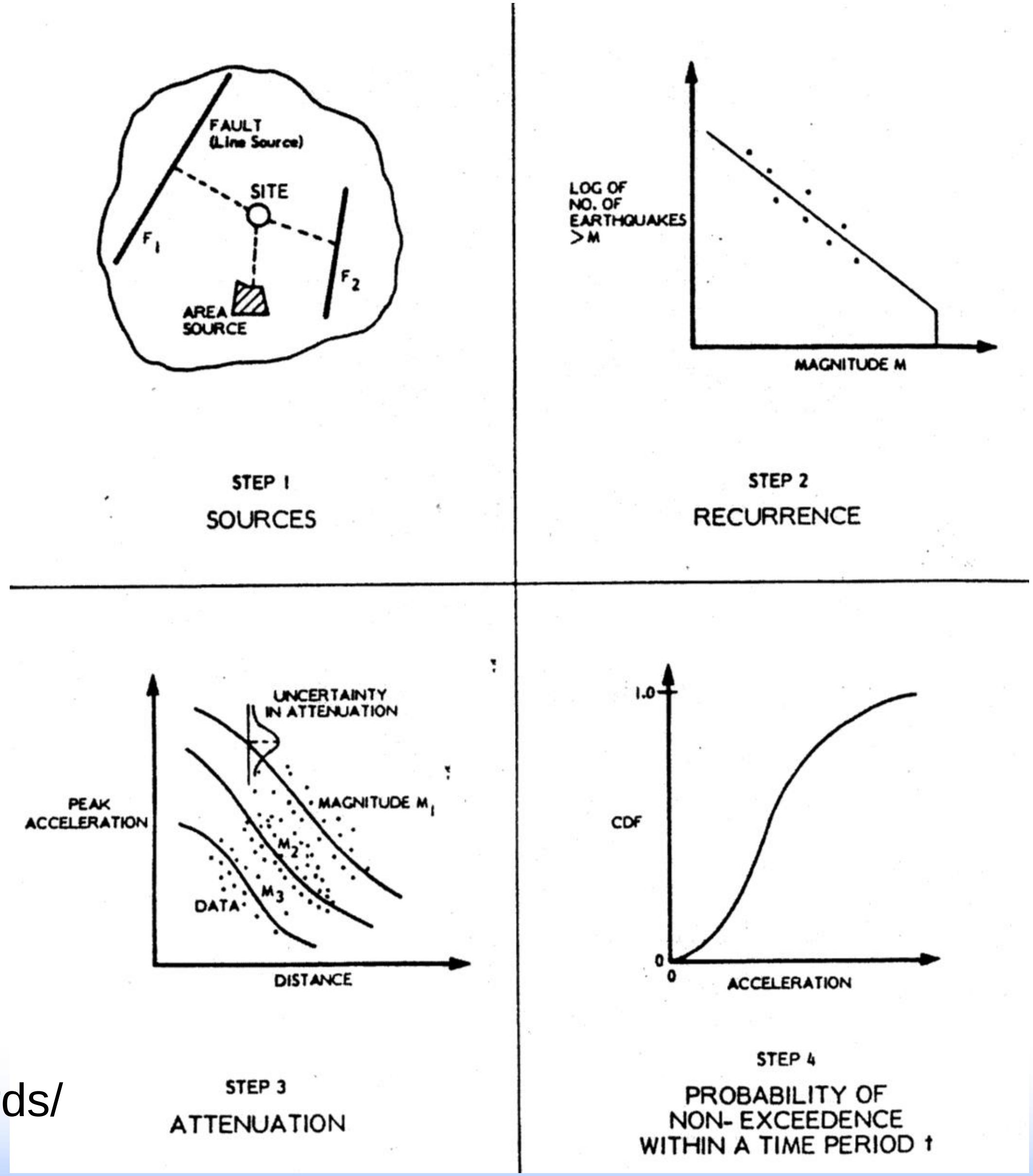
1. Identify seismic sources

2. Develop frequency-magnitude model for each source

3. Develop ground motion model for each source

4. Integrate over sources

http://earthquake.usgs.gov/hazards/



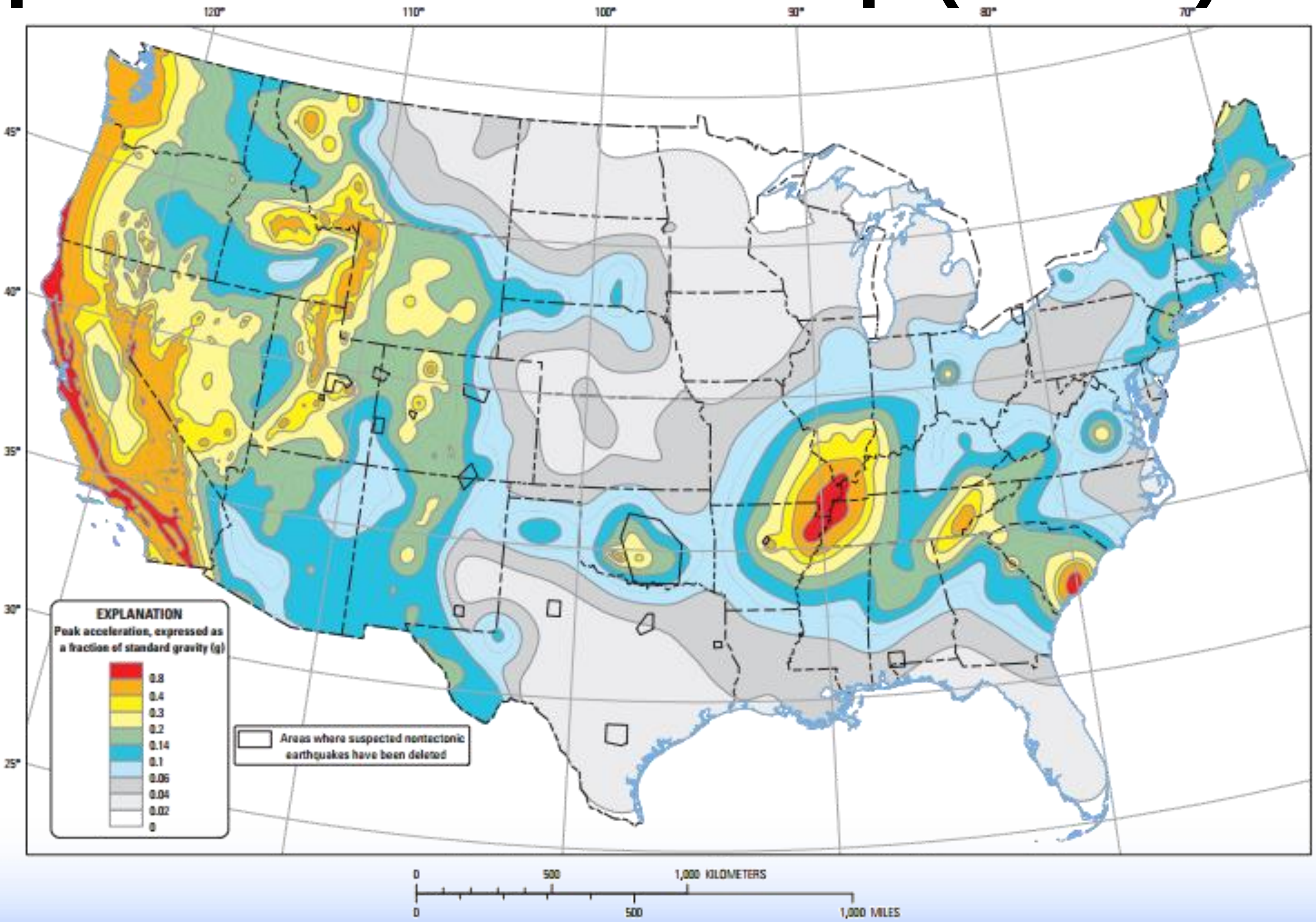
STEP 1
SOURCES

STEP 2
RECURRENCE

STEP 3
ATTENUATION

STEP 4
PROBABILITY OF NON- EXCEEDENCE WITHIN A TIME PERIOD t

# Updated US Hazard Map (USGS)


120°
110°
100°
90°
80°
70°
45°
40°
35°
30°
25°
EXPLANATION
Peak acceleration, expressed as a fraction of standard gravity (g)
0.8
0.4
0.3
0.2
0.14
0.1
0.06
0.04
0.02
0
Areas where suspected nontectonic earthquakes have been deleted
0
500
1,000 KILOMETERS
0
500
1,000 MILES

Two-percent probability of exceedance in 50 years map of peak ground acceleration

# Frequencies Estimated for Various Ground Acceleration Levels

- **Frequency of 0.1g, 0.2g, 0.3g, etc. earthquake estimated**
  - **This is the hazard curve**
- **Each g-level earthquake analyzed separately (i.e., as a separate and unique event)**
- **Failure probabilities of plant SSCs calculated based on g-level and fragility of SSC**
- **Internal events PRA re-evaluated using seismic failure probabilities (based upon g-level)**
  - **Core Damage (seismic) =** $\underbrace{f(\text{earthquake}_g)}_{\text{Hazard}} * \underbrace{Pr(\text{failures}_g)}_{\text{Fragility}}$

# Seismic Fragility Expressed in Terms of Peak Ground Acceleration

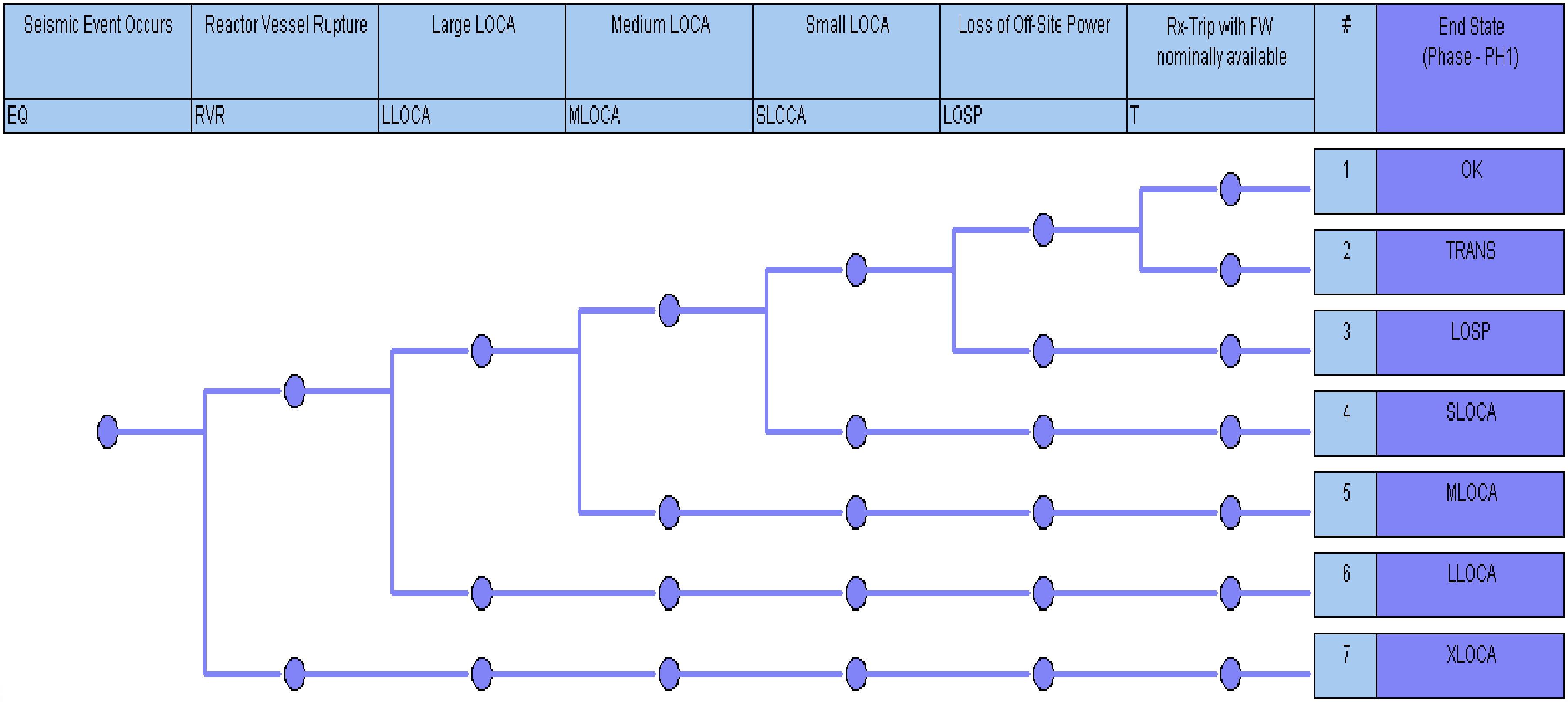
- **Fragility (A) = $A_m$ $\beta_R$ $\beta_U$ (lognormal model assumed)**
  - **$A_m$ = median ground acceleration capacity of SSC**
  - **$\beta_R$ $\beta_U$ = Measure of the uncertainty in median fragility due to randomness and confidence, respectively (can also be labeled aleatory and epistemic, respectively).**
  - **$A_m$ derived from various safety and response factors ($F_cF_{RE}F_{RS}A_{SSE}$), in turn are products of other factors**
    - **$F_C$ - Capacity Factor**
    - **$F_{RE}$ - Response factor for equipment**
    - **$F_{RS}$ - Response factor for structure**
    - **$A_{SSE}$ - Safe Shutdown Earthquake acceleration**

# Range of Seismic Fragilities for Selected Components*

| *Componenent/Structure* | *Dominant Failure Mode* | *Median Fragility Range (g)* |
|---|---|---|
| *Concrete containment building* | *Shear failure* | *2.50-9.20* |
| *Reactor Pressure Vessel* | *Anchor bolt* | *1.04-5.70* |
| *Flat-bottom tank* | *Shell wall buckling* | *0.20-1.00* |
| *Batteries and racks* | *Cases and plates* | *0.90-5.95* |
| *Motor control centers* | *Chattering* | *0.06-4.20* |
| *Diesel generator* | *Anchor bolt* | *0.70-3.89* |
| *Offsite power* | *Ceramic insulators* | *0.20-0.62* |

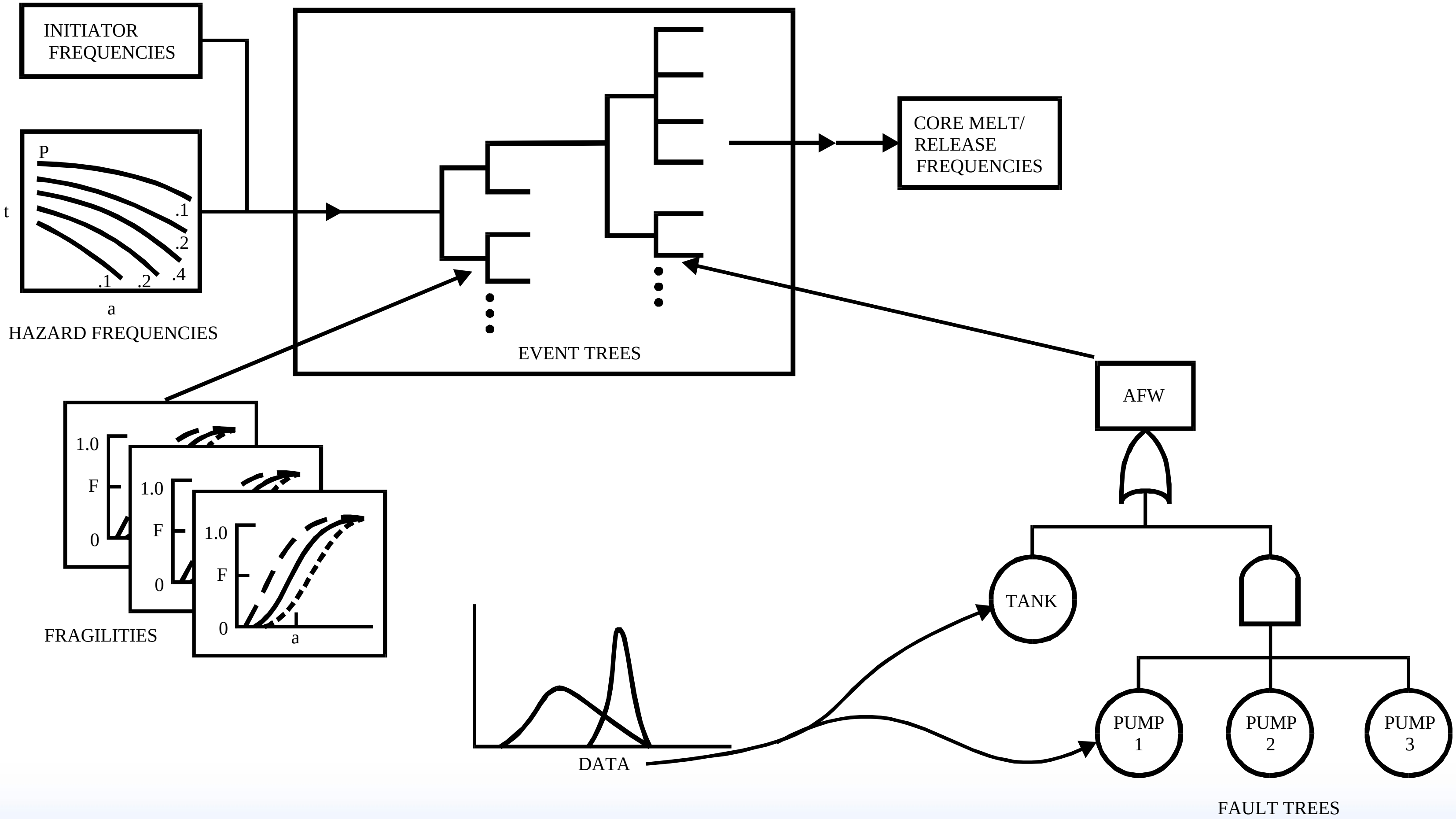
* *Y. J. Park, et al, Survey of Seismic Fragilities Using in PRA Studies of Nuclear Power Plants, Reliability Engineering and System Safety, Vol. 62, pages 185-195, 1998.*

# Probability of “Initiating Events” Estimated Given Occurrence of EE (Provides Link to Sequence Analysis)



| Seismic Event Occurs | Reactor Vessel Rupture | Large LOCA | Medium LOCA | Small LOCA | Loss of Off-Site Power | Rx-Trip with FW nominally available | # | End State (Phase - PH1) |
|---|---|---|---|---|---|---|---|---|
| EQ | RVR | LLOCA | MLOCA | SLOCA | LOSP | T | | |
| | | | | | | | 1 | OK |
| | | | | | | | 2 | TRANS |
| | | | | | | | 3 | LOSP |
| | | | | | | | 4 | SLOCA |
| | | | | | | | 5 | MLOCA |
| | | | | | | | 6 | LLOCA |
| | | | | | | | 7 | XLOCA |

# Seismic Analysis Approach



# Fire Analysis Follows Phased Approach

- Qualitative Screening
  - Fire in area does not cause a demand for reactor trip
  - Fire area does not contain safety-related equipment
  - Fire area does not have credible fire source or combustibles
- Quantitative Screening
  - Utilized existing internal events PRA
  - Estimate fire frequency for area and assume all equipment in fire area failed by fire, calculate CDF
- Detailed Analysis

SPAR-EE

# Detailed Fire Analysis Includes

- **Fire occurrence frequency assessment**
  - **Either location-based or component-based**
  - **Generic data updated with plant-specific experience**
- **Fire growth and propagation analysis**
  - **Considers**
    - **Combustible loading**
    - **Fire barriers**
    - **Fire suppression**
  - **Modeled with specialized computer codes (COMPBRN IIIe)**
- **Component fragilities and failure mode evaluation**
- **Fire detection and suppression modeling**
- **Detailed fire scenarios analyzed using transient event tree**

# Fire-Induced Vulnerability Evaluation (FIVE)

- Developed by EPRI as an alternative to a fire PRA for satisfying IPEEE requirements
- Equivalent to a fire-area screening analysis
  - Worksheet-based systematic evaluation using information from Appendix R implementation
  - Does not produce detailed quantification of fire CDF
- Most FIVE users (IPEEE) also quantified fire CDF of unscreened areas

# Current Activities in External Events PRA

- NFPA Std. 805 issued
- Many plants updating fire PRAs to meet NFPA standard
  - Risk-informing 10 CFR 50, App. R
- NUREG/CR-6850 documents updated fire PRA guidance
- Research ongoing for outstanding issues
  - Multiple spurious actuations
  - Hot shorts of cabling
  - Some final reports (NUREG/CR-7010, 7150, 2128)
- NRC expanding SPAR models to include external events

# Other External Events Analyzed Using Structured Screening Process

- IPEEE Guidance - Progressive Screening approach (see Figure 5.1 of NUREG-1407)
  - Review plant-specific hazard data and licensing basis (FSAR)
  - Identify significant changes, if any, since operating license issuance
  - Does plant/facility design meet 1975 SRP criteria (via quick screening & confirmatory walkdown)
    - If yes, no further analysis is needed
    - If no, continue analysis (next slide)

***Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants LWR Edition (NUREG-0800, Formerly issued as NUREG-75/087)**

# Examples of SRP Non-Conformance

- Flood
  - Probable Maximum Precipitation (PMP) at site based on old National Weather Service data
- High-Wind/Tornado
  - Design basis tornado missile spectrum different from that specified in SRP

# If 1975 SRP Criteria Not Met

- Is Hazard Frequency Acceptably Low (<1E-5/yr)?

  If Not:

- Does bounding analysis estimate CDF <1E-6/yr?

  If Not:

- Perform detailed PRA
  - Details of analysis are tailored to particular hazard

# Review of External Events

**Key Points of Section:**

- **External events refers to those events that are external to systems being analyzed. Includes fires, floods and earthquakes.**
- **General approach to External Events Analysis: Identify the hazard and its intensity, perform a conditional probability calculation of plant SSCs failure, and assess overall plant response to the event.**
- **Acceptable approaches (for IPEEE requirements):**
  - **For seismic analyses- Seismic PRA and Seismic Margins Assessment.**
  - **For fire analyses: Fire PRA and Fire-Induced Vulnerability Evaluation.**
  - **For other hazard analyses: External Event PRA, Screening analysis.**

**For more information on external events, see P-204 course**

# 11. Low-Power and Shutdown Risk

# Low-Power and Shutdown Risk

- Purpose: Discusses why low-power and shutdown modes of operation are of concern from a risk perspective, and how a SD PRA is organized.
- Objective: Understand the reasons for quantifying LP/SD risk and the issues of concern.
- References:
  - NUREG-1449 - Review of shutdown events
  - NUREG/CR-6143 and -6144 - Analysis of low-power shutdown risks at Grand Gulf and Surry, respectively
  - NUREG/CR-6616 - Risk comparison of scheduling preventive maintenance at shutdown versus at power operation for PWRs
  - SPAR LPSD models
  - Draft ANSI/ANS Std. for LPSD PRA

# Risk From Low-Power and Shutdown Operations Was Not Considered in Early PRAs

- **Low-power and shutdown (LPSD) encompasses operation when the reactor is subcritical or in transition between subcriticality and power operations up to ~15% of rated power**
- **In early risk studies, risk from full-power operation was assumed to be dominant because during shutdown:**
  - **Reactor is subcritical**
  - **Decay heat decreases with time**
    - **Longer time is available to respond to accidents**

# LPSD Operational Events Established the Significance of LPSD Risk

- Precursor events implied that potential generic vulnerabilities existed:
  - April 87 Diablo Canyon event resulting in loss of RHR while in hot mid-loop operation (and numerous similar events at other plants)
  - March 90 Vogtle plant loss of all AC power while shutdown
  - Numerous precursors to interfacing system LOCA during shutdown or startup
    - Led to GSI-105
  - Two generic letters were subsequently issued relating to low-power and shutdown operations:
    - GL 87-12 -- Loss of RHR while the RCS is partially filled
    - GL 88-17 -- Loss of Decay Heat Removal

# Other Factors Also Contribute to LPSD Risk

- Some systems may not be available since Tech. Specs. allow more equipment to be inoperable during LPSD than at power
- LPSD initiating events (by definition) impact the operable train of decay heat removal systems
  - IE for LPSD is a loss of shutdown cooling
- Human errors are more likely because of the increase in activity during shutdown
  - Unusual equipment line-ups also make mistakes more likely
  - Less procedural control during LPSD
  - Plant instruments and indications may not be available or accurate

# NRC Staff's Evaluation of LPSD Risk

- **Vogtle (1990) SBO investigation motivated broader look at LP/SD risk (NUREG-1449)**
  - **Study published in Sept 1993 documented significant technical findings including:**
    - **Outage planning is crucial to safety during LPSD**
    - **Significant maintenance activities increase potential for fires during shutdown**
    - **PWRs are more likely to experience events than BWRs; dominant contributor to PWRs is loss of RHR during operations with reduced inventory (midloop operation)**
    - **Extended loss of RHR in PWRs can lead to LOCAs caused by failure of temporary pressure boundaries in RCS or rupture of RHR system piping**

# LPSD Risk Focuses on Non-Power Operations

- Typical full-power PRA's examine plant risks associated with steady-state power operation (i.e., Mode 1)
  - Component unavailability and unreliability estimates based on Mode-1 Technical Specifications
- LPSD PRA considers all other operating modes
  - More complicated since plant can be in different states and configurations
  - Decay heat is a function of time after reactor shutdown (affects time available for recovery)

# PWR Operating Modes (Westinghouse Standard Tech. Specs.)

| Mode | Title | $K_{eff}$ | Thermal Power[a] | Ave. Coolant Temp. (°F) |
|---|---|---|---|---|
| 1 | Power Ops | ≥ 0.99 | > 5% | NA |
| 2 | Startup | ≥ 0.99 | ≤ 5% | NA |
| 3 | Hot Standby | < 0.99 | NA | ≥ 350 |
| 4 | Hot Shutdown[b] | < 0.99 | NA | 350 > T > 200 |
| 5 | Cold Shutdown[b] | < 0.99 | NA | ≤ 200 |
| 6 | Refueling[c] | NA | NA | NA |

a. Excluding decay heat

b. All reactor head bolts fully tensioned

c. One or more reactor head bolts less then fully tensioned

# BWR Operating Modes (BWR/4 Standard Tech. Specs.)

| Mode | Title | Reactor Mode Switch Position | Ave. Coolant Temp. (°F) |
|---|---|---|---|
| 1 | Power Ops | Run | NA |
| 2 | Startup | Refuel[a] or Startup/Hot-Standby | NA |
| 3 | Hot Shutdown[a] | Shutdown | > 200 |
| 4 | Cold Shutdown[a] | Shutdown | ≤ 200 |
| 5 | Refueling[b] | Shutdown or Refuel | NA |

a. All reactor head bolts fully tensioned

b. One or more reactor head bolts less then fully tensioned

# LPSD PRA Structured Around Plant Operating State

- PRA models (event trees and fault trees) developed for each plant operating state (POS) and each initiating event
  - SPAR model IE identifier
    - SD-M4-LOI, SD-M5-LORHR, SD-ML-LOOP, etc.
      - SD is shutdown mode of operation
      - M is mode of operation (4, 5 mid-loop)
      - LOI, LORHR, LOOP initiating event type
  - Data can be POS-dependent as well
    - Test or maintenance unavailability changes as Tech Specs change according to operating mode

# SPAR Plant Operating States (POSs)

| Standard Technical Specification Mode (SPAR POS) | POS Description | Technical Specification Mode Description |
|---|---|---|
| 1 | Low power and reactor shutdown | Power operation |
| 3 | Cooldown with SGs from operating temp to 345°F | Hot standby |
| 4 (4E) | Cooldown with RHR from 345°F to 200°F | Hot shutdown |
| 5 (5EF) | Cooldown with RHR below ~200°F | Cold shutdown |
| 5 (5EF) | Draining RCS to mid-loop | Cold shutdown |
| 5 (5ER) | Mid-loop operation | Cold shutdown |
| 6 (6) | Fill for refueling | Refueling |
| 6 (6) | Refueling | Refueling |
| 6 (6) | Draining RCS to mid-loop after refueling | Refueling |
| 5 (5LR) | Mid-loop operations after refueling | Cold shutdown |
| 5 (5LF) | Refilling RCS | Cold shutdown |
| 5 (5LF) | RCS heatup solid and draw bubble | Cold shutdown |
| 4 (4L) | RCS heatup to 350°F | Hot shutdown |
| 2 | RCS heatup with SGs available (above 350°F) | Startup |
| 1 | Startup and low power operations | Power operation |

# PRAs Analyze LPSD Operating Modes

- Typically include only time spent using shutdown cooling (SDC) systems, not normal power conversion system (PCS)
  - Difficult to analyze all possible operating modes and configurations
  - Time spent at low power and using PCS is short (few hours per year) compared to normal at-power operation (months per year) and SDC operation (weeks per year)
  - Also, low power ops using PCS still has all systems nominally available (at-power Tech Specs apply)
  - Therefore, risk associated with these transition states is assumed to be small compared to at-power and SD.

