

PRA TECHNOLOGY AND REGULATORY PERSPECTIVES P-111

Volume 1

July 2016

United States
Nuclear Regulatory Commission



PRA Technology and Regulatory Perspectives
P-111
Volume 1 Index

Index

Syllabus

Module A - Introduction to PRA and its use at the NRC

Module B - Traditional Engineering Analysis and PRA

Module C - Overview of PRA Process and Basic PRA Techniques

Module D - Initiating Events

Module E - Event Trees

Module F - Fault Trees

Module G - Parameter Estimation

Module H - Common-Cause Failure

Module I - Human Reliability Analysis

Module J - Accident Sequence Quantification

Module K - External Events

Module L - Level 2 & 3 Analysis

Module M - Shutdown Risk

Module N - Importance Measures

Module O - Uncertainty

Module P - Plant-Specific, Risk-Informed Applications

Module Q - Configuration Risk Management

Module R - Maintenance Rule Implementation

Module S - Mitigating System Performance Index (MSPI)

Module T - Significance Determination Process (SDP)

Acronyms

PRA Technology and Regulatory Perspectives (P-111) Syllabus

This course is intended to provide the PRA background required for reactor inspectors. The terminal objectives for the course are to provide:

- practical understanding of basic PRA concepts and terminology,
- practical experience using PRA information and results to improve accomplishment of inspection program requirements,
- understanding of PRA strengths and limitations,
- understanding of how PRA information may be integrated with traditional engineering analyses and assessments.

The course is divided into two parts. The first part of the course presents basic PRA concepts and terminology in a lecture format supplemented with student exercises, some exercises using actual plant PRAs, and required reading of agency PRA policy and guidance documents. This portion of the course includes a closed-book exam at the beginning of the second week. The second part of the course is a series of integrated workshops that build upon the material presented in the first part of the course. The second part culminates with an open-book exam at the end of the second week.

Syllabus of topics

Module A - Introduction to PRA and its Use at the NRC

Objectives:

- Define risk
- List the basic questions answered by PRA
- List three potential uses of PRA by inspectors
- Generally describe NRC's quantitative health objectives
- List the subsidiary numerical goals derived from the NRC's quantitative health objectives
- List three expected outcomes of the NRC PRA Policy Statement
- List one area explicitly precluded from PRA application
- Describe NRC's framework for incorporating PRA into facility regulation
- List two ways in which PRA is affecting plant licensing basis
- List examples of PRA strengths and limitations
- Discuss ways in which PRA limitations are addressed

Module B - Traditional Engineering Analysis and PRA

Objectives:

- Describe the traditional engineering approach to control risk
- Compare and contrast this approach with that used in PRA
- Give examples of how defense-in-depth is included in the design per the traditional approach, and how PRA illustrates the level of protection provided by the design

Module C - Overview of the PRA Process and Basic PRA Techniques

Objectives:

- Describe the major steps in the PRA process
- Describe the outputs of each of the “Levels” of PRA
- Describe why probabilistic models are used
- Give examples of disciplines required to perform a PRA
- Give examples of where traditional engineering inputs are used in the PRA process
- List basic probability operations
- Describe the difference between frequency and probability
- Calculate probabilities
- Define cut sets

Module D - Accident Sequence Initiating Events

Objectives:

- Understand the relationship between initiating event identification and other PRA related tasks
- Become familiar with the various ways to identify initiating events
- Understand how initiating events are grouped and quantified
- Understand the relationship between PRA “initiators” and “challenges” in a traditional safety analysis report (SAR)

Module E - Accident Sequence Analysis Using Event Trees

Objectives:

- Describe the purposes of event tree analysis
- Describe techniques and notations employed in event tree construction
- Describe the relationship between event tree construction and deterministically-identified success criteria
- Compare PRA accident sequences (as depicted by the event trees) and the traditional SAR design basis accidents

Module F - Systems Analysis Using Fault Trees

Objectives:

- List the purposes of fault tree analysis.
- Define the terminology, notation, and symbols used in fault tree analysis.
- Interpret the results of fault tree reduction.
- Define and correctly apply the definition of “minimal cut sets”.

Module G – Equipment Failure Modes and Data Sources for Parameter Estimation

Objectives:

- Understand failure modes typically modeled in PRA and what information is needed to estimate the parameter for each failure mode
- Define what is meant by “generic data” and list common sources
- List limitations associated with plant-specific data
- Explain qualitatively what Bayesian updating accomplishes

Module H - Common-Cause Failures

Objectives:

- Define several types of dependent failures and how they are modeled
- Give examples of dependent and common cause failures
- Describe the importance of modeling common cause failures in PRAs

Module I - Human Reliability Analysis

Objectives:

- 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

Module J - Accident Sequence Quantification

Objectives:

- Explain how the various aspects of accident sequence quantification are accomplished, including approximations that are used
- Describe the major processes for accident sequence quantification
- Describe the relationship between minimal cut sets and accident sequences, for a Fault Tree Linking approach and Event Tree with Boundary Conditions approach
- Given minimal cut sets of varying order (number of basic events), list the defense-in-depth features associated with each which are presumed to fail to get to core damage

Module K - External Events

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

Module L - Level 2 & 3 Analysis

Objectives:

- Describe the general purpose of Level 2 and 3 analyses
- List typical types of consequences from a Level 3 PRA

Module M - Shutdown Risk

Objectives:

- Describe how shutdown modes can be risk-significant
- Describe why PRA must treat separate modes of operation during shutdown
- Discuss the risk importance of systems available to maintain plant safety functions and the effect of equipment outages on shutdown risk

Module N - Importance Measures

Objectives:

- Identify four common quantitative importance measures
- Calculate values for four types of importance measures given Level 1 PRA results
- Discuss how importance measures are influenced by the value of the associated basic event, the values of other basic events, and modeling assumptions
- Understand implications of each importance measure for plant safety & inspection activities
- Explain why use of importance measures is considered valid for Maintenance Rule applications (i.e., binning SSCs into risk and non-risk categories)

Module O – Uncertainty

Objectives:

- List the types of uncertainty and their sources
- Understand how uncertainty is accounted for in PRA.

Module P - Plant-Specific, Risk-Informed Applications

Objectives:

- Understand the NRC PRA Policy Statement
- Understand Risk-Informed and Performance-Based Plan
- Understand general concepts of risk-informed regulation
- List potential PRA applications
- List the major elements of the decision logic used to review submittals containing changes to the current licensing basis and the role of the new Regulatory Guides and SRPs in this process, including the numerical decision criteria related to CDF and LERF

Module Q - Configuration Risk Management

Objectives:

- Explain why base case or nominal PRA results cannot be used for maintenance planning
- Explain what is meant by “configuration risk management” and how it is related to risk-informed regulation
- Evaluate “risk” profiles quantitatively

Module R - Maintenance Rule Implementation

Objectives:

- Explain the purposes of the Maintenance Rule and identify areas in which PRA can support the rule’s implementation
- Explain how performance goals/criteria are established using the “EPRI Method”

Module S - Mitigating System Performance Index (MSPI)

Objectives:

- Explain what is MSPI
- Explain why MSPI was developed
- Explain how MSPI is related to Δ CDF
- Explain how MSPI includes both unavailability and unreliability
- Explain how MSPI uses importance measures

Module T - Significance Determination Process (SDP)

Objectives:

- Explain the purpose and objectives of the SDP
- Explain the PRA basis behind the SDP
- Explain how SDP is consistent with PRA principles and practices

Closed-Book Exam (Time limit 2 hours; 60% of final grade)

Integrated Workshop #1 – Planning and Prioritizing Inspection Activities

Integrated Workshop #2 – Risk Significance of Findings and Events

Open-Book Exam (Time limit 2.5 hours; 40% of final grade)

TENTATIVE SCHEDULE FOR P-111

Note: The instructor will allow approximately 30 minutes at the beginning of each day and approximately 30-45 minutes at the end of each day for students to perform Module exercises, IPE “lookups” assigned at the end Modules, and Supplementary Reading. Each class starting session will have an answer/question period regarding assignments concerning each Module.

Day 1

Module A - Introduction to PRA and its Use at the NRC

Module B - Traditional Engineering Analysis and PRA

Module C - Overview of PRA Process

Supplementary Reading:

1. NRC Safety Goal Policy Statement of 1986 (51 FR 28044)
2. PRA Final Policy Statement
3. Kemeny Commission Report on TMI-2, Vol. 1, pp. 84-86.
4. Part 9900 Inspection Guidance, C.6 – Use of PRA in Operability Decisions (superseded by IMC-0326)
5. NUREG-0492, Secs. I and VI
6. PRA history article from RESS

Day 2

Module D - Accident Sequence Initiating Events

Module E - Accident Sequence Analysis Using Event Trees

Module F - System Analysis Using Fault Trees

Supplementary Reading:

1. NUREG/CR-2300, Sec. 3 through 3.5 (Event Trees)
2. NUREG-0492, Secs. III-V (Fault Trees)

Day 3

Module G - Estimation of Equipment Reliability and Unavailability

Module H - Estimation of Common-Cause Failure Probabilities

Module I - Human Reliability Analysis

Module J - Accident Sequence Quantification

Module K - External Events

Supplementary Reading:

1. NUREG/CR-6823, Ch. 2 (Equipment Reliability)
2. NASA PRA Procedures Guide, Ch. 10 (CCF)
3. NASA PRA Procedures Guide, Ch. 9 (HRA)
4. NUREG/CR-2300, Secs. 6.1-6.3 (Accident Sequence Quantification)
5. NUREG/CR-2300 Ch. 10, through 10.3.1 (External Events)

Day 4

Module L - Level 2 and 3 PRA

Module M - Shutdown Risk

Module N - Importance Measures

Module O - Uncertainty

Supplementary Reading:

1. NASA PRA Procedures Guide, Sec. 13.3 (skip 13.3.2) (Importance Measures)
2. NASA PRA Procedures Guide, Ch. 7 (Uncertainty)

Day 5

Module P - Plant-Specific, Risk-Informed Applications

Module Q - Configuration Risk Management

Review for closed-book exam

Supplementary Reading:

1. Reg. Guide 1.174
2. Reg. Guide 1.200 (PRA Quality)
3. IMC 0609, Apps. A (through Att. 2), G, and H
4. NUREG-1816, Ch. 2 (MSPI)

Day 6

Closed-Book Exam (Time limit: 2 hours)

Module R - Maintenance Rule Implementation

Module S - Mitigating System Performance Index (MSPI)

Module T - Reactor Safety Significance Determination Process (SDP)

Supplementary Reading:

Complete/Review if needed

Day 7

Integrated Workshop #1 – Planning and Prioritizing Inspection Activities

Integrated Workshop #2 – Risk Significance of Findings and Events

Supplementary Reading:

Complete/Review if needed

Day 8

Integrated Workshop #2 – Risk Significance of Findings and Events (continued)

Review for open-book exam

Supplementary Reading:

Complete/Review if needed

Day 9

Open-Book Exam (Time limit: 2.5 hours)

Student Guidance on the Use of IPEs and NUREG-1560 in P-111

The availability of every plant's IPE submittal is an important element in P-111 as a means of relating high-level PRA concepts to the details of plant design and operation most familiar to each individual inspector. It is imperative, however, that students understand that the IPEs are offered primarily as a means of improving plant-specific knowledge of plant responses to combinations of initiating events, component/system failures, and operator/human errors leading to core damage (i.e., severe accident sequences). The sequences estimated to contribute the most to current plant risk may have changed from those represented in the IPE, due to plant modifications or changes to the assumptions and/or methods of the PRA analysis. However, understanding the dominant accident sequence contributors in the IPE can provide a baseline for discussions with licensee PRA analysts on how and, more importantly, WHY the risk contributors may have changed since the IPE was performed. Students should be continually mindful that the "bottom line" numbers (i.e., CDF, LERF, %CDF for each initiating event and accident class, etc.) of any PRA are not as important to an inspector as is the use of PRA to better understand WHY certain core damage accident sequences are more likely than others. Studying the plant-specific IPEs followed by a discussion with licensee PRA analysts can help achieve these risk insights.

Because of the wide variability of the IPE submittals and methodologies, this is primarily an individual (self-directed) learning exercise. The two-week class schedule provides an opportunity for each student to review in detail an IPE of their own choosing while simultaneously learning related PRA concepts. Students will be assigned straightforward "lookup" questions for their IPEs daily, based on reinforcing and illustrating the day's lecture material. Students are encouraged, however, to raise questions about their IPE's in class and to take advantage of the instructor's expertise.

In addition, students are encouraged to compare their chosen plant's IPE results against other similar plant IPEs by reviewing applicable sections of NUREG-1560. In particular, refer to Chapters 2 (Impact on Reactor Safety), 3 (IPE Results Perspectives: Core Damage Frequency), 4 (Containment Performance Perspectives), 5 (Human Performance Perspectives), and related chapters in Volume 2 (Chapters 11, 12, 13) for more detailed information.



Idaho National Laboratory

MODULE A

Introduction to PRA and Its Use by the NRC

Introduction to PRA and Its Use by the NRC

- **Purpose**
 - Introduce use of PRA from perspective of NRC policy
 - Introduce PRA terminology
 - Introduce NRC perspective on relationship of PRA to inspection
 - Inspection planning
 - Evaluating findings
 - Evaluating licensee use of PRA

Objectives

- **Upon completion of this module, students should be able to**
 - **Define risk**
 - **List the basic questions answered by PRA**
 - **List three potential uses of PRA by inspectors**
 - **Generally describe NRC's quantitative health objectives**
 - **List the subsidiary numerical goals derived from the NRC's quantitative health objectives**
 - **List three expected outcomes of the NRC PRA Policy Statement**
 - **List one area explicitly precluded from PRA application**
 - **Describe NRC's framework for incorporating PRA into facility regulation**
 - **List two ways in which PRA is affecting licensing basis**
 - **List example PRA strengths and limitations**
 - **Discuss ways in which PRA limitations are addressed**

Outline of Topics

- **Basic terminology**
- **Risk definition and examples**
- **How PRA is being used**
- **NRC quantitative health objectives and subsidiary numerical goals**
- **NRC PRA Policy Statement**
- **Risk-Informed and Performance-Based Plan (RPP)**
- **Strengths and limitations of PRA**
- **How PRA limitations are addressed**
- **Standardized Plant Analysis Risk (SPAR) model**

Basic PRA Terminology

- **Frequency – Number of occurrences of an event per number of demands or per unit time**
 - Parameter used in model for stochastic (aleatory) uncertainty
 - Time-based frequencies can be any positive value (i.e., can be greater than one)
- **Probability – Likelihood of an event occurring**
 - Internal measure of certainty about the truth of a proposition
 - Unitless value which is always conditional
 - Value between 0 and 1
 - Typically used for all events in PRA except initiating events
- **Note: Frequency and Probability are different concepts, but sometimes numerically equal**
- **Consequence**
 - Result of event in terms of public health impact, economic impact, etc.
 - Intermediate consequence measures such as core damage frequency or large early release frequency are often used

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

$\langle S_i, P_i, C_i \rangle$

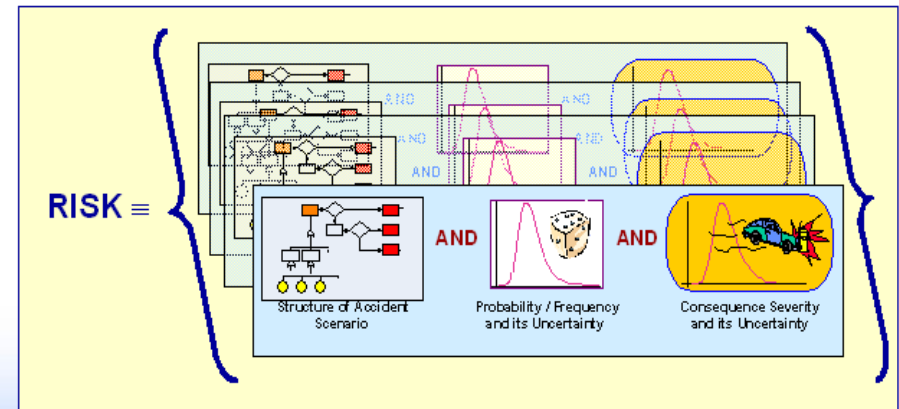
that answer the questions:

- What can go wrong?
(scenarios, S_i)
- How likely is it?
(probabilities, P_i)
- What are the consequences?
(adverse effects, C_i)

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

- 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
\vdots	\vdots	\vdots
S_N	p_N	C_N



Risk Units (in terms of frequency)

- Risk Calculation = Frequency x Consequences

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

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

Note that the frequency can be replaced by a probability

Quantitative Health Objectives- Death Due to Accidents

- **Societal Risk = 136,053 Accidental-Deaths/year**
- **Average Individual Risk**
= (136,053 Accidental-Deaths/Year)/318,856,137 Est. U.S. Pop.
= 4.3E-04 Accidental-Deaths/Person-Year
≈ 1/2,344 Accidental-Deaths/Person-Year
- **In any given year, approximately 1 out of every 2,344 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 2014, June 30, 2016, Volume 65, Number 4, 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 about 5.0E-4 Deaths/Person-year.**

Quantitative Health Objectives- Death Due to Cancer

- **Societal Risk = 591,699 Cancer-Deaths/year**
- **Average Individual Risk**
= (591,699 Cancer-Deaths/Year)/318,856,137 Est. U.S. Pop.
= 1.9E-03 Cancer-Deaths/Person-Year
≈ 1/539 Cancer-Deaths/Person-Year
- **In any given year, approximately 1 out of every 539 people in the entire U.S. population will die from a cancer death**
- **Note: Figures presented above are based on the National Vital Statistics Reports, Deaths: Final Data for 2014, June 30, 2016, Volume 65, Number 4, 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 about 2.0E-3 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 societal risks
 - Average individual (within 1 mile of plant) early fatality (*accident*) risk
 - $< 5E-7/\text{year}$
 - Average individual (within 10 miles of plant) latent fatality (*cancer*) risk
 - $< 2E- 6/\text{year}$
 - The “0.1%” was a subjective factor determined after much deliberation and consideration

Subsidiary QHOs

- 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-90-016, 6/26/90)
 - CDF < 1E-4/year
 - Large release frequency (LRF) < 1E-6/year
 - Conditional containment failure probability (CCFP) < 0.1

NRC QHOs (cont.)

- **The Commission has approved guidelines for using these QHOs in NRC decision-making**
 - **Plant-specific application of QHOs and subsidiary objectives (R.G. 1.174, “Module P” in this course)**
 - **“Small” increases in risk are allowable in changing plant licensing basis (R.G. 1.174, Module P)**

PRA is Technical Analysis Tool

- Probabilistic risk assessment (PRA) – an analytical tool that answers three questions (see article by Kaplan and Garrick):
 - What can go **wrong**?
 - Accident scenarios
 - How **likely** is each scenario?
 - 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?

PRA Now Widely Used by Nuclear Power Industry & NRC

- **Use by licensees initially (during IPE) to evaluate plant severe accident potential vulnerabilities**
- **Now being used to support submittals to NRC**
- **NRC has endorsed PRA as important element in licensing regulatory process**

NRC Applications of PRA

- **Monitoring reactor operations**
 - Maintenance Rule (“module R” in this course)
 - Mitigating System Performance Index (MSPI) (module S)
- **Value impact analysis for potential changes to licensed reactor design and operation (backfits)**
- **Efforts to Risk Inform – 10 CFR 50**
- **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 support (e.g., Senior Reactor Analysts in Region)**
 - Prioritization and planning of inspections
 - Evaluation of inspection findings (e.g., SDP)
 - Evaluation of licensee use of PRA

NRC Applications of PRA (cont.)

- **Resource allocation**
 - Regulatory requirements (e.g., risk-informing 10 CFR 50)
 - Research (e.g., fire protection issues)
 - Regulatory analysis (e.g., generic issue resolution)
- **Reactor design**
 - Identify weaknesses in design
 - Risk-significant Systems, Structures, Components (SSCs)
 - Risk-significant accident scenarios
 - Risk-significant human actions
- **Standardized Plant Analysis Risk (SPAR) Models**
- **Event analysis and risk significance**
 - Accident Sequence Precursors (ASP)
 - Significance Determination Process (SDP) (module T)
- **Risk Monitors**
- **Non-reactor issues**
 - Licensing high-level waste repository
 - Sealed sources
 - Spent fuel storage
 - Medical uses of byproduct materials
 - Others

Use of PRA by Inspectors

- **Uses can be categorized broadly as**
 - **Providing risk perspective for inspection planning (focus and priorities)**
 - **Evaluating risk significance of findings and events**
 - **Evaluating licensee uses of PRA (e.g., plant configuration control)**

Purposes of Individual Plant Examinations (IPE/IPEEE)

- **Systematically examine plant design, normal and emergency operation to**
 - Identify plant-specific severe accident vulnerabilities
 - Develop understanding of what could possibly go wrong, accident scenarios
 - Identify and evaluate means of improving plant and containment performance during such accidents
 - Decide upon improvements to implement (if any)
- **Supplement 4 to GL 88-20 requested same type of evaluation for selected external events (e.g., earthquake)**
 - Known as IPEEE

IPEs & IPEEEs Did Not Require PRA

- **All utilities chose to perform a PRA to address GL 88-20**
 - PRAs not performed to specified standards
 - No requirements specified for data or models
- **Not all utilities used PRAs for IPEEE (external events) portion of GL 88-20**
- **IPE not typically full-scope PRA (only full-power operation considered)**
- **Estimated CDF and probability of containment failure, but not source terms and offsite consequences (typical)**
- **IPE/IPEEE not performed to support risk-informed, performance-based regulation**

Use of IPE/IPEEE in Risk-Informed, Performance-Based Regulation

- **Requires more detailed reviews of models and data**
 - Initial NRC reviews done to ensure requirements of GL 88-20 met
 - SER (Staff Evaluation Report) issued for each plant [sometimes TER (Technical Evaluation Report) also]
 - Initial reviews did not validate modeling assumptions, data, or results

NRC PRA Policy Statement

- **Process to allow for increased use of PRA**
- **Develop from concerns that**
 - **PRA methods not applied consistently throughout NRC**
 - **Sufficient PRA/statistics expertise not available in NRC**
 - **Commission not deriving full benefit from NRC and industry investment in PRA methods**

- **The Policy**

Expand the use of PRA to extent supported by state of the art, in support of defense in depth and traditional engineering

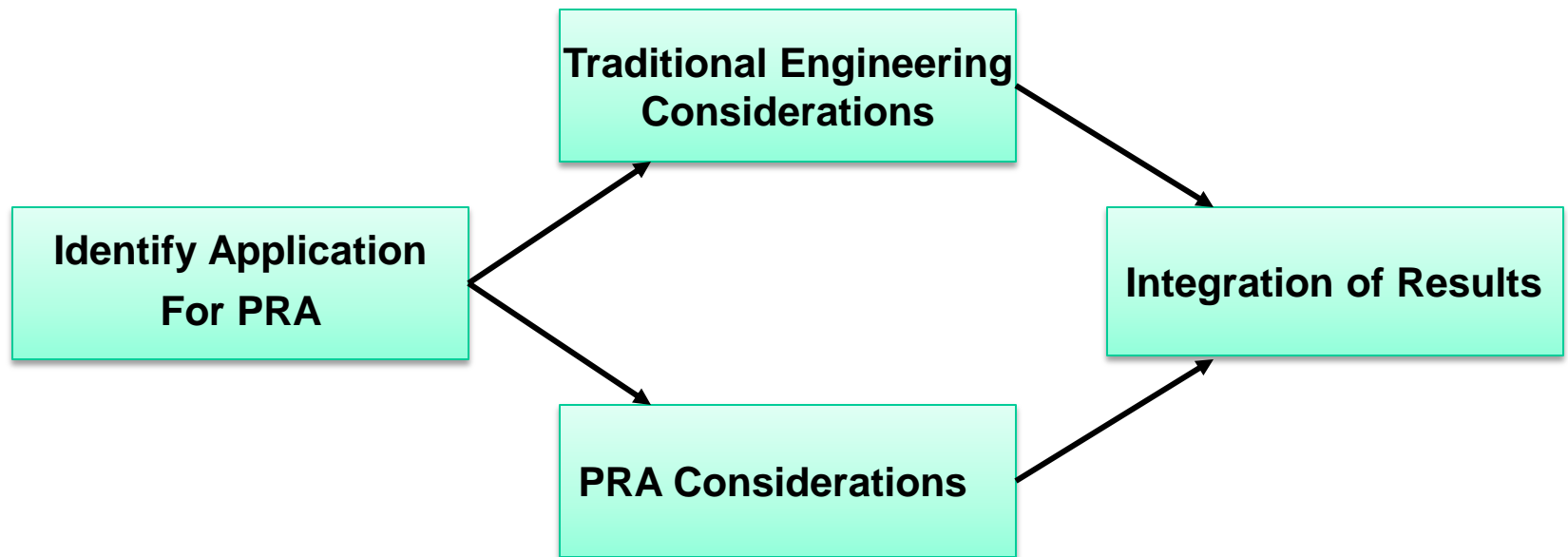
NRC PRA Policy Statement (cont.)