# Subsequent LPSD PRA Studies

- LPSD risks not studied as extensively as those for power operation
- However, several LPSD PRAs have been completed
  - Both for PWRs and BWRs (e.g., Zion, Seabrook, Surry, Grand Gulf)
  - Significant findings include:
    - CDF estimates for certain shutdown modes of operation are comparable to estimates for full-power operation
  - Some SPAR model LP/SD models completed

# Subsequent PRA Studies

- **Most significant issues identified from a LPSD risk perspective are:**
  - **Mid-loop operation (PWRs) of particular concern**
  - **Operator errors, especially**
    - **failure to determine proper actions to restore shutdown cooling**
    - **procedural deficiencies**
  - **Loss of RHR shutdown cooling, especially**
    - **operator induced**
    - **suction valve trips**
    - **cavitation due to overdraining of the RCS**
  - **Loss of offsite power**

# SPAR Program Developing Limited Number of LPSD Models

- 10 LPSD SPAR models available
- Initiating events include:
  - Loss of RHR
  - Loss of RHR given primary reactor coolant is at reduced inventory level
  - Loss of offsite power
  - Loss of primary reactor coolant Inventory

# Few LPSD PRAs Have Been Developed

- Perception continues that LPSD operations pose less risk than full-power
- LPSD PRA developed reputation of being very expensive and complicated process
  - NUREG/CR-6143, “Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1," July 1995
  - NUREG/CR-6144, “Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1," October 1995
- Most utilities have opted to manage LPSD risk using simpler configuration management approach
  - Vital safety functions defined - systems/trains needed to perform vital safety function maintained in-service

# How Utilities are Addressing LPSD Risk

- Some utilities have performed limited PRA studies of selected modes of operation
- Most utilities have adopted non-PRA approach
  - Approach based on guidance in NUMARC 91-06
  - Approach based on maintaining barriers during shutdown
  - EPRI sponsored development of ORAM (Outage Risk Assessment and Management) software to implement this approach

# Review of Low-Power and Shutdown Risk

- Key Points of Section:
  - Low-power and shutdown encompasses operation when the reactor is subcritical or in power operations below approximately 15% of rated power
  - Precursor events and operating experience insights exposed  the potential vulnerabilities that exist during LPSD
  - Currently, LPSD risks are not studied as extensively as those for power operation
  - NRC is working on developing LPSD SPAR models

# Section II. PRA Applications

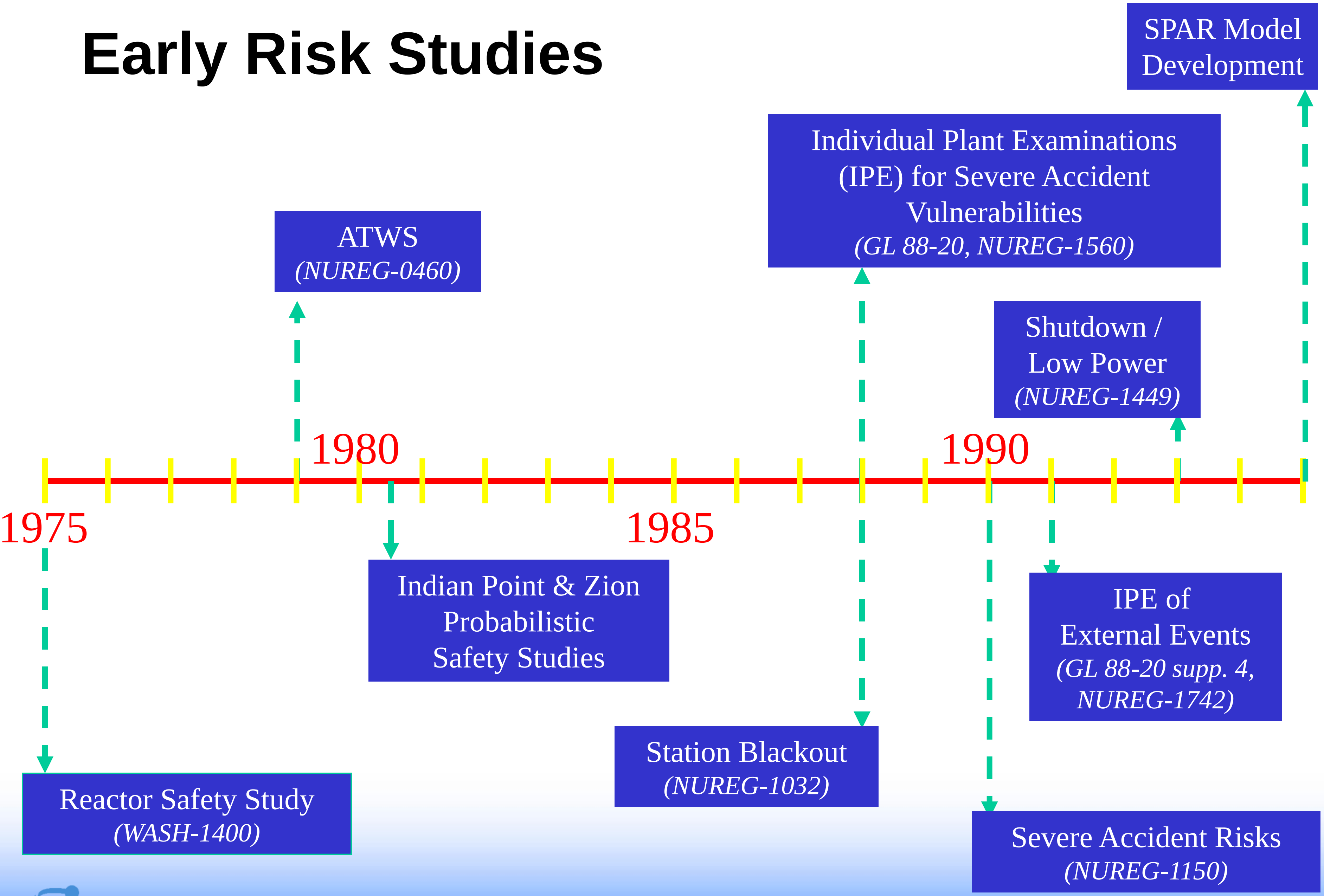
# PRA Timeline (history)

- **Congress establishes the Atomic Energy Commission (AEC) as part of the Atomic Energy Act (AEA) of 1946 for the responsibility of nuclear regulation, highlighted military aspects of nuclear energy and the need for secrecy and excluded commercial applications of atomic energy**
- **Congress replaces 1946 Act with the Atomic Energy Act of 1954 which made the commercial development of nuclear power possible**
- **WASH-740 (1957), first comprehensive look at consequences, 200 MW class of reactors in operation at the time and focused on large loss of coolant accidents (LLOCA)**
- **Energy Reorganization Act of 1974 created the Nuclear Regulatory Commission which assumed responsibility for civilian nuclear power regulation and assuring the protection of public health and safety**
- **WASH-1400 (1975), known as the Reactor Safety Study or better known as the Rasmussen Report (study started in 1972).**
- **TMI accident (1979)**
- **Plant owners completed PRAs; Zion (1981) and Indian Point -2 and -3 (1982)**

# PRA Timeline (history)

- NUREG/CR-2300: PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants; 1983
- 51FR30028 Safety Goal Policy Statement (1986); NRC provides additional guidance in 1990 regarding the Safety Goal, endorsing surrogate objectives concerning CDF and LERF
- NUREG-1150 (started in 1986 and published 1990)
- GL 88-20 (1988) IPE (completed PRAs by 1992)
- Supplement 4 to GL 88-20 (1991)
- NRC published 10 CFR 50.65 on July 10, 1991; nine pilot plants 1994 - 1995 ; Maintenance Rule becomes effective July 1996
- NRC issues its PRA Policy Statement in 1995
- SPAR Model development using “Daily Events Manual” (1995)
- NRC published series of Regulatory Guides in 1998 which adopted Risk-Informed Regulation
- NRC introduces its new Reactor Oversight Process in 1998

# Early Risk Studies



Reactor Safety Study
*(WASH-1400)*

ATWS
*(NUREG-0460)*

Indian Point & Zion Probabilistic Safety Studies

Station Blackout
*(NUREG-1032)*

Individual Plant Examinations (IPE) for Severe Accident Vulnerabilities
*(GL 88-20, NUREG-1560)*

Severe Accident Risks
*(NUREG-1150)*

IPE of External Events
*(GL 88-20 supp. 4, NUREG-1742)*

Shutdown / Low Power
*(NUREG-1449)*

SPAR Model Development

# PRA Timeline (history)

- **Reference:**
  - **Reliability Engineering and System Safety, 89 (2005), pg. 271 – 285, “A historical overview of PRA development and its use in the nuclear power industry: a tribute to the late Professor Norman Rasmussen”**

# Page Intentionally Left Blank

# 12. PRA Models –

## Generic Letter 88-20 Individual Plant Examinations (IPEs) and Individual Plant Examination for External Events (IPEEEs) and

## NRC Standardized Plant Analysis Risk Model (SPAR)

# PRA Models (history)

- Purpose: Discuss the scope, purpose, and requirements of GL 88-20 along with background information about the SPAR models.
- Objectives: At the conclusion of this topic, students will be able to:
  - Discuss GL 88-20 (scope, purpose, & requirements)
  - Describe differences between IPE and IPEEE
  - Identify intended uses of IPE and IPEEE
  - Background of SPAR Models
- References
  - GL 88-20
  - NUREG-1335, IPE Submittal Guidance
  - NUREG-1407, IPEEE Submittal Guidance
  - NUREG-1560, Perspectives Gained From IPE Program
  - NUREG-1742, Perspectives Gained From IPEEE Program

# Brief History of GL 88-20

- **1988-November: GL 88-20 issued requesting IPEs**
- **1989-August: GL 88-20 Supplement 1**
  - **Availability of NUREG-1335 – IPE Submittal Guidance**
- **1990-April: GL 88-20 Supplement 2**
  - **List of severe accident management strategies to consider in IPE (NUREG/CR-5474)**
- **1990-July: GL 88-20 Supplement 3**
  - **Announced completion of NRC Containment Performance Improvement (CPI) program**
- **1991-June: GL 88-20 Supplement 4**
  - **IPE for External Events (IPEEE)**
- **1995-Sept: GL 88-20 Supplement 5**
  - **Modified recommended scope of seismic analysis to include revised seismic hazard curves (NUREG-1488, "Revised Livermore Seismic Hazard Estimates for 69 Sites East of the Rocky Mountains," April 1994)**

# Purposes of IPEs/IPEEEs

- Systematically examine plant design, operation, and emergency operation
- Identify plant-specific vulnerabilities to severe accidents and possible scenarios
- Develop understanding of what could possibly go wrong in a plant
- Identify and evaluate means for improving plant and containment performance with respect to severe accidents
- Decide which of these improvements to implement and when
- Perform this examination for selected external events (IPEEE) (Supplement 4 to GL 88-20)

# Intent of IPEs (& IPEEES) was for Utilities to:

- Identify/understand potential severe accidents
- Evaluate/implement potential plant improvements
- Develop understanding of severe accident behavior
- Develop awareness of inherent margins “beyond design basis” and how to utilize these margins to manage/mitigate consequences of severe accidents

# IPEs (& IPEEEs) did not Require PRA

- All utilities chose to perform a PRA to address GL 88-20
  - PRAs were not performed to any specific standards
    - No requirements specified for data or models
- Not all utilities used PRAs to analyze external events
  - Earthquakes and fires can be analyzed via margins approach
- IPE submittal typically not a full PRA (level of detail varies widely, only full-power operation considered)
- IPEs not performed to support risk-informed, performance-based regulation

# Intended NRC Staff Uses of IPE Results

- Vulnerabilities that exist due to failure to meet NRC regulations to be corrected regardless of cost
- Enhancements to safety beyond current NRC regulations to be evaluated in accordance with 10 CFR 50.109 (Backfit Rule)
- Generic vulnerabilities evaluated to determine if existing regulations are adequate
  - Specifically: USI A-45, Shutdown Decay Heat Removal
  - In general: any other USIs or GSIs licensee choose to address

# Use of IPE Models and Results in Risk-Informed, Performance-Based Regulation

- Would require quality review of IPE models and data
  - NRC reviewed IPEs to ensure requirements of GL 88-20 were met by licensee submittal
  - Reviews did not validate modeling assumptions, input data, or results
  - Staff Evaluation Report (SER), and sometimes Technical Evaluation Report (TER) issued for each IPE

# IPE Results – NUREG-1560

- Few licensees explicitly identified vulnerabilities
  - 4 BWRs and 15 PWRs
- Almost all identified plant improvements
  - over 500 improvements proposed

    ~ 45% procedural/operational

    ~ 40% design/hardware

    some both

# BWR Vulnerabilities Identified

- Failure of water supplies to isolation condenser
- Failure to maintain HPCI and RCIC when RHR has failed
- Failure to control LPSI during ATWS
- Drywell steel liner melt-through for Mark-I containment

# PWR Vulnerabilities Identified

- Loss of RCP seals
- Turbine-driven AFW pump reliability
- Internal flooding caused by component failures
- Failure of operator to switch from HPI/LPI to HPR/LPR
- Loss of switchgear ventilation (leads to loss of bus)
- Operator failure to depressurize RCS during SGTR
- Inadequate surveillance of pressure isolation valves (increased likelihood of ISLOCA)
- Loss of specific electrical buses
- Compressed air system failures
- Inability to cross-tie electrical buses during loss of power

# Range of CDFs Reported in IPEs

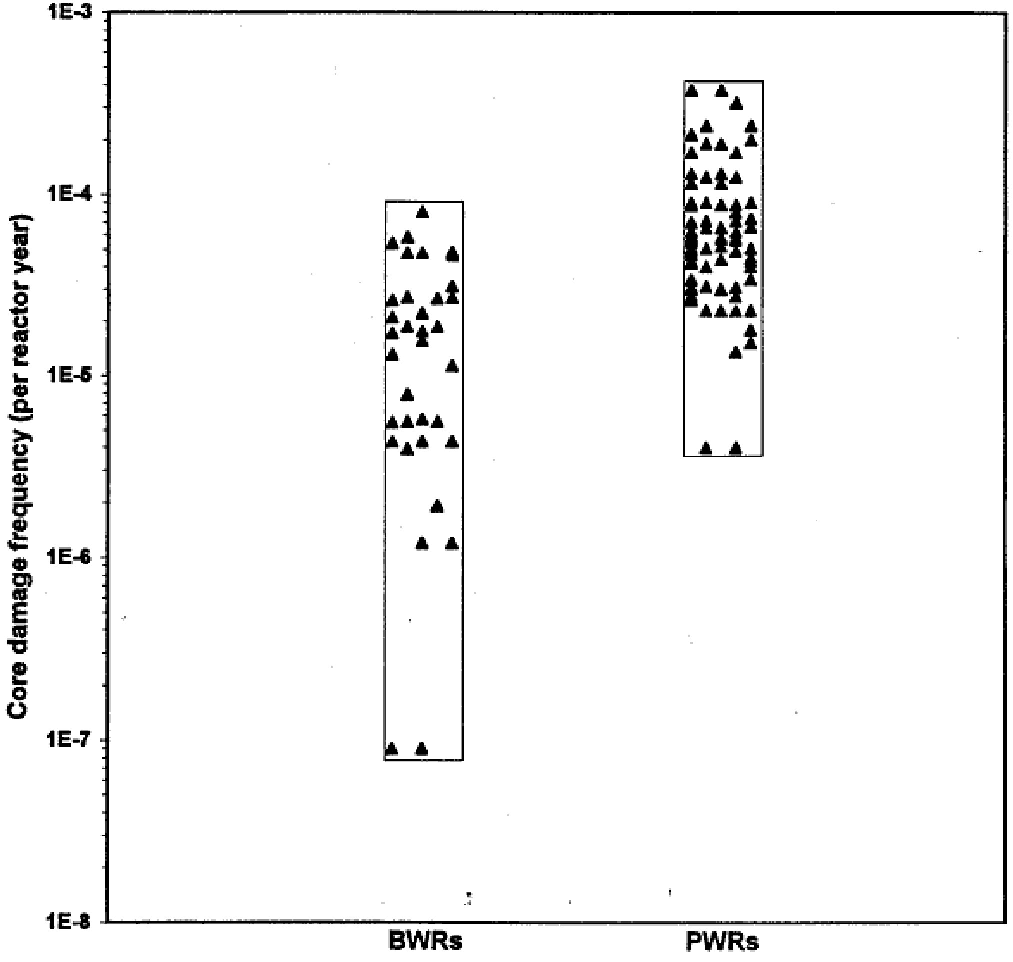


Figure E.1 Summary of BWR and PWR CDFs as reported in the IPEs.

# Range of CCFPs Reported in IPEs

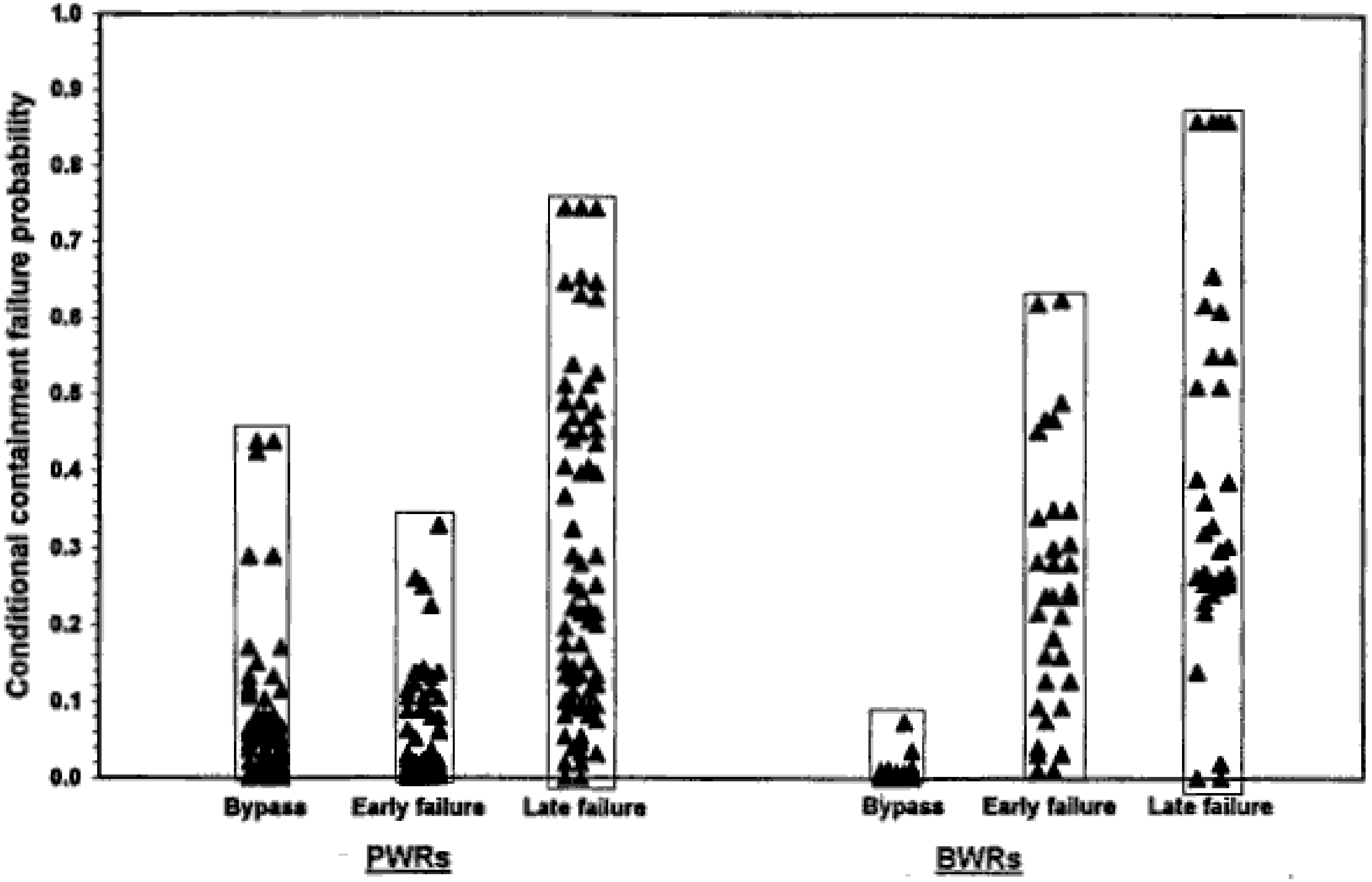
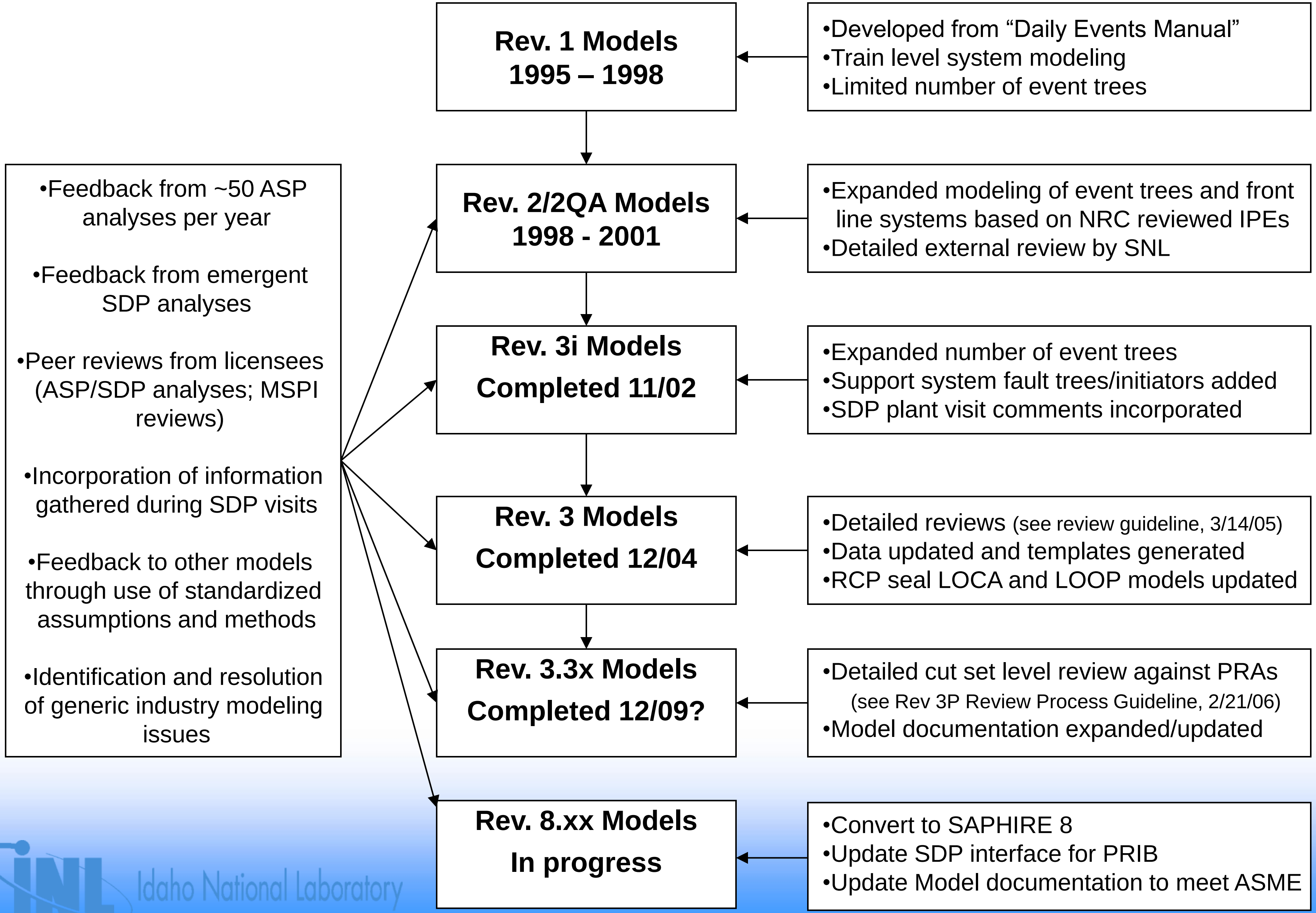


Figure E.2 Summary of conditional containment failure probabilities for BWRs and PWRs as reported in the IPEs.

# SPAR Models - Background

- History
  - Project started in the early 1990’s
  - Series of progressive enhancements yield rev 3 models
    - Then SPAR  = simplified plant analysis risk
    - Now SPAR = standardized plant analysis risk
    - Current version 8.xx
- 72 plant specific SPAR models covering 103 nuclear plants
  - Boolean logic used to quantify risk of core damage
  - Models quantified using SAPHIRE code
  - ~1000 basic events in SPAR models vs ~2000 in PSAs

# SPAR Model Development



**Rev. 1 Models**
**1995 – 1998**

- •Developed from “Daily Events Manual”
- •Train level system modeling
- •Limited number of event trees

**Rev. 2/2QA Models**
**1998 - 2001**

- •Expanded modeling of event trees and front line systems based on NRC reviewed IPEs
- •Detailed external review by SNL

**Rev. 3i Models**
**Completed 11/02**

- •Expanded number of event trees
- •Support system fault trees/initiators added
- •SDP plant visit comments incorporated

**Rev. 3 Models**
**Completed 12/04**

- •Detailed reviews (see review guideline, 3/14/05)
- •Data updated and templates generated
- •RCP seal LOCA and LOOP models updated

**Rev. 3.3x Models**
**Completed 12/09?**

- •Detailed cut set level review against PRAs (see Rev 3P Review Process Guideline, 2/21/06)
- •Model documentation expanded/updated

**Rev. 8.xx Models**
**In progress**

- •Convert to SAPHIRE 8
- •Update SDP interface for PRIB
- •Update Model documentation to meet ASME

- •Feedback from ~50 ASP analyses per year
- •Feedback from emergent SDP analyses
- •Peer reviews from licensees (ASP/SDP analyses; MSPI reviews)
- •Incorporation of information gathered during SDP visits
- •Feedback to other models through use of standardized assumptions and methods
- •Identification and resolution of generic industry modeling issues

# Standardized Structure

- Standardized Plant Analysis Risk (SPAR) Models
  - Evolution of the models
    - Initially a plant-specific implementation of the Daily Events Manual event trees.
    - Revision 2QA – Peer review by SNL, largely subcontracted to SAIC
    - Revision 3I (interim) – Upgraded during SDP notebook review process
    - Revision 3E (enhanced) – New Seal LOCA model, updated data/templates, updated LOOP/SBO
    - Revision 3P (plus) – Cut set level review
    - Revision 8.xx – SAPHIRE 8 conversion and continued updates to LOOP model, SDP interface, general maintenance

# Standardized Structure - continued

- Standardized elements of the SPAR models
  - Methodology
  - Assumptions
  - Initiating events (based on NUREG/CR-5750)
    - (Added PRA specific initiating events if they contribute >1% to overall CDF)
  - Event trees (based on peer reviewed class models and consensus elements of PSAs)
  - Fault trees (based on published system studies when possible)

# Standardized Structure - continued

- Standardized elements of the SPAR models - cont
  - Failure data
    - EPIX based template set (1998 – 2002)
      - Continually being updated (2005 – 2010)
    - Common cause failures
      - Methods (NUREG/CR-5485)
        - Will be updated based on latest Draft CCF NUREG.
      - Data (NPRDS, LERs, EPIX) (1990 – 2001)
    - Loss of offsite power frequency/recovery data (NUREG/CR-5496, 2005 Update to 5496)
  - Human reliability analysis and recovery modeling (SPAR-H, NUREG/CR-6883)

# How SPAR Models Are Used

- Accident Sequence Precursor (ASP) program
  - Yearly summary of risk significant events
- Significance Determination Program (SDP)
  - Real-time risk evaluation of plant events
- Mitigating Systems Performance Indicator (MSPI)
  - Real-time risk evaluation of equipment performance
- Various other programs:
  - Generic Safety Issues
  - License Amendment Reviews
  - Special Studies (e.g., LOOP/SBO)
  - Trending Studies

# Review of Generic Letter 88-20 IPEs and IPEEEs and SPAR Models

- **Key Points of Section:**
  - **Purpose of IPEs/IPEEEs:**
    - **Systematically examine plant design and operation.**
    - **Identify plant vulnerabilities.**
    - **Understand what could possibly go wrong**
    - **Study ways to improve plant and containment performance and decide which to implement.**
    - **Look at selected external events.**
  - **Intent of IPEs and IPEEEs with respect to utilities:**
    - **Understand potential severe accidents.**
    - **Study potential plant improvements.**
    - **Develop an awareness of safety margins.**
  - **Intent of IPEs and IPEEEs with respect to the NRC:**
    - **Correct vulnerabilities due to failure to meet NRC regulations.**
    - **Improve safety beyond current NRC regulations.**
    - **Evaluate vulnerabilities to improve existing regulations.**
  - **SPAR Model Background**

# 13. Introduction to Risk-Informed Regulation

# Introduction to Risk-Informed Regulation

- **Purpose: Students will be introduced to the NRC PRA Policy Statement, Risk-informed, Performance-based Plan (RPP), concepts of risk-informed regulation, and potential PRA applications.**
- **Objectives:**
  - – **Understand the NRC PRA Policy Statement**
  - – **Understand Risk-Informed Performance-Based Plan**
  - – **Understand general concepts of risk-informed regulation**
  - – **List potential PRA applications**

# PRA Policy Statement (1995)

- General Objectives
  - Improve regulatory decision making and, therefore, safety
  - Make more efficient use of Staff resources
  - Reduce unnecessary regulatory burden on industry

# PRA Policy Statement

- Use of PRA technology should be **increased** in all Regulatory matters to the extent supported by **state-of-the-art** in PRA methods and data and in a manner that **complements** the NRC's **deterministic approach** and supports the NRC's traditional **defense-in-depth philosophy**
- PRA and associated analyses should be used in Regulatory matters, where practical **within the bounds of state-of-the-art**, to **reduce unnecessary conservatism** associated with current Regulatory requirements, Regulatory guides, License commitments, and staff practices. Where appropriate, PRA should be used to **support** the **proposal for additional Regulatory requirements** in accordance with 10 CFR 50.109 (Backfit Rule). The existing rules and regulations shall be complied with unless these rules and regulations are revised.

# PRA Policy Statement (continued)

- PRA evaluations in **support** of **Regulatory decisions** should be as **realistic as practicable** and **appropriate supporting data** should be publicly available for review.
- The **Commission's safety goals** for nuclear power plants and **subsidiary numerical objectives** are to be used with appropriate consideration of **uncertainties** in making **regulatory judgments** on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

# PRA Implementation Plan - Overall Objectives and Scope

- Agency-wide plan to implement PRA Policy Statement
- Included on-going and new PRA-related activities
  - E.g., maintenance rule, IPE program, generic safety issues
- Provided mechanisms for monitoring programs and management oversight
  - Defined, scheduled, and assigned responsibilities for staff activities needed to accomplish goals of PRA Policy Statement
- Encompassed activities in NRR, RES, former AEOD, and NMSS
- Informed Commission of staff progress via quarterly updates and briefings
- Replaced with Risk-Informed Regulation Implementation Plan

# Risk-Informed Performance-Based Plan - Overall Objectives and Scope

- Name changed from Risk-Informed Regulation Implementation Plan in April 2007
  - Older plan focused on risk-informed initiatives
- Goal is to achieve holistic, risk-informed and performance-based regulatory structure
- Will include publicly accessible database of activities
- Identify criteria for the selection and prioritization of practices and policies to be risk-informed and guidelines for implementation
- Identify major pieces of work associated with these efforts and related major milestones, including plans for communicating information to stakeholders
- Commission informed of staff progress via annual updates and briefings

# Risk-Informed Regulation

- **Insights derived from probabilistic risk assessments are used in combination with traditional engineering analyses to focus licensee and regulatory attention on issues commensurate with their importance to safety.**
- **Various approaches are used in the resulting regulations:**
  - **Prescriptive (e.g., design feature, program elements)**
  - **Performance-oriented (e.g., maintenance rule, Performance Indicators)**
  - **Risk-oriented (e.g., R.G. 1.174)**

# NRC Applications of PRA

- **Monitoring reactor operations**
  - **Maintenance Rule**
  - **Mitigating System Performance Index (MSPI)**
- **Value impact analysis for potential changes to licensed reactor design and operations (backfits)**
- **Efforts to Risk-Inform 10 CFR 50**

# Applications of PRA

- Licensing advanced reactor designs
- Reactor operations
  - Evaluation of changes to licensing basis
    - General guidance - R.G. 1.174
    - IST - R.G. 1.175
    - ISI - R.G. 1.178
    - Graded QA - R.G. 1.176
    - Tech. Specs. - R.G. 1.177
  - Inspections
    - Prioritization and planning of inspections
    - Evaluation of inspection findings
    - Evaluation of licensee use of PRA

# Applications of PRA

- **Resource allocation**
  - **Regulatory requirements (e.g., NEI initiative)**
  - **Research (e.g., generic issue prioritization)**
  - **Regulatory analyses (e.g., generic issue resolution)**
- **Reactor design**
  - **Identify weaknesses in design**
    - **Risk-significant SSCs**
    - **Risk-significant accident scenarios**
    - **Risk-significant human actions**

# Applications of PRA

- Standardized Plant Analysis Risk (SPAR) Models
- Events analysis and risk significance
  - Accident Sequence Precursors (ASP)
  - Significance Determination Process (SDP)
  - Management Directive 8.3
- Risk Monitors
- Non-reactor issues
  - Licensing high-level waste repository
  - Sealed sources
  - Spent fuel storage
  - Others

# Factors Leading to Increased Use of PRA

- Recommendations of groups who reviewed TMI-2 accident
  - Increased use by NRC
- Challenger disaster
  - Increase use by NASA; relied largely on FMEAs before Challenger
- Chernobyl accident
  - Increase use for DOE reactors
- Fukushima accident
  - Increased use for external events
- Drell report to U.S. Congress
  - Increased use for risk assessments of nuclear weapons systems
- Economic pressures
- Increased understanding and acceptance of methods
- Increasing availability of cheap, powerful computers

# Key Points for Risk-Informed Regulation

- PRA Policy Statement
  - Improve regulatory decision making and therefore safety
  - More efficient use of Staff resources
  - Reduce regulatory burden on industry

- PRA Implementation Plan
  - Agency-wide plan to implement PRA Policy Statement for PRA-related activities
  - Provide mechanisms for monitoring programs and oversight
  - Replaced by Risk-Informed Regulation Implementation Plan

- Risk-Informed Performance-based Plan
  - Organized to track nuclear reactor, material, and waste safety
  - Provide clear objectives and identify criteria for the selection and prioritization of practices and policies

- Risk-Informed Regulation
  - Insights gained from using PRA in conjunction with traditional engineering analyses  to focus licensee and regulatory attention on issues with their importance to safety
  - Includes prescriptive, performance-oriented, and risk-oriented approaches for developing regulations

# 14. Configuration Risk Management

# Configuration Risk Management

- Purpose: To acquaint students with the basic concepts of using PRA models to control configuration risk by planning maintenance.
- Objectives: Students will be able to explain;
  - Why base case PRA results cannot be used for maintenance planning
  - What is meant by "configuration risk management"
  - How configuration risk management is related to risk-informed regulation
- References
  - Regulatory Guide 1.160 (rev. 3) - Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
  - NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications

# Configuration Risk Management

- Three primary elements to configuration risk management;
  - Configuration: Assess the plant configuration accounting for the status of plant components
  - Risk: Quantify a risk metric (e.g., core damage frequency, core damage probability, large early release frequency) for the assessed plant configuration which typically includes comparison against nominal plant configuration
  - Management: Take measures to avoid risk-significant configurations, acquire better understanding of the risk level of a particular plant configuration, and/or limit the duration and frequency of such configurations that cannot be avoided

# Configuration Risk Management
# Why an Issue?

- Economics - Plants perform maintenance while at power, to reduce outage durations
- Safety
  - Increased maintenance while at power not covered in IPEs/PRAs
  - Increased on-line maintenance can produce high-risk plant configurations

# Configuration Risk Management Traditional Approaches

- Technical Specifications and Limiting Conditions for Operation
  - Identifies systems/components important to safety based on traditional engineering approach
  - Limit component out-of-service times for individual outages and combinations of component outages (not based on formal risk analysis)
- Maintenance planning guidelines such as 12-week rolling schedule, etc.
  - Based on train protection concept and Technical Specifications
  - Provide guidance to work week planners on allowable maintenance/testing
- Operator judgment
  - If emergent work arises, decision to continue with schedule maintenance/testing

# Configuration Risk Management Traditional Approaches

- Weaknesses of Traditional Approaches
  - Generally based on engineering judgment and limited to Technical Specification equipment
- Is the traditional approach good enough, given the increased emphasis on on-line maintenance?
- How can PRA help?

# Configuration Risk Management

- **Configuration risk management: one element of risk-informed regulation**
- **Can be forward-looking or retrospective**
  - **Forward-looking to plan maintenance activities & outage schedules**
  - **Retrospective to evaluate risk significance of past plant configurations (e.g., Accident Sequence Precursor analyses or Significance Determination Process)**

# Configuration Risk Management

- Configuration risk has various measures
  - Core damage frequency (CDF) profile (instantaneous)
    - Baseline CDF (BCDF, i.e., the zero-maintenance CDF)
    - Configuration-specific (conditional) CDF (CCDF)
  - Incremental CDF (ICDF) (sometimes called $\Delta$CDF)

$$\text{ICDF} = \text{CCDF} - \text{BCDF}$$

  - Core damage probability (CDP) is found by multiplying CDF by the duration in a specific configuration

$$\text{CDP} \approx \text{CDF} * \text{duration}$$

$$\text{CCDP} \approx \text{CCDF} * \text{duration}$$

  - Incremental core damage probability (ICDP)

$$\text{ICDP} \approx \text{ICDF} * \text{duration}$$

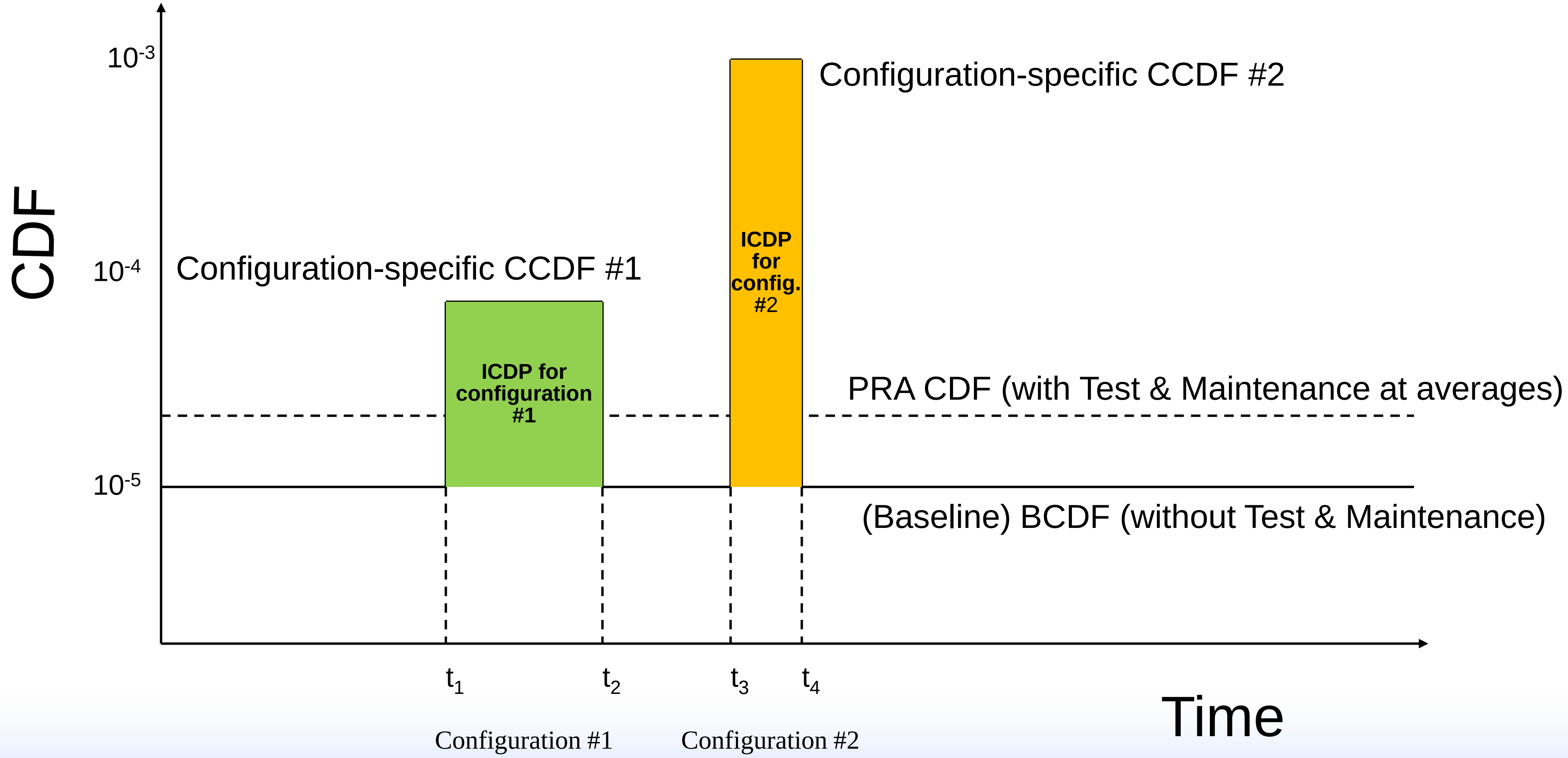
$$\text{ICDP} = \text{CCDP} - \text{BCDP}$$

  - Incremental large early release probability (ILERP)

$$\text{ILERP} \approx \text{ILERF} * \text{duration}$$

$$\text{ILERP} = \text{CLERP} - \text{BLERP}$$

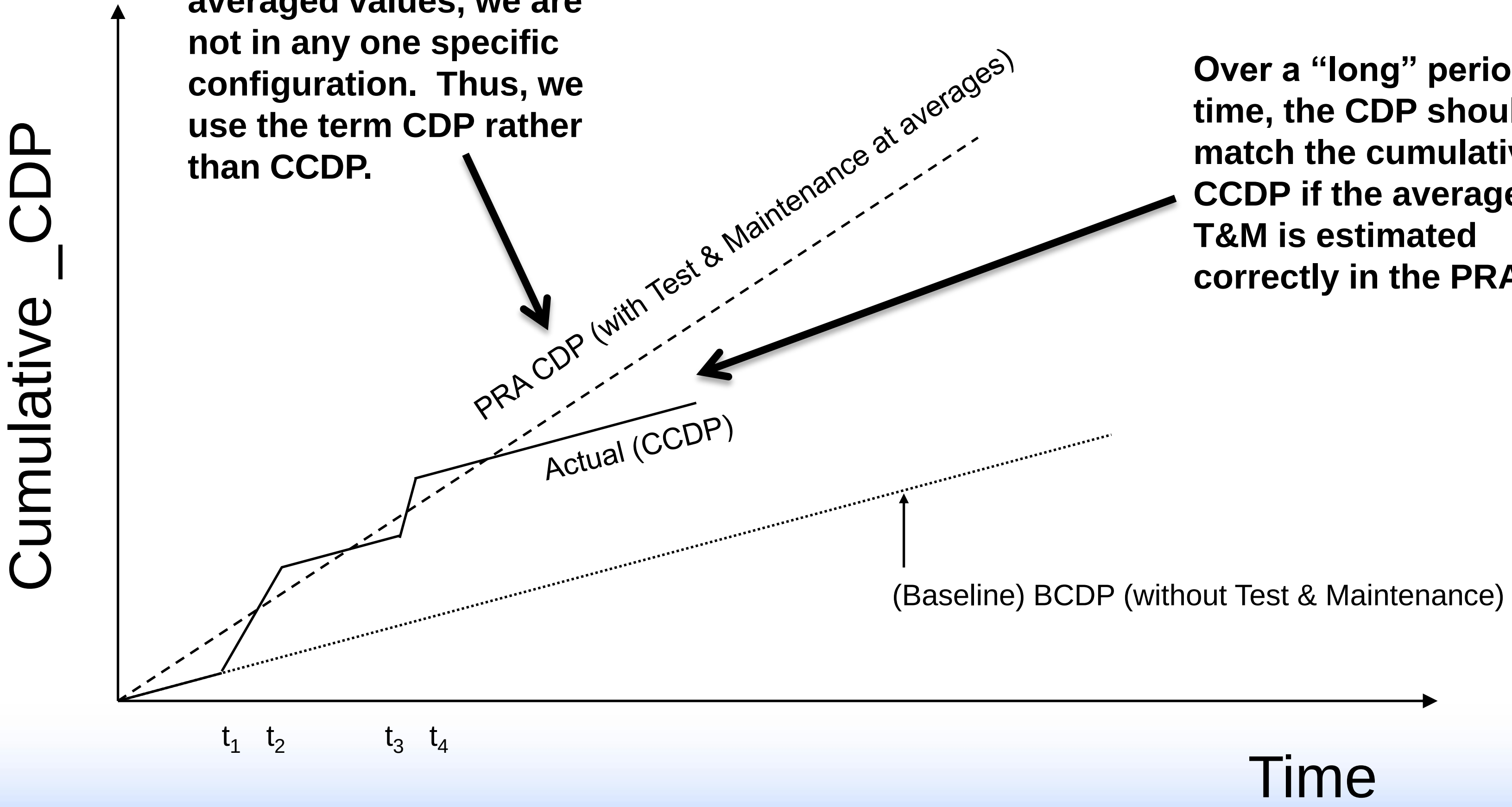
# CDF Profile


CDF
$10^{-3}$
$10^{-4}$
$10^{-5}$
Configuration-specific CCDF #2
Configuration-specific CCDF #1
ICDP for config. #2
ICDP for configuration #1
PRA CDF (with Test & Maintenance at averages)
(Baseline) BCDF (without Test & Maintenance)
$t_1$
$t_2$
$t_3$
$t_4$
Time
Configuration #1
Configuration #2

# Cumulative CDP Profile

Note:  When the PRA has the T&M set to averaged values, we are not in any one specific configuration.  Thus, we use the term CDP rather than CCDP.

Over a “long” period of time, the CDP should match the cumulative CCDP if the average T&M is estimated correctly in the PRA



# Configuration Risk Management

- **Includes management of:**
  - **OOS components**
    - **CCDF (configuration-specific CDF)**
  - **Outage time of components & systems**
    - **Configuration duration**
    - **CCDP**
    - **ICDP**
  - **Backup components**
    - **CCDF**
  - **Frequency of specific configuration**
    - **Cumulative CDP over time**

***(each of these discussed on the following slides)***

# Managing OOS Components

- Involves scheduling maintenance and tests to avoid having critical combinations of components or systems out of service concurrently
- For Maintenance Rule, 10 CFR 50.65
  - NUMARC 93-01 suggest a ceiling configuration-specific CCDF of 1E-3/year
    - Subject of such a ceiling value being studied by the NRC
    - NRC endorses the Feb. 22, 2000 revision of section 11 of NUMARC 93-01, but neither endorses nor disapproves the numerical value of 1E-3/year

# Managing Outage Time

- Must determine how long configuration can exist before risk incurred becomes significant
- Many utilities using EPRI PSA Application Guide numerical criteria, although not endorsed by NRC
  - NRC has no numerical criteria for temporary changes to plant
  - For Maintenance Rule (NUMARC 93-01, section 11),
    - If >1E-5 ICDP or >1E-6 ILERP
      - Then configuration Should not normally be entered voluntarily
    - If 1E-6 to 1E-5 ICDP or 1E-7 to 1E-6 ILERP
      - Then assess non quantifiable factors and establish risk management actions
    - If <1E-6 ICDP or <1E-7 ILERP
      - Then normal work controls
- For risk-informed Tech. Specs., for single permanent change to AOT acceptable if (RG 1.177):
    - ICCDP < 5E-7
    - ICLERP < 5E-8
- Must know compensatory measures to take to extend outage time without increasing risk

# Managing Backup Components

- Must determine which components can carry out functions of those out of service (OOS).
- Ensure availability of backup components while primary equipment OOS.

# Controlling Frequency

- Must track frequency of configurations and modify procedures & testing to control occurrences, as necessary and feasible.
- Repeated entry into a specific configuration might violate PRA assumptions with respect to assumed outage time.