- **Expected outcomes (became expected outcomes of risk-informed regulation, too)**
 - **Improved risk-effective decision-making**
 - **Staff takes consistent approach to regulatory decisions**
 - **More efficient use of NRC resources**
 - **Reduce unnecessary regulatory burden on licensees**
- **Initially put in place through PRA implementation Plan, then referred to as Risk-Informed Regulation Implementation Plan (RIRIP)**
- **As of April 2007 (SECY-07-0074) it is now referred to as Risk-Informed and Performance-Based Plan (RPP)**

Area Currently Excluded from the PRA Application

- **Equipment operability determination (for Tech. Specs.)**
 - Unless your plant has implemented risk-informed Technical Specifications (RG 1.177)

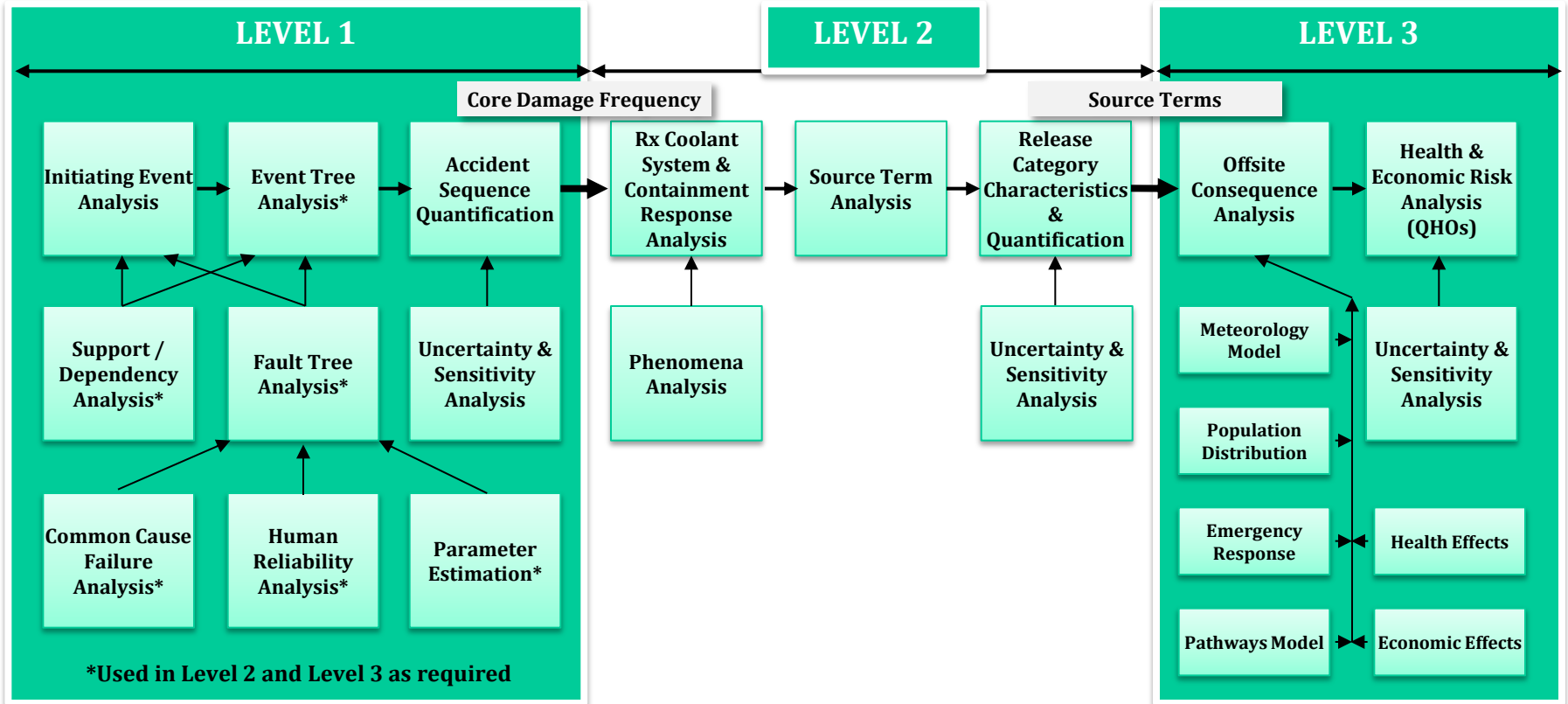
NRC Framework for Applying PRA in Reactor Regulation



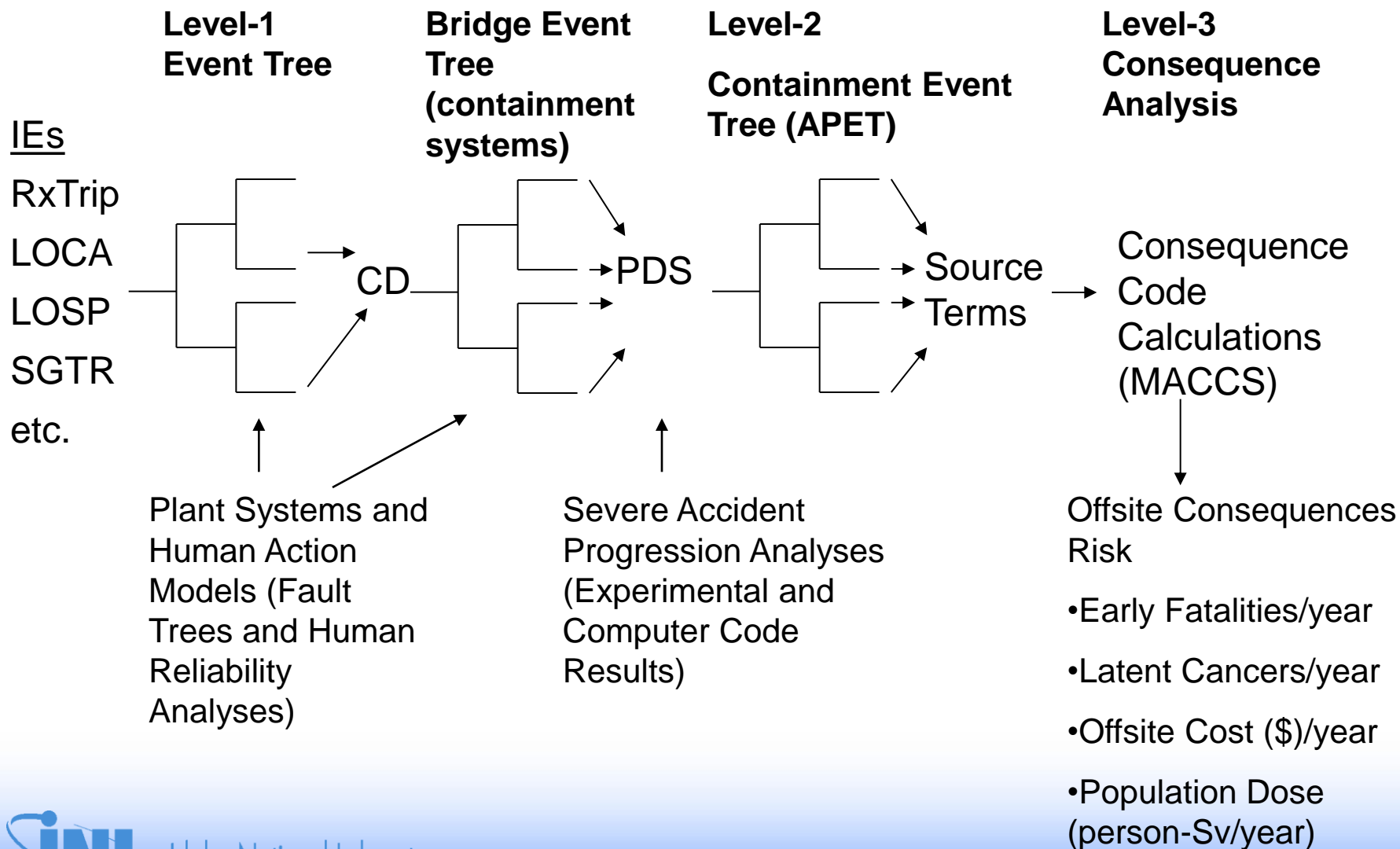
PRA is Impacting Licensing Basis

- **Examines whether risk-significant issues exist that are currently outside the licensing basis**
 - E.g., Station-blackout rule
- **Examines areas within the licensing basis where current regulations are too strict or overly conservative**
 - E.g., reduced requirements for containment leak-rate testing

Principal Steps in PRA



Overview of Level-1/2/3 PRA



PRA Strengths

- **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 priorities according to dominant risk contributors
 - Provides a framework for a monitoring / trending program to detect risk-significant adverse trends in performance

PRA Strengths (cont.)

- **Rigorous, systematic tool for analyzing complex systems**
- **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**

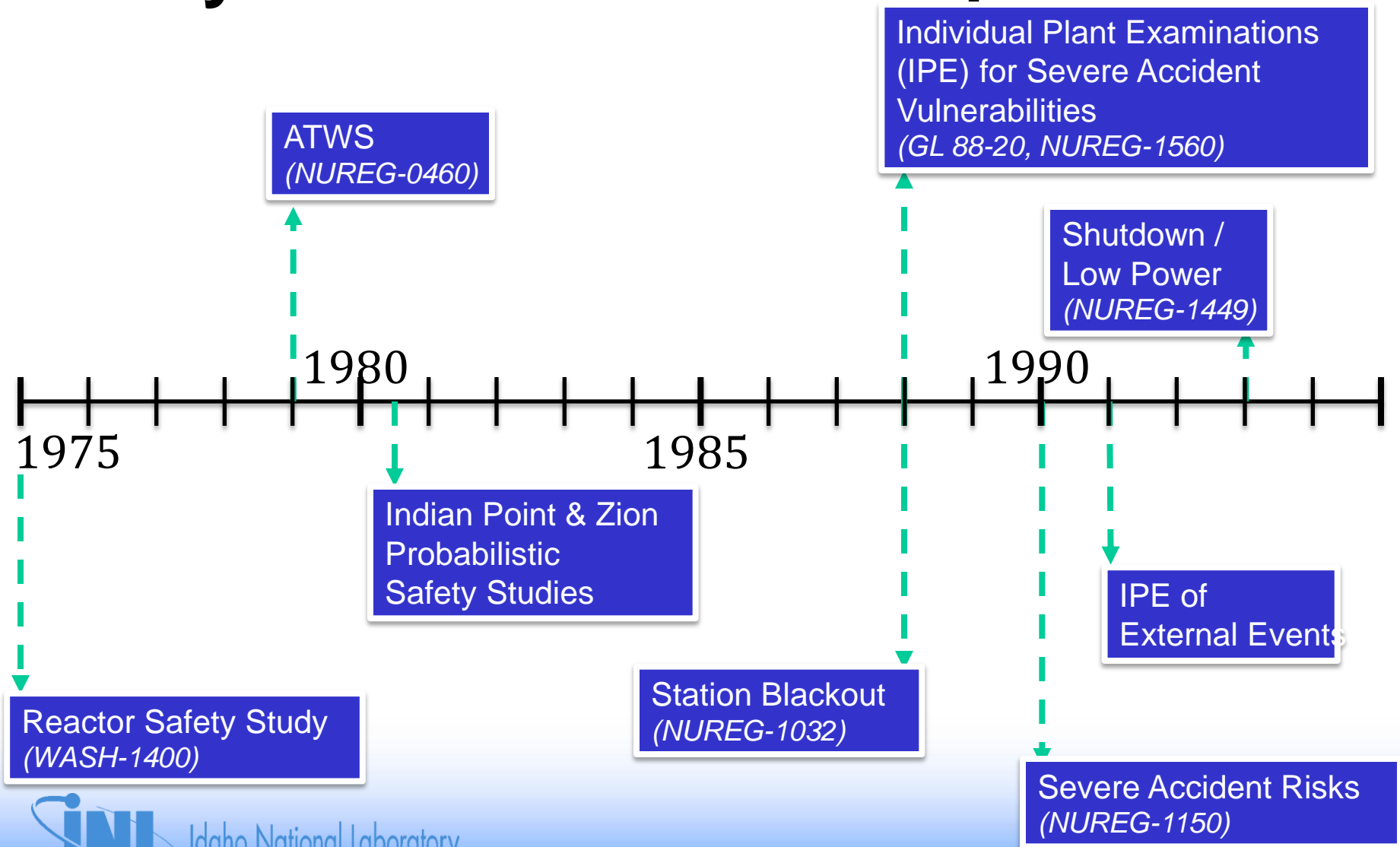
Principal PRA Limitations (see also Module O)

- **Adequacy of data base for hardware and human performance**
- **Incomplete understanding of severe accident behavior**
 - Results may be sensitive to analytical assumptions
- **Constraints on modeling effort (limited resources)**
 - Simplifying assumptions
 - Incomplete solution of models (truncation of results) during quantification
 - Less of a limitation now than in the past
- **Lack of completeness**
 - Less than full scope with respect to initiators and modes of operation
 - Not all scenarios included
 - Some missed by oversight
 - Some cannot be modeled at present
- **PRA is typically a snapshot in time**
 - This limitation may be addressed by having a “living” PRA (Note: Living PRA required for new reactor designs)
 - 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

Addressing PRA Limitations

- **Sensitivity studies on data and modeling assumptions**
- **Use of expert judgment**
- **Peer review**
- **Use results in conjunction with traditional engineering analysis and philosophy of defense in depth**
 - Regulation is risk-informed, not risk-based
- **Basis for PRA results must be understood before using them**
 - Training on and use of PRA technology

Early Risk Studies and Reports



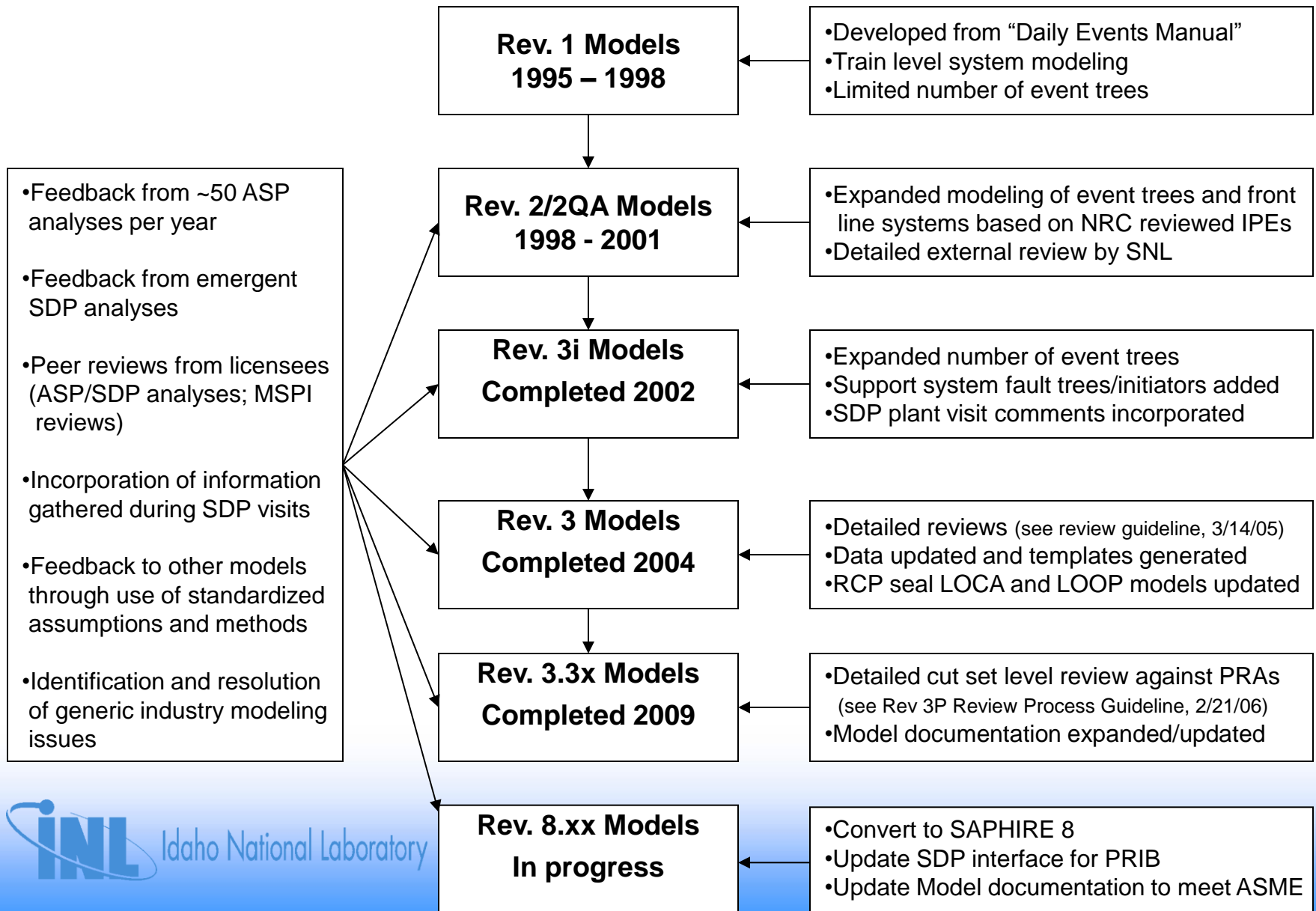
WASH-1400 (~ 1975)

- **New hazards were identified (over DBAs)**
 - For example: “Event V”, entailing interfacing systems LOCA and containment bypass
 - Risk significance of transients and small-break loss of coolant events was seen to be greater than had been supposed
- **Before, people thought that**
 - Severe accidents were almost incredible...
 - ... but would be extremely catastrophic if they occurred
- **WASH-1400 seemed to be saying that severe accidents in US plants**
 - Are unlikely but not incredible
 - Not as extremely catastrophic as previously thought

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



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
 - Nomenclature
 - 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 – 2012)
 - 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 NUREG/CR-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



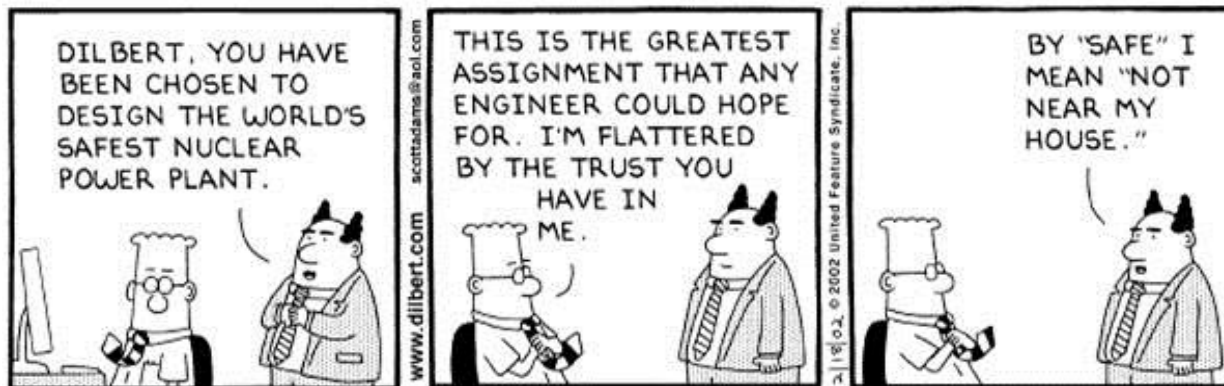
Idaho National Laboratory

MODULE B

Traditional Engineering Analysis and PRA Approaches To Safety Analysis

Traditional Engineering Analysis And PRA Approaches To Safety Analysis

- Purpose
 - This module compares and contrasts the traditional engineering and PRA approaches to safety analysis



Objectives

- **Upon completion of this module, students should be able to**
 - **Describe the traditional engineering approach to control risk**
 - **Compare and contrast this approach with that used in PRA**
 - **Give examples of how defense-in-depth is included in the design the traditional approach, and how PRA illustrates the level of protection provided by design**

Outline

- **Design Basis Approach to Risk**
- **Role of Defense-in-Depth in Design**
- **Limitations of the Traditional Approach**
- **The PRA Approach to Assessing Risk**
- **How PRA Illustrates Defense-in-Depth**

Design Basis (Traditional) Approach to Risk

- Focused on setting design requirements
- Specific accidents to be analyzed and designed for Design Basis Accidents (DBAs)
 - Definition → 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.
- Includes worse-case **single active** failure
- Only safety-related equipment is credited
- Operator actions generally not included

Design Basis (Traditional) Approach to Risk (cont.)

- **Includes margins to address uncertainties**
- **Establishes requirements for**
 - **Engineering margin**
 - **Quality assurance**
 - **Analysis methodology**
- **Requires redundancy and separation for critical systems**
- **Establishes principles for Defense-in-Depth**

Defense in Depth

- **Definition:**
 - An element of NRC's safety philosophy that is used to address uncertainty by employing successive measures including safety margins to prevent and mitigate damage if a malfunction, accident or naturally caused event occurs at a nuclear facility
- **Provides Barriers**
 - (Physical, Procedural, Organizational) To fission product release and layers of protection

Layers of Defense in Depth (Establishes Design & Operational Requirements)

Layers of defense in depth	Objective	Approach
1	Prevention of abnormal operation and failures	Training, conservative design (redundancy, engineering margin) and high quality in construction and operation
2	Control of abnormal operation and detection of failures	Control, limiting, & protection systems and other surveillance features
3	Control of accidents within the design basis	Engineered safety features and emergency operating procedures
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Accident mitigation strategies
5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

Examples of Layer 1 Barriers and Layer of Protection Prevention of Abnormal Operation and Failures

Ceramic fuel pellets	Only a fraction of gaseous and volatile fission products is released from the pellets
Metal cladding	Cladding contains fission products from the pellets
Reactor vessel and piping	Contains fission products & other radioactive materials
Procedures	Plant/Unit operating procedures, system operating procedures, surveillance procedures
Fire prevention	Fire prevention program required - e.g. restricting storage/use of flammable materials, good electrical practice

Examples of Layer 2 Barriers and Layer of Protection Control of Abnormal Operation and Detection of Failures

Metal cladding	<0.5% of fuel pins permitted to develop pinhole sized leaks over life of fuel
Reactor vessel and piping	Leak detection system and In-Service Inspection required
Reactor Control System	Shutdown response to certain abnormal conditions
Fire detection	Detection systems required
Tech Specs	Limiting safety system settings
Procedures	Abnormal operating procedures reduce human error

Examples of Layer 3 Barriers and Layer of Protection Control of Accidents within the Design Basis

RPS	Limits energy deposition of accidents
ECCS	Protects cladding integrity
Procedures	Emergency operating procedures reduce human errors
Fire control	Fire suppression systems are required
Reactor vessel and piping	8- to 10-inch thick steel vessel and 3- to 4-inch thick steel piping contain reactor coolant and any fission products released from the fuel cladding

Examples of Layer 4 Barriers and Layer of Protection

Control of Severe Plant Conditions, Including Prevention of Accident Progression and Mitigation of the Consequences of Severe Accidents

Containment	Contains any fission products released from the reactor vessel or coolant piping
Tech Specs	Indirectly limit hydrogen generation from cladding metal/water reaction -> protects containment integrity
Containment pressure suppression and cooling	Protects containment integrity
Fire areas	Redundant systems are required to be in separate fire areas to reduce the threat from fire
Separation of redundant systems	Redundant systems are also required to be separated to be reduce the common threat from other hazards

Examples of Layer 5 Barriers and Layer of Protection

Mitigation of Radiological Consequences of Significant Releases of Radioactive Material

Exclusion area	Separates plant from public; entrance restricted
LPZ/evacuation plan	Residents in low population zone are protected by emergency evacuation plans
Population center distance	Plants are located at a distance from population centers (>25,000)

Limitations of Traditional Approach

- **Types of accidents considered is limited**
 - Single active failures only
 - Limited treatment of operators
- **Use of margins to address uncertainties, based on engineering judgment**
 - Can lead to excessively conservative design
 - Can lead to belief that DBAs are limiting
- **No direct assessment of risk significance (importance)**
- **Does not provide quantitative risk results for decision-making (risk metrics)**

PRA Approach to Assessing Risk

- **Focused on estimating the level of risk and risk-contributing features of design**
 - **PRA identifies accident initiators and derives accident scenarios**
 - **Not limited to predetermined set of accidents**
 - **Analyzes multiple failures, including failures of redundant barriers**
 - **Non-safety equipment is credited when the equipment is specifically called out in Emergency Operating Procedures (EOPs)**
 - **More extensive treatment of operator actions**
 - **Avoids use of conservative margins**
 - **Focus on “best-estimate” analysis where possible**
 - **Goes beyond Design Basis**
- **Assesses risk-significance of modeled elements**
- **Provides quantitative results and models for decision-making**

ECCS Single Failure Analysis Example

from FSAR Chapter 6, NUREG-0800 Requirements

- **The single failure criterion imposes redundancy in safety systems, reducing failure likelihood**
- **Single Failure Analysis consists of postulating:**
 - **Initiating occurrence (including multiple failures from a single cause)**
 - **Probability = 1.0**
 - + **Single Active Component Failure (or passive failure during long term recirculation cooling following an accident)**
 - **Probability = 1.0**
 - + **Other appropriate hazard (e.g. DBE)**
 - **Probability = 1.0**
- **In some respects this approach *appears* overly conservative because failures are considered to be certain**
- **However, many types of common cause failures are ignored**

Single Failure Analysis Example (cont.)

Contrast with PRA

Traditional Engineering Single Failure Analysis	PRA
Evaluates a random failure and its consequential effects, in addition to an initiating occurrence, that result in the loss of capability of a component to perform its intended nuclear safety function Evaluates each component, one at a time	Evaluates likelihood of consequences of the failure of all components modeled
Assumes component fails with a probability of 1.0	Assumes each component fails with a best estimate failure rate and uncertainty
No credit for non-qualified components	Credit given for non-qualified components when appropriate
No common cause failure	Accounts for common cause failure
Limited credit for human actions	Credit for human actions

How PRA "Illustrates" Defense-in-Depth (analyzes effectiveness of design/operational barriers)

Defense-in-Depth Layer	Objective	Approach	PRA Treatment
1	Prevention of abnormal operation and failures	Training, conservative design (redundancy, margin), quality construction and operation	Models frequency of initiating events
2	Control of abnormal operation and detection of failures	Control, limiting, and protection systems and other surveillance features	As above and models systems (see below) and surveillance failures
3	Control of accidents within design basis	Engineered safety features and emergency operating procedures	Models safety, non-safety systems and human response
4	Control of severe plant conditions	Accident mitigation strategies	Models RCS and containment response and other severe accident mitigation measures in Level 2
5	Mitigation of radiological consequences	Offsite emergency response	Models emergency response and estimates health effects in Level 3

Exercise Demonstrating Traditional Engineering vs. PRA Approach to Safety

- In an instructor-led discussion, have the class design a system made up of piping, pumps, normally-closed injection valves, and supporting power & actuation circuits which will successfully deliver water from a single tank to a single vessel upon low level in the vessel without operator intervention, while meeting the following traditional engineering requirements:
 - Can handle the worst-case single active failure within the system
 - Must be able to handle loss of an entire division of power as a DBA
 - Must be able to handle a 0.2g safe shutdown earthquake (SSE) as another DBA
- From a PRA approach to looking at the system we have designed:
 - What active or passive failures (singularly or in multiples) are factors in assessing the overall "goodness" of our system design?
 - How might operator action be credited in the reliability of the system even though an original design constraint was that the system work without operator action?
 - While the system is designed for the SSE, what other types of outside challenges to the system might we want to consider in assessing the system's overall strengths and weaknesses?
- During the exercise, have the class comment on defense-in-depth features included in our design and how PRA might be used to "measure the goodness" of our use of these "defense-in-Depth" features.