# Why Configuration Risk Management is Needed…

- PRA/IPE assumes random failures of equipment (including equipment outages for testing & maintenance)
  - Importance measures based on random, independent maintenance of components
- PRA/IPE baseline model does not explicitly model simultaneous outages of critical components
  - Treats maintenance as independent, so simultaneous outages unlikely
- Simultaneous outages (i.e., plant configurations) can increase risk significantly above the PRA/IPE baseline
- Lack of configuration management can affect initiating events and equipment designed to mitigate initiating events, leading to increased risk

# Preventive Maintenance Risk Calculations

- Risk impact of PM on single component
- Risk impact of maintenance schedule
- Risk impact of scheduling maintenance
  - Maintenance performed when at power versus shutdown then perform maintenance
    - Compare the risk profiles for both conditions

# Risk Monitors

- **On-line risk monitors can be used to evaluate plant configurations for a variety of purposes:**
  - **To provide current plant risk profile to plant operators**
  - **As a forward-looking scheduling tool to allow decisions about test and maintenance actions weeks or months in advance of planned outages**
  - **As a backward-looking tool to evaluate the risk of past plant configurations**

# Current Risk Monitor Software Packages

- Erin Engineering Sentinel
- Scientech/NUS Safety Monitor
  - The NRC acquired this package from Scientech, and has an agency-wide license covering its use
- EPRI R&R Workstation (EOOS) [PHEONIX Risk Monitor – latest version of software package]
  - The NRC acquired this package from EPRI, and has an agency-wide license covering its use
- Specialized packages developed for specific plants, e.g., South Texas Project

# Requisite Features

- Risk monitor software requires (at a minimum) the following features:
  - PRA solution engine for analysis of the plant logic model
    - Can be ET/FT
    - Single FT
    - Cut set equation
  - Database to manage the various potential plant configurations
    - That is, a library of results for configurations of interest
  - Plotting program to display results

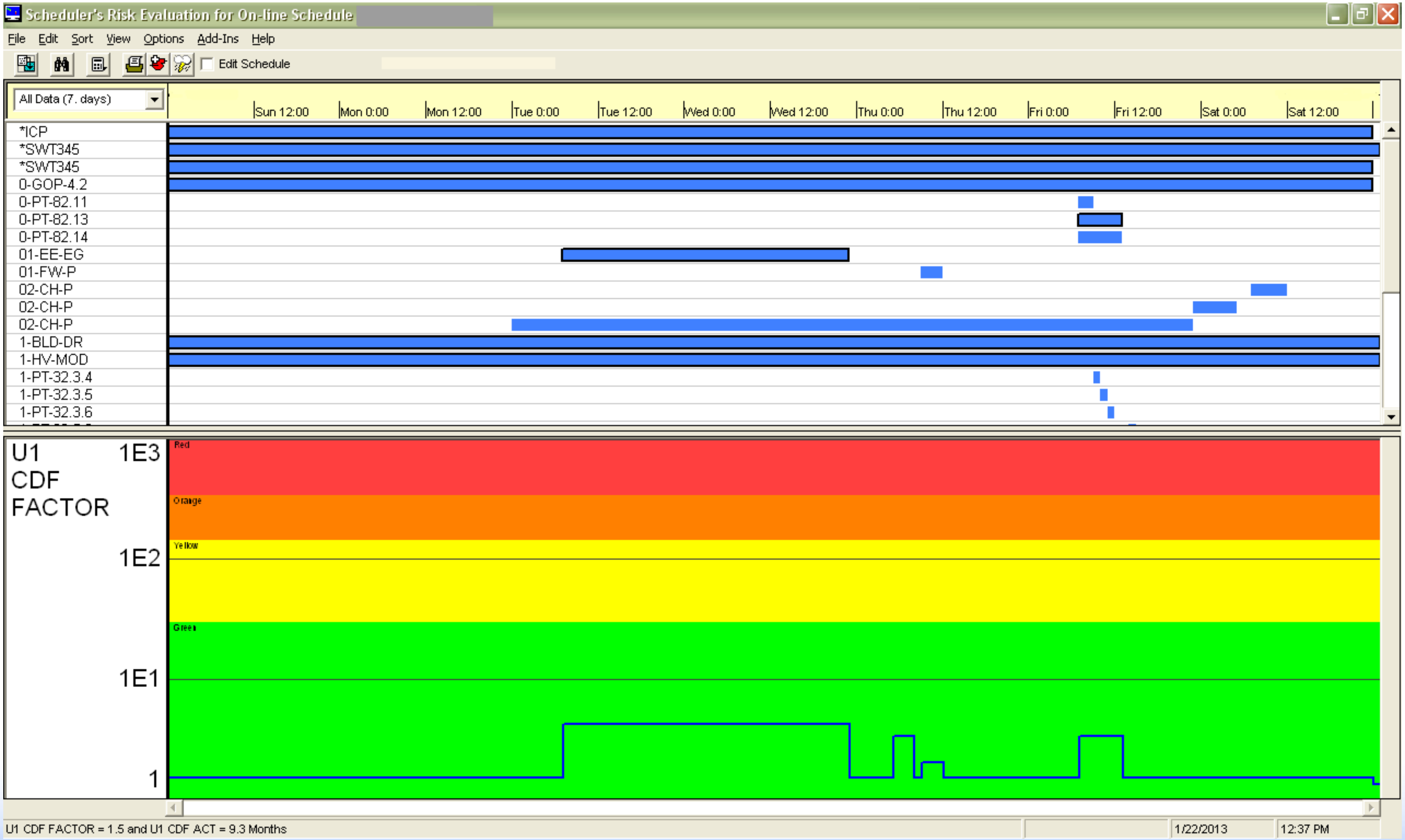
# Risk Monitor Capabilities

- **As a tool for plant operators to evaluate risk based on real-time plant configuration:**
  - **Calculates measure of risk for current or planned configurations**
  - **Displays maximum time that can be spent in that particular configuration without exceeding pre-defined risk threshold**
  - **Provides status of plant systems affected by various test and maintenance activities**
  - **Operators can do quick sensitivity studies to evaluate the risk impacts of proposed plant modifications**

# Risk Monitor Capabilities

- As a tool for plant scheduling for maintenance and outage planning:
  - Generates time-line that shows graphically the status of plant systems and safety functions
  - Generates risk profile as plant configuration varies over time
  - Identifies which components have strongest influence on risk
  - Includes environmental risk (external events)
    - Seismic Activities
    - High Winds
    - Etc.

# Plant Configuration Profile



U1 CDF FACTOR = 1.5 and U1 CDF ACT = 9.3 Months

# Risk Monitor Strengths and Weaknesses

- **Risk Monitor Strengths**
  - **Provides risk determinations of current and proposed plant configurations**
  - **Compact model**
  - **Many current PRA models can be converted into risk monitor format**
  - **Can obtain importance and uncertainty information on results**
  - **Provides risk management guidance by indicating what components should be restored first**

# Risk Monitor Strengths and Weaknesses

- Risk Monitor Limitations
  - For some PRA codes, difficulty of converting PRA models into master logic diagram (e.g., Large Event Tree approach models)
  - Effort required to set up databases to link master logic diagram events to plant components and electronic P&IDs, and interface with scheduling software (e.g., map PRA basic events into component IDs and procedures)
  - Analysis Approximations
    - Effects on IE frequencies
    - CCF adjustments
    - Human recovery modeling
    - Consideration of plant features not normally modeled in PRA studies
    - Truncation limits

# Review of Configuration Risk Management

- **Key Points of Section:**
  - Configuration risk management involves implementing measures to avoid risk-significant configurations and limiting the duration and frequency of those configurations that cannot be avoided.
  - Configuration risk management is important with regard to economics and safety.
  - Traditional Approaches: Technical Specifications and limiting conditions for operation, maintenance planning guidelines, operator judgment.
  - PRA can help with management of OOS components, outage time of components and systems (CCDP, ICDP), backup components, and frequency of specific configuration.
  - Risk monitors can be used to evaluate plant configurations.
    - Assists in the determinations of current and proposed plant configurations.
    - Provides risk management guidance by indicating what components should be restored first.

# Additional Sources of Information

- Further details on configuration risk management can be found in NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications
- Risk Assessment for Event Evaluation (P-302) course in the PRA Technology Transfer Program curriculum explores the use of PRA techniques for evaluating the risk significance of operational events, as well as plant configuration risk management, discusses the other risk measures mentioned in this module (e.g., CCDP and event importance), and illustrates use of ECA workspace in SAPHIRE to perform the necessary PRA calculations.
- NRC Risk Assessment Standardization Program (RASP) Handbook describes use of SPAR models for ASP, SDP, and MD 8.3 evaluations.

# Page Intentionally Left Blank

# 15. Mitigating System Performance Index (MSPI)

# Mitigating System Performance Index

- **Purpose: Provide overview of MSPI, with special emphasis on its PRA basis**
- **Objectives: At the conclusion of this section, students will understand;**
  - **What is MSPI**
  - **Why MSPI was developed**
  - **How MSPI is related to ΔCDF**
  - **How MSPI includes both unavailability and unreliability**
  - **How MSPI uses importance measures**
- **References**
  - **NEI 99-02, Rev. 6, August 2009**
  - **NUREG-1816, *Independent Verification of the Mitigating Systems Performance Index (MSPI) Results for the Pilot Plants,* February 2005**

# What is MSPI?

- *Mitigating System Performance Index* ***(MSPI)*** **is the sum of changes in a simplified core damage frequency evaluation resulting from differences in unavailability and unreliability relative to industry standard baseline values. The MSPI is supplemented with system component performance limits.**
- **MSPI is the numerical sum of the deviation between a system's actual unavailability and unreliability values for a calendar quarter and the established baseline values.**
- **MSPI takes into account plant specific risk importance measures in the calculation.**
- **MSPI = Unavailability Index + Unreliability Index**

  **= UAI + URI**

# MSPI – Indicator Definition/Aspects Monitored

- **Unavailability**
  - The ratio of the hours the train/system was unavailable to perform its monitored functions (as defined by PRA success criteria and mission times) due to planned and unplanned maintenance or test during the previous 12 quarters while critical to the number of critical hours during the previous 12 quarters.
- **Unreliability**
  - The probability that the train/system would not perform its monitored functions, as defined by PRA success criteria, for a 24 hour mission time (run), when called upon during the previous 12 quarters.
- **Baseline Values**
  - The values for unavailability and unreliability against which current plant unavailability and unreliability are measured.
- **Component Performance Limit**
  - A measure of degraded performance that indicates when the performance of a monitored component in an MSPI system is significantly lower than expected industry performance.

# MSPI – Calculated Separately for Five Systems for Each Reactor Type

- BWRs:
  - Emergency AC power system
  - High Pressure Injection System (high pressure coolant injection, high pressure core spray, or feedwater coolant injection)
  - Reactor Core Isolation Cooling (or isolation condenser)
  - Residual Heat Removal System (or the equivalent function as described in the Additional Guidance for Specific Systems section of Appendix F)
  - Cooling Water Support System (includes direct cooling functions provided by service water and component cooling water or their cooling water equivalents for the above four monitored systems)
- PWRs:
  - Emergency AC Power System
  - High Pressure Safety Injection System
  - Auxiliary Feedwater System
  - Residual Heat Removal System (or the equivalent function as described in the Additional Guidance for Specific Systems section of Appendix F)
  - Cooling Water Support System (includes direct cooling functions provided by service water and component cooling water or their cooling water equivalents for the above four monitored systems)

# Why Was MSPI Developed?

- **Problems identified with safety system unavailability (SSU) performance indicator**
  - **Uses short-term unavailability to approximate unreliability**
  - **Uses same performance threshold regardless of risk significance**
  - **Potential for double-counting support system failures**
  - **SSU inconsistent with Maintenance Rule definition of unavailability**
  - **Inconsistent with indicators promulgated by World Association of Nuclear Operators (WANO) and Institute of Nuclear Power Operations (INPO)**
    - **Requires plant personnel to track plant data three different ways**

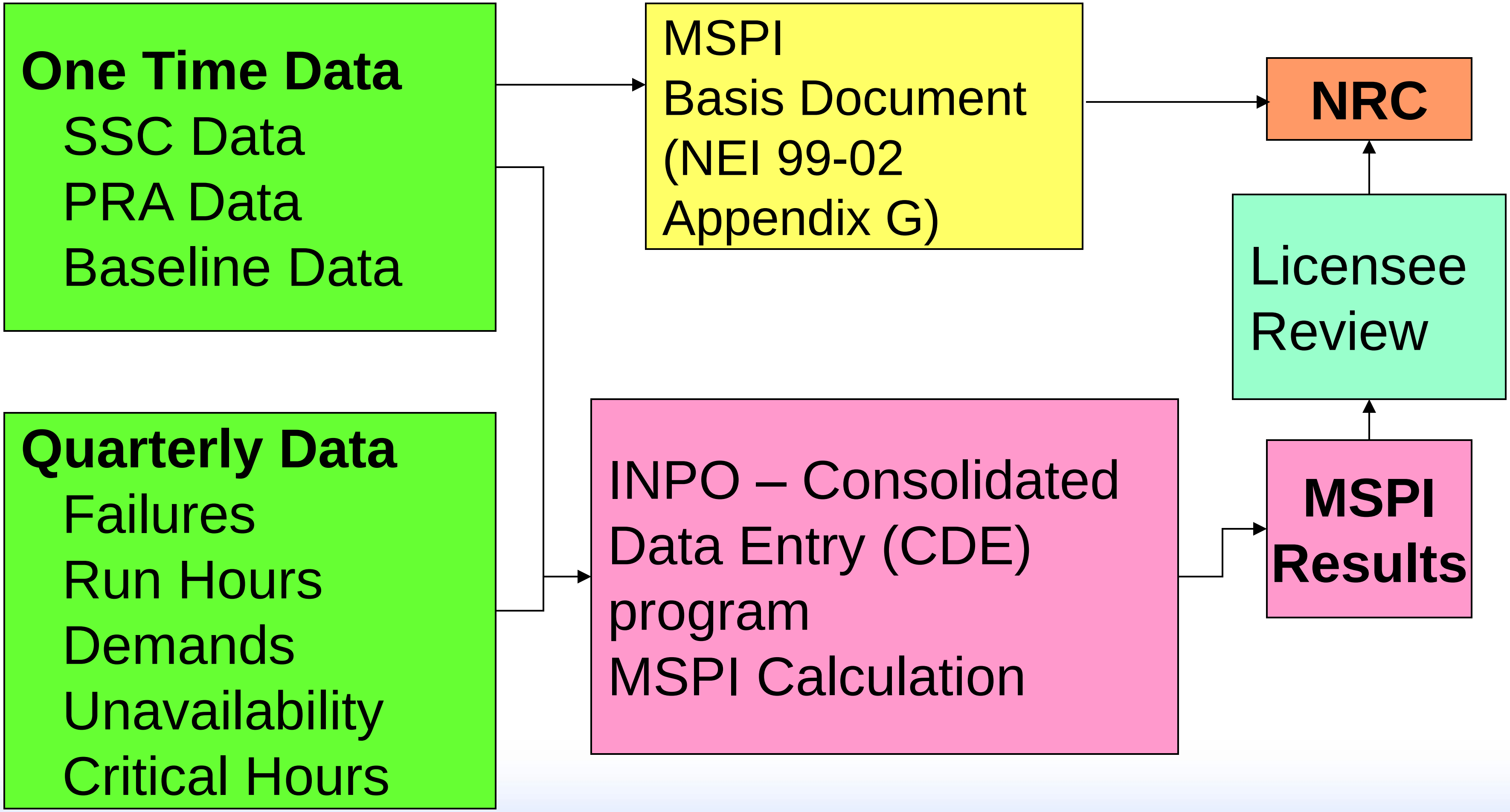
# Development Timeline

- **NRC initiates Risk-Based Performance Indicator program**
  - **NUREG-1753 issued in 2002**
    - **Proposed indicators that incorporated risk significance, as measured by SPAR models**
    - **Plant-specific thresholds for indicators**
- **MSPI Pilot Program initiated in Summer 2002**
  - **20 plants participated**
  - **Provided V&V of**
    - **Baseline data**
    - **Current performance data**
    - **Importance measures**
    - **Spreadsheet calculations**
    - **Overall MSPI results**
- **NRC gave NEI agreement to proceed with MSPI in August 2004**

# MSPI Objectives

- **Provide a risk-informed, plant specific, indication of mitigating system performance.**
  - **Reflect risk impact of system availability and reliability at each plant**
  - **System performance requirements based on PRA system success criteria rather than design basis criteria**
  - **Monitor most risk significant components**

# MSPI Overall Process



**One Time Data**
SSC Data
PRA Data
Baseline Data

MSPI
Basis Document
(NEI 99-02
Appendix G)

**NRC**

Licensee
Review

**Quarterly Data**
Failures
Run Hours
Demands
Unavailability
Critical Hours

INPO – Consolidated
Data Entry (CDE)
program
MSPI Calculation

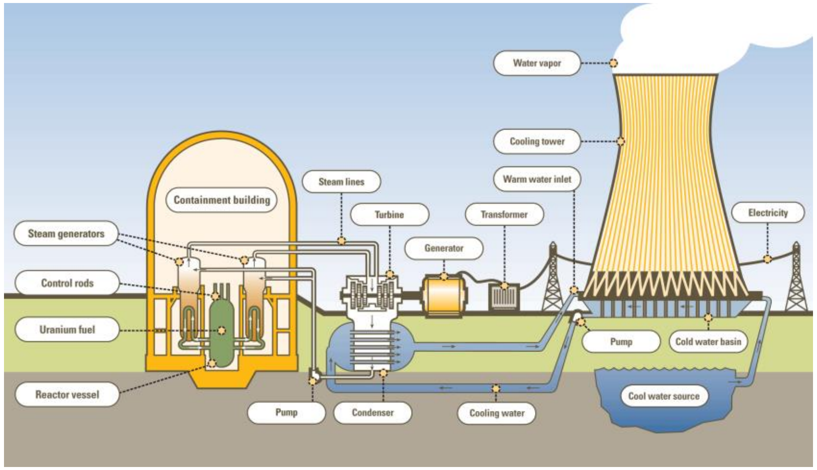
**MSPI**
**Results**

# Guidance Documents

- NEI 99-02 Section 2.2
  - Basic Definitions
- NEI 99-02 Appendix F
  - Details of Calculation Methods
  - Detailed Definition of Inputs
- NUREG-1816
  - Technical bases
  - Description of pilot program
  - Recommended enhancements
  - MSPI limitations

# MSPI Concept

$$\mathbf{MSPI = \Delta CDF = CDF_1 - CDF_0}$$



**$CDF_1$ = Actual Performance**

**$CDF_0$ = Industry Baseline Performance**

# How To Calculate MSPI

- Includes unavailability and unreliability in single risk measure
- MSPI = UAI + URI
  - UAI is Unavailability Index
  - URI is Unreliability Index
- MSPI $\approx \Delta$CDF = $\text{CDF}_1 - \text{CDF}_0$
  - $\text{CDF}_1$ is actual plant performance
  - $\text{CDF}_0$ is industry baseline performance
- Because MSPI $\approx \Delta$CDF can apply “colors” from SDP
  - MSPI $\leq 10^{-6}$ GREEN
  - $10^{-6} <$ MSPI $\leq 10^{-5}$ WHITE
  - $10^{-5} <$ MSPI $\leq 10^{-4}$ YELLOW
  - MSPI $> 10^{-4}$ RED

# Calculating UAI

- UAI is sum of contributions from each train of a monitored system:

$$UAI = \sum_{j=1}^{n} UAI_{tj}$$

  - n = # trains in a system

- UAI$_{tj}$ is unavailability index for each train

# Calculating $\text{UAI}_t$

$$UAI_t = CDF\left[\frac{FV_{UA_{PRA}}}{UA_{PRA}}\right](UA_t - UA_{BLt})$$

**where:**

**CDF = plant specific core damage frequency**

**$\text{FV}_{\text{UAPRA}}$ = train-specific Fussell-Vesely value for unavailability**

**$\text{UA}_{\text{PRA}}$ = plant specific PRA value of unavailability for the train**

**$\text{UA}_t$ = actual unavailability of train t, defined as:**

$$UA_t = \left[\frac{\text{Unavailable hours (planned and unplanned) during previous 12 quarters while critical}}{\text{Critical hours during previous 12 quarters}}\right]$$

**$\text{UA}_{\text{BLt}}$ = historical baseline unavailability value for the train**

# Calculating URI

$$URI = CDF \sum_{j=1}^{n} \left\{ \left[ \frac{FV_{UR_{PRA,j}}}{UR_{PRA,j}} \right]_{\max} \left( UR_{BC,j} - UR_{BL,j} \right) \right\}$$

**Where:**

**CDF = Plant core damage frequency**

**$FV_{URPRA,j}$ = Fussell-Vesely value from plant specific PRA (component's failure modes [i.e., MDP fails to run])**

**$UR_{PRA,j}$ = Plant specific unreliability (probability of component's failure modes [i.e., MDP fails to run])**

**$UR_{BC,j}$ = Bayesian corrected plant-specific value for the component's specific failure modes [i.e., MDP fails to run]**

**DEMAND**

**$UR_{BC,jd} = (N_d + a)/(a + b + D)$**

**$N_d$ is the total number of failures of on demand during previous 12 quarters**

**D is total number of demands during the previous 12 quarters**

**a and b are parameters of the industry prior, derived from industry experience (Appendix F NEI99-02)**

**RUNNING**

**$UR_{BC,jr} = [(N_r + a)/(T_r + b)] * T_m$**

**$N_r$ is the total number of failures to run during previous 12 quarters**

**$T_r$ is total number of run hours during the previous 12 quarters**

**$T_m$ is mission time for the component based on PRA model assumption.**

**a and b are parameters of the industry prior, derived from industry experience (Appendix F NEI99-02)**

**$UR_{BL,j}$ = historical baseline values of unreliability for the component's failure modes [i.e., MDP fails to run]**

- **URI includes both demand failures and running failures**
  - **Details can be found in App. F to NEI 99-02**

# Color Scale for MSPI

- MSPI = UAI + URI
- MSPI is calculated for each monitored system and compared to risk thresholds
  - MSPI $\leq 10^{-6}$ GREEN
  - $10^{-6} <$ MSPI $\leq 10^{-5}$ WHITE
  - $10^{-5} <$ MSPI $\leq 10^{-4}$ YELLOW
  - MSPI $> 10^{-4}$ RED

# MSPI Front-Stop

- **Don't want single failure to result in MSPI being WHITE**
  - For example, expected to see three failures over a three year period. Due to variability, it can be expected to see 2 or 4 failures in three year period.
  - It is not appropriate that a system should be placed in WHITE band due to expected variation.
- **Avoid this by capping most risk-significant failure at $5\times10^{-7}$ (from risk-informed Tech. Specs.)**
  - This ensures that one failure beyond expected alone doesn't result in MSPI > $1\times10^{-6}$

# MSPI Back-Stop

- For systems with low Birnbaum importance, performance could degrade significantly without MSPI crossing WHITE threshold
- To prevent this, a maximum number of failures is determined as the threshold to the WHITE band, even though the calculated MSPI < $1\times10^{-6}$
- Appendix E to NUREG-1816 or Appendix F of NEI 99-02 gives formula for finding maximum allowed failures, even if MSPI is still GREEN

# Additional Importance Measures - Relationships

- **Relationship to Fussell-Vesely importance**

$$FV(x) = \frac{p_x Bi(x)}{CDF}$$

- **Birnbaum importance**

$$Bi(x) = \frac{\partial(CDF)}{\partial p_x} = CDF(x=1) - CDF(x=0)$$

- **$\Delta$CDF $\approx$ $\Sigma$Bi(x)$\Delta$p$_x$**
- **Thus change in CDF can be proportional to change in component probability multiplied by Birnbaum of component**

# Page Intentionally Left Blank

# 16. Significance Determination Process (SDP) Principles

# Significance Determination Process (SDP)

- Purpose: To acquaint students with the purpose of the SDP, the PRA basis underlying SDP, and how the SDP principles are consistent with PRA principles and practices.
- Objectives: Students will be able to explain;
  - the purpose and objectives of the SDP
  - the PRA basis behind the SDP
  - how SDP is consistent with PRA principles and practices
- Reference: NRC Inspection Manual Chapter (IMC) 0609, Significance Determination Process

# SDP Purpose

- **SDP Purpose:**
  - **Use risk insights (results of evaluation):**
    - **To help NRC inspectors and staff determine the safety or security significance of inspection findings**
    - **Findings are identified from the seven cornerstones of safety at operating reactors**
      - **Initiating events; mitigating systems; barrier integrity; emergency preparedness; public radiation safety; occupational radiation safety; and physical protection**
  - **Each SDP supports a cornerstone associated with the strategic performance areas as defined in**
    - **Inspection Manual Chapter (IMC) 2515, “Light-Water Reactor Inspection Program- Operations Phase” and**
    - **IMC 2201, “Security and Safeguard Inspection Program for Commercial Power Reactors.”**

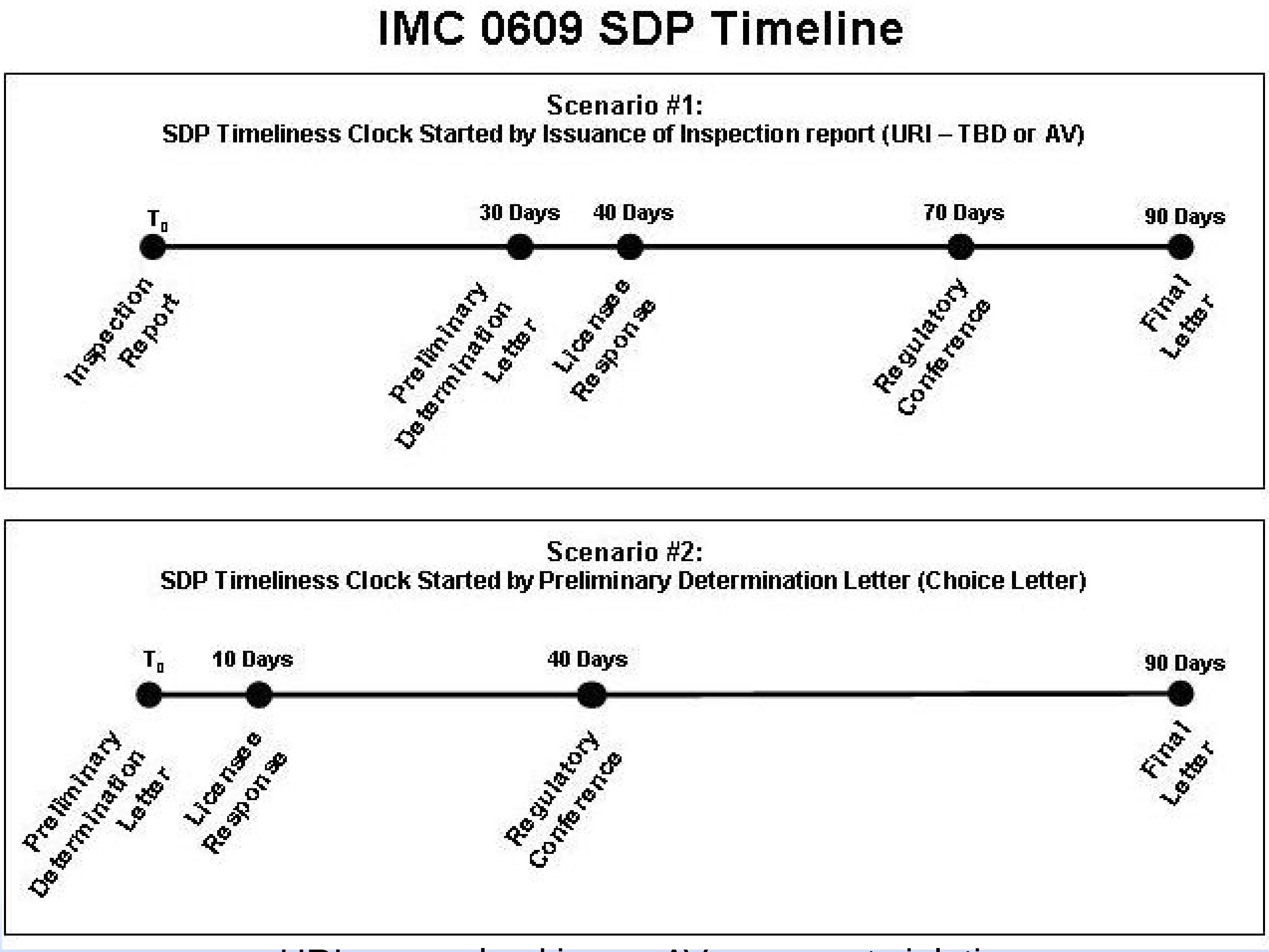
# SDP Purpose (cont.)

- SDP Purpose:
  - A risk-informed process
    - To use the results of the safety significance findings, combined with the results of the risk-informed performance indicator (PI) program
    - To determine a licensee’s level of safety performance, and to define the level of NRC engagement with the licensee.
  - SDP determinations for inspection findings and the Performance Indicator (PI) information are combined for use in assessing licensee performance in accordance with
    - IMC 0305, “Operating Reactor Assessment Program” and
    - IMC 0320, “Operating Reactor Security Assessment Program.”

# SDP Objectives

- SDP Objectives:
  - Characterize significance of inspection findings for the Reactor Oversight Process (ROP), using best available risk insights as appropriate.
  - Provide all stakeholders an objective and common framework for communicating the potential safety or security significance of inspection findings.
  - Provide a basis for timely assessment and/or enforcement actions associated with an inspection finding.
  - Provide inspectors with plant-specific risk information for use in risk-informing the inspection program.