Idaho National Laboratory

MODULE C

Overview of the PRA Process and Basic PRA Techniques

Purposes & Objectives

- **Purpose:** Provide an overview of the PRA process and describe why probabilistic models are used.
- **Objectives:** Upon completion of this module, students should be able to
 - Describe the major steps in the PRA process
 - Describe the outputs of each of the "Levels" of PRA
 - Describe why probabilistic models are used
 - Give examples of disciplines required to perform a PRA
 - Give examples of where traditional engineering inputs are used in the PRA process
 - List basic probability operations
 - Describe the difference between frequency and probability
 - Calculate probabilities
 - Define cut sets

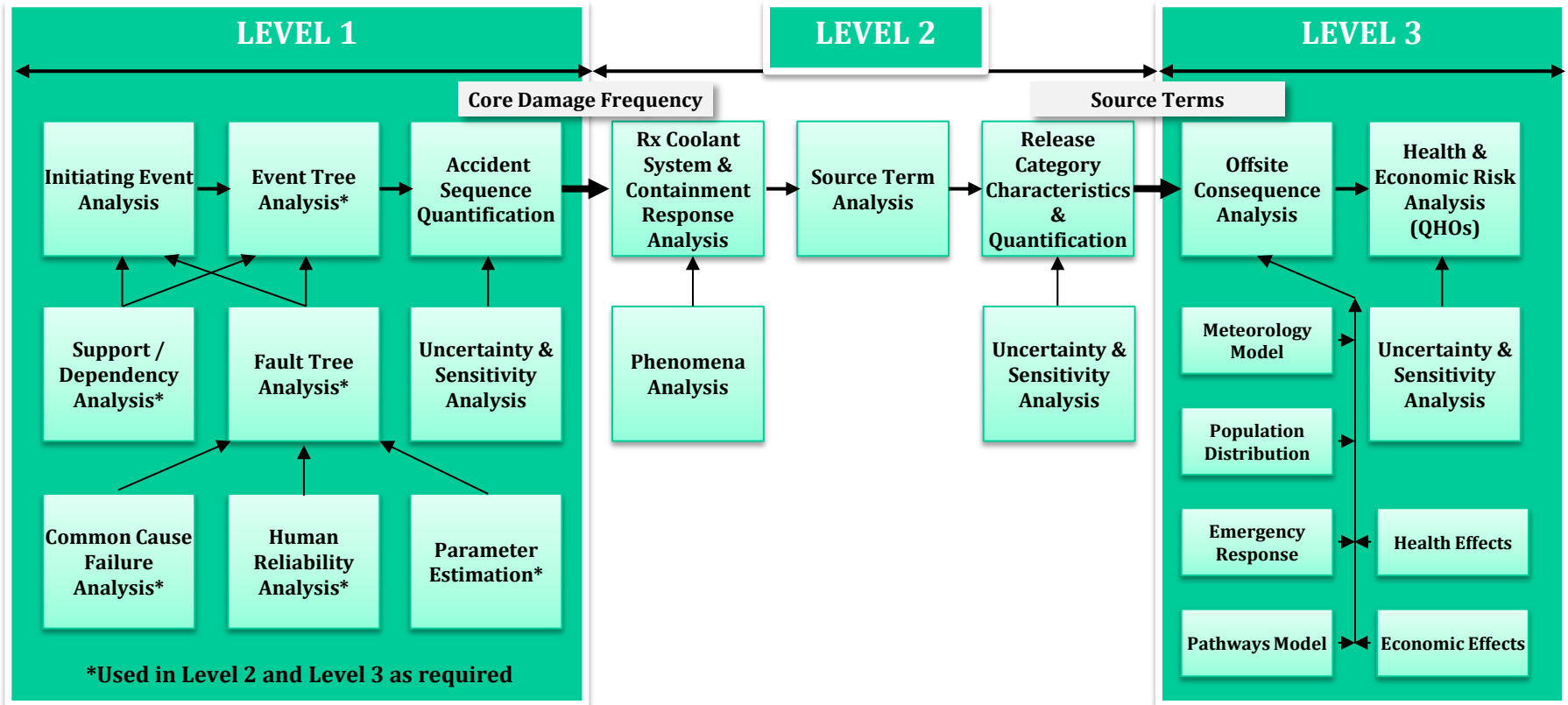
Probabilistic Risk Assessment (PRA)

- **PRA is a method that**
 - **Estimates a frequency (or probability) of risk (performance shortfall) in terms of basic failures of the system, components, and human actions**
 - **Provides a qualitative insight of system, structure, component and human interactions leading to a failure**
 - **Provides quantitative insights of system, structure, component and human interactions leading to a failure**

Probabilistic Risk Assessment (PRA)

- PRA is also a technical method to systematically answer:
 - three questions commonly referred to as the risk triplet:
 - What can go **wrong**?
 - Identify accident scenarios
 - How **likely** is it?
 - Estimate likelihood (frequency, probability) of each accident scenario
 - What will be the **outcome**?
 - Estimate consequences of each accident scenario
 - 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?

Principal Steps in PRA



Overview of PRA Process

- PRAs are performed to find vulnerabilities to safety and provide quantitative results to support decision-making
- Three levels of PRA have evolved:

Level	Type of Analysis	Assessment of:	Results
1	Systems analysis	Plant accident initiators and response of systems and operators	Core damage frequency & contributors
2	Containment analysis	Frequency and modes of containment failure	Categorization & frequencies of releases from containment
3	Radiological consequences	Public health consequences	Estimation of public & economic risks

Level 1 PRA

- **Level 1 PRA assesses frequency of core damage**
- **Level 1 PRA consists of six major steps:**
 1. **Identification and grouping of initiating events including initiators of traditional DBAs [operations experience]**
 2. **Establishment of success criteria based on traditional engineering analyses [mechanical engineers/computer specialists]**
 3. **Accident sequence modeling (event tree and fault tree development) [system engineers, operations & maintenance input, PRA modelers]**
 4. **Parameter estimation (e.g., component failure rates) [statistical experts, human performance specialists]**
 5. **Accident sequence quantification [PRA specialists]**
 6. **Documentation and evaluation of results [all]**

Level 2 PRA

- **Level 2 PRA assesses probability of containment failure & characteristics of releases from containment**
 - **Progression of severe core damage accidents evaluated by:**
 - Investigating phenomenology of the core-melt process [experimentalists, physicists]
 - Analyzing response of containment to structural challenges based on structural analyses [structural engineers]
 - **Level 2 analysis used to identify, order, and quantify physical phenomena that could affect progression of severe accidents**
 - Largely based on deterministic computer codes but with probabilistic input where outcome is random or uncertain
 - **Final product of Level 2 analysis includes:**
 - Probabilities of particular containment failure modes
 - Timing of containment failure
 - Fraction of radionuclides released to atmosphere (source term)

Level 3 PRA

- **Level 3 PRA assesses public health and economic consequences of radiological releases**
- **Comprises four major modeling processes (PRA specialists, meteorologists, health effects...):**
 - 1. Atmospheric transport and deposition model to estimate**
 - Direction & quantity of source-term plume release from containment
 - Area expected to be contaminated
 - Timing processes relative to emergency response
 - 2. Pathways model considers:**
 - Routes by which radiation enters body
 - Accumulated dose to various organs
 - 3. Health effects model estimates:**
 - Fatalities and injuries expected to occur within one year of accident
 - Cancer deaths expected to occur over lifetime of exposed population
 - 4. Models relating to other consequence factors such as:**
 - Population distribution
 - Emergency response
 - Economic effects

Level 3 PRA (cont.)

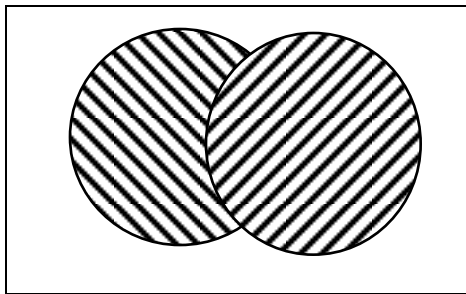
- **Integrated risk result is frequency with which a consequence of a particular magnitude will be exceeded**
- **NRC Quantitative Health Objectives (see Module A) constitute risk guidelines for commercial nuclear power plants**

Why Probabilistic Modeling?

- **Some problems/issues are too complex to treat deterministically; for example**
 - **Want to determine if emergency diesel generator (EDG) will start on next demand**
 - **Would require complete knowledge of initial and boundary conditions (e.g., how wearing of piece parts affects start capability)**
 - **Our lack of knowledge forces us to treat EDG performance as a random process (i.e., probabilistically)**

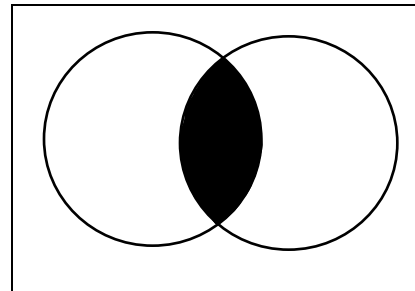
Basic Probability Concepts Used in PRAs

A or B
 $A + B$

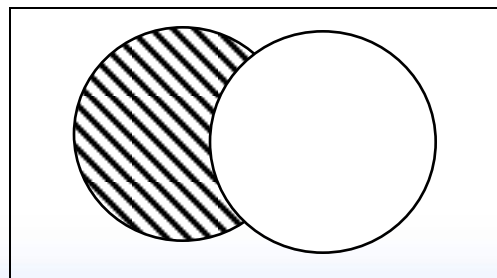


Venn Diagram

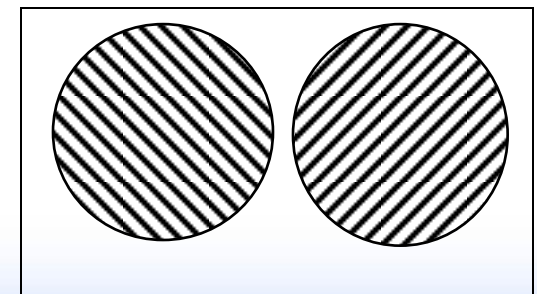
A and B
 $A * B$



A and /B
 $A * /B$

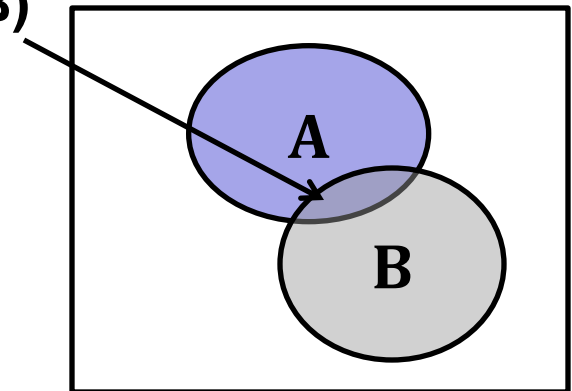


A or B
 $A + B$
with the two events mutually exclusive



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 $A \cup B$
- Rules for the OR Operation
 - In general, if A, B are not disjoint (*not mutually exclusive*)
 - $\Pr(A \text{ or } B) = \Pr(A) + \Pr(B) - \Pr(A \text{ AND } B)$
 - Can extend to three or more events
 - If A, B are disjoint (*mutually exclusive*)
 - $\Pr(A \text{ or } B) = \Pr(A) + \Pr(B)$
 - Example:
with a die, $\Pr(1 \text{ or } 2) = \Pr(1) + \Pr(2)$
because outcomes are disjoint



Venn Diagram

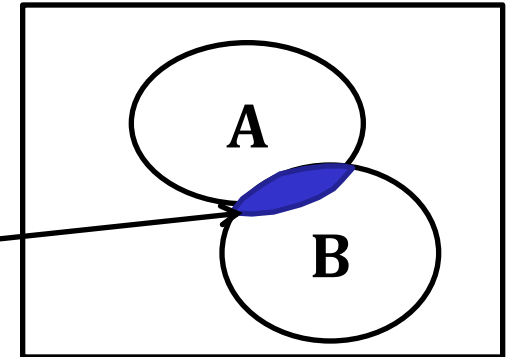
Rules for Manipulating Probabilities – AND (Intersection)

- The AND (or intersection) operation
 - A **AND** B = combined event containing everything that is both in A or in B
 - Also written $A \cap B$

- Rules for the AND operation

- If A, B are independent

- $\Pr(A \text{ AND } B) = \Pr(A) \cdot \Pr(B)$ (definition)



- If A, B are not independent (i.e., dependent)

- $\Pr(A \text{ AND } B) = \Pr(A) \cdot \Pr(B|A) = \Pr(B) \cdot \Pr(A|B)$

- $\Pr(B|A)$ 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
 - $\Pr(A \text{ AND } B) = \Pr(A) \cdot \Pr(B | A)$
 - The conditional probability is last term, $\Pr(B | A)$, so
 - $\Pr(B | A) = \Pr(A \text{ AND } B) / \Pr(A)$, $\Pr(A) \neq 0$
 - $\Pr(A | B) = \Pr(A \text{ AND } B) / \Pr(B)$, $\Pr(B) \neq 0$
 - 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 $\Pr(A \text{ and } B) = \Pr(A) * \Pr(B)$
 - Example: $\Pr(H \text{ and } T \mid \text{two tosses}) = \Pr(H)*\Pr(T)$

- **Mutually Exclusive**

- Means that events (such as A and B) **cannot both happen** on a single trial of an experiment (same time)
- With the toss of a coin, either a Head or a Tail is the expected outcome, cannot possibly get both a Head & a Tail as an outcome on a single toss
- This property allows us to write (if A and B are mutually exclusive)
 - $\Pr(A \text{ or } B) = \Pr(A) + \Pr(B)$
 - $\Pr(A \text{ and } B) = \Pr(A)*\Pr(B|A) = \Pr(B)*\Pr(A|B) = 0$
 - Example: $\Pr(H \text{ or } T \mid \text{one toss}) = \Pr(H) + \Pr(T) \quad \therefore \Pr(H \text{ and } T \mid \text{one toss}) = 0$

Basic Probability Concepts

- **Dependent**

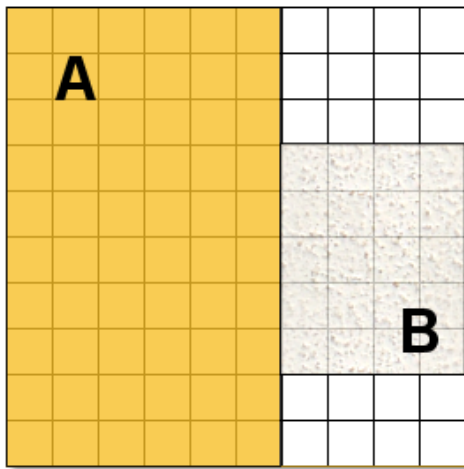
- Means that the occurrence (or non-occurrence) of an event (such as A) **has an influence** on the subsequent occurrence (or non-occurrence) of another event (such as B) and vice versa
- For example, if a resistor overheats in an electronic circuit, it may very well change the failure probability of a nearby transistor or related circuitry.
- This property allows us to write
 - If A and B are dependent events, then
$$\Pr(A \text{ and } B) = \Pr(A) * \Pr(B|A) = \Pr(B) * \Pr(A|B)$$
 - 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”)**

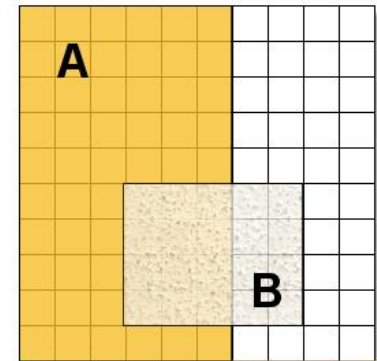
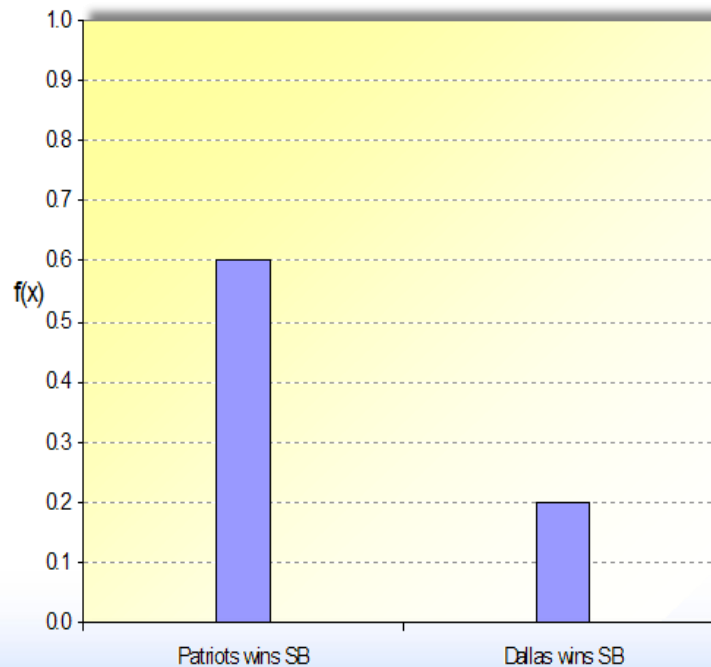
- Means the probability is “1 -” the probability of event
 - $\Pr(\text{not } A) = 1 - \Pr(A)$

Independent versus Disjoint

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



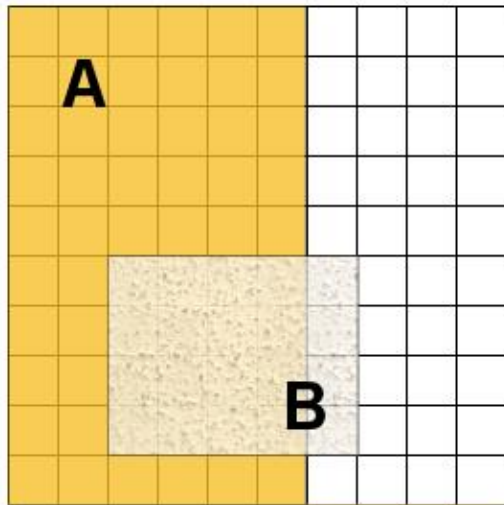
Disjoint



$\Pr(A \text{ AND } B) = 0.12$
if A, B were
independent...

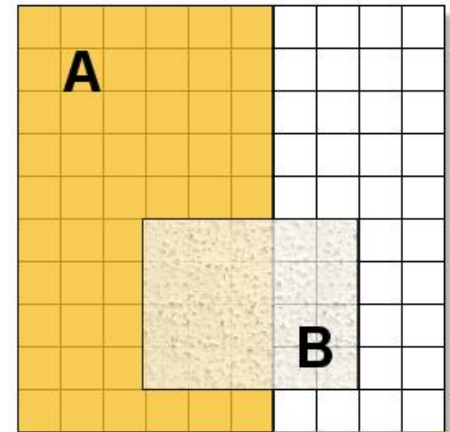
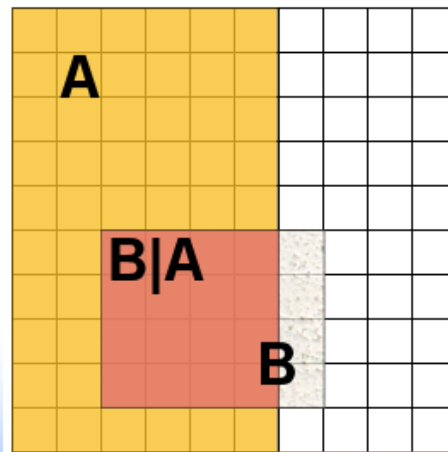
Independent versus Dependent

- An example using dependent events
 - If $\Pr(A) = 0.6$, $\Pr(B) = 0.2$, and $\Pr(A \text{ AND } B) = 0.16$, then
 - $\Pr(B|A) = \Pr(A \text{ AND } B)/\Pr(A) = 0.16/0.6 = 0.2667$
 - since $\Pr(A \text{ AND } B) = \Pr(A) \cdot \Pr(B|A)$
 - $\Pr(A|B) = \Pr(A \text{ AND } B)/\Pr(B) = 0.16/0.2 = 0.80$
 - since $\Pr(A \text{ AND } B) = \Pr(B) \cdot \Pr(A|B)$



A and B are dependent

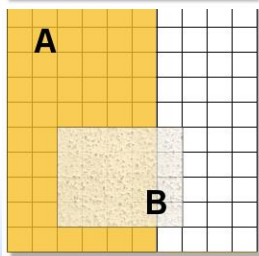
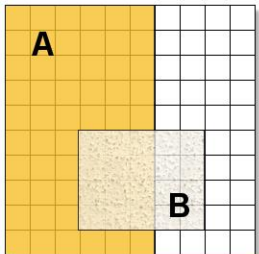
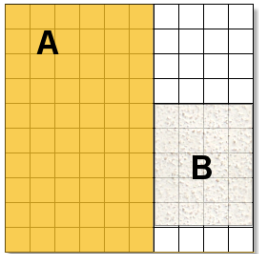
Where is $\Pr(B|A)$ on the Venn diagram?
 $16 \text{ blocks} / 60 \text{ blocks} = 0.2667$



$\Pr(A \text{ AND } B) = 0.12$
 if A, B were independent...

Disjoint, Independent, Dependent Summary

- Table below summarized the probability rules



Case	Operation	Rule
Disjoint	OR	$p(A \text{ OR } B) = p(A) + p(B)$
	AND	$p(A \text{ AND } B) = 0$
Independent	OR	$p(A \text{ OR } B) = p(A) + p(B) - p(A \text{ AND } B)$
	AND	$p(A \text{ AND } B) = p(A)p(B)$
Dependent	OR	$p(A \text{ OR } B) = p(A) + p(B) - p(A \text{ AND } B)$
	AND	$p(A \text{ AND } B) = p(A)p(B A)$ $= p(B)p(A B)$

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

- **Frequency**
 - Parameter used in model for stochastic (aleatory) uncertainty
 - Events **per unit of time**
 - Frequency can be any positive value (i.e., can be greater than one)
 - Typically used for initiating events and failure rates
- **Probability**
 - Internal measure of certainty about the truth of a proposition
 - Always conditional
 - **Unitless**
 - Value between 0 and 1
 - 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)**

- $P[r \text{ failures in } N \text{ trials } | p] = \binom{N}{r} p^r (1-p)^{N-r}$
 - **Recall:** $\binom{N}{r} = \frac{N!}{r!(N-r)!}$

- **Probability of failure for a single demand**

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

- **Binomial Example:**

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

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

Common Probability Models (cont.)

- Poisson (used for failures/events in time)

- $P[r \text{ failures in } (0,t) | \lambda] = \frac{(\lambda t)^r e^{-\lambda t}}{r!}$

- Probability of **one or more failures**

- $P[T_f < t | \lambda] = 1 - e^{-\lambda t} \approx \lambda t$ (for small λt ; when $\lambda t < 0.1$)

- Example: estimate of product λt 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 $\lambda = 1\text{E-}4$ failures per operating hour

- Probability of failure to run for 24 hours?

- $P[T_f < 24 \text{ hours} | 1\text{E-}4 \text{ failures/hour}]$

- $= 1 - e^{-(1\text{E-}4/\text{hour})(24 \text{ hours})} = 1 - e^{-(2.4\text{E-}3)} = 1 - (0.9976028) = 0.0023971$

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

Probability of Core Damage

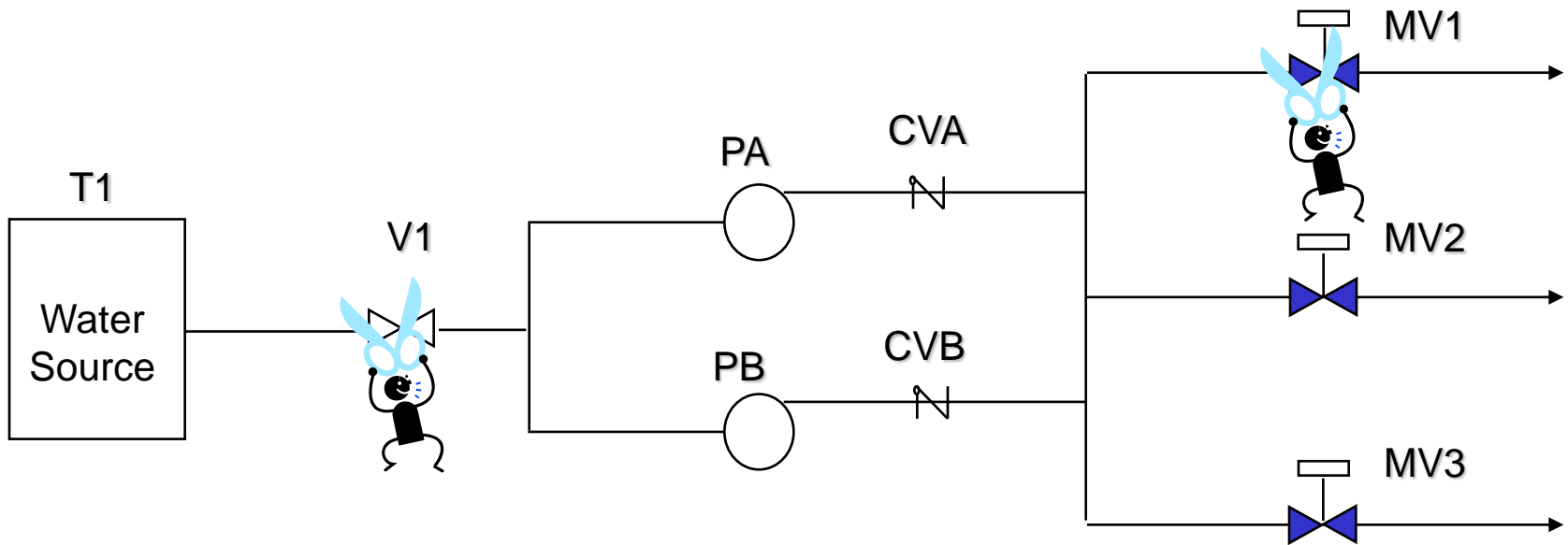
- Assume 100 plants, each with CDF = 1E-4/yr
- Assume operation over 40 years
- What is probability of at least one core damage accident during that time?

$$\begin{aligned} & P(\geq 1 \text{ core damage} \mid \text{CDF} = 1\text{E-}4/\text{yr}) \\ &= 1 - \exp[-(1\text{E-}4/\text{plant-yr})(40 \text{ yr})(100 \text{ plants})] \\ &= 0.33 \end{aligned}$$

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 (“min cut”) Approximation**

Exact Solution

- **Exact Solution for Cut Sets = A OR B**
 - $P(\text{Exact Solution}) = P(A + B) = P(A) + P(B) - P(AB)$
- **Cross terms become unwieldy for large lists of cut sets**

– E.g., if Cut Sets = A OR B OR C, then:

– $P(\text{Exact Solution for Cut Sets}) =$

$$P(A)+P(B)+P(C) - P(AB) - P(AC) - P(BC) + P(ABC)$$



Add the Singles



Subtract the Doubles



Add the Triples

...

Rare Event Approximation

- **Rare Event Approximation for Cut Sets = A OR B**
 - P(Union of Cut Sets) \approx sum of the probabilities of each individual cut set
 - P(Union of Cut Sets) $\approx \sum_{k=1}^K P(\text{Cut Set}_k)$
 - 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} $\leq \sum_{k=1}^K P(\text{Cut Set}_k)$

Minimal Cut Set Upper Bound

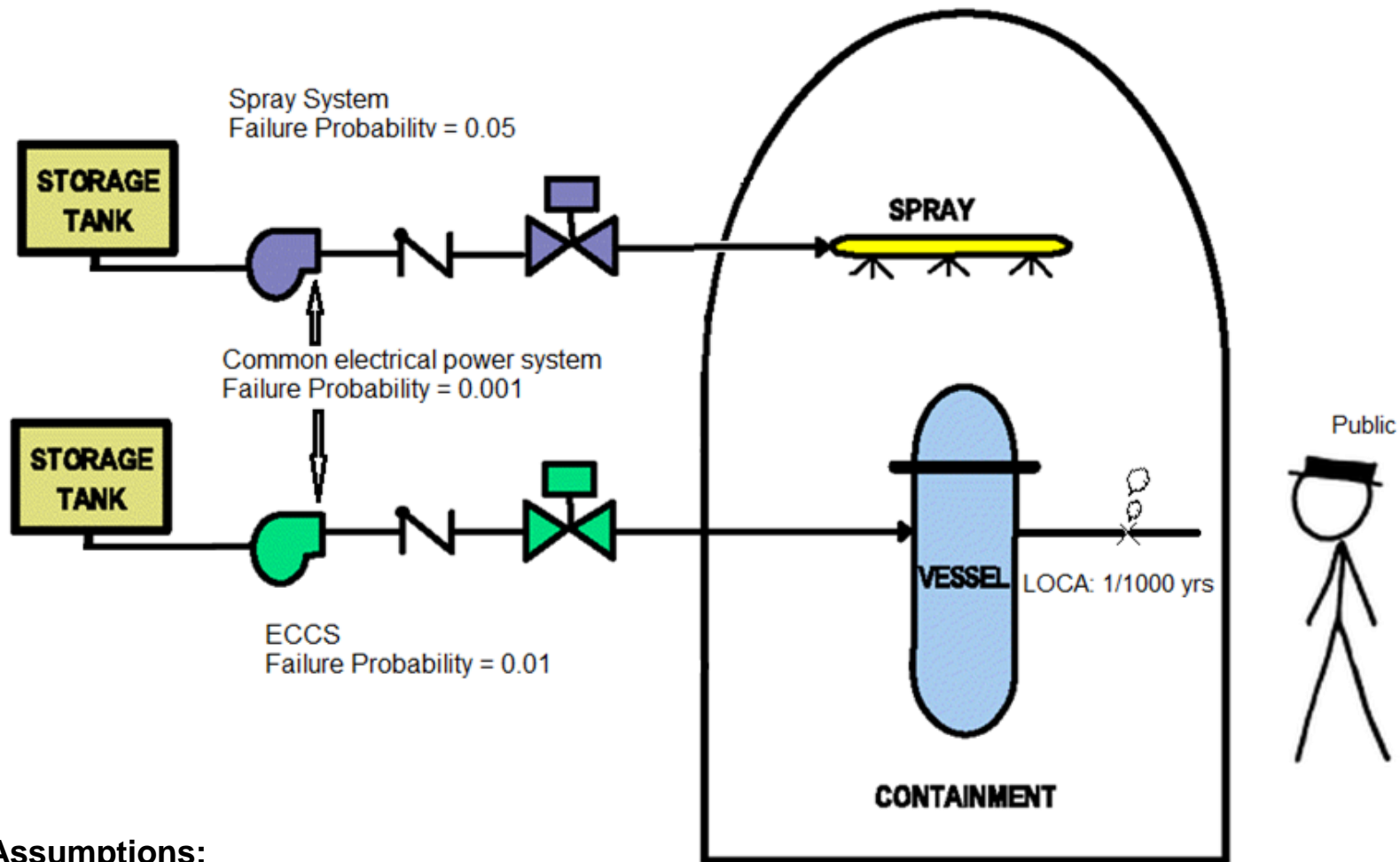
- **Minimal Cut Set Upper Bound (“min cut”)**
Approximation for Cut Sets = A OR B
 - P(Minimal Cut Set Upper Bound for Cut Sets) \approx 1.0 minus the product of each individual cut set NOT occurring
 - Failure = 1 - Success
 - $P(\text{MCSUB for Cut Sets}) \approx 1 - \prod_{k=1}^K [1 - P(\text{Cut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

Examples of Cut Set Quantification Methods for P(A OR 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 <i>not</i> independent (they have shared basic events); individual cut set values low
Cut-Sets = A OR B	P(A) = 0.01 P(B) = 0.03	P(A) = 0.4 P(B) = 0.6	Cut Set A = BE1 * BE2 Cut Set B = BE2 * BE3 P(BE1) = 0.1 P(BE2) = 0.1 P(BE3) = 0.3
Exact	= 0.01 + 0.03 - (0.01*0.03) = 0.04 - 0.0003 = 0.0397	= 0.4 + 0.6 - (0.4*0.6) = 1.0 - (0.24) = 0.76	= (BE1*BE2) + (BE2*BE3) - BE1*BE2*(BE2*BE3) = (BE1*BE2) + (BE2*BE3) - (BE1*BE2*BE3) = 0.01 + 0.03 - 0.003 = 0.04 - 0.003 = 0.037
Rare Event	= 0.01 + 0.03 = 0.04	= 0.4 + 0.6 = 1.0	= 0.01 + 0.03 = 0.04
MinCut UB	= 1 - [(1-0.01) * (1-0.03)] = 1 - [(0.99) * (0.97)] = 1 - [0.9603] = 0.0397	= 1 - [(1-0.4) * (1-0.6)] = 1 - [(0.6) * (0.4)] = 1 - [0.24] = 0.76	= 1 - [(1-0.01) * (1-0.03)] = 1 - [(0.99) * (0.97)] = 1 - [0.9603] = 0.0397

Exercise Demonstrating PRA Process

- **For the simple plant shown (next page)**
 - **What can go wrong?**
 - **Assume Loss-of-Coolant Accident (LOCA) is the initial challenge (initiating event) during normal plant operation**
 - **What else could go wrong in terms of the three systems shown?**
 - **Success or failure of electric power system**
 - **Success or failure of emergency core cooling system (ECCS)**
 - **Success or failure of containment spray system (CSS)**
 - **How likely is each combination of events identified above?**
 - **Use LOCA frequency and given probabilities to calculate scenario frequencies**
 - **What are the consequences?**
 - **What happens to core in each scenario?**
 - **What happens to containment?**
 - **Characterize expected release offsite**
 - **Which level of PRA would be involved in each of these questions?**



Assumptions:

- 1 – Electric system powers both ECCS and Spray System
- 2 – If ECCS fails, core is damaged
- 3 – If spray system fails, containment is damaged
- 4 – If spray system is successful, containment does NOT fail – even with core damage (i.e., ECCS failed)
- 5 – If spray system fails, containment is damaged and ECCS will subsequently fail if not already failed

******IPE Exercise******

- **Using your choice of a plant's IPE (most are available on the NRC internal web site), determine the following:**
 1. **Level of PRA detail that was analyzed**
 2. **Estimated core damage frequency (CDF)**
 3. **Compare estimated CDF with 1E-4 goal**
 4. **Dominant (highest frequency) type of accident sequence**
 5. **Estimated large, early release frequency (LERF)**
 6. **Compare estimated LERF with 1E-5 goal**

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?

 - 3.3. If the experiment is repeated 4 times, what is the probability of observing the following number of failures;
 - 0
 - 0 or 1
 - 0 or 1 or 2
 - 0 or 1 or 2 or 3
 - 0 or 1 or 2 or 3 or 4

Answers to the 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?
 - $P\{\text{event} < 1 \text{ year}\} = 1 - e^{-(2E-2)(1)} = 1 - 0.9802 = 0.0198 = 1.98E-2$
 - Or $P\{\text{event} < 1 \text{ year}\} \approx \lambda t \approx (2E-2)(1) \approx 2E-2$
 - 1.2. What is the probability that at least one event will occur within 50 years?
 - $P\{\text{event} < 50 \text{ years}\} = 1 - e^{-(2E-2)(50)} = 1 - e^{-1} = 1 - 0.3679 = 0.6321 = 6.321E-1$
- 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 $P(A + B) = P(A) + P(B) - P(AB) = 1 - e^{-(\lambda A + \lambda B)t} = 1 - e^{-(0.1 + 0.3)5} = 1 - 0.1353 = 8.647E-1$

Answers to the 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?**

- **$P[\text{exactly 1 failure in 4 trials} \mid 0.1] =$**

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

- **3.2. What is the probability of observing at least one failure if the experiment is repeated 4 times?**

- **$P[\text{at least 1 failure in 4 trials} \mid 0.1] =$**

- **$P[1] + P[2] + P[3] + P[4] = 0.2916 + 0.0486 + 0.0036 + 0.0001 = 0.3439$**

or

- **$1 - P[0 \text{ failures in 4 trials} \mid 0.1] = 1 - 0.6561 = 0.3439$**

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

Answers to the Probability and Frequency Questions

- 3.3. If the experiment is repeated 4 times, what is the probability of observing the following number of failures;
 - 0
 - $P[0] = 0.6561 = 0.6561$
 - 0 or 1
 - $P[0] + P[1] = 0.6561 + 0.2916 = 0.9477$
 - 0 or 1 or 2
 - $P[0] + P[1] + P[2] = 0.6561 + 0.2916 + 0.0486 = 0.9963$
 - 0 or 1 or 2 or 3
 - $P[0] + P[1] + P[2] + P[3] = 0.6561 + 0.2916 + 0.0486 + 0.0036 = 0.9999$
 - 0 or 1 or 2 or 3 or 4
 - $P[0] + P[1] + P[2] + P[3] + P[4] = 0.6561 + 0.2916 + 0.0486 + 0.0036 + 0.0001 = 1.0000$

Answers to the Probability and Frequency Questions

- $P\{\text{exactly 0 failures in 4 trials} \mid 0.1\} =$
- $= \frac{4!}{0!(4-0)!} 0.1^0(1-0.1)^4 = (1)(1)(0.6561) = 0.6561$
- $P\{\text{exactly 1 failure in 4 trials} \mid 0.1\} =$
- $= \frac{4!}{1!(4-1)!} 0.1^1(1-0.1)^3 = (4)(0.1)(0.729) = 0.2916$
- Or use EXCEL

	A	B	C	D	E
8	X	Pr(X n=4)			
9		0	0.6561	=BINOM.DIST(A9,4,\$B\$1,0)	
10		1	0.2916	=BINOM.DIST(A10,4,\$B\$1,0)	
11		2	0.0486	=BINOM.DIST(A11,4,\$B\$1,0)	
12		3	0.0036	=BINOM.DIST(A12,4,\$B\$1,0)	
13		4	0.0001	=BINOM.DIST(A13,4,\$B\$1,0)	



Idaho National Laboratory

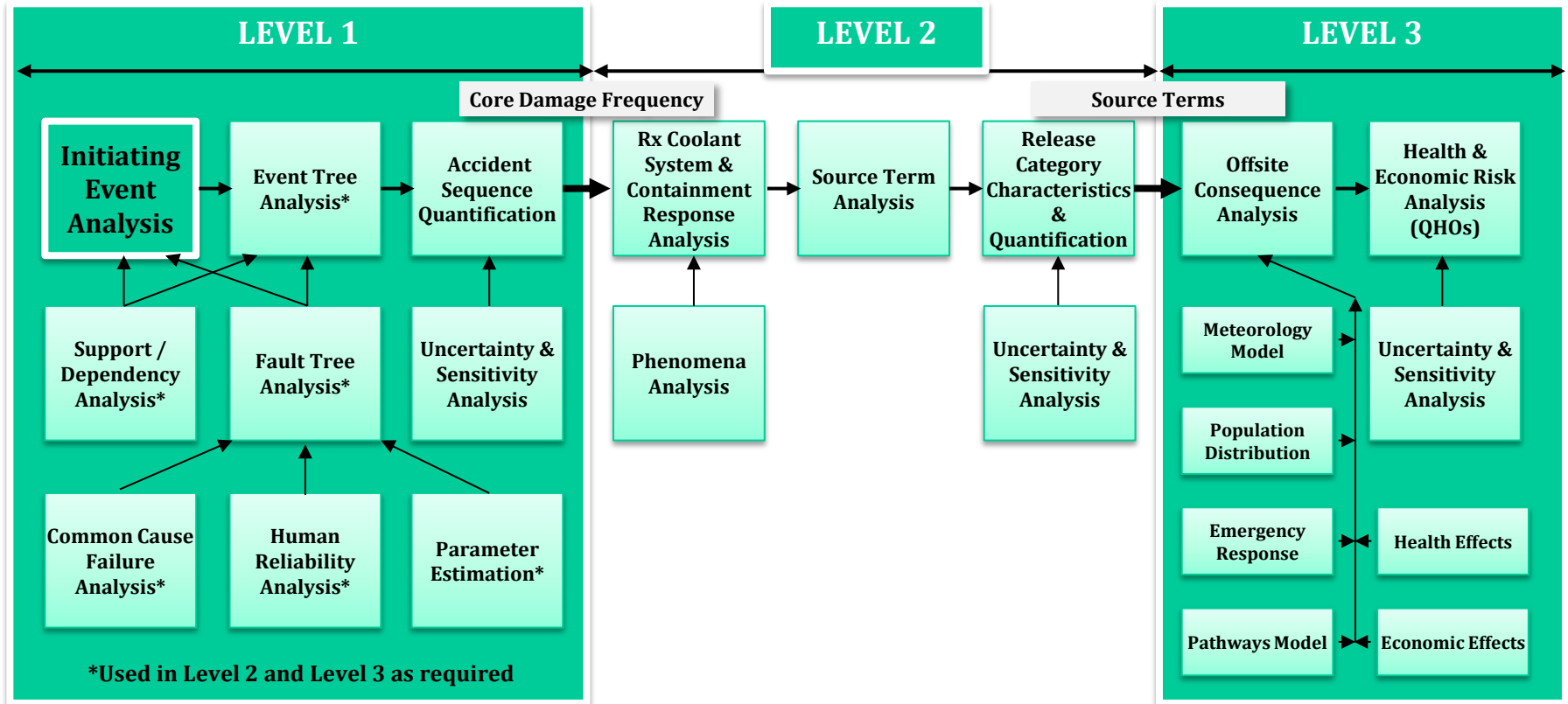
MODULE D

ACCIDENT SEQUENCE INITIATING EVENTS

Accident Sequence Initiating Events

- **Purpose:** Students will learn how initiating events (IEs) are identified and grouped. Students will be exposed to the methods used to estimate initiating event frequencies and to sources of generic data for initiating events.
- **Objectives:**
 - Understand the relationship between initiating event identification and other PRA related tasks.
 - Become familiar with the various ways to identify initiating events.
 - Understand how initiating events are grouped and quantified.
 - Understand the relationship between PRA "initiators" and "challenges" in a traditional safety analysis report (SAR).

Principal Steps in PRA



Initiating Events

- **Definition → Any potential occurrence that could disrupt plant operations**
 - Initiating events are quantified in terms of their frequency of occurrence (i.e., number of events per year)
- **Can occur while reactor is: at full power, at low power, at shutdown**
- **Most PRAs examine full power only**
- **Broad categories include: LOCAs and Transients (both from "internal" and "external" events)**
- **Initiating event identification consists of**
 - Identifying comprehensive list of potential initiators that could upset plant operations
 - Grouping initiating events into categories based on their impact on plant accident response systems
 - Quantifying applicable initiating event category frequencies

Illustrative List of Events and Frequencies (from North Anna IPE and comparable NUREG/CR-6928)

North Anna IPE				NUREG/CR-6928	
Category	Initiating Event	Frequency (per Rx Yr)	Return Period (Rx Yr)	Frequency (per Rx Yr)	Return Period (Rx Yr)
T1	Loss of offsite power	1.1E-01	9.1	2.8E-02	35
T2	Transient with nonrecoverable loss of MFW	5.0E-02	20	5.9E-02	17
T2A	Transient w/recoverable loss of MFW	5.5E-01	1.8	6.9E-02	15
T3	Transient w/MFW available initially	1.35	0.74	0.69	1.4
T4	Loss of RCP seal cooling	6.0E-07	1,666,667		
T5	Nonrecoverable loss of DC bus	6.0E-03	167	7.4E-04	1,357
T6	Loss of service water	6.3E-06	158,730	2.5E-04	4,065

Illustrative List of Events and Frequencies (from North Anna IPE and comparable NUREG/CR-6928) (cont.)

North Anna IPE				NUREG/CR-6928	
Category	Initiating Event	Frequency (per Rx Yr)	Return Period (Rx Yr)	Frequency (per Rx Yr)	Return Period (Rx Yr)
T7	Steam generator tube rupture	1.0E-02	100	2.1E-03	483
T8	Loss of emergency switchgear room cooling	6.6E-03	152		
T9	Loss of 4.1kV emergency buses	1.8E-02	56	4.4E-03	230
A	Large LOCA	5.0E-04	2,000	2.5E-06	400,000
S1	Medium LOCA	1.0E-03	1,000	1.5E-04	6,667
S2	Small LOCA	2.0E-02	50	3.7E-04	2,725
V	Interfacing system LOCA	1.6E-06	625,000		

Illustrative List of Initiating Events and Frequencies (from North Anna IPE) (cont.)

- **Some possible initiating events may not be modeled explicitly**
 - **Frequency is very low**
 - **Unisolated feedwater line break**
 - **Effect is slow, easily identified, and recoverable**
 - **Loss of control room HVAC**
 - **Effect covered by existing initiating event category and frequency accounted for**
 - **Loss of instrument air under T2 – loss of feedwater**
 - **Effect does not cause an automatic or immediate administrative demand for shutdown**
 - **Waste treatment failure**

Role of Initiating Events in PRA

- **Identifying initiating events is the first step in the development of accident sequences**
 - What can go wrong and how often can it go wrong?
- **Accident sequences can be conceptually thought of as:**
 - An initiating event, which triggers a series of plant and/or operator responses
 - Then the initiating event in combination of success and/or failure of the plant and/or operator responses that result in some core damage state
- **Initiating event identification is an iterative process that requires feedback from other PRA processes for completeness.**
 - Support/dependency analysis
 - Review of plant experience and data

Example Categories of Initiating Events (SAR compared with PRA)

In Safety Analysis Report

In PRA

-
- | | |
|--|---|
| <ul style="list-style-type: none">•Increase in secondary system heat removal<ul style="list-style-type: none">•Increase in FW flow•Opening of SG relief valve•Balance-of-plant upsets•Decrease in secondary system heat removal<ul style="list-style-type: none">•Turbine trip•MSIV closure•Loss of FW flow•Decrease in RCS flow rate<ul style="list-style-type: none">•RCP trip•Power anomalies<ul style="list-style-type: none">•Uncontrolled rod withdrawal•Boron dilution•Decrease in RCS inventory<ul style="list-style-type: none">•SGTR•LOCAs | <ul style="list-style-type: none">•T3 - transient w/MFW available•T2A - transient w/MFW recoverable
•T3 - transient w/MFW available•T3 - transient w/MFW available•T2 - transient w/MFW not recoverable
•T3 - transient w/MFW available
•T3 - transient w/MFW available•T3 - transient w/MFW available
•SGTR•LOCAs |
|--|---|

Sources Used to Identify Initiating Events

- Review of existing PRAs
- Review of plant experience and procedures
- Feedback from other PRA tasks
- Generic databases
- Various NRC and industry sponsored studies
- It should be noted that PRA initiators:
 - Encompass all SAR initiators plus others
 - Individual events grouped into categories for similar plant responses

Initiating Event Grouping

- **For each identified initiating event**
 - Identify safety functions required to prevent core damage
 - Identify plant systems that can provide the required safety functions
- **Group initiating events into categories that require the same plant response**
- **This is an iterative process, closely associated with the event tree construction task (see Module E)**
- **Grouping ensures**
 - All functionally distinct accident sequences will be included
 - Overlapping of similar accident sequences will be prevented
 - A single event tree can be used for all IEs in a category (group)

Initiating Event Grouping Example

Table 3.3.1: Success Criteria Of Front Line Equipment For Core Damage Mitigation Functions

Initiator Class	Reactivity Control	RCS Inventory Control	RCS Pressure Boundary Integrity	RCS and Core Heat Removal		
				Primary-Secondary Heat Removal	Feed and Bleed Cooling	Long Term RCS Cooling/Inventory Control
Transients	RPS, or EB for RPS signal failure	Not needed if RCS is Intact	(SDBC, or PORVs/SRVs) and (PORVs and SRVs reclose)	(1 MFW or 1 AFW ^{**}) and (SDBC or ADV or MSSV)	1 PORV, ^{***} and 1 HPSI	Continued Primary/Secondary Heat Removal or SDC or 1/3 HPR if feed & bleed in Initiated
Small LOCA	RPS, or Manual for RPS signal failure	1/3 HPSI ^{***}	N/A	(1 AFW ^{**}) and (SDBC or ADV or MSSV)	1 PORV ^{***}	1/3 HPR or SDC
Medium LOCA	N/A	1/3 HPSI	N/A	N/A	N/A	1/3 HPR
Large LOCA	N/A	1/3 HPSI & 3/4 SIT or [*] 1/2 LPSI & 2/4 SIT	N/A	N/A	N/A	1/3 HPR or 1/2 LPR (Cold Leg Recirculation)
SGTR	RPS, or Manual for RPS signal failure	1/3 HPSI ^{***}	(SDBC or ADV or MSSV)	(1 MFW or 1 AFW ^{**}) and (SDBC or ADV or MSSV)	1 PORV ^{***}	Continued RCS Inventory makeup or SDC
ISLOCA	RPS, or Manual for RPS signal failure	1/3 HPSI	(SDBC or ADV or MSSV) or Low Pressure System Intact	(1 MFW or 1 AFW ^{**}) and (SDBC or ADV or MSSV)	N/A	Continued RCS Inventory makeup or SDC

* Large LOCA success criteria based on calculations performed for (< 3 ft² equivalent area) credible pipe break, and realistic post-accident thermal hydraulic system performance.

** If AFW is not initially available, the time available for recovery is 1 hour.

*** Feed-and-Bleed is required in conjunction with a total loss of feedwater. The inventory control aspect is provided by 1 of 3 HPSI pumps. Pressure control is provided by the PORV.

Initiating Event Quantification

- **Use values based on type and frequency of events industry-wide**
 - Useful for rare events not expected to occur during the life of the plant
- **Use plant-specific data to update generic values when such data is available**
 - Uses Bayesian updating process that will be discussed later
- **Modeling and/or mechanistic analysis techniques**
 - Useful for very rare events where we have little data
- **All of the above are used in a typical PRA**

Exercise: Initiating Event Frequency

- **Estimate a transient initiating event frequency based on the following information:**
 - **A plant has 10 years of data, and the plant's capacity factor was 85% over that 10 year period. Transients over that 10 year period;**

<u>Year</u>	<u>Number of Transients</u>
2000	2
2001	0
2002	1
2003	0
2004	1
2005	0
2006	2
2007	0
2008	0
2009	1

Generic Initiating Event Frequencies

- **Generic initiating event frequencies can be obtained from the following sources.**
 - NUREG/CR-4550, Vol.1 Methods and Data for NUREG-1150
 - NUREG/CR-3862, Development of Transient Initiating Event Frequencies (pre-1986)
 - NUREG/CR-5750, Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995
 - NUREG/CR-6365, Steam Generator Tube Failures
 - NUREG/CR-6890, Reevaluation of Station Blackout Risk at Nuclear Power Plants: 1986 - 2004
 - NUREG/CR-4407, Pipe Break Frequency Estimation for Nuclear Power Plants
 - NUREG-1829, Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process
 - NSAC-154, ISLOCA Evaluation Guidelines
 - EPRI TR-100380, Pipe Failures in U.S. Commercial Nuclear Power Plants
 - EPRI TR-1003113, An Analysis of Loss of Decay Heat Removal Trends and Initiating Event Frequencies (1989 – 2000)
 - NUREG/CR-6850, EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Plants
 - NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants
- **Note that the above cite industry-wide yearly averages. Plant-to-plant differences can and do exist, and on any given day can be dependent on existing plant configuration and environmental conditions. Therefore....**

A Cautionary Note

- **Plant PRA initiating event frequencies should**
 - Reflect unique plant characteristics
 - May not be appropriate in a specific operational condition or environment
- **For example**
 - Generic loss of offsite power frequency is 0.05/yr
 - Plant X is located in "tornado alley"
 - Possible questions to consider:
 - Does the loss of offsite power frequency for this plant reflect its location?
 - Should plant configuration control decisions be made during the peak of tornado season using the generic frequency?

*** IE Exercise ***

Given the following PRA results:

IE	IE Frequency (per yr)	% Contribution to CDF by IE	CDF Contribution by IE (per year)	New CDF Contribution by IE (per year)
LLOCA	5E-5	3%	2.1E-6	
MLOCA	1E-4	10%	7.0E-6	
SLOCA	1E-3	15%	1.1E-5	
ISLOCA	2E-6	1%	7.0E-7	
All Others	NA	71%	5.0E-5	
Total Internal CDF = 7E-5			New Total Internal CDF =	

The licensee finds that a number of RCS instrument lines are experiencing excessive mechanical fatigue due to lack of proper supports.

Estimate the change in CDF if the IE frequency of SLOCA increases by a factor of 2 as a result of this condition.