# SDP Timeline



IMC 0609 SDP Timeline

Scenario #1:
SDP Timeliness Clock Started by Issuance of Inspection report (URI – TBD or AV)

T$_0$ – Inspection Report

30 Days – Preliminary Determination Letter

40 Days – Licensee Response

70 Days – Regulatory Conference

90 Days – Final Letter

Scenario #2:
SDP Timeliness Clock Started by Preliminary Determination Letter (Choice Letter)

T$_0$ – Preliminary Determination Letter

10 Days – Licensee Response

40 Days – Regulatory Conference

90 Days – Final Letter

URI=unresolved issue, AV=apparent violation

# SDP Types

- Many types of SDPs exist at the NRC

| | |
|---|---|
| 0609 App A | The SDP for Findings At-Power |
| 0609 App B | Emergency Preparedness SDP |
| 0609 App C | Occupational Radiation Safety SDP |
| 0609 App D | Public Radiation Safety SDP |
| 0609 App F | Fire Protection SDP |
| 0609 App G | Shutdown Operations SDP |
| 0609 App H | Containment Integrity SDP |
| 0609 App I | Operator Requalification Human Performance SDP |
| 0609 App J | Steam Generator Tube Integrity Findings SDP |
| 0609 App K | Maintenance Risk Assessment & Risk Management SDP |
| 0609 App L | B.5.b SDP |
| 0609 App M | SDP Using Qualitative Criteria |

# Significance Determination Process (SDP)

- **Risk Significance:**
  - **SDP estimates risk significance of licensee performance problems**
    - **Does not include equipment out of service for test or maintenance, unless related specifically to performance problem**
    - **Therefore, final result is increase in CCDP, or incremental CCDP, caused by the performance problem**
      - **Classified as ΔCDF, i.e., averaged over 1 yr**
  - **The results are color coded (next slide)**

# Level of significance associated with inspection findings

- Red – high risk significance – supplemental inspection (IP 95003)
- Yellow – substantive risk significance – supplemental inspection (IP 95002)
- White – low to moderate risk significance – supplemental inspection (IP 95001)
- Green - very low risk significance - baseline inspection

| | |
|---|---|
| 🟥 | $\Delta\text{CDF} > 1\text{E-}4/\text{yr}$ |
| 🟨 | $1\text{E-}4/\text{yr} \geq \Delta\text{CDF} > 1\text{E-}5/\text{yr}$ |
| ⬜ | $1\text{E-}5/\text{yr} \geq \Delta\text{CDF} > 1\text{E-}6/\text{yr}$ |
| 🟩 | $1\text{E-}6/\text{yr} \geq \Delta\text{CDF}$ |

**(colors in terms of increase in annual time-averaged CDF)**

# Definitions

- **Inspection findings are assigned a color representing the significance**
- **Definitions include the quantitative and qualitative aspects for each color and need to be applied appropriately to each SDP appendix in IMC 0609.**
  - **Red (high safety or security significance) is quantitatively greater than 10-4ΔCDF or 10-5ΔLERF. Qualitatively, a Red significance indicates a decline in licensee performance that is associated with an unacceptable loss of safety margin. Sufficient safety margin still exists to prevent undue risk to public health and safety.**
  - **Yellow (substantial safety or security significance) is quantitatively greater than 10-5 and less than or equal to 10-4 ΔCDF or greater than 10-6 and less than or equal to 10-5ΔLERF. Qualitatively, a Yellow significance indicates a decline in licensee performance that is still acceptable with cornerstone objectives met, but with significant reduction in safety margin.**
  - **White (low to moderate safety or security significance) is quantitatively greater than 10-6 and less than or equal to 10-5ΔCDF or greater than 10-7 and less than or equal to 10-6ΔLERF. Qualitatively, a White significance indicates an acceptable level of performance by the licensee, but outside the nominal risk range. Cornerstone objectives are met with minimal reduction in safety margin.**
  - **Green (very low safety or security significance) is quantitatively less than or equal to 10-6ΔCDF or 10-7ΔLERF. Qualitatively, a Green significance indicates that licensee performance is acceptable and cornerstone objectives are fully met with nominal risk and deviation.**

# SDP - Process

- Inspection finding was observed and was identified as performance deficiency that is "more than minor"
- IMC 0609 Attachment 4 – Initial Characterization of Findings
  - This attachment is broken down into three parts to help characterize and evaluate the finding
  - Part 1 - Finding Consolidated Information Sheet (Table 1)
    - Objective of Table 1 is to provide the inspector and management the opportunity to document and review all the supporting information pertaining to a finding in a concise format.
  - Part 2 - Cornerstones Affected by Degraded Condition or Programmatic Weakness (Table 2)
    - Objective of Table 2 is to support the identification of safety cornerstone(s) affected by the degraded condition or programmatic weakness
    - Affected cornerstone(s) may already have been identified (e.g., scope of the inspection procedure, inspector experience and knowledge of the ROP); however, Table 2 helps to support this determination.

# SDP – Process (cont.)

- IMC 0609 Attachment 4 – Initial Characterization of Findings
  - Part 3 - SDP Appendix Router (Table 3)
    - After the affected cornerstone(s) are identified,
      - Use the SDP Appendix Router (Table 3) to facilitate determining the appropriate SDP appendix for further evaluation.
      - If more than one cornerstone was affected and results in direction to more than one SDP appendix, the inspector should identify one SDP appendix for use based on reasonable judgment of the specific situation.
      - If more than one cornerstone was affected but results in direction to one SDP appendix, the inspector and management should initially identify one cornerstone based on reasonable judgment of the situation.

# SDP (continued)

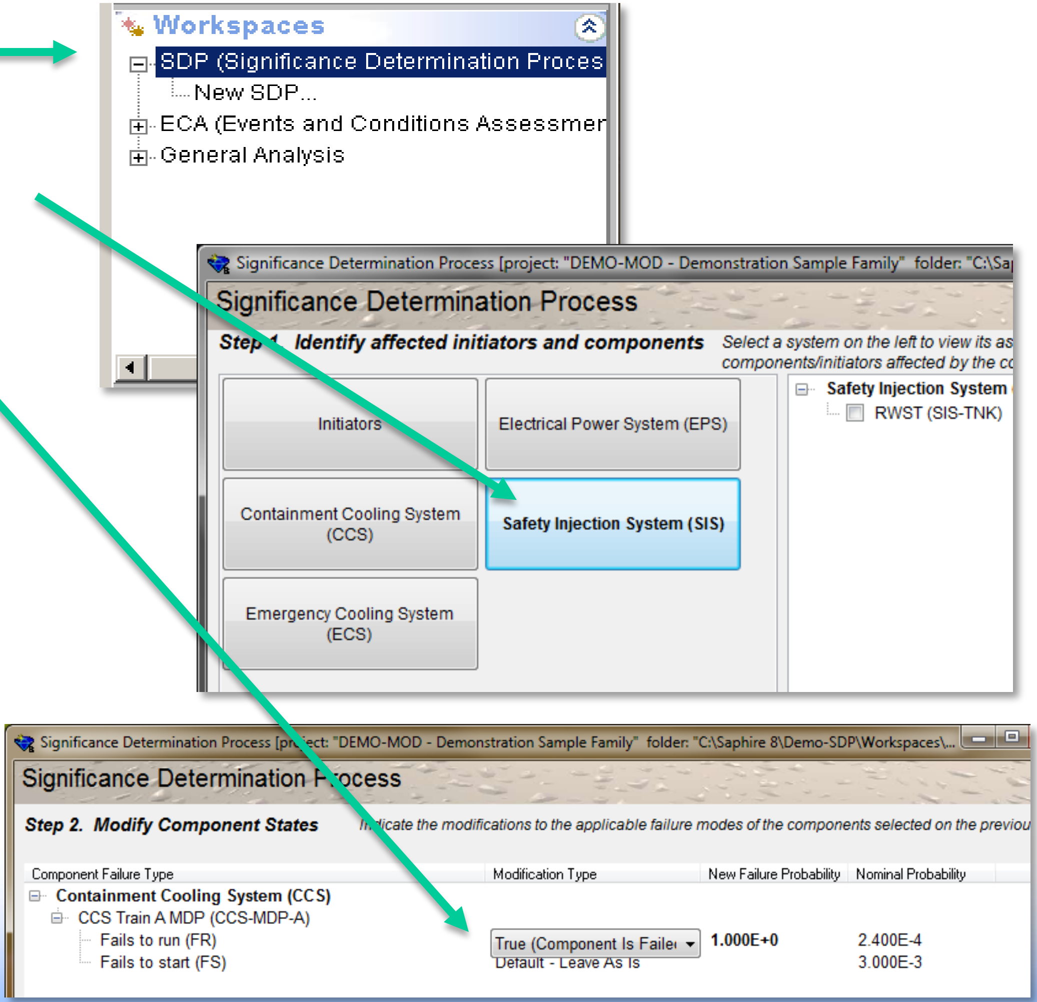
- **IMC 0609 Appendix A – The Significance Determination Process (SDP) for Findings At-Power**
  - **Appendix A is divided into two functional parts:**
    1. **Screening tool that uses a series of logic questions to determine whether or not the finding can be characterized as having low safety significance (i.e., Green) and preclude a more detailed risk evaluation.**
    2. **Guidance provided in determining the risk significance of a finding that did not screen to Green in part one.**
  - **Detailed Risk Evaluation is needed for findings that do not screen to green.**

# SDP - Detailed Risk Evaluation

## Steps to using SDP Workspace

**Start a SDP**

1. **Select the affected system and component**
2. **Modify the component that is affected**
3. **Specify analysis details**
   - **Duration of component outage**
   - **Truncation level**
   - **Name/description to save analysis**



Workspaces
SDP (Significance Determination Proces
New SDP...
ECA (Events and Conditions Assessmer
General Analysis

Significance Determination Process [project: "DEMO-MOD - Demonstration Sample Family" folder: "C:\Sa

Significance Determination Process

*Step 1. Identify affected initiators and components* — *Select a system on the left to view its as components/initiators affected by the c*

Initiators
Electrical Power System (EPS)
Containment Cooling System (CCS)
Safety Injection System (SIS)
Emergency Cooling System (ECS)
Safety Injection System
□ RWST (SIS-TNK)

Significance Determination Process [project: "DEMO-MOD - Demonstration Sample Family" folder: "C:\Saphire 8\Demo-SDP\Workspaces\...

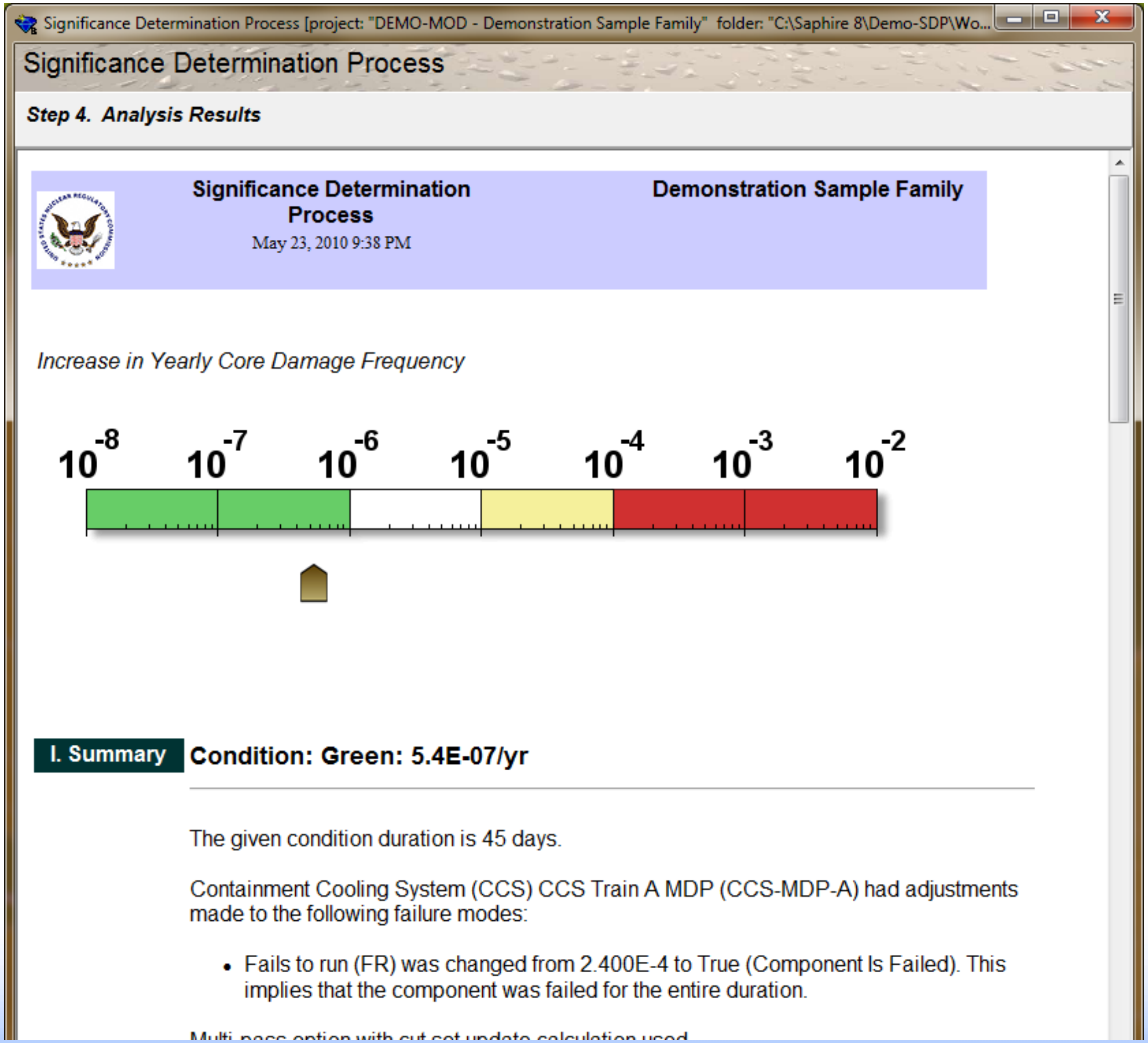
Significance Determination Process

*Step 2. Modify Component States* — *Indicate the modifications to the applicable failure modes of the components selected on the previou*

| Component Failure Type | Modification Type | New Failure Probability | Nominal Probability |
|---|---|---|---|
| **Containment Cooling System (CCS)** | | | |
| CCS Train A MDP (CCS-MDP-A) | | | |
| Fails to run (FR) | True (Component Is Faile | **1.000E+0** | 2.400E-4 |
| Fails to start (FS) | Default - Leave As Is | | 3.000E-3 |

# SDP - Detailed Risk Evaluation

4. **Calculate!**



Significance Determination Process [project: "DEMO-MOD - Demonstration Sample Family" folder: "C:\Saphire 8\Demo-SDP\Wo...

Significance Determination Process

***Step 4. Analysis Results***

**Significance Determination Process**

May 23, 2010 9:38 PM

**Demonstration Sample Family**

*Increase in Yearly Core Damage Frequency*

**I. Summary** **Condition: Green: 5.4E-07/yr**

The given condition duration is 45 days.

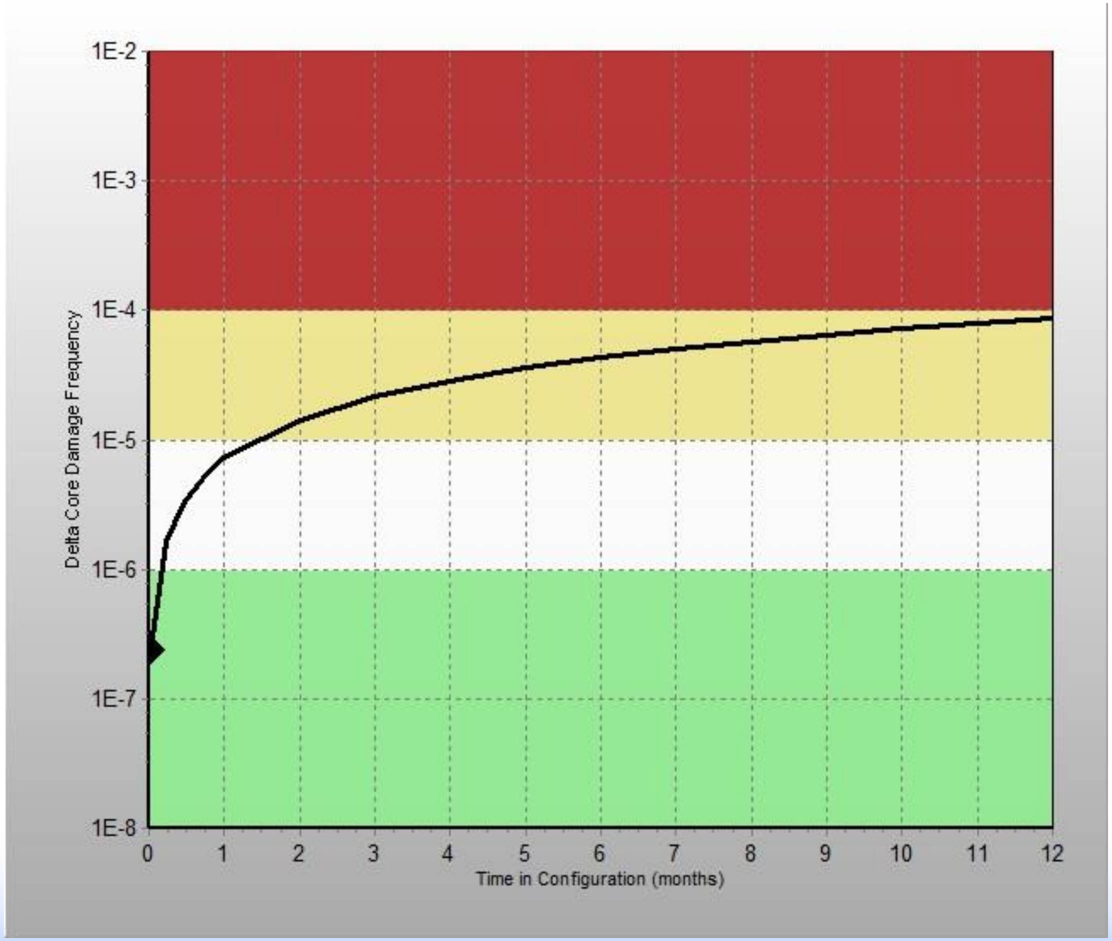
Containment Cooling System (CCS) CCS Train A MDP (CCS-MDP-A) had adjustments made to the following failure modes:

- Fails to run (FR) was changed from 2.400E-4 to True (Component Is Failed). This implies that the component was failed for the entire duration.

Multi-pass option with cut set update calculation used.

# SDP - Detailed Risk Evaluation

## Example SPAR model Results



# Final Risk Significance of Inspection Finding

- SDP Evaluation:
  - Cannot assess impact of degraded equipment reliability
  - Set up to analyze conditions that exist for a period of time, not set up for initiating event assessments (IE has occurred)
    - Initiating event assessment results in CCDP "spike," which is different type of assessment than the SDP assessment
  - Estimates risk significance of licensee performance problems
  - Final result is increase in CCDP, or incremental CCDP, caused by the performance problem

# Final Risk Significance of Inspection Finding

- **SDP Results are calculated:**
  - **Incremental Core Damage Probability (ICDP), also referred to as incremental conditional core damage probability (ICCDP)**

    **= (CCDF - CDF) * duration**

    **= ICDF * duration; or**

    **= CCDP - BCDP**

  - **Incremental Large Early Release Probability (ILERP), also referred to as incremental conditional large early release probability (ICLERP )**

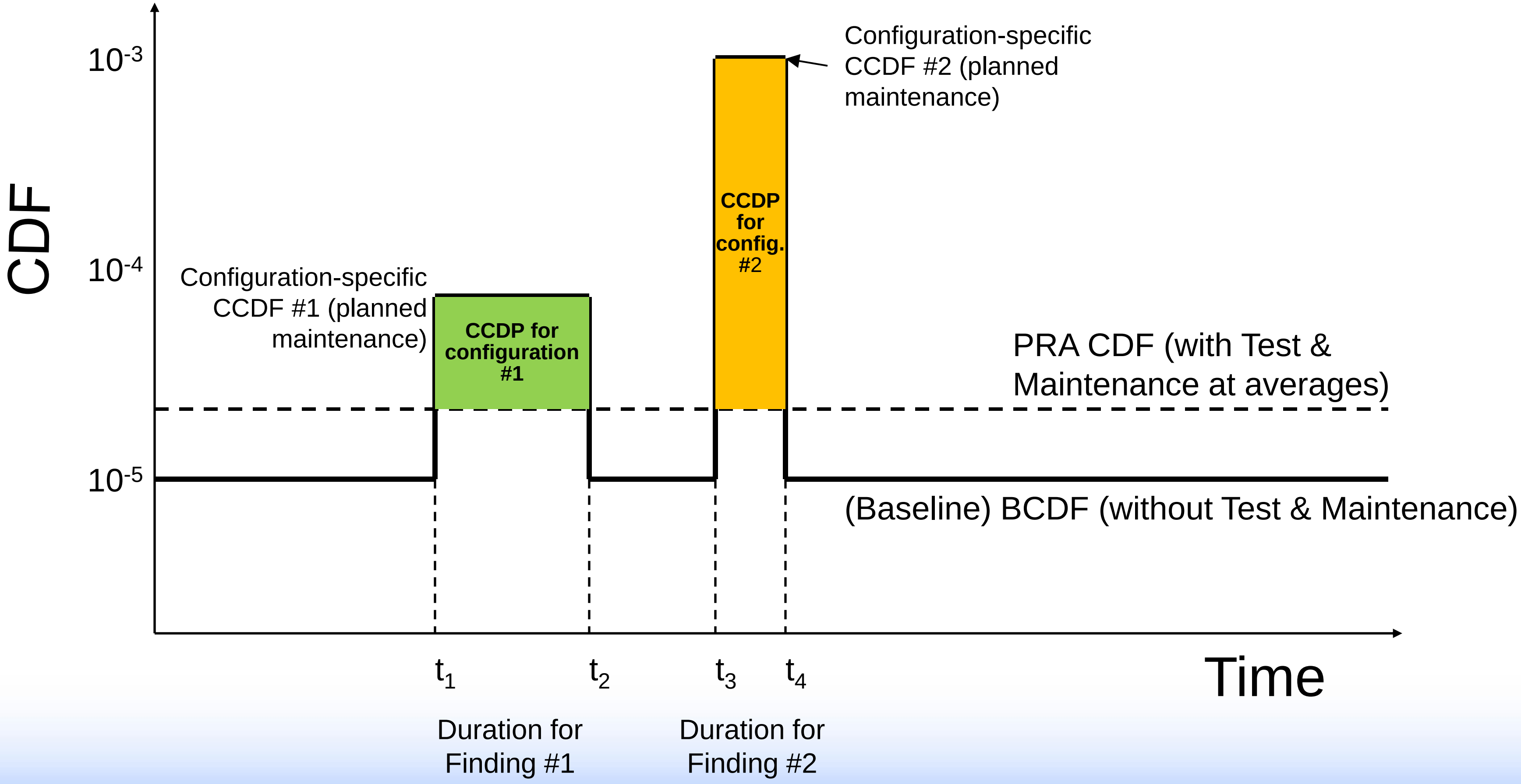
    **= (CLERF - LERF) * duration**

    **= ILERF * duration; or**

    **= CLERP - BLERP**

**NOTE: ∆LERF (ILERF) criteria is an order of magnitude less than ∆CDF (ICDF)**

# Conditional Core Damage Probability (CCDP)



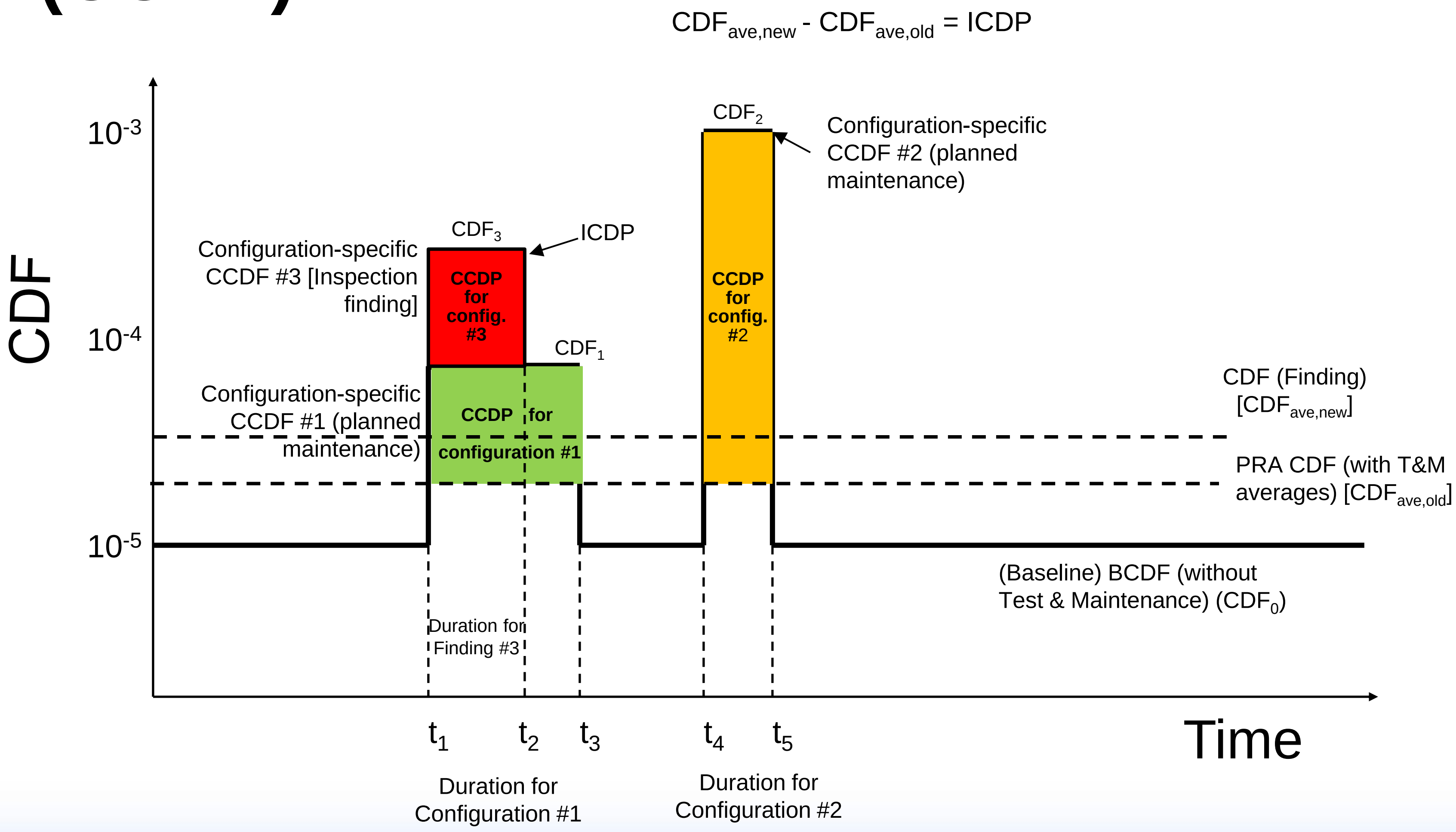
# Final Risk Significance of Inspection Finding