Note: $CDF = IE * Pr(\text{system failures})$
 e.g., $LLOCA = 2.1E-6 = 5E-5 * Pr(\text{system failure})$
 $\therefore Pr(\text{system failure}) = 2.1E-6/5E-5 = 4.2E-2$

***** PRA Exercise *****

- **Answer the following from your plant's IPE/PRA**
 - **What are the transient initiator groups used in the analysis?**
 - **If more than one group is used,**
 - **What are the transient group frequencies?**
 - **Which transient group has the highest frequency?**
 - **Does the way in which transients have been grouped seem reasonable?**
 - **How many different LOCAs are modeled?**
 - **What are their frequencies?**



Idaho National Laboratory

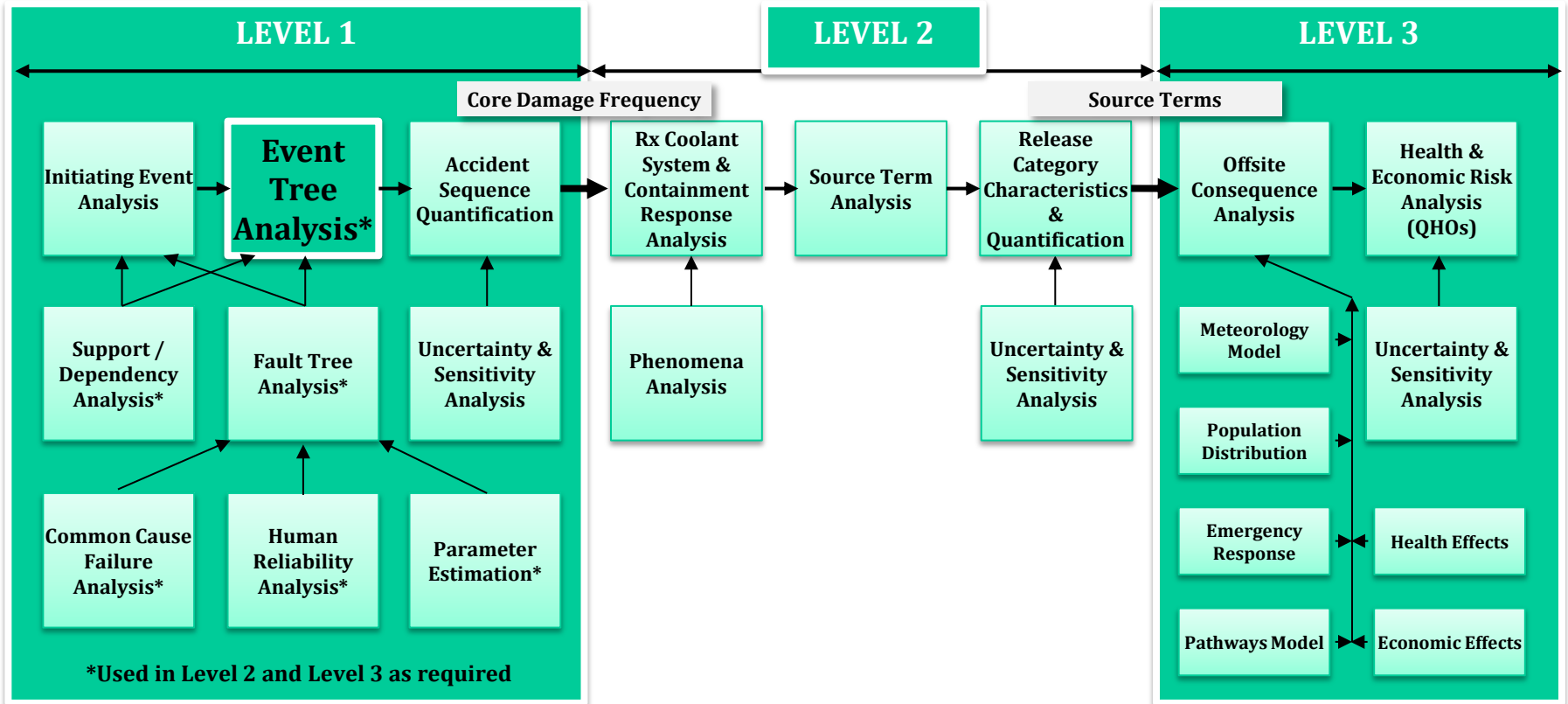
MODULE E

ACCIDENT SEQUENCE ANALYSIS USING EVENT TREES

Accident Sequence Analysis Using Event Trees

- **Purpose:** Students will learn purposes and techniques of event tree analysis. Students will learn how event tree analysis is related to the identification and quantification of accident sequences.
- **Objectives:**
 - Describe the purposes of event tree analysis
 - Describe techniques and notations employed in event tree construction
 - Describe the relationship between event tree construction and deterministically-identified success criteria
 - Compare PRA accident sequences (as depicted by the event trees) and the traditional SAR design basis accidents
- **References:** NUREG/CR-2300

Principal Steps in PRA



Event Trees

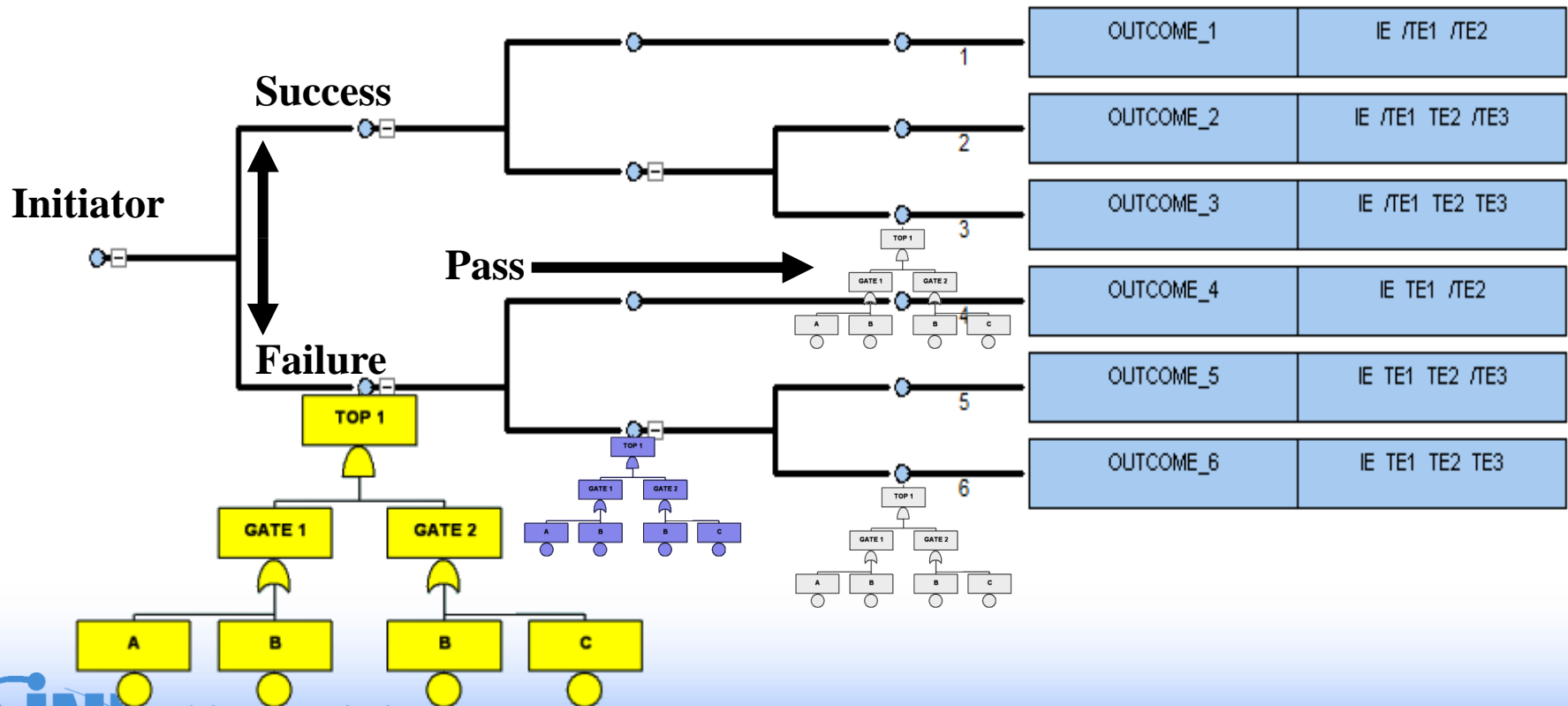
- Typically used to model the response to an initiating event
- Features:
 - One event tree for each initiating event (or initiating event group)
 - Related to plant functions/systems/operations
 - Identifies **relationships** in event occurrence
 - Identifies relative **timing** of event occurrence
 - Provides event sequence progression
 - Provides 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

Traditional Event Tree Format

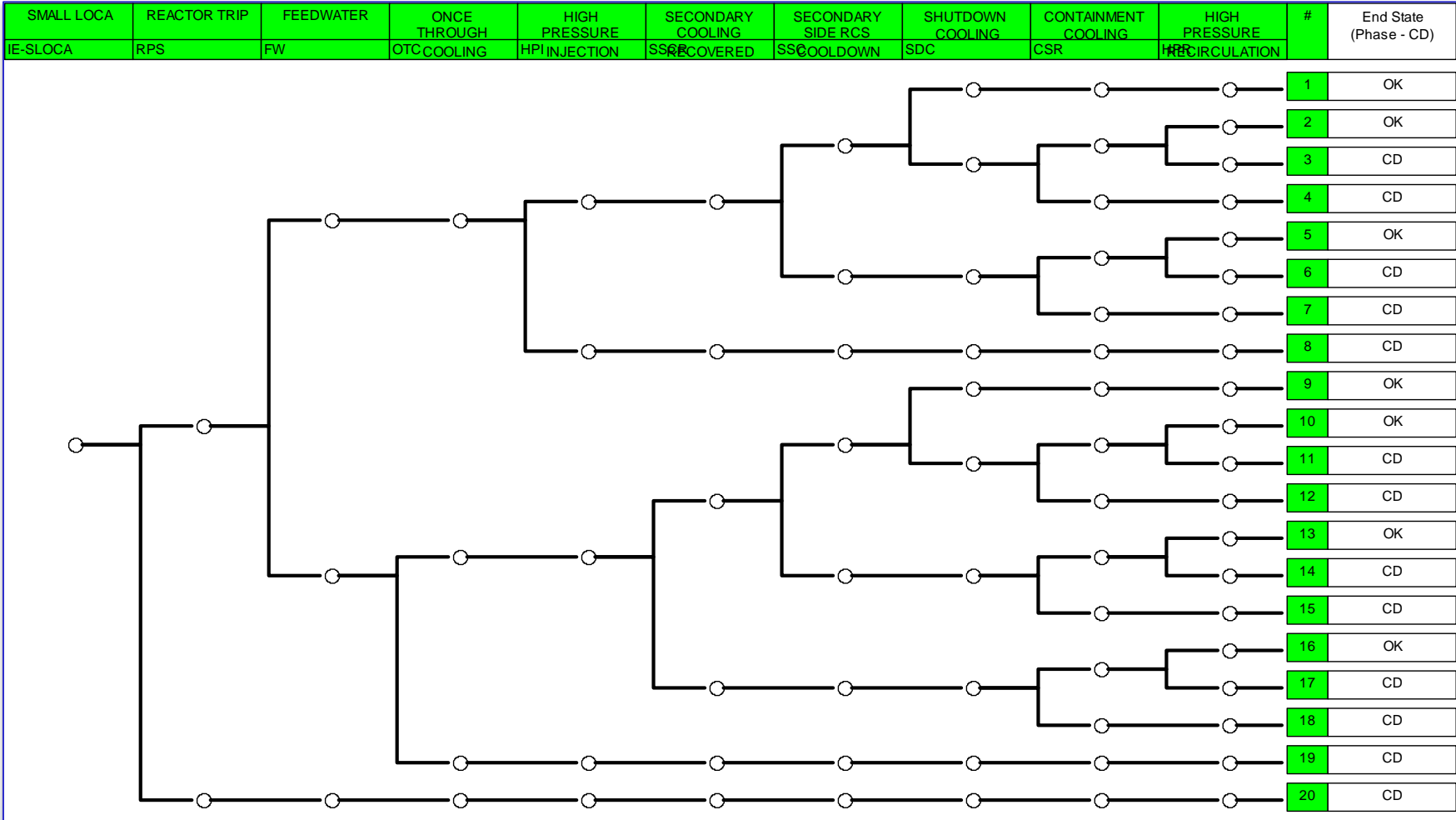
Top Events

End State

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		

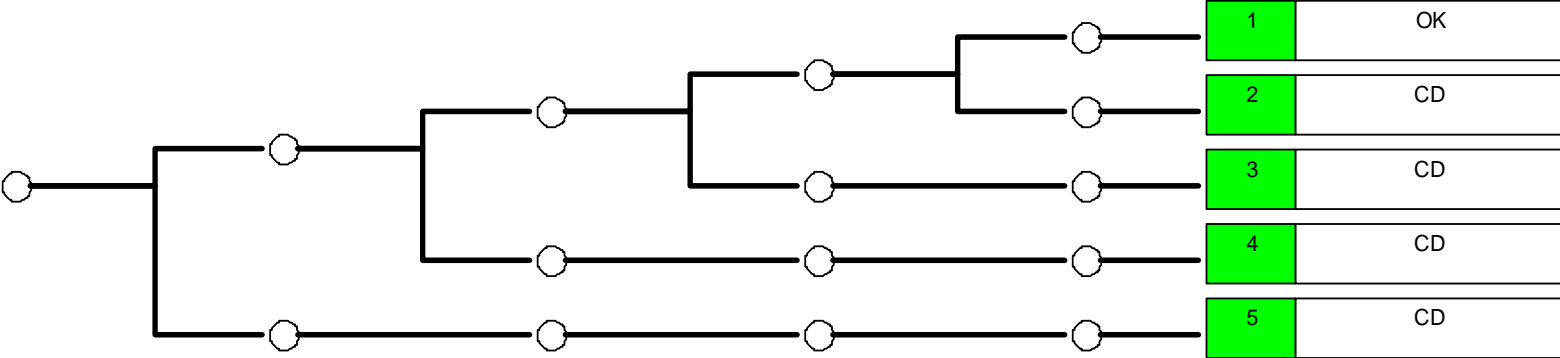


Small LOCA



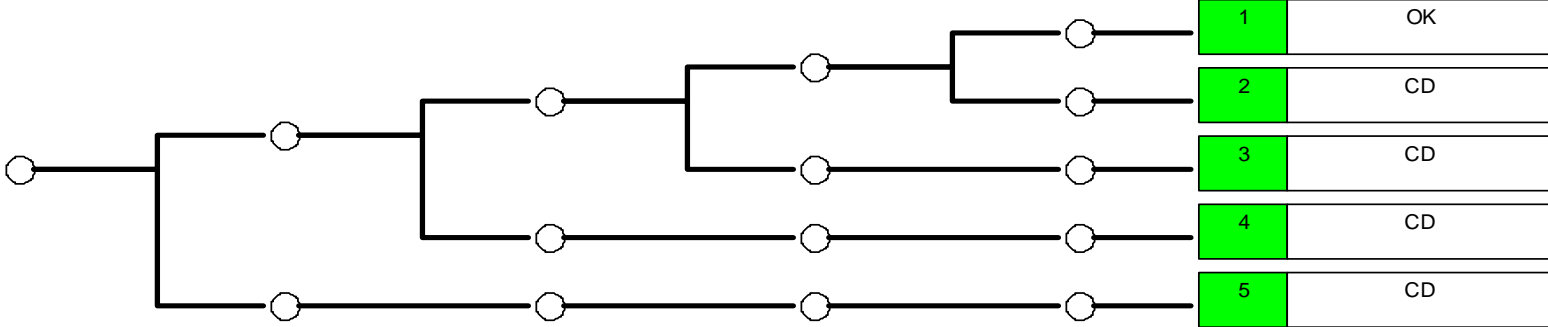
Medium LOCA

MEDIUM LOCA	REACTOR TRIP	HIGH PRESSURE INJECTION	CONTAINMENT COOLING	HIGH PRESSURE RECIRCULATION	#	End State (Phase - CD)
IE-MLOCA	RPS	HPI	CSR	HPR		



Large LOCA

LARGE LOCA IE	SAFETY INJECTION TANKS	LPSI OR HPSI INJECTION FROM SIRWT	CONTAINMENT COOLING	HIGH PRESSURE RECIRCULATION	#	End State (Phase - CD)
IE-LLOCA	SIT	LPI-HPI	CSR	HPR		



Principal Steps in Event Tree Development

- **Determine boundaries of analysis**
- **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 times**
 - How long do specific systems/functions/components need to operate?
- **Dependencies among safety functions or systems**
- **Sequence end states - undesired outcome**
 - Core damage
 - Core vulnerable
 - Containment vulnerable
- **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 the reactor core and containment**
 1. Reactor subcriticality
 2. Core inventory makeup
 3. Core heat removal
 4. Containment pressure suppression
 5. Containment heat removal
 6. Containment integrity

Success Criteria (cont.)

- Identify systems which can perform each of the required fundamental safety functions
- Identify the **minimum** required equipment necessary to perform the 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 should be best-estimate, rather than conservative, since this assumption goes into the PRA
- May credit non-safety-related equipment where feasible

Example of Success Criteria Variability

- **Examples from Combustion Engineering Owners' Group (CEOG)**
- **Looking at the Safety Injection (SI) Tank Allowed Outage Time analyses for Large LOCAs, to have success**
 - **Fort Calhoun: Needs 3 of 3 SI Tanks to unbroken legs**
 - **Millstone 2: Needs 2 of 3 SI Tanks to unbroken legs**
 - **St. Lucie: Needs 3 of 4 SI Tanks to unbroken legs**
 - **Palo Verde 1, 2, 3: Needs 2 of 3 SI Tanks to unbroken legs**

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)**

Plant Damage States

- Also called "Accident Classes" or "Endstates"
- 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

SPAR Model Event Trees

- **In an instructor-led discussion with the class, investigate the following about a SPAR model**
 - **Documentation for of initiating event information**
 - **Initiating event groups?**
 - **Support system initiators?**
 - **Required functions and systems (success criteria)**
 - **Look at an event tree model to find**
 - **Top events (compared with success criteria) and their ordering**
 - **System logical dependencies (pruning)**
 - **Sequence “logic”**
 - **Endstates (OK and core damage)**
 - **Discuss what is happening in selected sequences**

Additional: Event Tree Interpretation Exercise

- **In an instructor-led discussion with the class, investigate the following about the North Anna IPE:**
 - Sources of initiating event information (Table 3.1.1-1 on p. 3-145)
 - Initiating event classes (Table 3.1.1-2 on p. 3-146)
 - Distinction between T2 and T2A (Tables 3.1.1-7, 3.1.1-8, and actual events in Table 3.1.1-10. See pp. 3-151 through 3-158 and 3-160 through 3-165)
 - Support system initiators (Table 3.1.1-12, pp. 3-170 through 3-174)
 - Required functions and systems (success criteria) for T2A (Table 3.1.1-15 on p. 3-178)
 - On T2A event tree (p. 3-343) and using the event tree heading information on pp. 3-188 to 3-193, note the following:
 - Top events (compared with success criteria) and their ordering
 - System logical dependencies (pruning)
 - Endstates (OK and core damage with different "containment states" for Level 2 PRA)
 - Which sequences depict a SAR DBA scenario (only sequence P01)
 - Discuss what is happening in selected sequences



Idaho National Laboratory

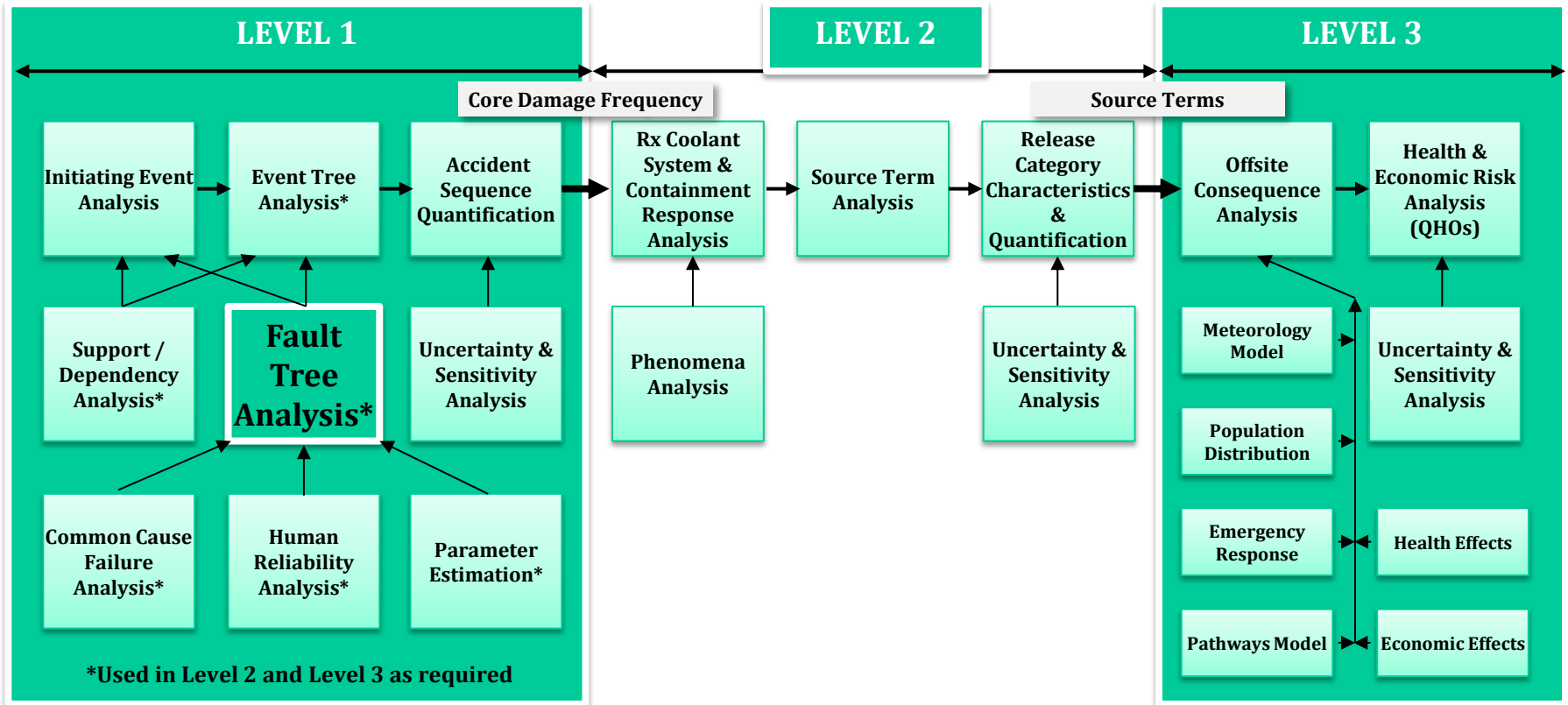
MODULE F

SYSTEMS ANALYSIS USING FAULT TREES

Fault Tree Concepts

- **Purpose:** Students will learn the purposes of fault tree analysis. Students will learn how the appropriate level of detail for a fault tree analysis is established. Students will become familiar with the terminology, notation, and symbols employed in fault tree analysis.
- **Objectives:**
 - List the purposes of fault tree analysis
 - Define the terminology, notation, and symbols used in fault tree analysis
 - Interpret the results of fault tree reduction
 - Define and correctly apply the definition of "minimal cut sets"
- **References:**
 - NUREG/CR-2300, PRA Procedures Guide:
 - NUREG-0492, Fault Tree Handbook

Principal Steps in PRA



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.”*

Fault Tree Handbook, NUREG-0492, 1981

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 cause 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

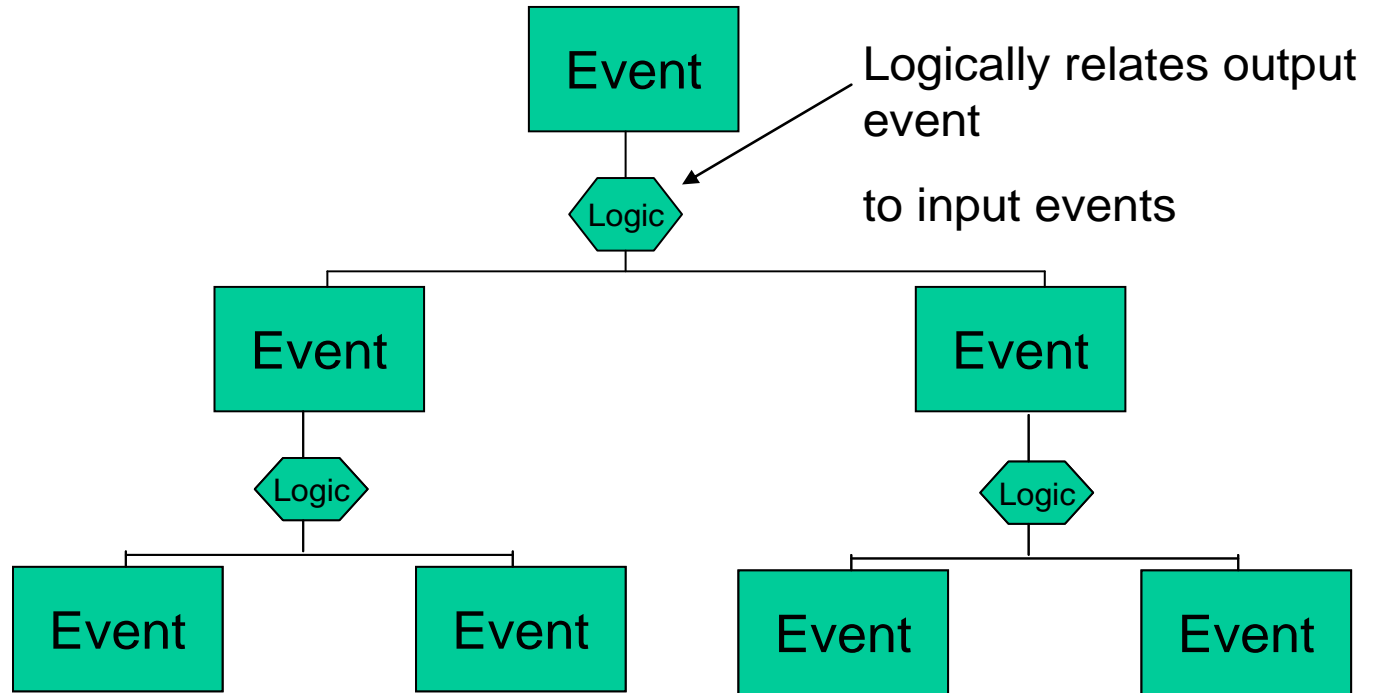
Purpose of Fault Tree Analysis

- **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 to represent 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 represent “low level” failures such as
 - Component failures (pump fails to _____)
 - Human errors (operator fails to _____)
 - Phenomenological event
 - 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