- **SDP Results (cont.)**
  - **The result of SDP is a difference or change in a probability**
    - **Probability of core damage given a degraded condition for a specified duration minus the probability of core damage given no degraded condition for the same specified duration**
    - **It turns out that, numerically, the incremental CCDP is equal to the increase in the time-weighted average CDF, if the averaging is done for a period of one year**
  - **SDP risk significance colors in terms of increase in annual time-averaged CDF;**
    - **Red** if $\Delta$CDF is $> 10^{-4}$/yr
    - **Yellow** if $\Delta$CDF is $> 10^{-5}$/yr and $\leq 10^{-4}$/yr
    - **White** if $\Delta$CDF is $> 10^{-6}$/yr and $\leq 10^{-5}$/yr
    - **Green** if $\Delta$CDF is $\leq 10^{-6}$/yr

# Risk Significance of Maintenance-Related Inspection Finding

- Maintenance-related SDP estimates risk significance of licensee performance problems
  - Does not include equipment out of service for test or maintenance, unless related specifically to performance problem
  - Evaluation result is increase in CDP
    - Called ICDP (see 0609 Appendix K)
- Inspection findings assigned a color representing significance of the finding

# Conditional Core Damage Probability (CCDP)



$CDF_{ave,new} - CDF_{ave,old} = ICDP$
CDF
$10^{-3}$
$10^{-4}$
$10^{-5}$
$CDF_2$
Configuration-specific CCDF #2 (planned maintenance)
$CDF_3$
ICDP
Configuration-specific CCDF #3 [Inspection finding]
CCDP for config. #3
CCDP for config. #2
$CDF_1$
Configuration-specific CCDF #1 (planned maintenance)
CCDP for configuration #1
CDF (Finding) $[CDF_{ave,new}]$
PRA CDF (with T&M averages) $[CDF_{ave,old}]$
(Baseline) BCDF (without Test & Maintenance) $(CDF_0)$
Duration for Finding #3
$t_1$
$t_2$
$t_3$
$t_4$
$t_5$
Time
Duration for Configuration #1
Duration for Configuration #2

# Significance Determination Process (SDP) Principles

- Key Points of Section:
  - SDP Purpose: To use risk insights to help NRC inspectors and staff determine the safety or security significance of inspection findings. These findings are combined with the Performance Indicator information in assessing licensee performance.
  - SDP Objectives: To characterize the significance of inspection findings, to provide a common framework communicating tool, provide a basis for timely assessment and enforcement actions, and to provide inspectors with plant-specific risk information for use in risk-informing the inspection program.
  - Final Risk Significance of Inspection Finding (with $\Delta$LERF findings an order of magnitude less)
    - Red: $\Delta CDF > 10^{-4}/yr$
    - Yellow: $10^{-4}/yr \geq \Delta CDF > 10^{-5}/yr$
    - White: $10^{-5}/yr \geq \Delta CDF > 10^{-6}/yr$
    - Green: $10^{-6}/yr \geq \Delta CDF$

# Page Intentionally Left Blank

# 17. Introduction to Risk-Informed Decision-Making

# Introduction to Risk-Informed Decision-Making

- **Purpose: Discuss the principal steps in making risk-informed regulatory decisions, including the acceptance guidance contained in the Standard Review Plans (SRP) addressing this subject.**
- **Objective: Understand the basic philosophy behind risk-informed regulation and the primary source documents that describe the process.**

# Risk-Informed Regulatory Guides and SRPs

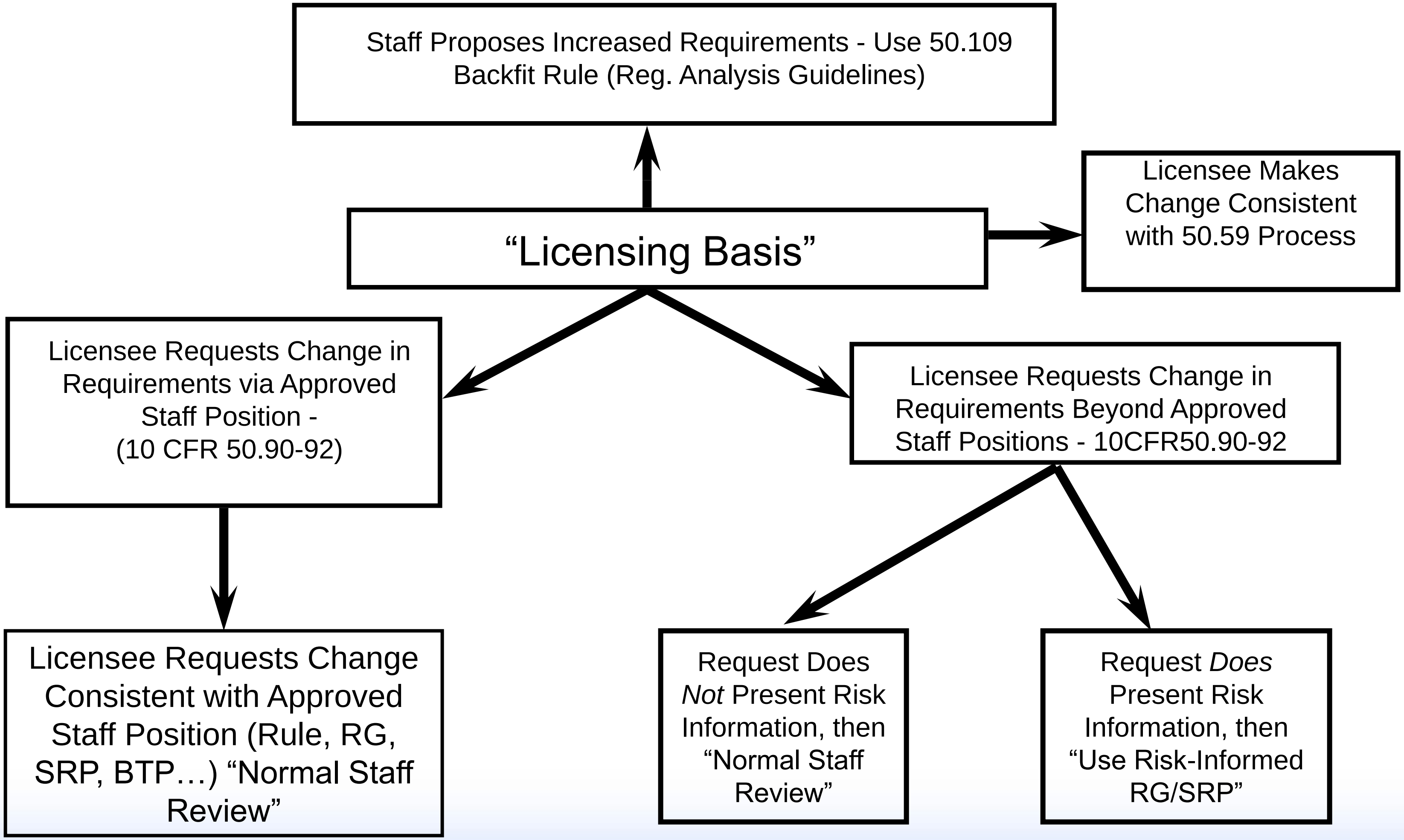
## Regulatory Guide

- R.G. 1.174 - General guidance to licensees for using PRA in risk-informed decisions for changes to licensing basis
- R.G. 1.175 - Application-specific guidance for inservice testing
- R.G. 1.177 - Application-specific guidance for technical specifications*
- R.G. 1.178 - Application-specific guidance for inservice inspection of piping*
- R.G. 1.200 – An approach for determining technical adequacy of PRA results for risk-informed activities

## Standard Review Plan

- SRP Chapter 19.2 - General guidance to staff for review of risk information used to support permanent changes to licensing basis
- SRP Section 3.9.7 - Application-specific guidance for inservice testing
- SRP Section 16.1 - Application-specific guidance for technical specifications
- SRP Section 3.9.8 - Application-specific guidance for inservice inspection of piping
- SRP Chapter 19.1 – Determining the technical adequacy of PRA results for risk-informed activities

# Decision Logic for Submittal Reviews



Staff Proposes Increased Requirements - Use 50.109 Backfit Rule (Reg. Analysis Guidelines)

"Licensing Basis"

Licensee Makes Change Consistent with 50.59 Process

Licensee Requests Change in Requirements via Approved Staff Position - (10 CFR 50.90-92)

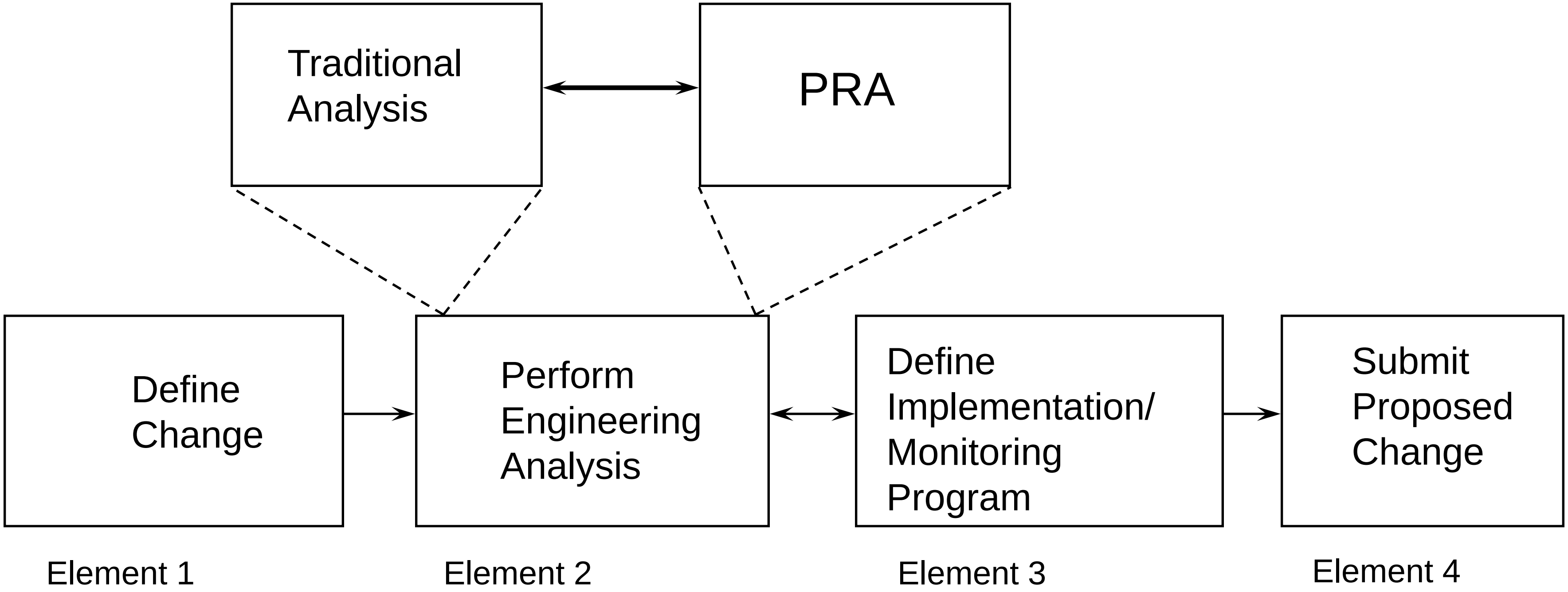
Licensee Requests Change in Requirements Beyond Approved Staff Positions - 10CFR50.90-92

Licensee Requests Change Consistent with Approved Staff Position (Rule, RG, SRP, BTP…) "Normal Staff Review"

Request Does *Not* Present Risk Information, then "Normal Staff Review"

Request *Does* Present Risk Information, then "Use Risk-Informed RG/SRP"

# Principal Elements of Risk-Informed Plant-Specific Decision Making



# Principles of Risk-Informed Regulation

- The proposed change meets current regulations unless it is explicitly related to a requested exemption or rule change
- The proposed change is consistent with the defense-in-depth philosophy
- The proposed change maintains sufficient safety margins
- Proposed increases in core damage frequency and risk are small and are consistent with the intent of the Commission's Safety Goal Policy Statement
- The impact of the proposed change should be monitored using performance measurement strategies

# Expectations from Risk-Informed Regulation (from RG-1.174)

- **All safety impacts of the proposed change are evaluated in an integrated manner as part of an overall risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions broadly by identifying and taking advantage of opportunities for reducing risk, and not just to eliminate requirements the licensee sees as undesirable. For those cases where risk increases are proposed, the benefits should be described and should clearly outweigh the proposed risk increases. The approach used to identify changes in requirements should be used to identify areas where requirements should be increased, as well as where they could be reduced.**

# Expectations from Risk-Informed Regulation

- **Acceptability of proposed changes should be evaluated by the licensee in an integrated fashion that ensures that all principles are met**
- **The use of core damage frequency (CDF) and large early release frequency (LERF) as bases for probabilistic risk assessment acceptance guidelines is an acceptable approach. Use of the Commission's Safety Goal Quantitative Health Objectives (QHOs) for this purpose is acceptable in principle and licensees may propose their use; however, in practice, implementing such an approach would require careful attention to the methods and assumptions used in the analysis, and treatment of uncertainties.**

# Expectations from Risk-Informed Regulation

- Increases in estimated CDF and LERF resulting from proposed changes will be limited to small increments and the cumulative effect of such changes should be tracked
- The scope and quality of the engineering analyses (including traditional and probabilistic analyses) conducted to justify the proposed change should be appropriate for the nature and scope of the change and should be based on the as-built and as-operated and maintained plant, including reflection of operating experience at the plant
- Appropriate consideration of uncertainty is given in analyses and interpretation of findings
- A program of monitoring, feedback, and corrective action should be used to address significant uncertainties

# Expectations from Risk-Informed Regulation

- The plant-specific PRA supporting licensee proposals has been subjected to quality controls such as an independent peer review or certification
  - Note: Owner’s groups have been conducting PRA reviews
- Data, methods, and assessment criteria used to support regulatory decision-making must be scrutable and available for public review

# Acceptance Guidelines

- Defense-in-depth is maintained
  - A reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved
  - Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided
  - System redundancy, independence, and diversity are preserved commensurate with the expected frequency and consequences of challenges to the system (e.g., no risk outliers)
  - Defenses against potential common-cause failures are preserved and the potential for introduction of new common-cause failure mechanisms is assessed

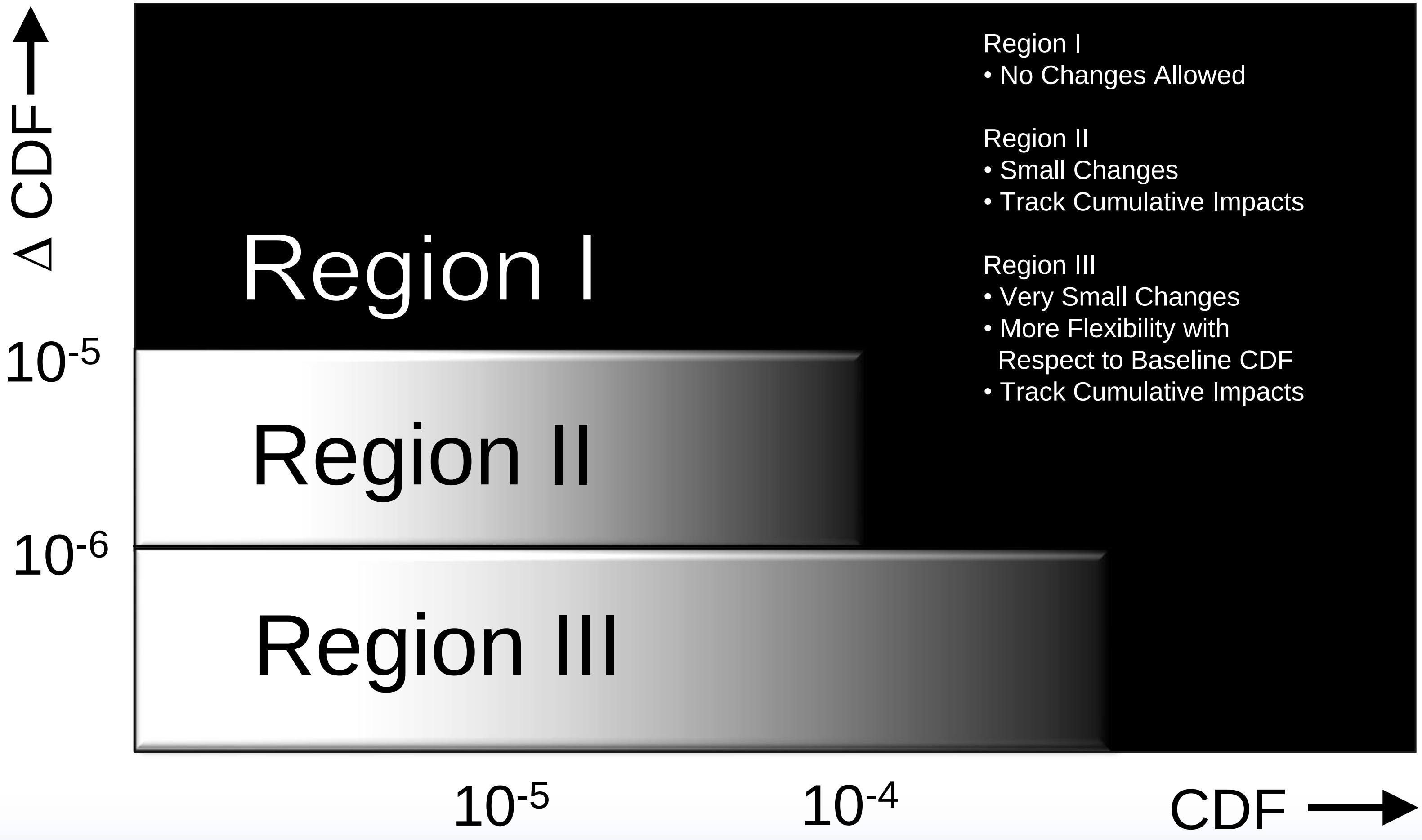
# Acceptance Guidelines

- Defense-in-depth is maintained
  - Independence of barriers is not degraded
  - Defenses against human errors are preserved
  - The intent of the General Design Criteria in 10 CFR 50, App. A, are maintained
- Sufficient safety margins are maintained
  - Codes and standards or alternatives approved for use by the NRC are met
  - Safety analysis acceptance criteria in the licensing basis (e.g., FSAR, supporting analyses) are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty

# Acceptance Guidelines

- Risk guidelines on following slides are met
  - Risk guidelines are intended for comparison with full-scope PRA results
    - Internal events (full power, low-power/shutdown)
    - External events (seismic, fire, etc.)
    - Use of less than full scope PRA may be acceptable in certain circumstances

# Mean Core Damage Frequency Acceptance Guidelines (RG 1.174)



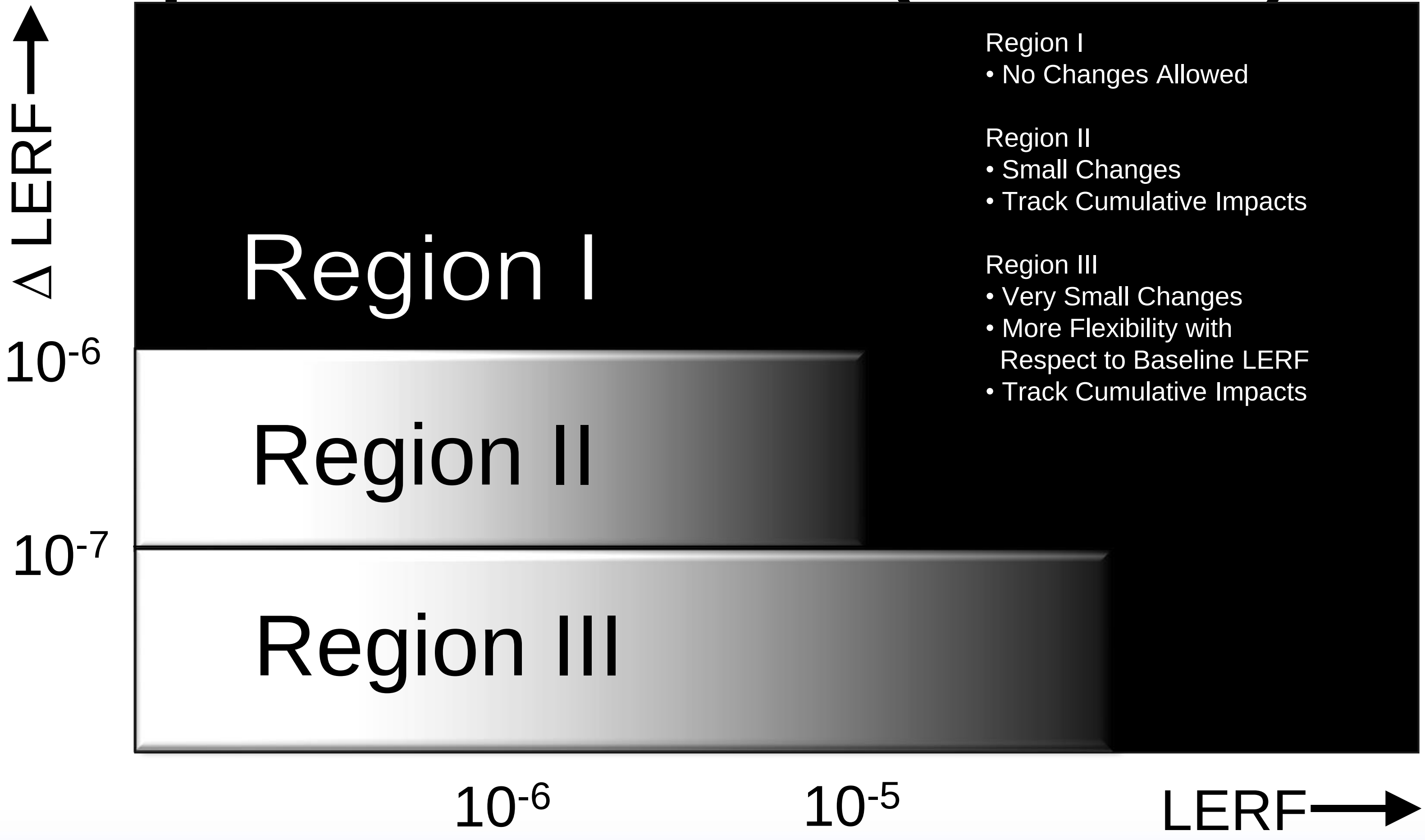
Region I
- No Changes Allowed

Region II
- Small Changes
- Track Cumulative Impacts

Region III
- Very Small Changes
- More Flexibility with Respect to Baseline CDF
- Track Cumulative Impacts

Figure 3. Acceptance Guidelines for Core Damage Frequency (CDF)

# Mean Large Early Release Frequency Acceptance Guidelines (RG 1.174)



Region I
- No Changes Allowed

Region II
- Small Changes
- Track Cumulative Impacts

Region III
- Very Small Changes
- More Flexibility with Respect to Baseline LERF
- Track Cumulative Impacts

Figure 4. Acceptance Guidelines for Large Early Release Frequency (LERF)

# Increased Management Attention

- Application is given increased NRC management attention when the calculated values of the changes in the risk metrics, and their baseline values when appropriate, approach the guidelines.  The issues addressed by management will include
  - Cumulative impact of previous changes and trend in CDF and LERF (licensee’s risk management approach)
  - Impact of proposed change on operations complexity, burden on operating staff, and overall safety practices
  - Benefit of the change with respect to its risk increase
  - Level 3 PRA information, if available

# Consideration of Uncertainties

- Use mean values (not median) of CDF and LERF used for comparison with guidelines
- Identify important sources of uncertainty
  - Parameter
  - Modeling
  - Completeness
- Perform sensitivity calculations on parameter and modeling uncertainties
- Perform quantitative or qualitative analysis on completeness uncertainties
- Results of sensitivity studies should generally meet guidelines
- Region III - no need to calculate uncertainty on baseline CDF/LERF

# Combined Change Requests

- Several changes can be combined in one submittal
- Will be reviewed against acceptance guidelines
  - Individually with respect to defense in depth
  - Cumulatively
- Combined changes should be related.  For example
  - Be associated with same system, function, or activity
  - Changes reviewed individually against risk criteria if not closely related
- Combined changes should not trade many small risk decreases for a large risk increase (i.e., create a new significant contributor to risk)

# Key Issues in PRA Quality

- Ensure that, within scope, PRA analysis is complete and has appropriate level of detail
  - Consideration of relevant initiating events, plant systems, and operator actions
  - Analysis reflects plant-specific operating experience, design features, and accident response
  - All calculations are documented
- PRA methodology and associated input
  - Influence of models, input data, and assumptions on results and conclusions
- Licensee review and QA process
  - Peer review
    - Nuclear Energy Institute, “Probabilistic Risk Assessment Peer Review Process Guidance,” NEI-00-02, Revision A3, March 20, 2000.
  - Certification
  - Standards
    - American Society of Mechanical Engineers, “Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, Addenda to ASME/ANS RA-S-2008,” ASME/ANS RA-Sa-2009, February 2, 2009.
    - American Nuclear Society, “American National Standard External-Events PRA Methodology,” ANSI/ANS-58.21-2007
  - Regulatory Guides
    - Regulatory Guide 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities,” March 2009.