LOGIC
AND or OR

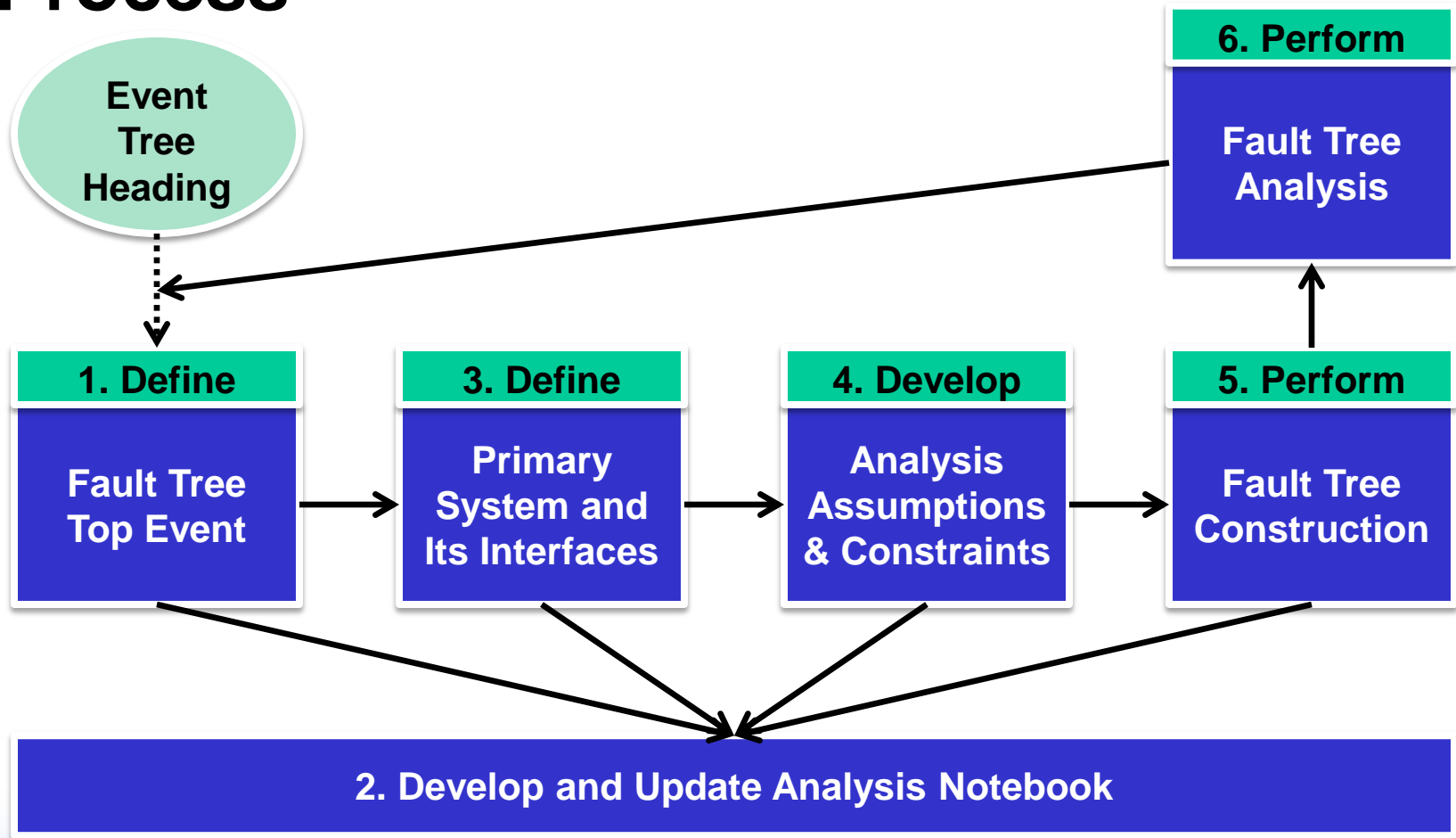
AND Gate occurs if
all its inputs occur

OR Gate occurs if
any one of its inputs occur

Relationship Between Fault Trees and Event Trees

- From Module E, event trees consist of a series of nodes (or branches)
 - Each node represents the success or failure of a particular system, component, or operation
- For systems, fault tree models are used to
 - Model system failure
 - Estimate the system's probability of failure
- Thus, the **top event** of a fault tree corresponds to the **failure branch** of its associated event tree node

Fault Tree Development and Analysis Process



1. Define Top Event

- **Undesired event or state of system**
 - Often corresponds to an 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 and Update System Notebooks

- **Fault tree development is an iterative process, that is related to the other PRA processes**
- **A system notebook should be started at the onset of fault tree development; it should be maintained and updated periodically**
 - **A system notebook should contain the following:**
 - **Scope of analysis**
 - **System definition and boundaries**
 - **System design information**
 - **Drawings or diagrams used for model development**
 - **System operational information**
 - **Applicable Technical Specifications**
 - **Test and maintenance information and data**
 - **Analytical assumptions**
 - **Component failure rate data**
 - **Fault tree results**
 - **System notebooks were typically developed during the IPE process**
 - **System notebooks may not be included in the IPE submittal**

3. Define the System and Interfaces

- **Define system/component boundaries based on**
 - Information required from the analysis
 - Basic event level (i.e., level of resolution of available data)
 - Function of the system being modeled
 - Note: boundaries may not be consistent with those used by plant engineering
- **Identify shared components with other systems**
- **Identify dependencies on other systems**

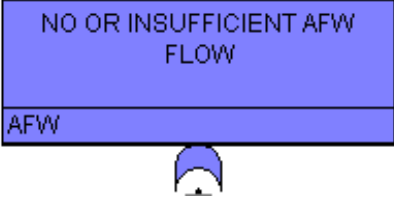
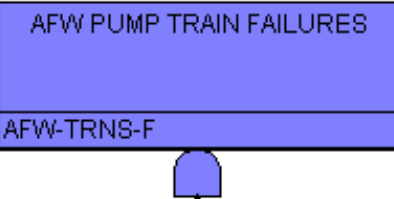
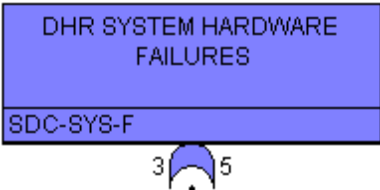
4. Develop Analysis Assumptions and Constraints

- **Analytical assumptions must be made to compensate for incomplete knowledge of**
 - **Plant response**
 - **System response**
 - **System operation**
 - **Failure modes and mechanisms**
 - **Potential recovery actions.**
- **The rationale for assumptions should be specified and documented**
 - **Whenever possible, it should be supported by engineering analysis.**
- **Time and/or budget constraints, as well as the tools available for performing the analysis, can contribute to defining the analysis scope**

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 symbols to represent the logic is used**
- **Postulation should be consistent with the level of resolution in the available data and the analytical assumptions**
- **Fault tree construction is an iterative process requiring constant feedback from the other PRA processes as well as the other steps in the fault tree development process**
- **Can employ different strategies for construction**
 1. **Output-to-input**
 2. **Functional blocks**

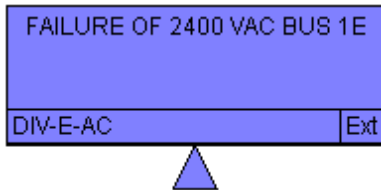
Fault Tree Symbols used during FT Construction

Symbol		Description
 <p>A rectangular symbol with a blue background. The top half contains the text "NO OR INSUFFICIENT AFW FLOW". The bottom half contains the text "AFW". Below the rectangle is a semi-circular gate symbol with a small triangle at its base.</p>	"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.
 <p>A rectangular symbol with a blue background. The top half contains the text "AFW PUMP TRAIN FAILURES". The bottom half contains the text "AFW-TRNS-F". Below the rectangle is a semi-circular gate symbol with a small triangle at its base.</p>	"AND" Gate	Logic gate providing a representation of the Boolean intersection of input events. The output will occur if all of the inputs occur.
 <p>A rectangular symbol with a blue background. The top half contains the text "DHR SYSTEM HARDWARE FAILURES". The bottom half contains the text "SDC-SYS-F". Below the rectangle is a semi-circular gate symbol with a small triangle at its base. The number "3" is on the left and "5" is on the right of the gate symbol.</p>	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.)

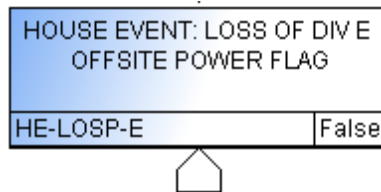
Symbol

Description



Transfer Gate

A transfer symbol to connect various parts of the fault tree



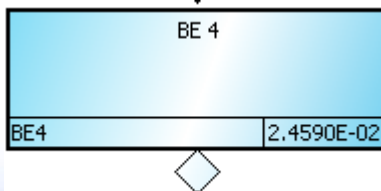
House Event

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.



Basic Event

A basic component fault which requires no further development. Consistent with level of resolution in databases of component faults.

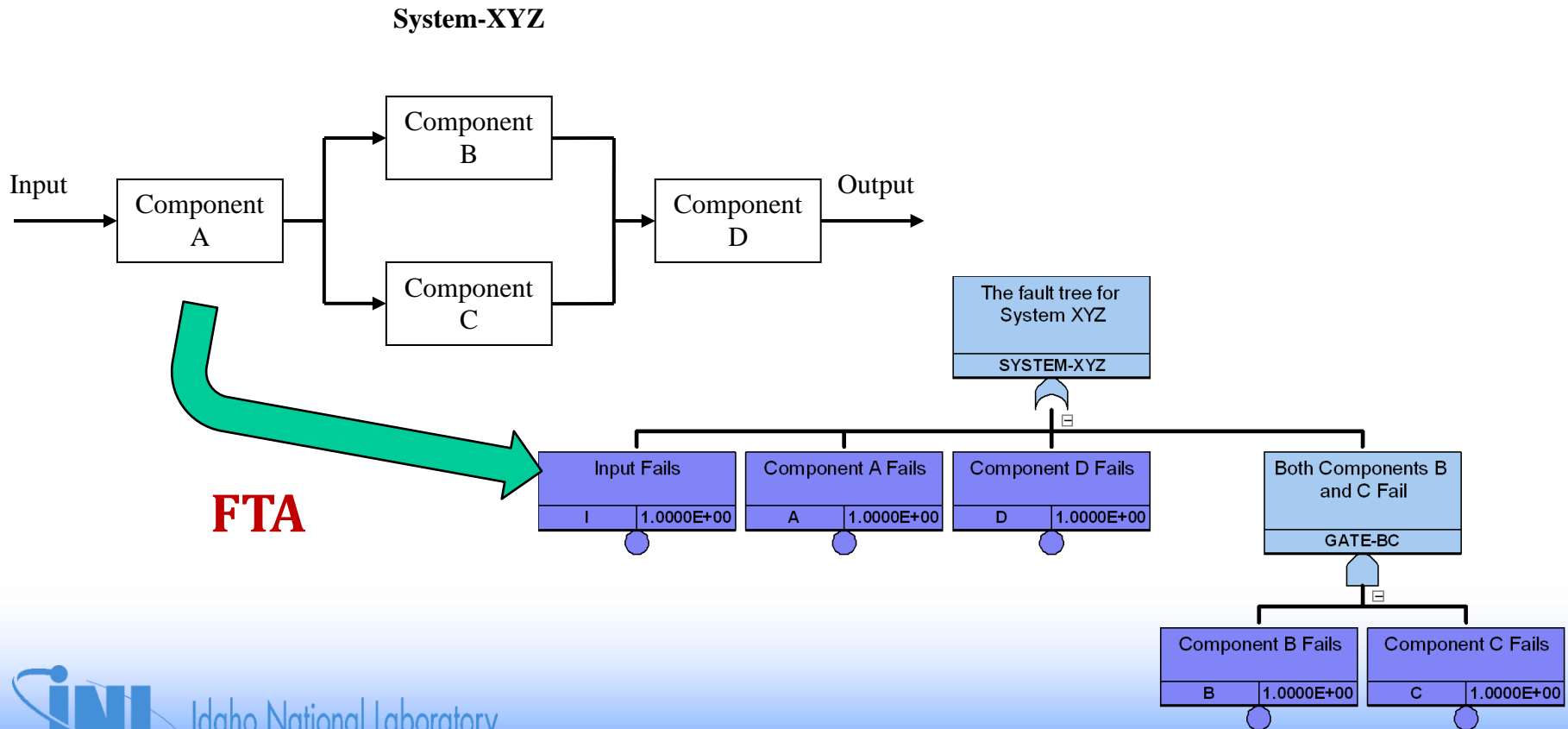


Undeveloped Event

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

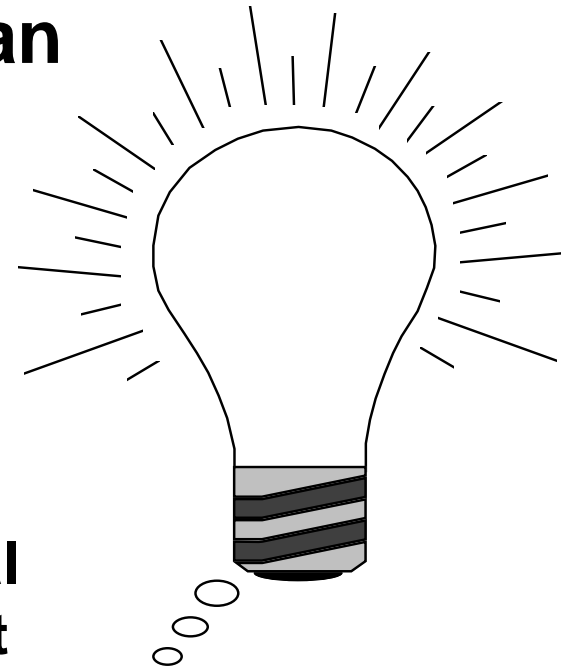


6. Fault Tree Solution

- **Due to the complexity of most fault trees, computers are used to generate results**
 - This solution 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

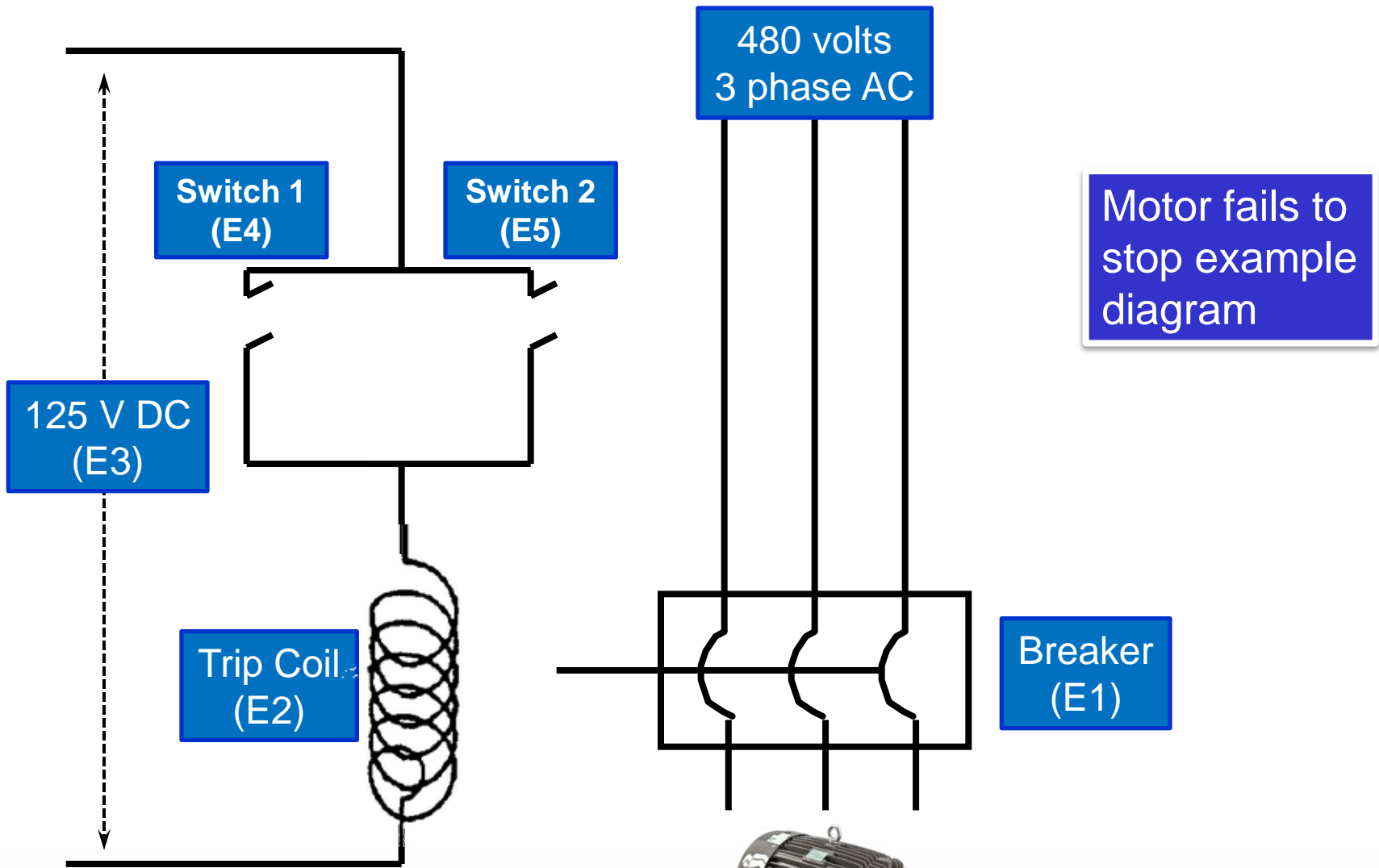
A group of basic failures (component failures and/or human failures) that are ***collectively necessary*** and ***sufficient*** to cause the TOP event to occur.



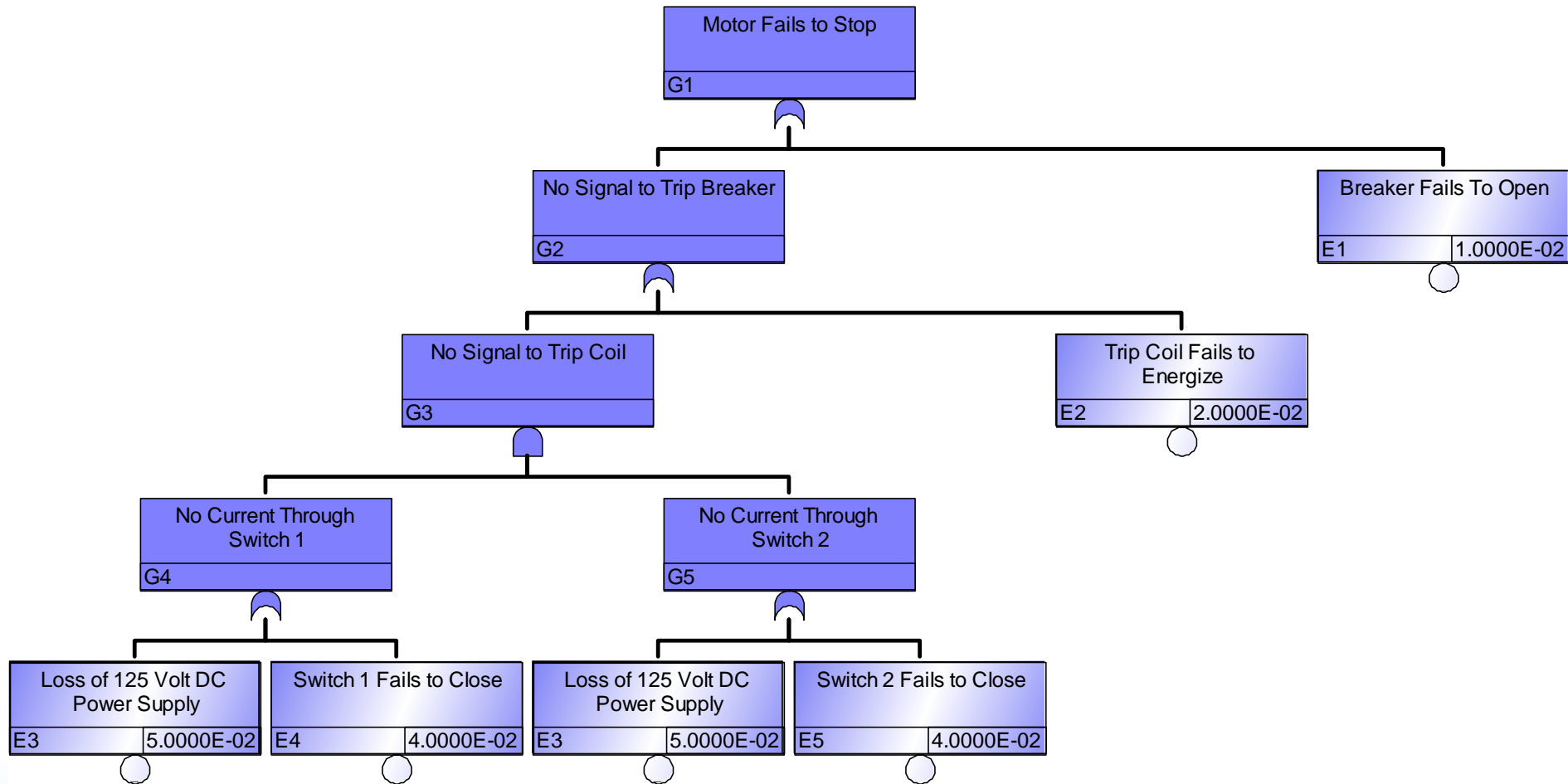
Understanding the concept of minimal cuts sets is one of the most important steps in understanding PRA

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 125 V DC power supply
- **Will solve fault tree and discuss "meaning" of the solution process**



Corresponding Fault Tree



Boolean Fault Tree Reduction

1. Express a fault tree's logic as a Boolean Equation
 2. Apply rules of Boolean Algebra to reduce the 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 Notation	Engineering Notation	Designation
(1a) $X \cap Y = Y \cap X$ (1b) $X \cup Y = Y \cup X$	$X * Y = Y * X$ $X + Y = Y + X$	Commutative Law
(2a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ (2b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X * (Y * Z) = (X * Y) * Z$ $X + (Y + Z) = (X + Y) + Z$	Associative Law
(3a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ (3b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X * (Y + Z) = (X * Y) + (X * Z)$ $X + (Y * Z) = (X + Y) * (X + Z)$	Distributive Law
(4a) $X \cap X = X$ (4b) $X \cup X = X$	$X * X = X$ $X + X = X$	Idempotent Law
(5a) $X \cap (X \cup Y) = X$ (5b) $X \cup (X \cap Y) = X$	$X * (X + Y) = X$ $X + (X * Y) = X$	Law of Absorption

Reduction of Example Fault Tree

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

$$G1 = G2 + E1$$

$$G2 = E2 + G3$$

$$G3 = G4 * G5$$

$$G4 = E3 + E4$$

$$G5 = E3 + E5$$

- Back-substitute

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

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

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

Reduction of Example Fault Tree (cont.)

- 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 "+"

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

$$\text{Pr}(G1) \approx \text{Pr}(E1) + \text{Pr}(E2) + \text{Pr}(E3) + [\text{Pr}(E4) * \text{Pr}(E5)]$$

Fault Tree Results

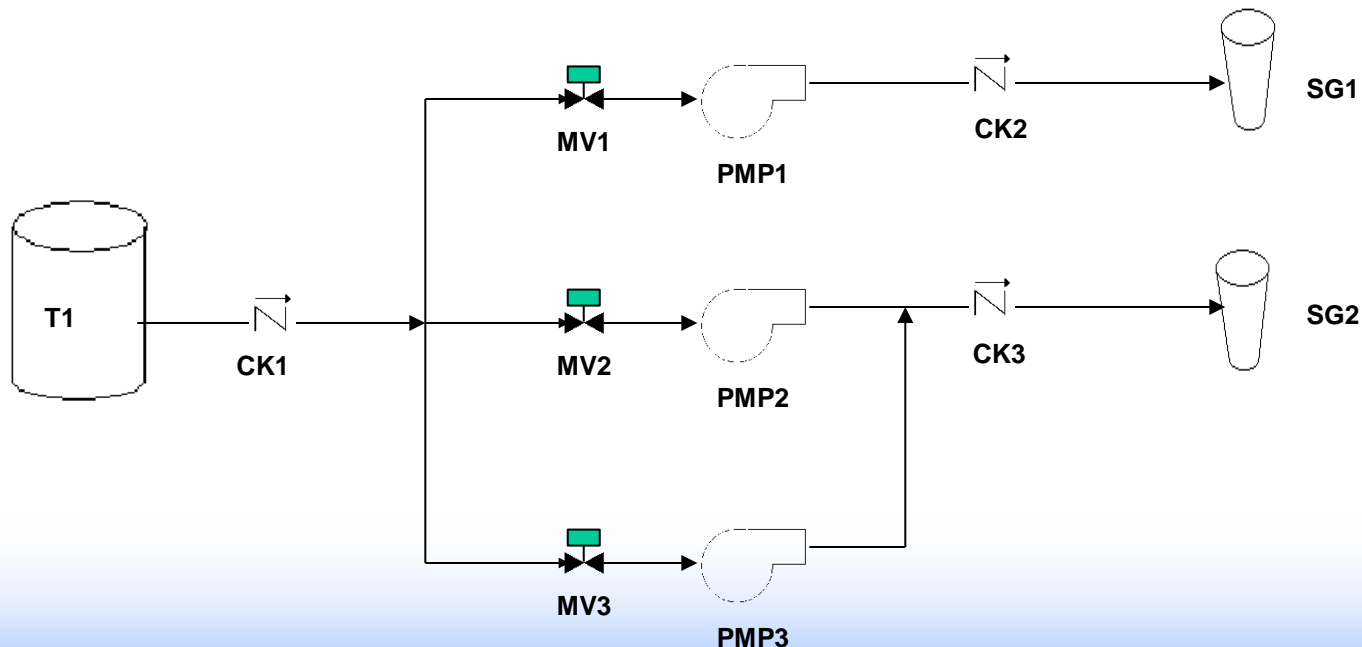
- **Fault tree solution results in a list of minimal cut sets**
- **Each minimal cut set is a combination of basic events**
- **Each minimal cut set has an individual probability of occurrence that is equal to the product of the basic event failure probabilities**
- **The probability that the top event will occur is approximately the sum of the individual cut set probabilities**
 - **When using the rare event approximation**

***** Fault Tree Exercise *****

- **Using the AFW fault tree from North Anna IPE (provided in Volume 2 of course material) or a PWR SPAR model, identify various fault tree elements;**
 - **Top event,**
 - **The various types of logic gates and gate names**
 - **The use of house events (if any)**
 - **Transfers (including transfers to support systems),**
 - **Basic events and basic event names**
 - **Note examples of human error and common cause failure**
- **Review your PRA for fault trees and note the various fault tree elements**

Optional: Fault Tree Workshop

- Create a fault tree for the 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.





Idaho National Laboratory

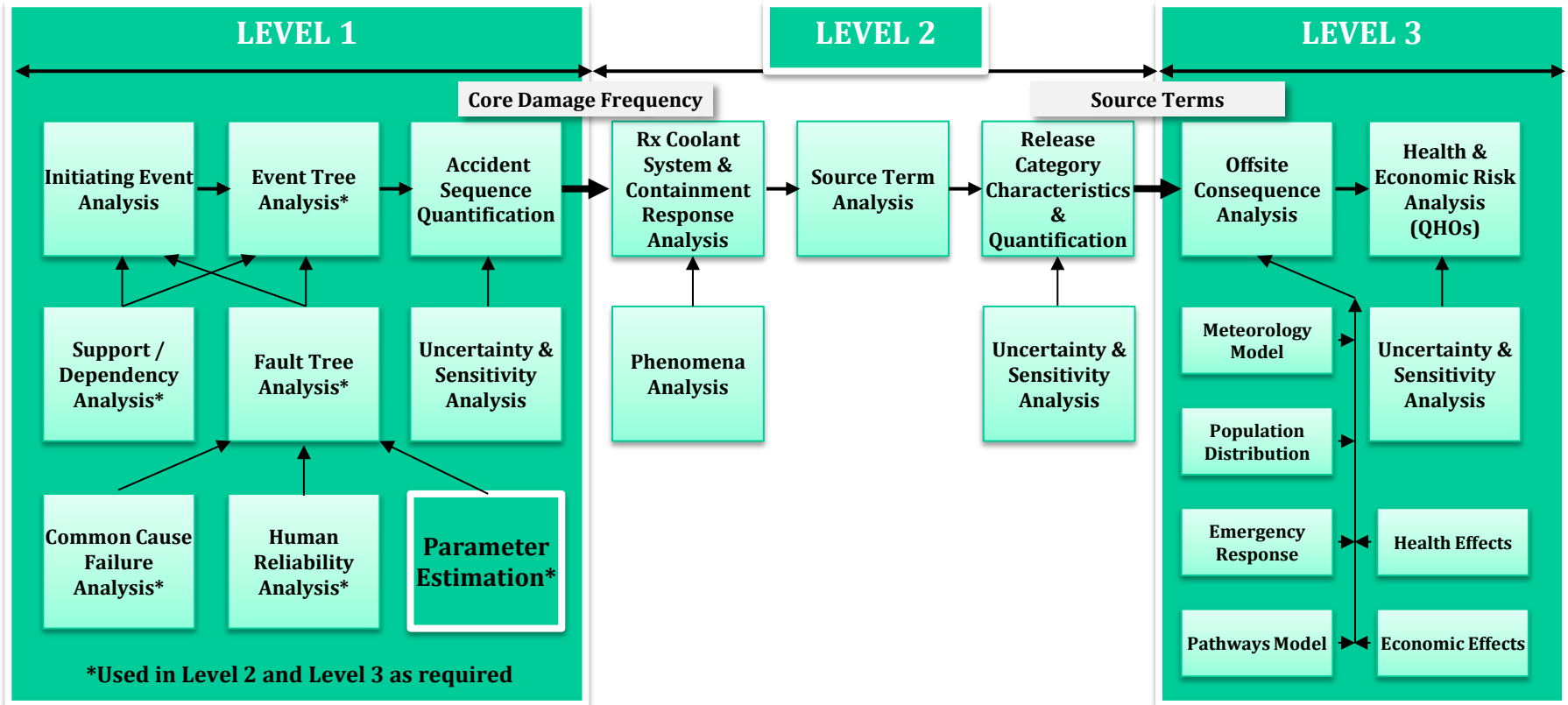
MODULE G

EQUIPMENT FAILURE MODES AND DATA SOURCES FOR PARAMETER ESTIMATION

Equipment Failure Modes and Data Sources for Parameter Estimation

- **Purpose:** Students will be presented with equipment failure modes included in PRA, parameters to be estimated for each failure mode, sources of data for these parameters, both generic and plant-specific, and limitations of plant-specific data. Finally, students will be presented with a qualitative description of Bayesian updating.
- **Objectives:** Students will be able to:
 - Understand failure modes typically modeled in PRA and what information is needed to estimate the parameter for each failure mode
 - Define what is meant by "generic data" and list common sources
 - List limitations associated with plant-specific data
 - Explain qualitatively what Bayesian updating accomplishes
- **References**
 - NUREG/CR-6823, Handbook of Parameter Estimation for PRA

Principal Steps in PRA



Component Failure Type Dictates the Basic Event Probability 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

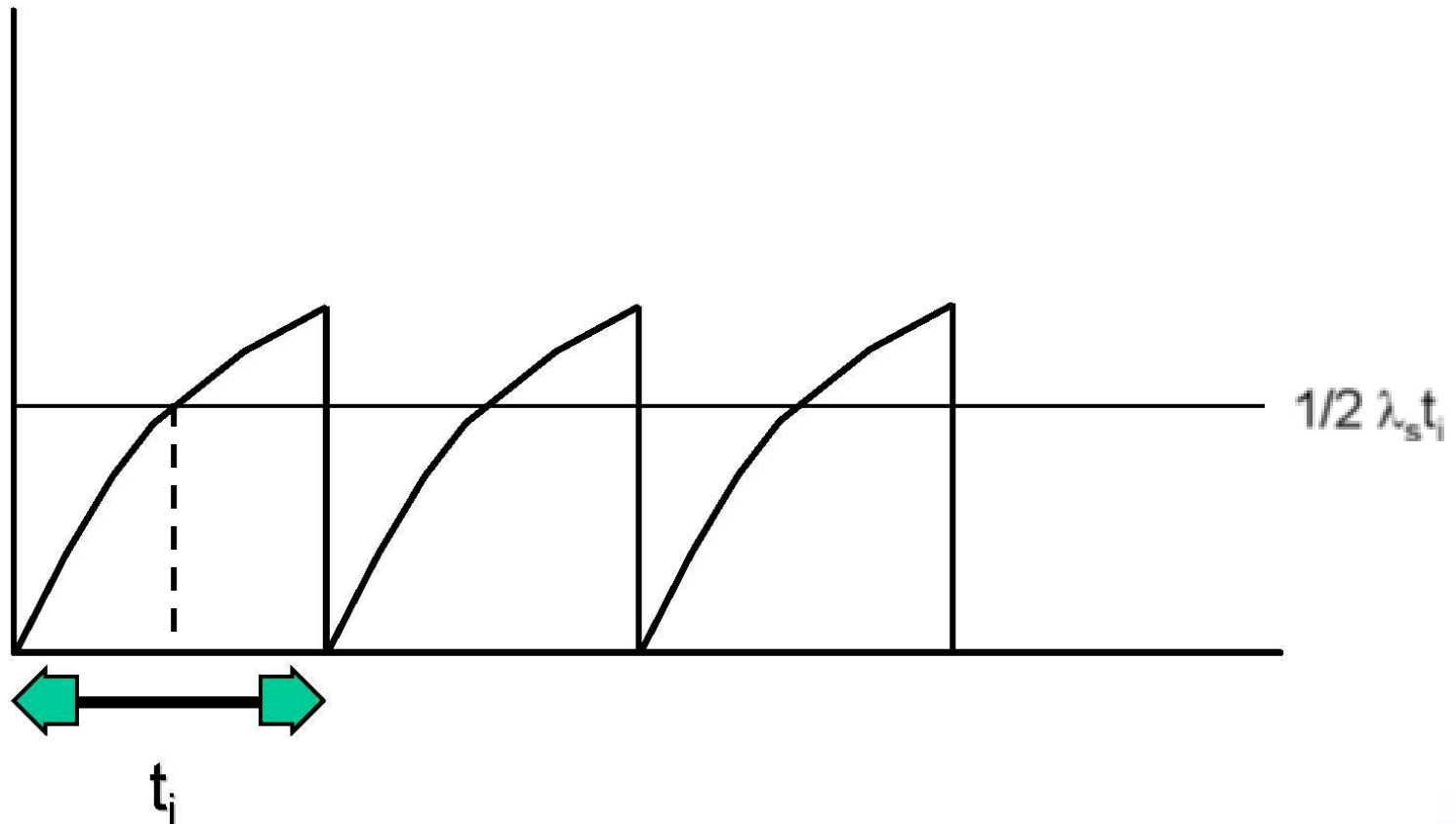
Parameter Estimation

- **Purpose**
 - Estimates parameter values for component failure and initiating events in the PRA model
- **Quantitative inputs to basic events for fault tree and event tree models**
- **Must gather data for**
 - Random failure (failure rates and demand failure probabilities)
 - Unavailability due to test and maintenance
 - Common cause failure (see Module H)
 - Initiating event frequencies (see Module D)

System Models Need Following Types of Component Parameter Estimates

Failure Contribution	Calculational Formula	Type of Measure	Parameter Definition
Hardware Failure on Demand	$Q_d = p$	Demand failure probability	p = Demand failure probability; need number of failures and number of demands
Hardware Failure of Operating Component	$Q_r = 1 - e^{-\lambda_o t_m}$ $\approx \lambda_o t_m$ (for small λt ; when $\lambda t < 0.1$)	Unreliability (mission failure)	λ_o = Operating failure rate; need number of failures and total operating time t_m = Mission time
Test/Maintenance Outage	$Q_m = \lambda_m d_m$ $= t_{oos}/t_{total}$	Unavailability (Average)	λ_m = Frequency of test or maintenance d_m = Test or maintenance outage time t_{oos} = Total out of service time t_{total} = Total time
Hardware Failure while in Standby Component	$Q_s \approx \lambda_s t_i/2$	Standby failure probability Unavailability (Average)	λ_s = Standby failure rate; need number of failures and total time in standby t_i = Test interval

On Average, Standby Equipment can be Unavailable for $\frac{1}{2}$ the Test Interval



*** Parameter Estimation Exercise ***

- **Over several years, a standby component has the following operating history**
 - 60 test/maintenance outages (test interval is 720 hours and each outage has a demand) and 4 unplanned demands
 - Failures: 1 demand failure, 1 failure in standby (failure uncovered during testing), and 1 failure to run
 - Total run time is 200 hours
 - Average test/maintenance outage time is 1.8 hours
- **From this history, estimate:**
 - Demand failure probability
 - Standby failure rate and standby unavailability
 - Operating failure rate and unreliability for a mission time of 12 hours
 - Test/maintenance unavailability

Data Collection and Analysis to Support Parameter Estimation

- **Identify systems and components for which data should be collected**
- **Define component boundaries and failure modes**
- **If plant-specific data is not available or time does not permit collection and analysis, identify generic data sources**

Data Sources

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

NRC Operating Experience (OE)

- **Parameter Estimates**
 - **Industry Average Parameter Estimates**
 - **Common-Cause Failure Parameter Estimates**
 - **Loss of Offsite Power**
 - **Industry Performance of Relief Valves**
- **Trends and Insights**
 - **Initiating Events**
 - **System Studies**
 - **Component Performance**
 - **Common-Cause Failure Insights**
 - **International Common-Cause Failures**
 - **Fire Events**

Generic Data Issues

- **Key issue is whether data is applicable for the specific plant being analyzed**
 - **Data of mid-1980s or earlier vintage**
 - **Some IE frequencies known to have decreased over the last decade**
 - **Frequencies updated in NUREG/CR-5750 and -6890**
 - **Criteria for judging data applicability not well defined**
 - **Do not forget important engineering considerations that could affect data applicability**

Plant-Specific Data Collection and Analysis

- **Objective: Gather data to obtain raw information needed for estimating event parameters**
 - **Determine period of time for obtaining plant data**
 - **Most recent data should be used to represent current maintenance practices and component performance**
 - **Maintenance Rule and Performance Indicators will enhance collection of this information for some components**
 - **Five to ten years of data is desirable for most components**
 - **Collect plant data information from plant records and documents**
 - **Licensee Event Reports (LERs)**
 - **Can also be a source of generic data**
 - **Maintenance reports and work orders**
 - **System Engineer files**
 - **Control room logs**
 - **Interpret the information to obtain variables of interest (e.g., failures, demands, operating hours)**
 - **Estimate parameter values from these data**

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 typically very limited**
 - Small statistical sample size
- **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 bases**

Bayes' Theorem is Basis for Bayesian Updating of Data

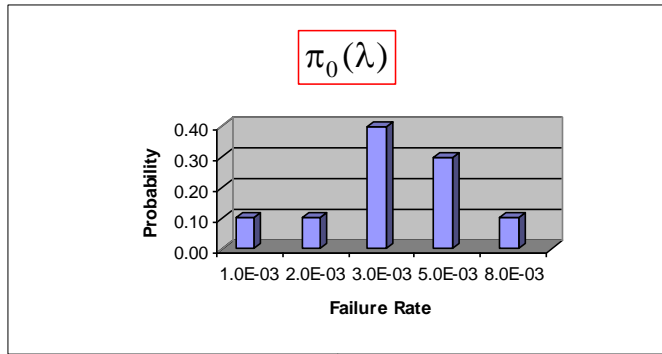
- Typical use: sparse plant-specific data combined with generic data using Bayes' Theorem:

This goes into the PRA basic event

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

- Where:
 - θ is parameter of interest
 - $\pi_0(\theta)$ 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



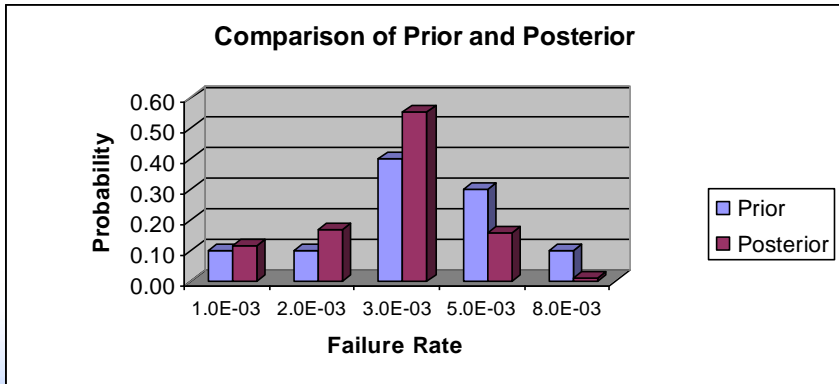
$$L(E|\lambda) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

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

Our prior knowledge about the failure rate

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

Our model and observed data (evidence E)

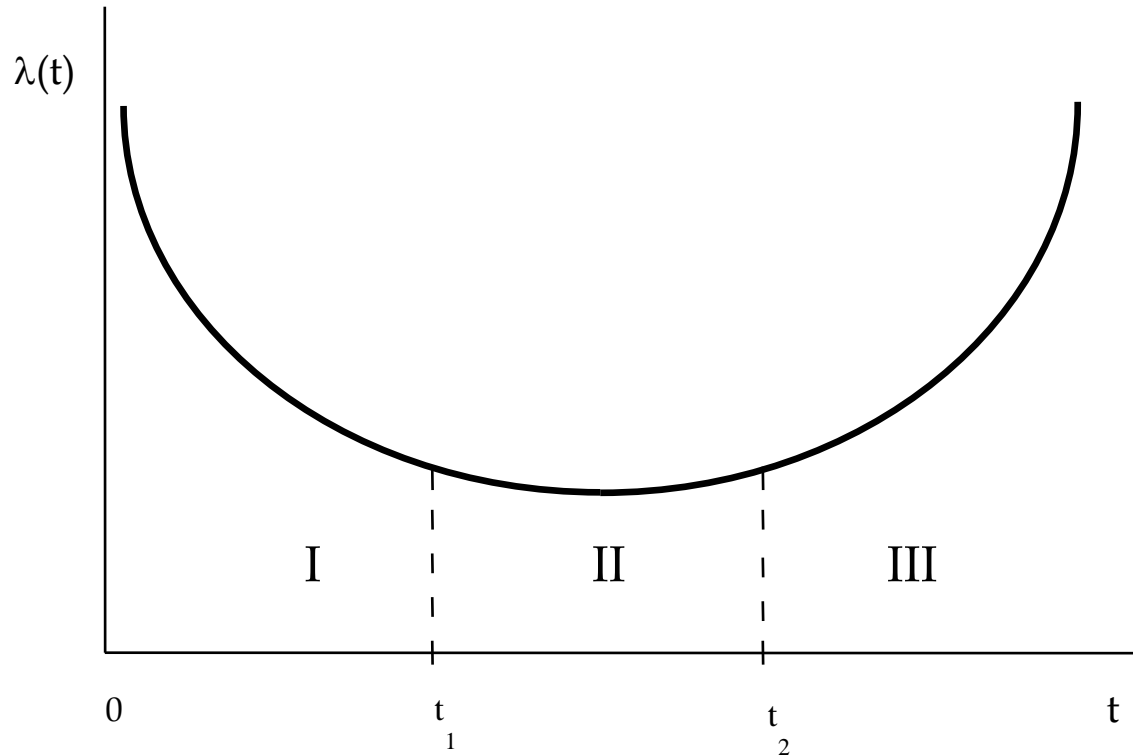


Use Bayes' Theorem to combine our prior knowledge and our evidence

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 λ or p to decrease over time
 - Aging can cause λ 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**

Exercise PRA Component Failure Data

- **Based on experience, determine a consensus ranking of the following component failure modes (highest to lowest)**
 - ___ **Diesel generator fails to start on demand**
 - ___ **Check valve fails to open on demand**
 - ___ **Motor-operated valve fails to open on demand**
 - ___ **Motor-driven pump fails to start on demand**
 - ___ **Turbine-driven pump fails to start on demand**
- **Based on probability values found in a SPAR model, how did your qualitative ranking agree with the a quantitative ranking?**



Idaho National Laboratory

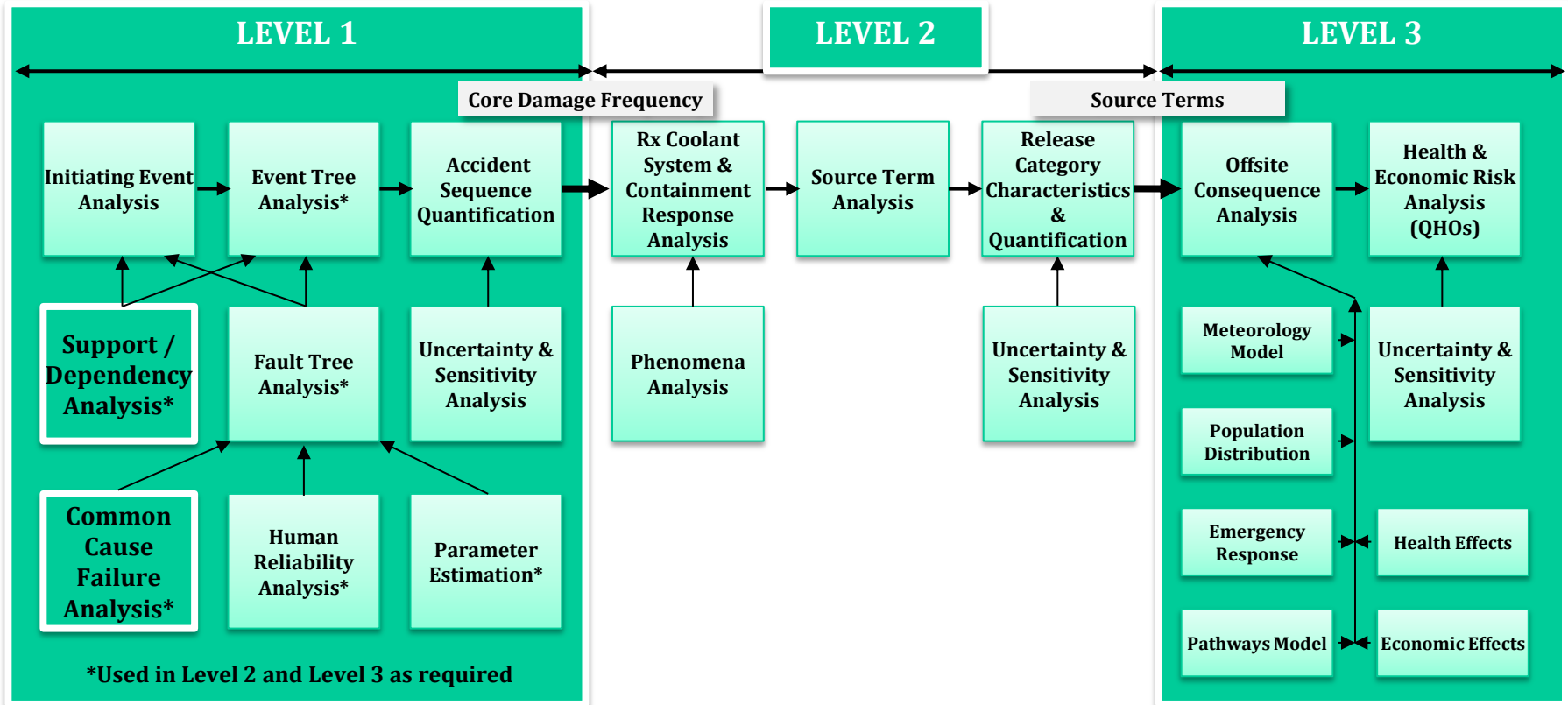
MODULE H

COMMON CAUSE FAILURES

Common Cause Failures

- **Purpose:** Students will be introduced to the concept of how common cause failures and other dependencies are treated in the PRA
- **Objectives:** Students will be able to:
 - Define several types of dependent failures and how they are modeled
 - Give examples of dependent and common cause failures
 - Describe the importance of modeling common cause failure in PRA
- **References:**
 - NUREG/CR-4780, Procedures for Treating CCF in Safety & Reliability Studies
 - EPRI NP-3967, Classification and Analysis of Reactor Operating Experience Involving Dependent Events
 - 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

Principal Steps in PRA



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
 - Represents complex dependencies not explicitly modeled
 - Quantified with parametric CCF models

Common Cause Failures

- Failure of 2 or more components, subsystem, or system due to shared causes which have not been accounted for explicitly
- Common cause failures are important since they:
 - Defeat **redundancy** and/or diversity
 - Data suggest high probability of occurrence relative to the combination of **independent** failures of components, subsystems or systems

Common Cause Failure Mechanisms

- **Environment**
 - Radioactivity
 - Temperature
 - Corrosion
- **Design deficiency**
- **Manufacturing defect**
- **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 the 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**
 - **Pumps**
 - **Batteries**

CCF Modeling in PRA

Model	Parameters	General Form for Multiple Component Failure
Beta Factor	<p>Q_t, β where:</p> <ul style="list-style-type: none"> Q_t is the total probability of each component failing due to all independent and common cause events. 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)	<p>$Q_t, \beta, \gamma, \dots$ where:</p> <ul style="list-style-type: none"> Q_t is the total probability of each component failing due to all independent and common cause events. 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. 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. 	$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \prod_{i=1}^k \rho_i (1 - \rho_{k-1}) Q_t$ <p>$\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \dots, \rho_{m+1} = 0$</p>
Alpha Factor	<p>$Q_t, \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_m$ where:</p> <ul style="list-style-type: none"> Q_t is the total probability of each component failing due to all independent and common cause events. α_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.. 	<p>Non-staggered testing (all components tested simultaneously):</p> $Q_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \quad k = 1, \dots, m$ <p>Staggered testing (components tested sequentially):</p> $Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t \quad k = 1, \dots, m$ <p>where:</p> $\alpha_t = \sum_{k=1}^m k \alpha_k$ $\binom{m-1}{k-1} = \frac{(m-1)!}{(m-k)! (k-1)!}$

Beta Factor Example

- **Basic events for example (HPI-MDP-FS-A, HPI-MDP-FS-B)**
 - Data → 47 MDP failures to start in approximately 15,667 demands
(47 failures)/(15,667 demands) $\approx 3.0\text{E-}3$
- **Common Cause Failure (Beta Factor)**
 - 10 common cause failures out of the 47 failures

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

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

- **HPI-MDP-CCF-CCFAB $\approx (2.1\text{E-}1 * 3.0\text{E-}3) = 6.3\text{E-}4$**
- **Total fails to start for the redundant system**

$$\begin{aligned} \text{Pr(system)} &= \text{HPI-MDP-FS-A} * \text{HPI-MDP-FS-B} + \text{HPI-MDP-CF-CCFAB} \\ &= (3.0\text{E-}3) * (3.0\text{E-}3) + 6.3\text{E-}4 \approx 6.39\text{E-}4 \end{aligned}$$

Current Limitations of CCF Modeling

- **Limited data; hence generic data often used**
 - Applicability issue for specific plant
- **Screening values may be used**
 - Potential to skew the results
- **Not typically modeled across systems since data is collected/analyzed for individual systems**
- **Not typically modeled for diverse components**
 - e.g., Motor- Driven Pump/Turbine Driven Pump
- **Causes not explicitly modeled**
 - Each failure mechanism not explicitly modeled
 - CCF treatment is statistical

*** CCF Exercise ***

- Using a PWR SPAR model → AFW fault tree pages and schematic
- Identify CCFs modeled by identifying basic events with the following labels in the basic event names
 - AFW-xxx-**CF**-yyyy
- Postulate why (i.e., causes) such CCFs might exist
- Compare the CCF basic event failure probability with its corresponding component independent failure probability

** Optional: Common Cause Exercise **

- **AFW system from Module F:**

- Based on the fault tree and minimal cut sets from Module F

- Which components and what corresponding hardware failure modes would you expect to be modeled in the PRA as Common Cause Failure (CCF) events?
- If the CCF Beta-factor for the identified components is 0.05 and the probabilities for the components are

$$T1 = 1.0E-6$$

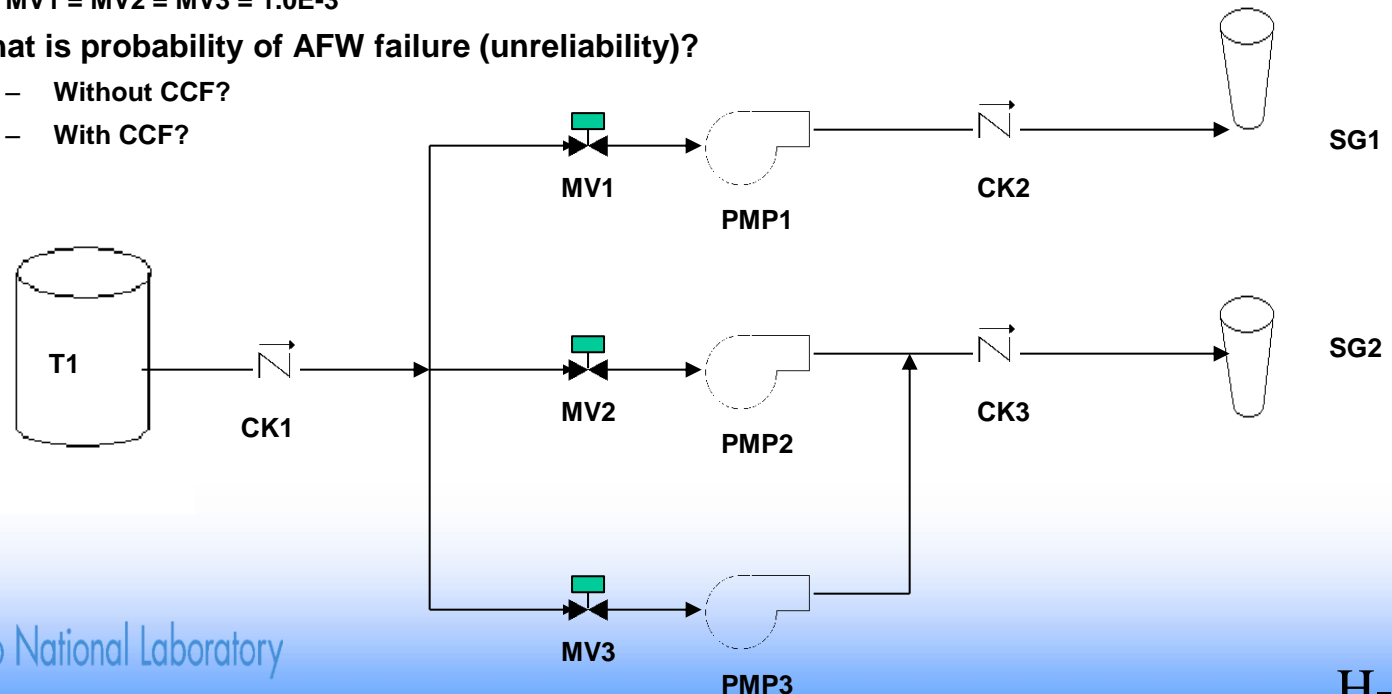
$$CK1 = CK2 = CK3 = 5.0E-5$$

$$PMP1 = PMP2 = PMP3 = 2.0E-3$$

$$MV1 = MV2 = MV3 = 1.0E-3$$

- What is probability of AFW failure (unreliability)?