# NRC Staff and Management Responsibilities

- Ensure that licensing submittals are identified and processed in accordance with risk-informed guidance
- Identify current requirements that could be significantly enhanced with a risk-informed and/or performance-based approach
- Ensure objectives of risk-informed regulation are met
  - Enhanced safety decisions
  - Efficient use of NRC resources
  - Reduced unnecessary regulatory burden on industry
- Ensure adequate staff training on use of risk-informed guidance and underlying PRA technical disciplines
- Maintain current levels of safety

# Review of Introduction to Risk-Informed Decision-Making

- **Key Points of Section:**
  - **With Risk-Informed Decision-Making, PRA is used in conjunction with traditional analysis to submit a proposed change in regulation.**
  - **Principles of Risk-Informed Regulation:**
    - **The proposed change meets current regulations**
    - **Defense-in-depth philosophy is kept in tack**
    - **Proposed changes maintain sufficient safety margins**
    - **Increases in CDF are small**
    - **The impact of the change should be monitored.**
  - **NRC Staff and Management Responsibilities:**
    - **Ensure that licensing submittals follow the risk-informed guidance**
    - **Identify current requirements  that could be enhanced with a risk-informed approach**
    - **Ensure that the objectives of risk-informed regulation is met**
    - **Ensure adequate staff training on the use of risk-informed guidance**
    - **Maintain current levels of safety!**

Page Intentionally Left Blank

# Appendix

# Acronyms and Abbreviations

# Acronyms and Abbreviations (1 of 3)

| | |
|---|---|
| AC | Alternating current |
| ACRS | Advisory Committee on Reactor Safeguards |
| ADS | Automatic depressurization system |
| ADV | Atmospheric dump valve |
| AEOD | Office for Analysis and Evaluation of Operational Data |
| AFW | Auxiliary feedwater |
| AOP | Abnormal Operating Procedure |
| AOT | Allowed outage time |
| AOV | Air-operated valve |
| APB | Accident progression bin |
| APET | Accident progression event tree |
| ASEP | Accident Sequence Evaluation Program |
| ASP | Accident Sequence Precursor |
| ATHEANA | A Technique for Human Event Analysis |
| ATWS | Anticipated transient without scram |
| BC | Boundary condition |
| BNL | Brookhaven National Laboratory |
| BTP | Branch Technical Position |
| BWR | Boiling water reactor |
| BWROG | BWR Owners' Group |
| BWST | Borated water storage tank |
| CCDF | Complementary cumulative distribution function |
| CCDP | Conditional core damage probability |
| CCFP | Conditional containment failure probability |
| CCF | Common-cause failure |
| CCI | Core-concrete interaction |
| CCW | Component Cooling Water |
| CDC | Centers for Disease Control and Prevention |
| CDE | Consolidated Data Entry program |
| CDF | Core damage frequency |
| CDF | Cumulative Density Function |
| CDFM | Conservative Deterministic Failure Margin |
| CDP | Core damage probability |
| CE | Combustion Engineering |
| CEOG | Combustion Engineering Owners' Group |
| CFR | Code of Federal Regulations |
| CLB | Current licensing basis |
| CRD | Control rod drive |
| CSIP | Charging/safety injection pump |
| CST | Condensate storage tank |
| CW | Circulating water |
| DBA | Design basis accident |
| DC | Direct current |
| DCH | Direct containment heating |
| DF | Decontamination factor |
| DFSD | Dominant functional sequence diagram |
| DHR | Decay heat removal |
| ECCS | Emergency core-cooling system |
| EDG | Emergency diesel generator |
| EOOS | Equipment Out of Service System |
| EOP | Emergency Operating Procedure |
| EPA | Environmental Protection Agency |
| EPIX | Equipment performance and information exchange system |
| EPRI | Electric Power Research Institute |
| ESF | Engineered safeguards feature |
| ESW | Emergency service water |
| ESWGR | Emergency switchgear |
| ET | Event tree |
| FCI | Fuel-coolant interaction |
| FIVE | Fire-Induced Vulnerability Evaluation |
| FMEA | Failure modes and effects analysis |
| FSAR | Final Safety Analysis Report |
| FT | Fault tree |
| F-V | Fussell-Veseley (importance) |
| FW | Feedwater |
| GE | General Electric |
| GL | Generic Letter |
| GOTHIC | Generation of Thermal-Hydraulic Information for Containment |
| GSI | Generic Safety Issue |
| HCLPF | High confidence, low probability of failure |
| HCR | Human Cognitive Reliability |
| HEP | Human error probability |
| HHSI | High-head safety injection |
| HLW | High-level waste |
| HPCI | High-pressure coolant injection |

# Acronyms and Abbreviations (2 of 3)

| | |
|---|---|
| HPCS | High-pressure core spray |
| HPI | High-pressure injection |
| HPR | High-Pressure re-circulation |
| HPSI | High-pressure safety injection |
| HRA | Human reliability analysis |
| HVAC | Heating, ventilation, and air conditioning |
| HTGR | High-Temperature Gas Reactor |
| HX | Heat exchanger |
| ICDP | Incremental core damage probability |
| ICCDP | Incremental conditional core damage probability |
| ILERP | Incremental large early release probability |
| ICLERP | Incremental conditional large early release probability |
| IE | Initiating event |
| IMC | Inspection Manual Chapter |
| INL | Idaho National Laboratory |
| INPO | Institute for Nuclear Plant Operations |
| IPE | Individual Plant Examination |
| IPEEE | Individual Plant Examination for External Events |
| IREP | Interim Reliability Evaluation Program |
| ISA | Integrated Safety Analysis |
| ISI | In-service inspection |
| ISLOCA | Interfacing system loss-of-coolant accident |
| IST | In-service testing |
| JCO | Justification for Continued Operation |
| LB | Licensing basis |
| LCO | Limiting Condition for Operation |
| LER | Licensee Event Report |
| LERF | Large early release frequency |
| LERP | Large early release probability |
| LRF | Large release frequency |
| LLNL | Lawrence Livermore National Laboratory |
| LLW | Low-level waste |
| LOCA | Loss-of-coolant accident |
| LOOP | Loss of offsite power |
| LOSP | Loss of offsite power |
| LP/SD | Low power and shutdown |
| LPCI | Low-pressure coolant injection |
| LPCS | Low-pressure core spray |
| LPI | Low-pressure injection |
| LPR | Low-pressure re-circulation |
| LPSI | Low-pressure safety injection |
| LPZ | Low population zone |
| LWR | Light water reactor |
| MAAP | Modular Accident Analysis Program |
| MACCS | MELCOR Accident Consequence Code System |
| MCS | Minimal cut set |
| MCSUB | Minimal cut set upper bound |
| MDP | Motor-driven pump |
| MGL | Multiple Greek letter |
| MOV | Motor-operated valve |
| MSIV | Main steam isolation valve |
| MSP | Maintenance and Surveillance Program |
| MSPI | Mitigating System Performance Index |
| NCV | Non-cited violation |
| NEI | Nuclear Energy Institute |
| NFPA | National Fire Protection Association |
| NMSS | Office of Nuclear Materials Safety and Safeguards |
| NOED | Notice of Enforcement Discretion |
| NPP | Nuclear Power Plant |
| NPRDS | Nuclear Plant Reliability Data System |
| NRC | Nuclear Regulatory Commission |
| NRR | Office Nuclear Reactor Regulation |
| NUMARC | Nuclear Management and Resources Council |
| OOS | Out of service |
| ORAM | Outage Risk Assessment and Management |
| ORNL | Oak Ridge National Laboratory |
| OSHA | Occupational Safety and Health Administration |
| P&ID | Piping and instrumentation diagram |
| PA | Performance assessment |
| PCC | PRA Coordinating Committee |
| PCS | Power conversion system |
| PDS | Plant damage state |
| PI | Performance Indicator |

# Acronyms and Abbreviations (3 of 3)

| | |
|---|---|
| PM | Preventive maintenance |
| PORV | Power-operated relief valve |
| POS | Plant operating state |
| PRA | Probabilistic risk assessment |
| PRT | Plant response tree |
| PRV | Pressurizer power-operated relief valves |
| PSA | Probabilistic safety assessment |
| PSF | Performance shaping factor |
| PTFG | PRA Training Focus Group |
| PTS | Pressurized thermal shock |
| PWR | Pressurized water reactor |
| QA | Quality Assurance |
| QHO | Quantitative health objective |
| QRA | Quantitative risk analysis |
| RAW | Risk achievement worth |
| RASP | Risk Assessment Standardization Program |
| RBCCW | Reactor building closed cooling water |
| RCIC | Reactor core isolation cooling |
| RCP | Reactor coolant pump |
| RCS | Reactor coolant system |
| RES | Office of Nuclear Regulatory Research |
| RG | Regulatory Guide |
| RHR | Residual heat removal |
| RI | Resident Inspector |
| ROP | Reactor Oversight Process |
| RPP | Risk-informed Performance-based Plan |
| RPS | Reactor protection system |
| RPV | Reactor pressure vessel |
| RRW | Risk reduction worth |
| RSS | Reactor Safety Study |
| RVC | Relief valve re-close |
| RWST | Refueling water storage tank |
| S/D | Shutdown |
| SAR | Safety Analysis Report |
| SBO | Station blackout |
| SDC | Shutdown cooling |
| SDP | Significance Determination Process |
| SER | Safety Evaluation Report or Staff Evaluation Report for IPE/IPEEE |
| SG | Steam generator |
| SGTR | Steam generator tube rupture |
| SHARP | Systematic Human Action Reliability Procedure |
| SI | Safety injection |
| SIF | Seal injection flow |
| SIT | Safety injection tank |
| SLOCA | Small loss-of-coolant accident |
| SNL | Sandia National Laboratory |
| SPAR | Standardized Plant Analysis Risk |
| SRA | Senior Reactor Analyst |
| SRI | Senior Resident Inspector |
| SRP | Standard Review Plan |
| SRV | Safety/relief valve |
| SSC | Structures, systems, and components |
| SSET | Support state event tree |
| STG | Source term group |
| SW | Service water |
| SWGR | Switch gear |
| TBCCW | Turbine building closed cooling water |
| TDP | Turbine-driven pump |
| TER | Technical Evaluation Report |
| THERP | Technique for Human Error Rate Prediction |
| TRC | Time reliability correlation |
| UAI | Unavailability Index |
| URI | Unreliability Index |
| USI | Unresolved Safety Issue |
| VCT | Volume control tank |
| WANO | World Association of Nuclear Operators |
| WOG | Westinghouse Owners' Group |

# Brief Annotated Bibliography

# Bibliography (1 of 2)

U.S. NRC Intranet – see Office of Nuclear Regulatory Research web page; Risk Assessment Standardization Project (RASP) toolbox

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.
Original full Level-3 PRA of Peach Bottom and Surry, NRC sponsored, project team headed by Prof. N. Rasmussen (MIT).

Kaplan, S. and B.J. Garrick, 1981, "On the Quantitative Definition of Risk," *Risk Analysis*, 1, 11-27.
Established basic concepts still used in PRA.

U.S. NRC, 1981, *Fault Tree Handbook*, NUREG-0492, January 1981.
Basics on probability theory, set theory, Boolean algebra, and fault trees. This report is available in PDF form from NRC Internet home page.

U.S. NRC, 1994, *A Review of NRC Staff Uses of Probabilistic Risk Assessment*, NUREG-1489, March 1994.
Survey of how staff uses PRA, identification of limitations on use of PRA, development of guidance on specific PRA uses, and identification of needed skills, training, and methods.

Apostolakis, G. and S. Kaplan, 1981, “Pitfalls in Risk Calculations,” *Reliability Engineering*, 2, 135-145.
Identifies and discusses some common mistakes made in PRAs.

ANS/IEEE, 1983, *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*, NUREG/CR-2300, January 1983.
Basic reference on “how to do a PRA,” still commonly used.

Vesely, W. E. et al., 1983, *Measures of Risk Importance and Their Applications*, NUREG/CR-3385.
Importance measures.

Kolaczkowski, A. et al., Good Practices for Implementing Human Reliability Analysis, NUREG-1792, April 2005. Expands upon the ASME PRA standard as it relates to HRA.

# Bibliography (2 of 2)

Forester, J. et al., Evaluation of Human Reliability Analysis Methods Against Good Practices, NUREG-1842, September 2006. A companion report to NUREG-1792 in which the authors of that report evaluate domestic HRA methods against the HRA Good Practices. Written with a general audience of NRC submittal reviewers in mind who are not experts in HRA.

Apostolakis, G., 1990, "The Concept of Probability in Safety Assessments of Technological Systems," *Science*, 250, 1359-1364.
Interesting reading with respect to how the term probability is interpreted.

U.S. NRC, 1990, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, Vol. 1-3.
Second major assessment (after WASH-1400) of NPP risks sponsored by NRC. Supporting work documented in series of NUREG/CRs (NUREG/CR-4550, Vol. 1-7. Rev. 1 – Level-1 PRAs; NUREG/CR-4551, Vol. 1-7, Rev. 1 – Level-2 portions of the PRAs).

IAEA, 1990, *Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessment*, IAEA-TECDOC-543.
International perspective on PRA (commonly referred to as PSA outside the U.S.).

Kumamoto, Hieromitsu and Henley, Ernest J., Probabilistic Risk Assessment and Management for Engineers and Scientists, Second Edition, IEEE Press, 1996. Textbook on PRA.

Bedord, Tim and Cooke, Roger, Probabilistic Risk Analysis: Foundations and Methods, Cambridge University Press, 2001. Another PRA text, more oriented toward mathematical foundations. Covers state-of-the-art topics such as binary decision diagrams (BDDs) and software reliability. Includes material on decision analysis.

Keller, William and Modarres, Mohammed, “A Historical Overview of Probabilistic Risk Assessment Development and Its Use in the Nuclear Power Industry: a Tribute to the Late Professor Norman Rasmussen,” Reliability Engineering and System Safety, 89 (2005) 271-285.

# Major Journals and Conferences

# Major Journals and Conferences

- Journals
  - Reliability Engineering and System Safety, published by Elsevier.
  - Risk Analysis, published by the Society for Risk Analysis
  - IEEE Transactions on Reliability, published by IEEE
- Conferences
  - Probabilistic Safety Assessment & Management (PSAM), held every two years.
  - Probabilistic Safety Assessment (PSA), sponsored by ANS, held every two years.
  - U.S. Nuclear Regulatory Commission's (USNRC's) Regulatory Information Conference (RIC), held every year.

# Risk Assessment Training Courses

# Risk Assessment Training Courses

- P-102  Bayesian Inference in Risk Assessment - (5 days)  This course covers basic applications of Bayesian statistical inference in risk assessment. Through lectures, workshop problems, and case studies participants are presented with mathematical techniques from probability and Bayesian inference that are currently being applied in risk assessments. The topics covered include a review of probability, selected probability models important to risk assessment, elementary Bayesian parameter estimation, introduction to Bayesian model validation, and uncertainty propagation through risk assessment models. The course is computer-based and utilizes Excel, RADS, and OpenBUGS, which is useful for more advanced problems. Students should be familiar with the basic operations of Excel, but do not need to be familiar with RADS or OpenBUGS.

- P-502  Bayesian Inference in Risk Assessment - Advanced Topics - (5 days)  This course explores advanced applications of Bayesian statistical inference in risk assessment through lectures and hands-on case studies using OpenBUGS. Students should have completed Bayesian Inference in Risk assessment (P-102) course. Students are expected to be familiar with OpenBUGS at the level as presented in P-102.

# Risk Assessment Training Courses

- P-105 PRA Basics for Regulatory Applications - (3 days) This course addresses the special needs of the regulator who requires knowledge of probabilistic risk assessment (PRA) issues and insights to better evaluate the effects of design, testing, maintenance, and operating strategies on system reliability. The full range of PRA topics is presented in abbreviated form with the goal of introducing the regulatory staffs to the basic concepts and terminology of PRA as applied to the inspection process. The course uses actual plant PRAs and IPEs and stresses the uses and applications of these publications in planning audits and inspections and evaluating plant safety issues.

- P-108 NRC MC 0609 Appendix F Fire Protection SDP Training - (3 days) This course introduces the methodology described in Appendix F to the NRC Manual Chapter 0609, Fire Protection Significance Determination Process (SDP). Students will be introduced to the underlying theory of this SDP and will be taught to use PC-based tool for aiding in the execution of the SDP.

# Risk Assessment Training Courses

- P-109 Assessing the Adequacy of Models for Risk-Informed Decisions - (1 day) This course is aimed at improving awareness of the factors that contribute to uncertainty in predictive models (both probabilistic and deterministic), and the need to identify, characterize and communicate the uncertainties to risk-informed decision makers. This course discusses the fact that all models are just estimates of reality and subject to many implicit assumptions and biases. It is the responsibility of the analyst to explicitly understand and communicate those assumptions, the limits of model applicability, and the uncertainty on the output. Much time is spent in the class on developing an appreciation for the value of a questioning attitude toward model use and reliance.

- P-111 PRA Technology and Regulatory Perspectives - (9 days) This course addresses the special needs of Regional Inspectors, Resident Inspectors, and other technical personnel who require knowledge of probabilistic risk assessment (PRA) issues and insights to better evaluate the effects of design, testing, maintenance, and operating strategies on system reliability. The course will concentrate on the use of PRA results in inspection planning, monitoring licensee performance, and reviewing licensee risk-informed submittals.

# Risk Assessment Training Courses

- P-200 System Modeling Techniques for PRA - (4 days) This course will help develop advanced user level skills in performing event tree and fault tree analysis, with numerous practice workshops. The course covers the calculation of initiating event frequencies, component failure rate, and the use of "super components" to create fault trees. A second focus of the course is dependent failure analysis, including multiple Greek letter, binomial failure rate, basic parameter methods, and alpha factor methods for estimating common cause/common mode failure probabilities.

- P-201 SAPHIRE Basics - (4 days) This course provides hands-on training in the use of Systems Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE) to perform PRA on a PC. When the course is completed, the participants are able to: build fault tree models on the PC, assign reliability data, analyze the fault trees and develop minimal cut sets, calculate various importance measures, perform uncertainty analysis, analyze accident sequences, create and quantify accident sequences, and generate reports.

- P-202 Advanced SAPHIRE - (4 days) This course provides hands-on training in the advanced features of Systems Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE) to perform PRA on a PC. SAPHIRE allows the user to build and evaluate the models used in PRA. Participants will learn advanced features such as Flag Sets, advanced basic events (i.e., template, compound, common-cause, and human error events), and various rule editors (i.e., event tree linking, recovery, and partition rules).

# Risk Assessment Training Courses

- P-203  Human Reliability Assessment - (4 days)  This course serves as an introduction to Human Reliability Assessment (HRA) including the methods used in modeling of human errors and various methods of estimating their probabilities. This course is designed to teach introductory level skills in HRA and includes a broad introduction to HRA and its applications. A discussion of HRA strengths, limitations, and results is also included.

- P-204  External Events - (4 days)  This course deals with the analysis of external events such as fires, floods, earthquakes, high winds, and transportation accidents. The course has been developed to provide the student with information that can be used in the review of IPEEE results.

- P-300  Accident Progression Analysis - (3 days)  This course deals with the portion of probabilistic risk assessment typically referred to as Level 2 analysis. The course will address accident phenomenology under post-core damage conditions and will discuss development of PRA models for this severe accident regime. The emphasis of the course is on the important modeling issues and how they are dealt with, rather than how to use specific modeling software.

# Risk Assessment Training Courses

- P-301 Accident Consequence Analysis - (5 days) This course deals with the portion of PRA typically referred to as Level 3 analysis. The course addresses environmental transport of radionuclides and the estimation of offsite consequences from core damage accidents. The major emphasis of the course is on important modeling issues and how they are dealt with, with a secondary emphasis on how to use specific modeling software. Hands-on modeling examples using the MACCS2 (MELCOR Accident Consequence Code System) software code are covered in the course.

- P-302 Risk Assessment in Event Evaluation - (4 days) This course covers the use of PRA techniques to assess the risk significance of initiating events and condition assessments that occur at operating reactors. The course addresses the use of simplified PRA models to estimate conditional damage probability using SAPHIRE. In addition, common cause and non-recovery probabilities will also be addressed. The course includes conventional workshops and SAPHIRE program workshops.

- P-501 Advanced Risk Assessment Topics – (4 days) The primary objective of this course is to provide a hands-on approach to the investigation and application of a variety of advanced risk assessment methods, tools, and techniques. This objective will be accomplished by discussing select topics followed by hands-on application for example exercises. As a result of these hands-on exercises, the student will become more proficient with Bayesian methods and the use of tools such as SAPHIRE, Excel, and OpenBUGS for numerical analysis.

# Risk Assessment Training Courses

- P-400 Introduction to Risk Assessment for Materials Safety and Waste Management – (3 days) This course introduces risk assessment concepts for nuclear materials and radioactive waste applications. The NRC’s policy on the use of risk information as well as the framework for employing risk-informed regulation for nuclear materials and radioactive waste applications is presented. Various risk assessment concepts and methodologies are introduced and discussed. Examples of the risk assessment methodologies are presented, and some of the strengths and weaknesses associated with the various methodologies are addressed. Several case studies are presented to demonstrate the risk assessment methodology used for the respective study and the risk insights gained are discussed. This course also addresses the perception, communication, and management of risk based on the results obtained from the risk assessment.

- P-401 Introduction to Risk Assessment for Materials Safety and Waste Management Overview – (1 day) This course provides a brief overview of risk assessment concepts for nuclear materials and radioactive waste applications. The NRC's policy on the use of risk information as well as the framework for employing risk-informed regulation for nuclear materials and radioactive waste applications is presented. Various risk assessment concepts and methodologies are introduced and discussed. Examples of the risk assessment methodologies are presented, and some of the strengths and weaknesses associated with the various methodologies are addressed. This course also addresses the topics of risk perception, risk communication, and risk management.

- P-406 Human Reliability Analysis for Materials Safety and Waste Management – (3 days) This course serves as an introduction to Human Reliability Analysis for nuclear materials and radioactive waste applications. This course provides an overview of HRA, introduces the concepts and methods useful in examining human error, sensitizes staff to recognize the need and importance of HRA in their daily work, and reviews the contribution of human error to selected events for nuclear materials and radioactive waste applications. As part of this overview, students are introduced to key components of HRA - error taxonomies, performance shaping factors and context, error identification, error modeling and error quantification. This course also introduces various methods for estimating human error probabilities. A discussion of HRA strengths, limitations, and results is also included.

Idaho National Laboratory

# Workshop Solutions

# Probability and Frequency Questions

- 1. An event occurs with a frequency of 0.02 per year.
  - 1.1. What is the probability that at least one event will occur within a given year?
    - P{event <1 year} = $1\text{-}e^{-(2E\text{-}2)(1)}$ = 1-0.9802 = 0.0198 = 1.98E-2
    - Or P{event <1 year} ≈ $\lambda t$ ≈ (2E-2)(1) ≈ 2E-2
  - 1.2. What is the probability that at least one event will occur within 50 years?
    - P{event <50 years} = $1\text{-}e^{-(2E\text{-}2)(50)}$ = $1\text{-}e^{-1}$ = 1-0.3679 = 0.6321 = 6.321E-1
- 2. Event A occurs with a frequency of 0.1 per year. Event B occurs with a frequency of 0.3 per year.
  - 2.1. What is the probability that at least one event (either A or B) will occur within a given year?
    - P(A) = $1 - e^{-(\lambda A)t}$ = $1 - e^{-(0.1)1}$ = 1 – 0.9048 = 0.0952
    - P(B) = $1 - e^{-(\lambda B)t}$ = $1 - e^{-(0.3)1}$ = 1 – 0.7408 = 0.2592
    - P(A + B)=P(A)+P(B)-P(AB)=0.0952+0.2592–[(0.0952)(0.2592)]=0.3543–0.0247=0.3297
    - Or P(A + B) = P(A) + P(B) - P(AB) = $1 - e^{-(\lambda A + \lambda B)\ t}$ = $1 - e^{-(0.1 + 0.3)\ 1}$ = 1 – 0.6703 = 0.3297
  - 2.2. What is the probability that at least one event (either A or B) will occur within 5 years?
    - P(A) = $1 - e^{-(\lambda A)t}$ = $1 - e^{-(0.1)5}$ = 1 – 0.6065 = 0.3935
    - P(B) = $1 - e^{-(\lambda B)t}$ = $1 - e^{-(0.3)5}$ = 1 – 0.2231 = 0.7769
    - P(A + B)=P(A)+P(B)-P(AB)=0.3935+0.7769–[(0.3935)(0.7769)]=1.1703–0.3057=0.8647
    - Or P(A + B) = P(A) + P(B) - P(AB) = $1 - e^{-(\lambda A + \lambda B)\ t}$ = $1 - e^{-(0.1 + 0.3)\ 5}$ = 1 – 0.1353 = 8.647E-1

# Probability and Frequency Questions

- 3. An experiment has a probability of 0.1 of producing a failure.
  - 3.1. What is the probability of observing exactly one failure if the experiment is repeated 4 times?
    - P[exactly 1 failure in 4 trials | 0.1] =

$$=\left(\frac{4!}{1!(4-1)!}\right)(0.1)^{1}(1-0.1)^{4-1}=\left(\frac{4!}{1!3!}\right)(0.1)^{1}(0.9)^{3}=(4)(0.1)(0.7290)=0.2916$$

  - 3.2. What is the probability of observing at least one failure if the experiment is repeated 4 times?
    - P[at least 1 failure in 4 trials | 0.1] =
    - P[1] + P[2] + P[3] + P[4] =
    - 0.2916 + 0.0486 + 0.0036 + 0.0001 = 0.3439
    - 1 – P[0 failures in 4 trials | 0.1] =

$$=1-\frac{4!}{0!(4-0)!}0.1^{0}(1-0.1)^{4-0}=1-\frac{4!}{0!4!}0.1^{0}0.9^{4}=1-(1)(1)(0.6561)=0.3439$$

# Probability and Frequency Questions

- **P[exactly 0 failures in 4 trials | 0.1] =**
- = $\frac{4!}{0!(4-0)!}$ **$(0.1)^0(0.9)^4$ = (1)(1)(0.6561) = 0.6561**

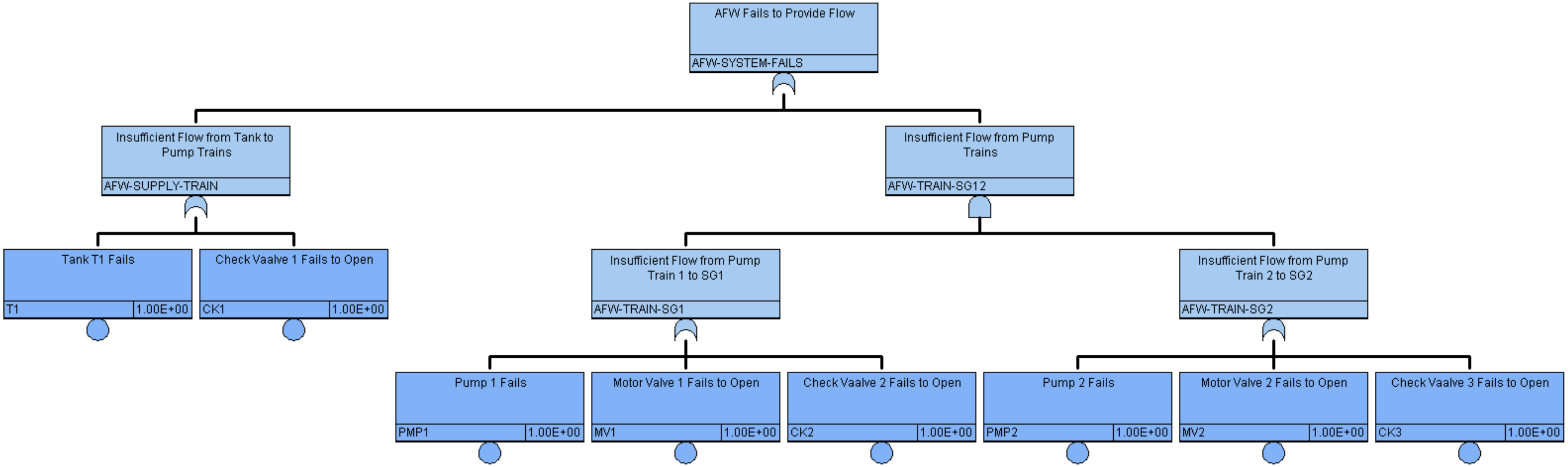
- **P[exactly 1 failure in 4 trials | 0.1 ] =**
- = $\frac{4!}{1!(4-1)!}$ **$(0.1)^1(0.9)^3$ = (4)(0.1)(0.7290) = 0.2916**

- **P[exactly 2 failures in 4 trials | 0.1 ] =**
- = $\frac{4!}{2!(4-2)!}$ **$(0.1)^2(0.9)^2$ = (6)(0.01)(0.81) = 0.0486**

- **P[exactly 3 failure in 4 trials | 0.1 ] =**
- = $\frac{4!}{3!(4-3)!}$ **$(0.1)^3(0.9)^1$ = (4)(0.001)(0.9) = 0.0036**

- **P[exactly 4 failures in 4 trials | 0.1 ] =**
- = $\frac{4!}{4!(4-4)!}$ **$(0.1)^4(0.9)^0$ = (1)(0.0001)(1) = 0.0001**

# Fault Tree for AFW



AFW Fails to Provide Flow
AFW-SYSTEM-FAILS

Insufficient Flow from Tank to Pump Trains
AFW-SUPPLY-TRAIN

Insufficient Flow from Pump Trains
AFW-TRAIN-SG12

Tank T1 Fails
T1 1.00E+00

Check Vaalve 1 Fails to Open
CK1 1.00E+00

Insufficient Flow from Pump Train 1 to SG1
AFW-TRAIN-SG1

Insufficient Flow from Pump Train 2 to SG2
AFW-TRAIN-SG2

Pump 1 Fails
PMP1 1.00E+00

Motor Valve 1 Fails to Open
MV1 1.00E+00

Check Vaalve 2 Fails to Open
CK2 1.00E+00

Pump 2 Fails
PMP2 1.00E+00

Motor Valve 2 Fails to Open
MV2 1.00E+00

Check Vaalve 3 Fails to Open
CK3 1.00E+00

# Cut Sets for AFW

*AFW-SYSTEM-FAILS =*

*T1*

+ *CK1*

+ *MV1 * MV2*

+ *MV1 * PMP2*

+ *MV1 * CK3*

+ *PMP1 * MV2*

+ *PMP1 * PMP2*

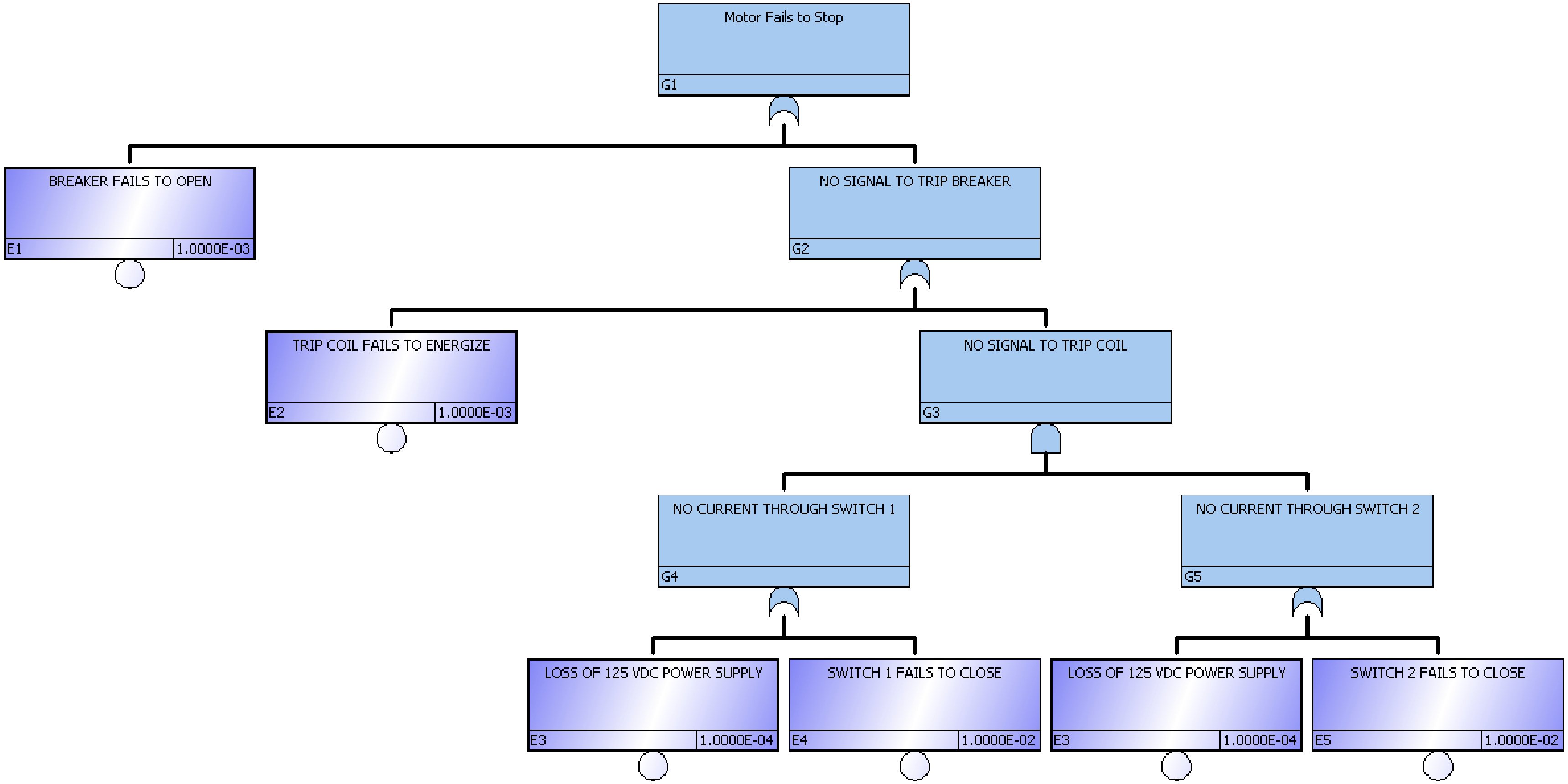
+ *PMP1 * CK3*

+ *CK2 * MV2*

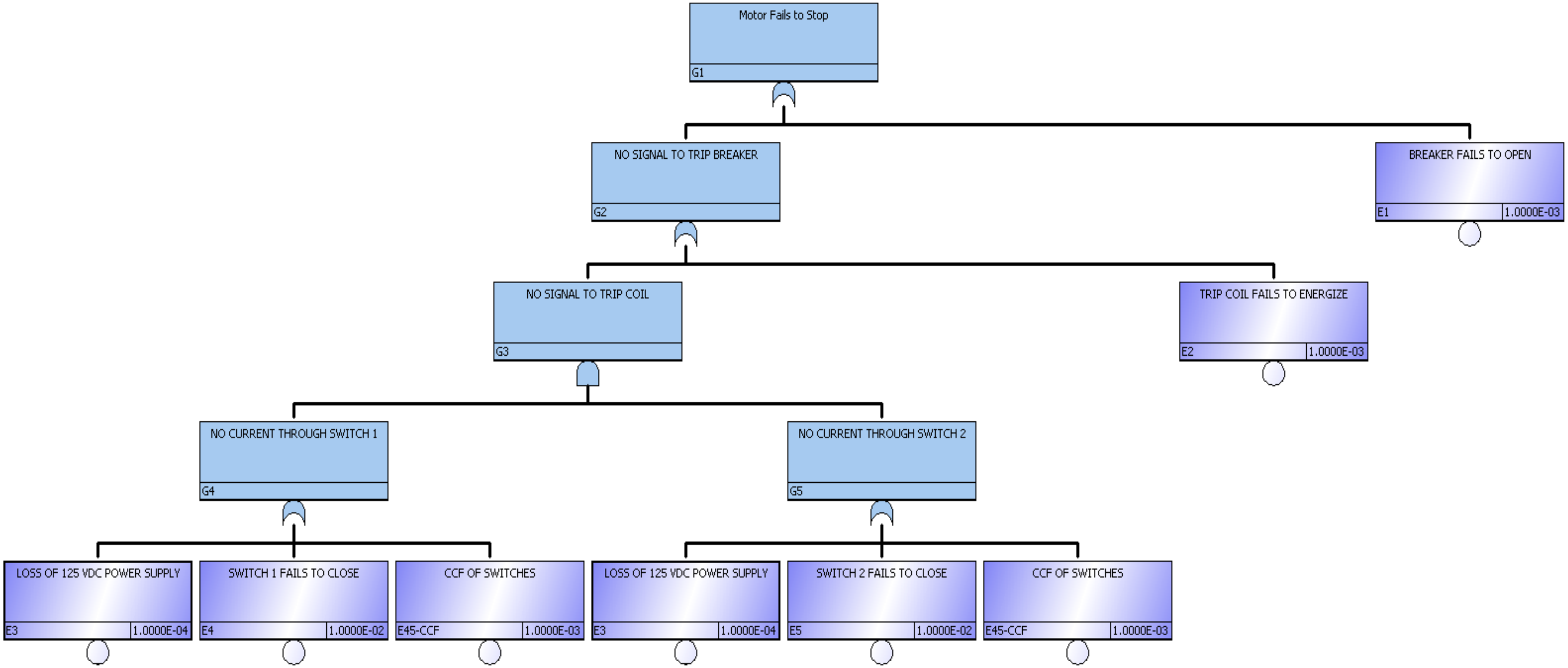
+ *CK2 * PMP2*

+ *CK2 * CK3*

# Fault Tree for Motor Fails to Stop



# Fault Tree Motor Fails to Stop with CCF



# Cut Sets for Motor Fails to Stop

G1

Min Cut Upper Bound:  2.199E-003

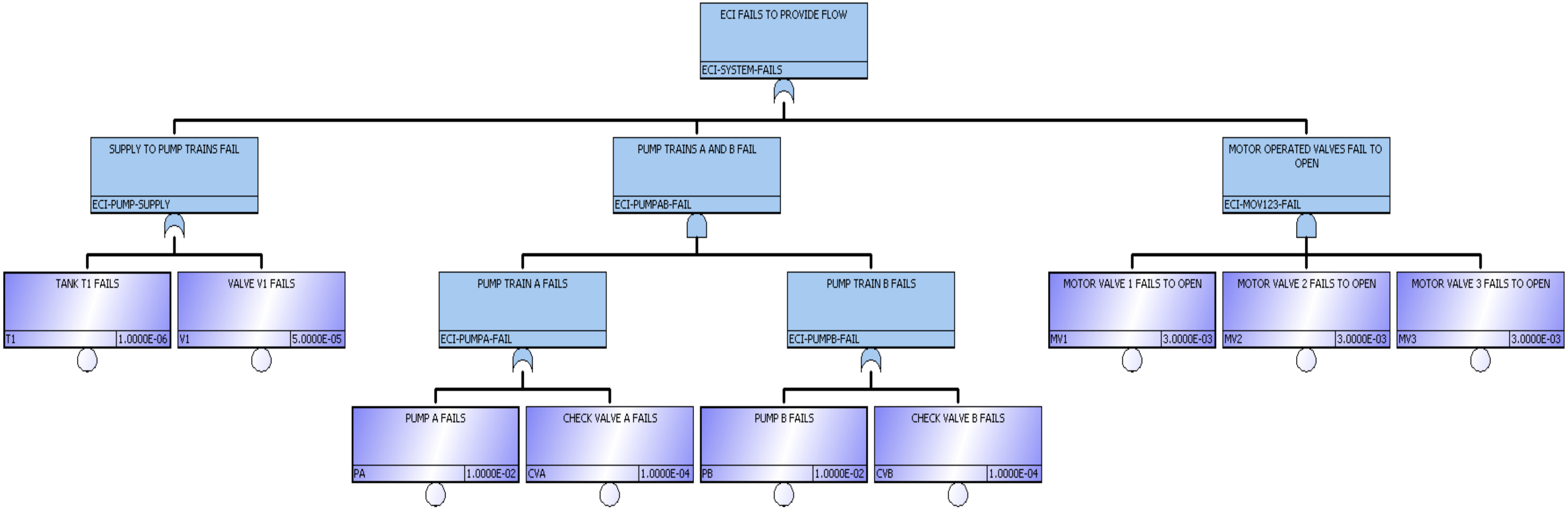
| Cut No. | % Total | % Cut Set | Probability | Cut Sets |
|---|---|---|---|---|
| 1 | 45.48 | 45.48 | 1.000E-003 | E1 |
| 2 | 90.96 | 45.48 | 1.000E-003 | E2 |
| 3 | 95.51 | 4.55 | 1.000E-004 | E4, E5 |
| 4 | 100.00 | 4.55 | 1.000E-004 | E3 |

G1-CCF

Min Cut Upper Bound:  3.196E-003

| Cut No. | % Total | % Cut Set | Probability | Cut Sets |
|---|---|---|---|---|
| 1 | 31.29 | 31.29 | 1.000E-003 | E1 |
| 2 | 62.58 | 31.29 | 1.000E-003 | E2 |
| 3 | 93.87 | 31.29 | 1.000E-003 | E45-CCF |
| 4 | 97.00 | 3.13 | 1.000E-004 | E4, E5 |
| 5 | 100.00 | 3.13 | 1.000E-004 | E3 |

# Fault Tree for ECI – w/o CCF events



ECI FAILS TO PROVIDE FLOW
ECI-SYSTEM-FAILS

SUPPLY TO PUMP TRAINS FAIL
ECI-PUMP-SUPPLY

PUMP TRAINS A AND B FAIL
ECI-PUMPAB-FAIL

MOTOR OPERATED VALVES FAIL TO OPEN
ECI-MOV123-FAIL

TANK T1 FAILS
T1 1.0000E-06

VALVE V1 FAILS
V1 5.0000E-05

PUMP TRAIN A FAILS
ECI-PUMPA-FAIL

PUMP TRAIN B FAILS
ECI-PUMPB-FAIL

MOTOR VALVE 1 FAILS TO OPEN
MV1 3.0000E-03

MOTOR VALVE 2 FAILS TO OPEN
MV2 3.0000E-03

MOTOR VALVE 3 FAILS TO OPEN
MV3 3.0000E-03

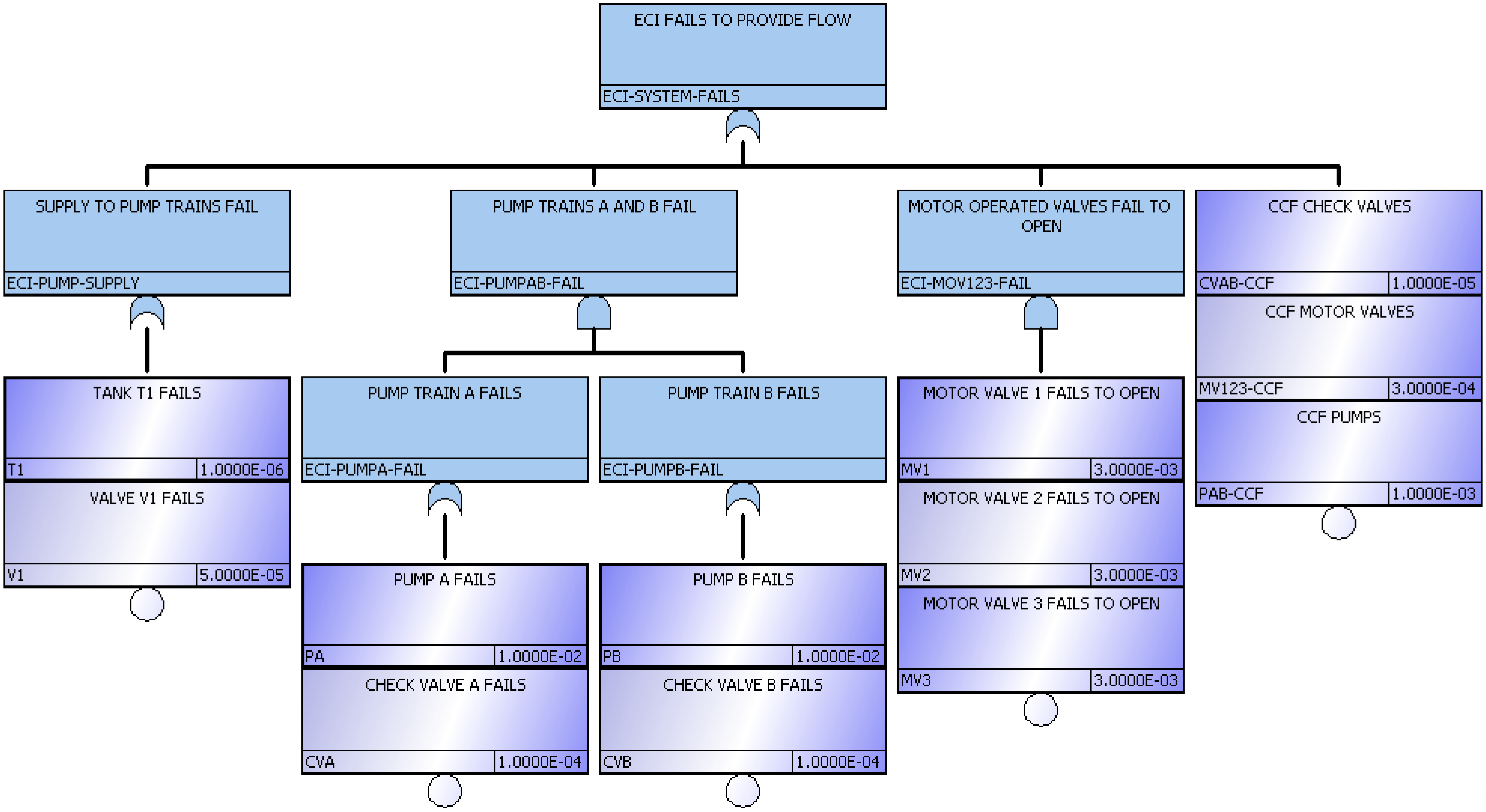
PUMP A FAILS
PA 1.0000E-02

CHECK VALVE A FAILS
CVA 1.0000E-04

PUMP B FAILS
PB 1.0000E-02

CHECK VALVE B FAILS
CVB 1.0000E-04

# Fault Tree for ECI – w CCF events



# Cut Sets for ECI System

ECI-SYSTEM-FAILS-2
Min Cut Upper Bound:  1.530E-004

| Cut No. | % Total | % Cut Set | Probability | Cut Sets |
|---|---|---|---|---|
| 1 | 65.35 | 65.35 | 1.000E-004 | PA, PB |
| 2 | 98.02 | 32.67 | 5.000E-005 | V1 |
| 3 | 98.67 | 0.65 | 1.000E-006 | CVB, PA |
| 4 | 99.32 | 0.65 | 1.000E-006 | CVA, PB |
| 5 | 99.97 | 0.65 | 1.000E-006 | T1 |
| 6 | 99.99 | 0.02 | 2.700E-008 | MV1, MV2, MV3 |
| 7 | 100.00 | 0.01 | 1.000E-008 | CVA, CVB |

ECI-SYSTEM-FAILS-2-CCF
Min Cut Upper Bound:  1.463E-003

| Cut No. | % Total | % Cut Set | Probability | Cut Sets |
|---|---|---|---|---|
| 1 | 68.38 | 68.38 | 1.000E-003 | PAB-CCF |
| 2 | 88.89 | 20.51 | 3.000E-004 | MV123-CCF |
| 3 | 95.73 | 6.84 | 1.000E-004 | PA, PB |
| 4 | 99.15 | 3.42 | 5.000E-005 | V1 |
| 5 | 99.83 | 0.68 | 1.000E-005 | CVAB-CCF |
| 6 | 99.90 | 0.07 | 1.000E-006 | CVA, PB |
| 7 | 99.97 | 0.07 | 1.000E-006 | CVB, PA |
| 8 | 100.00 | 0.07 | 1.000E-006 | T1 |
| 9 | 100.00 | 0.00 | 2.700E-008 | MV1, MV2, MV3 |
| 10 | 100.00 | 0.00 | 1.000E-008 | CVA, CVB |

# Importance Measures for Motor Fails to Stop

**G1 Min Cut Upper Bound = 2.199E-003**

| Event Name | Count | Probability | FV | RIR | RRR | Birnbaum | RII | RRI |
|---|---|---|---|---|---|---|---|---|
| E1 | 1 | 1.000E-3 | 4.548E-1 | 4.548E+2 | 1.832E+0 | 9.988E-1 | 9.978E-1 | 9.988E-4 |
| E2 | 1 | 1.000E-3 | 4.548E-1 | 4.548E+2 | 1.832E+0 | 9.988E-1 | 9.978E-1 | 9.988E-4 |
| E3 | 1 | 1.000E-4 | 4.548E-2 | 4.548E+2 | 1.048E+0 | 9.979E-1 | 9.978E-1 | 9.979E-5 |
| E4 | 1 | 1.000E-2 | 4.548E-2 | 5.493E+0 | 1.048E+0 | 9.979E-3 | 9.879E-3 | 9.979E-5 |
| E5 | 1 | 1.000E-2 | 4.548E-2 | 5.493E+0 | 1.048E+0 | 9.979E-3 | 9.879E-3 | 9.979E-5 |

**G1-CCF Min Cut Upper Bound = 3.196E-003**

| Event Name | Count | Probability | FV | RIR | RRR | Birnbaum | RII | RRI |
|---|---|---|---|---|---|---|---|---|
| E1 | 1 | 1.000E-3 | 3.129E-1 | 3.129E+2 | 1.454E+0 | 9.978E-1 | 9.968E-1 | 9.978E-4 |
| E2 | 1 | 1.000E-3 | 3.129E-1 | 3.129E+2 | 1.454E+0 | 9.978E-1 | 9.968E-1 | 9.978E-4 |
| E3 | 1 | 1.000E-4 | 3.129E-2 | 3.129E+2 | 1.032E+0 | 9.969E-1 | 9.968E-1 | 9.969E-5 |
| E45-CCF | 1 | 1.000E-3 | 3.129E-1 | 3.129E+2 | 1.454E+0 | 9.978E-1 | 9.968E-1 | 9.978E-4 |
| E4 | 1 | 1.000E-2 | 3.129E-2 | 4.088E+0 | 1.032E+0 | 9.969E-3 | 9.869E-3 | 9.969E-5 |
| E5 | 1 | 1.000E-2 | 3.129E-2 | 4.088E+0 | 1.032E+0 | 9.969E-3 | 9.869E-3 | 9.969E-5 |

# Importance Measures for ECI System

ECI-SYSTEM-FAILS-2 Min Cut Upper Bound = 1.530E-004

| Event Name | Count | Probability | FV | RIR | RRR | Birnbaum | RII | RRI |
|---|---|---|---|---|---|---|---|---|
| T1 | 1 | 1.000E-6 | 6.535E-3 | 6.535E+3 | 1.007E+0 | 9.998E-1 | 9.998E-1 | 9.998E-7 |
| V1 | 1 | 5.000E-5 | 3.267E-1 | 6.535E+3 | 1.485E+0 | 9.999E-1 | 9.998E-1 | 4.999E-5 |
| CVA | 2 | 1.000E-4 | 6.600E-3 | 6.698E+1 | 1.007E+0 | 1.010E-2 | 1.010E-2 | 1.010E-6 |
| CVB | 2 | 1.000E-4 | 6.600E-3 | 6.698E+1 | 1.007E+0 | 1.010E-2 | 1.010E-2 | 1.010E-6 |
| PA | 2 | 1.000E-2 | 6.600E-1 | 6.633E+1 | 2.941E+0 | 1.010E-2 | 9.997E-3 | 1.010E-4 |
| PB | 2 | 1.000E-2 | 6.600E-1 | 6.633E+1 | 2.941E+0 | 1.010E-2 | 9.997E-3 | 1.010E-4 |
| MV1 | 1 | 3.000E-3 | 1.764E-4 | 1.059E+0 | 1.000E+0 | 8.999E-6 | 8.972E-6 | 2.700E-8 |
| MV2 | 1 | 3.000E-3 | 1.764E-4 | 1.059E+0 | 1.000E+0 | 8.999E-6 | 8.972E-6 | 2.700E-8 |
| MV3 | 1 | 3.000E-3 | 1.764E-4 | 1.059E+0 | 1.000E+0 | 8.999E-6 | 8.972E-6 | 2.700E-8 |

ECI-SYSTEM-FAILS-2-CCF Min Cut Upper Bound = 1.463E-003

| Event Name | Count | Probability | FV | RIR | RRR | Birnbaum | RII | RRI |
|---|---|---|---|---|---|---|---|---|
| CVAB-CCF | 1 | 1.000E-5 | 6.838E-3 | 6.838E+2 | 1.007E+0 | 9.985E-1 | 9.985E-1 | 9.985E-6 |
| MV123-CCF | 1 | 3.000E-4 | 2.051E-1 | 6.838E+2 | 1.258E+0 | 9.988E-1 | 9.985E-1 | 2.997E-4 |
| PAB-CCF | 1 | 1.000E-3 | 6.838E-1 | 6.838E+2 | 3.159E+0 | 9.995E-1 | 9.985E-1 | 9.995E-4 |
| T1 | 1 | 1.000E-6 | 6.838E-4 | 6.838E+2 | 1.001E+0 | 9.985E-1 | 9.985E-1 | 9.985E-7 |
| V1 | 1 | 5.000E-5 | 3.419E-2 | 6.838E+2 | 1.035E+0 | 9.986E-1 | 9.985E-1 | 4.993E-5 |
| CVA | 2 | 1.000E-4 | 6.906E-4 | 7.894E+0 | 1.001E+0 | 1.008E-2 | 1.008E-2 | 1.009E-6 |
| CVB | 2 | 1.000E-4 | 6.906E-4 | 7.894E+0 | 1.001E+0 | 1.008E-2 | 1.008E-2 | 1.009E-6 |
| PA | 2 | 1.000E-2 | 6.906E-2 | 7.827E+0 | 1.074E+0 | 1.009E-2 | 9.984E-3 | 1.009E-4 |
| PB | 2 | 1.000E-2 | 6.906E-2 | 7.827E+0 | 1.074E+0 | 1.009E-2 | 9.984E-3 | 1.009E-4 |
| MV1 | 1 | 3.000E-3 | 1.846E-5 | 1.006E+0 | 1.000E+0 | 8.987E-6 | 8.960E-6 | 2.696E-8 |
| MV2 | 1 | 3.000E-3 | 1.846E-5 | 1.006E+0 | 1.000E+0 | 8.987E-6 | 8.960E-6 | 2.696E-8 |
| MV3 | 1 | 3.000E-3 | 1.846E-5 | 1.006E+0 | 1.000E+0 | 8.987E-6 | 8.960E-6 | 2.696E-8 |