- Without CCF?
- With CCF?





Idaho National Laboratory

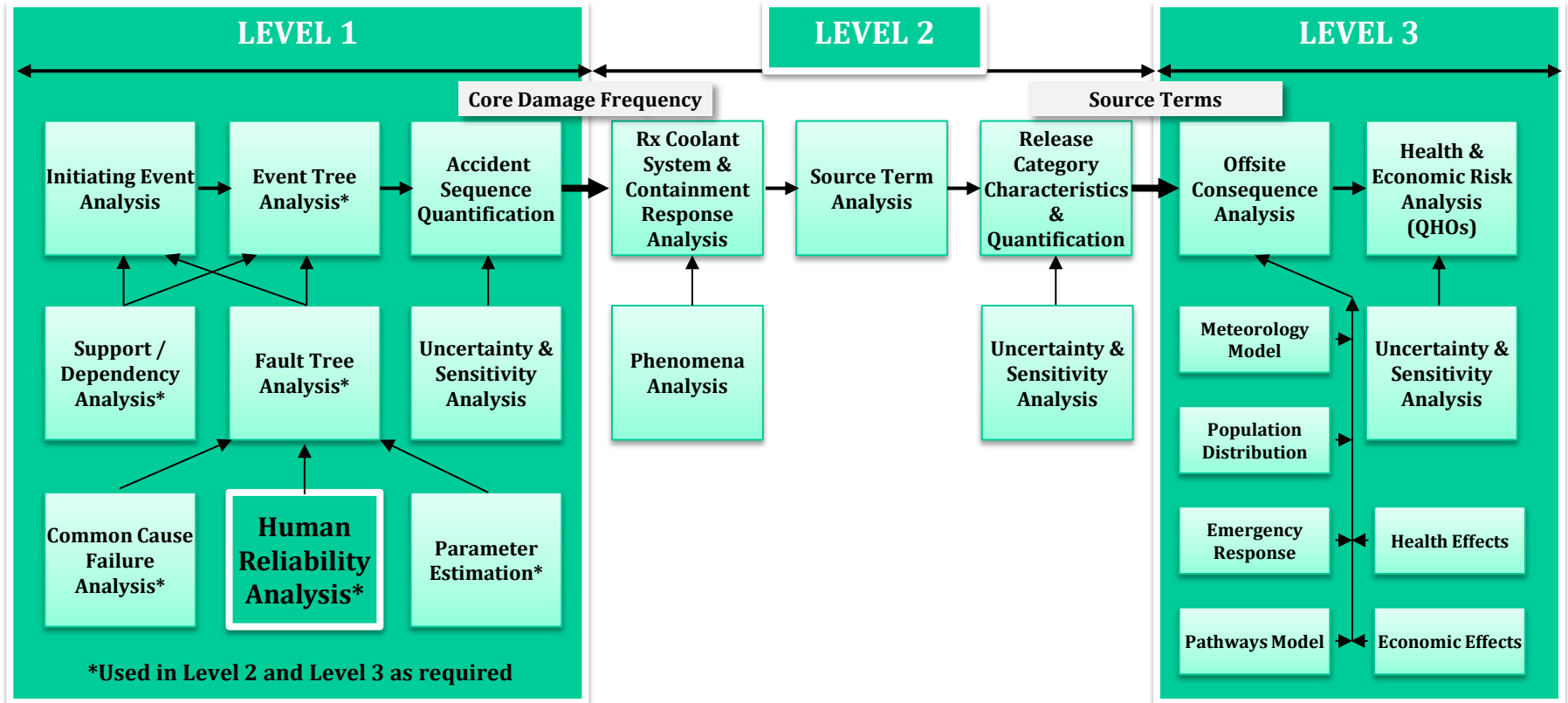
MODULE I

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-6775, Human Performance Characterization in the Reactor Oversight Process, 2002
 - 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

Principal Steps in PRA



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)

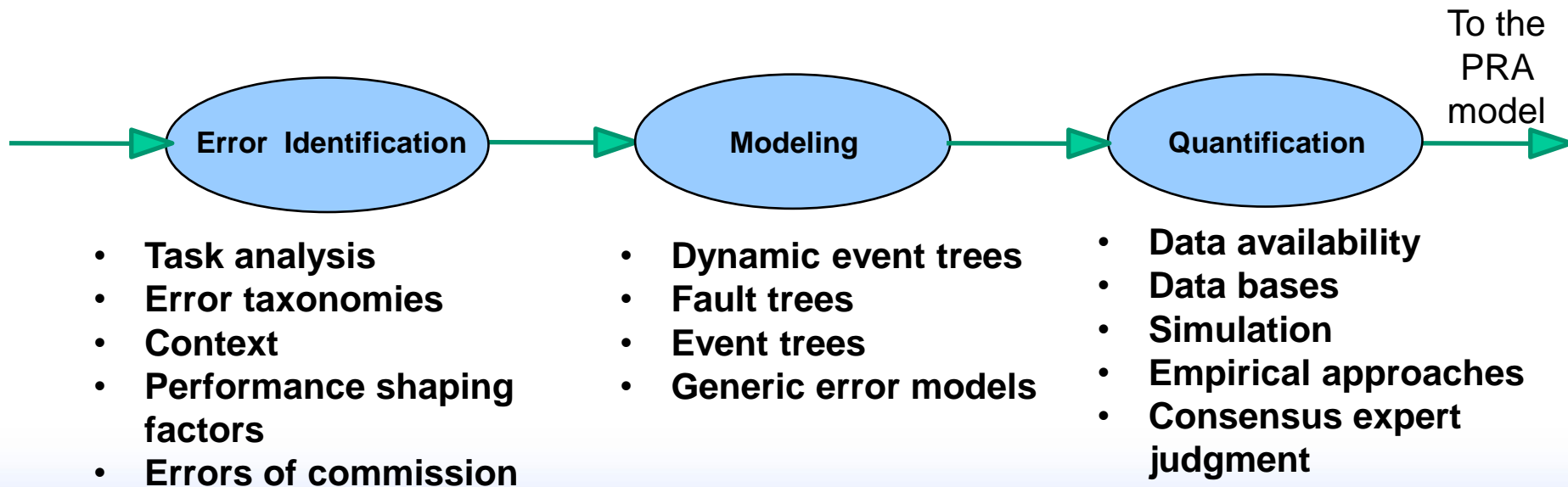
- **Starts with the basic premise that the humans are, in effect, part of the system**
 - Thus, nuclear power plants and systems which comprise them are “human-machine systems”
- **Identifies and quantifies the ways in which human actions contribute to the**
 - Initiation
 - Propagation
 - Termination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

“Human Reliability” is the probability that a person will

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

Three Basic Phases of HRA

- **HRA is a formal process to:**
 - **Identify sources of human errors and error likely scenarios**
 - **Model those human errors into an overall risk model**
 - **Quantify Human Error Probabilities (HEPs)**



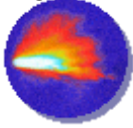
HRA Methods Timeline

CD's First Released



1983

Return of Halley's Comet



1986

Hubble Telescope Launched



1990

Existence of Black Holes Proven



1994

Olympic Games Atlanta



1996

First Balloon Trip Around the World



1999

Today



2013

THERP (1983)
Pre-IE
Post-IE
Recovery
Dependency

ASEP (1987)
Simplified
THERP

ASP/SPAR (1994)

ATHEANA (1996)

ATHEANA (Rev.1 2000)

SPAR-H (2005)

CREAM (1998)

NARA (2004)

HEART (1986)

SHARP (1984)
HRA Framework

SHARP1 (1991)
Revised
Framework

CAHR (1999)

HCR (1984)
First HCR

ORE (1989)
Operator
Reliability
Experiments

MERMOS (1998)

EPRI (2000)
HRA Users Group

SLIM-MAUD (1984)

CBDTM (1992)
Cause-Based
Decision
Trees



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**
 - **Failure to operate components which can be operated from the control room or components that must be manually operated locally**
 - **Failure to operate components which 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)**
 - **Failure to take recovery actions (consideration of actions that may be taken to recover from a fault depending upon actions required and amount of time available)**

Typical Human Error Probabilities Span a Significant Range of Values

Failure Probability	Comment	Typical Characteristics
0.1 or greater (success = 90% or less)	Some post-initiator events may lie in this range	<ul style="list-style-type: none"> Very short time available Complex task Multiple actions outside control room High degree of burden Little or confusing plant status information Little training High stress
0.001 - 0.1 (success = 90% - 99.9%)	Where most human error lies with the exception of most pre-initiator events and some human post-initiators	<div style="text-align: center;">  As these vary, so does the human error probability  </div>
Less than 0.001 (success = 99.9% or more)	Where most pre-initiator events lie and some "automatic" post-initiator events	<ul style="list-style-type: none"> Lots of time Straight forward task steps No burden Lots of training or routinely performed Performed "automatically" Low or no stress

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 initiate feed-and-bleed**
 - **Errors of commission**
 - **Action performed incorrectly or wrong action performed, e.g., opening the wrong valve, turning off safety injection**
- **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 errors of commission**

HRA Used to Identify Errors

- **Identify Human Errors 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 (cont.)

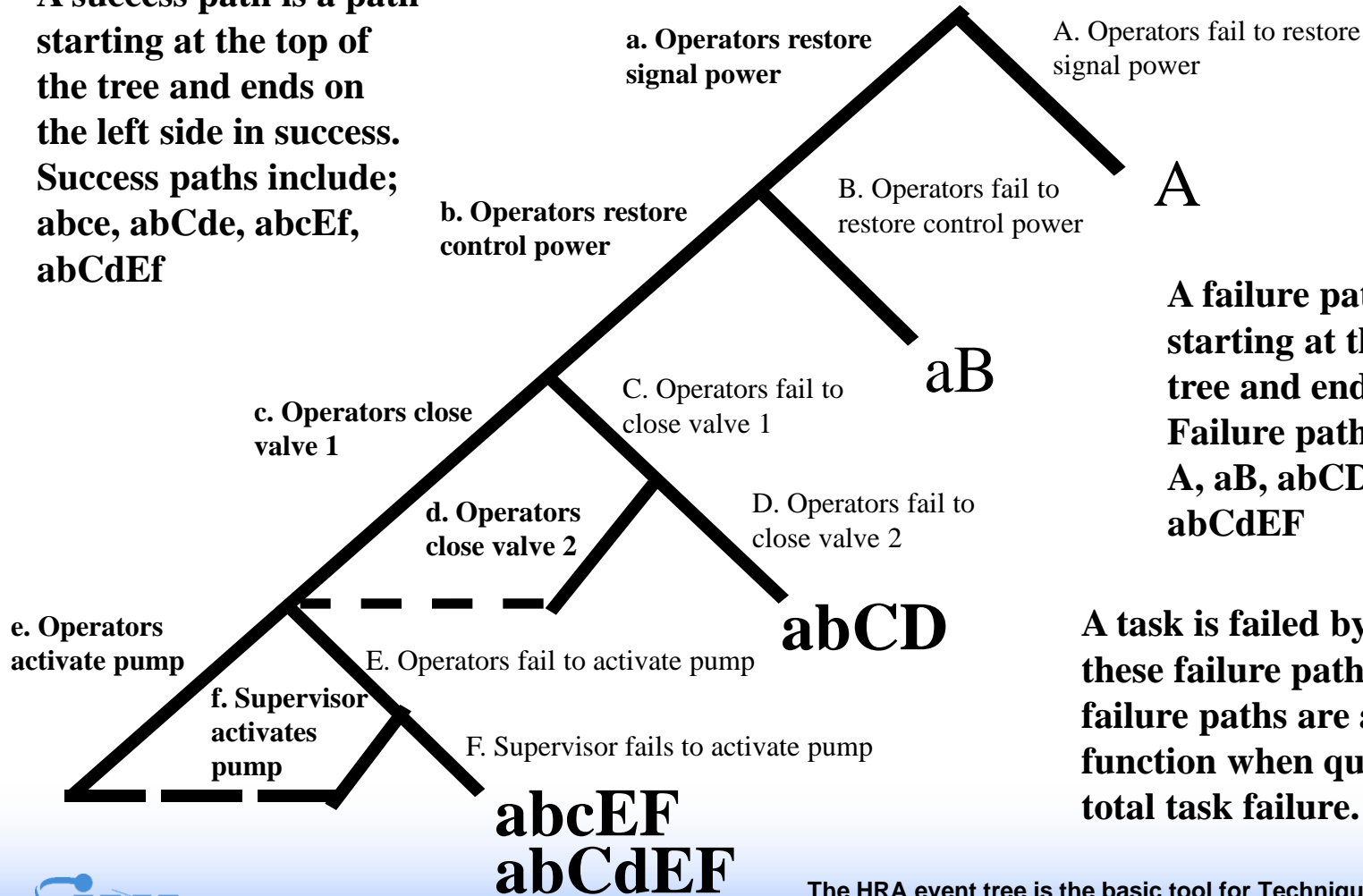
- **Perform screening analysis**
 - **Uses deliberately conservative estimates of human error probability**
 - **Solve model and evaluate human failure events that become dominant**
 - **Screening methods include ASEP**
 - **Leaves smaller set of human failure events for more detailed analysis**

HRA Process (cont.)

- **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**

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

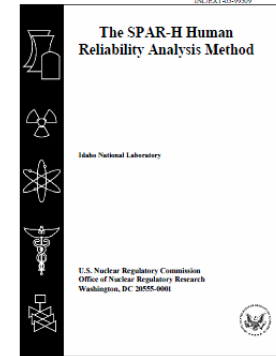
A task is failed by any of these failure paths. The failure paths are an OR function when quantifying total task failure.

Performance Shaping Factors (PSFs)

- Are people-, task-, or environment-centered influences that alter base 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))

- 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

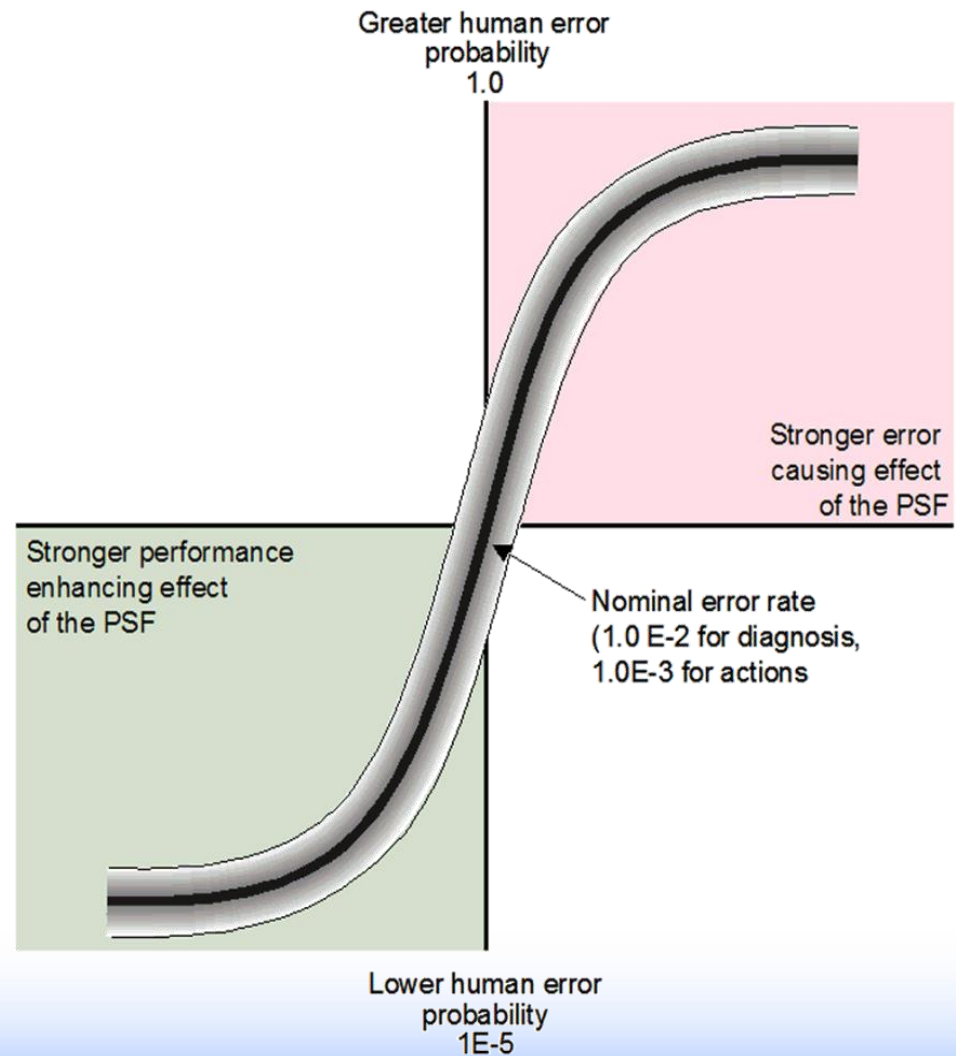
- SPAR-H Worksheets are used to quantify HEPs by considering factors that may increase/decrease likelihood of error
 - Available time
 - Complexity
 - Procedures
 - Fitness for duty
 - Stress/stressors
 - Experience/training
 - Ergonomics/HMI
 - Work processes
- In SPAR-H, these influences are specifically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

Example: Available Time

- *inadequate time* → $p(\text{failure}) = 1.0$
- *barely adequate time* → $p(\text{failure}) = \text{HEP} \times 10$
- *nominal time* → $p(\text{failure}) = \text{HEP} \times 1$
- *extra time* → $p(\text{failure}) = \text{HEP} \times 0.1$
- *expansive time* → $p(\text{failure}) = \text{HEP} \times 0.01$

PSFs Shown Graphically

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



SPAR-H Worksheet Process

- What an example SPAR-H worksheet looks like
- In general, filling out the worksheet follows

Step 1 – Task error ID and question diagnosis

Step 2 – If diagnosis is applicable, complete Table 1

Step 3 – If action is applicable, complete Table 2

Step 4 – Estimate HEP via Table 3

Step 5 – Adjust HEP for dependencies

- The SPAR-H calculation is built into the SAPHIRE software

SPAR Model Human Error Worksheet (Page 2 of 3)

Table 2. Action worksheet.

PSFs	PSF Levels	Multiplier for Action	If non-nominal PSF levels are selected, please note specific reasons in this column
1. Available Time	Inadequate	1.0 ^a	It is assumed that the operators have just enough time to recover the SWS.
	Time available = time required	10✓	
	Nominal	1	
	Available > 50x time required	0.01	
2. Stress	Extreme	5	It is assumed that the stress level is greater than nominal.
	High	2✓	
	Nominal	1	
3. Complexity	Highly	5✓	It is assumed that the complexity is greater than nominal.
	Moderately	2	
	Nominal	1	
4. Experience/ Training	Low	3	
	Nominal	1✓	
	High	0.5	
5. Procedures	Not available	50	
	Available, but poor	5	
	Nominal	1✓	
6. Ergonomics	Missing/Misleading	50	
	Poor	10	
	Nominal	1✓	
	Good	0.5	
7. Fitness for Duty	Unfit	1.0 ^a	
	Degraded Fitness	5	
	Nominal	1✓	
8. Work Processes	Poor	2	
	Nominal	1✓	
	Good	0.8	

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**

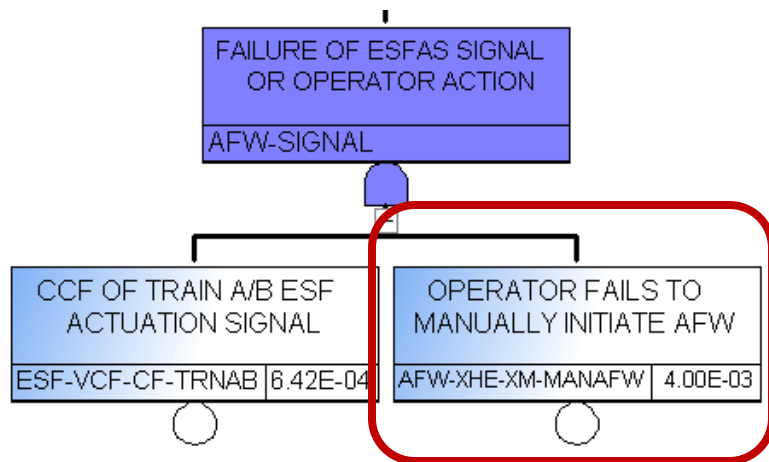
Item	Value
ModelType	RAIDOM
Uses Template	Not Assigned
Description	
Calculated Probability	1.10E-02
Process Flag	Failure=> System Logic Success=> Delete Term
Failure Model	SPAR-H human reliability model (X)
Uncertainty Distribution	Constrained Noninformative
Diagnosis	Yes
Available Time	
Stress/Stressors	
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	

How Human Actions Are Incorporated Into PRA Model

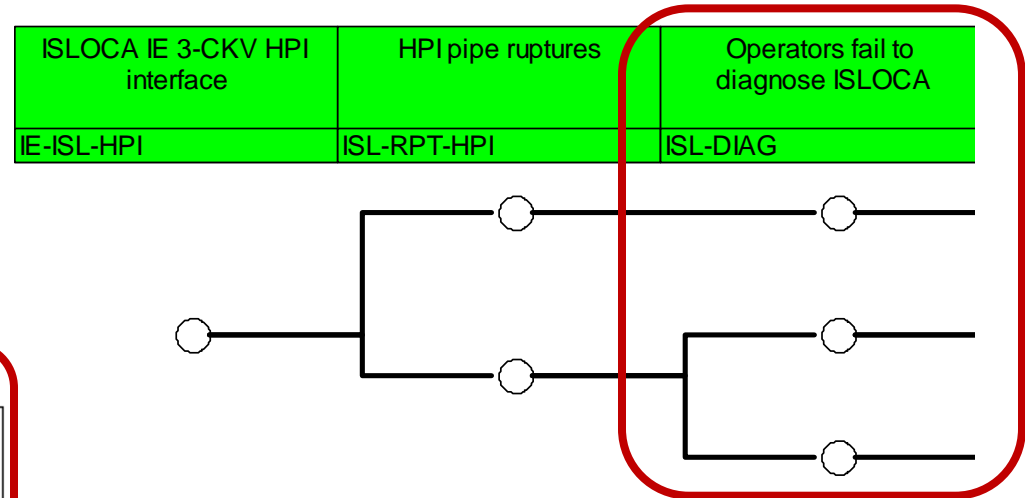
- **Most human errors appear as fault tree basic events**
- **Some errors modeled in event trees**
 - **BWR failure to depressurize**
- **Recovery actions included in the model cut sets**
 - **Actual Failure = Failure + Not Recovered**

Incorporating HEPs Into a PRA Model

Basic events on fault trees



Top events on event trees



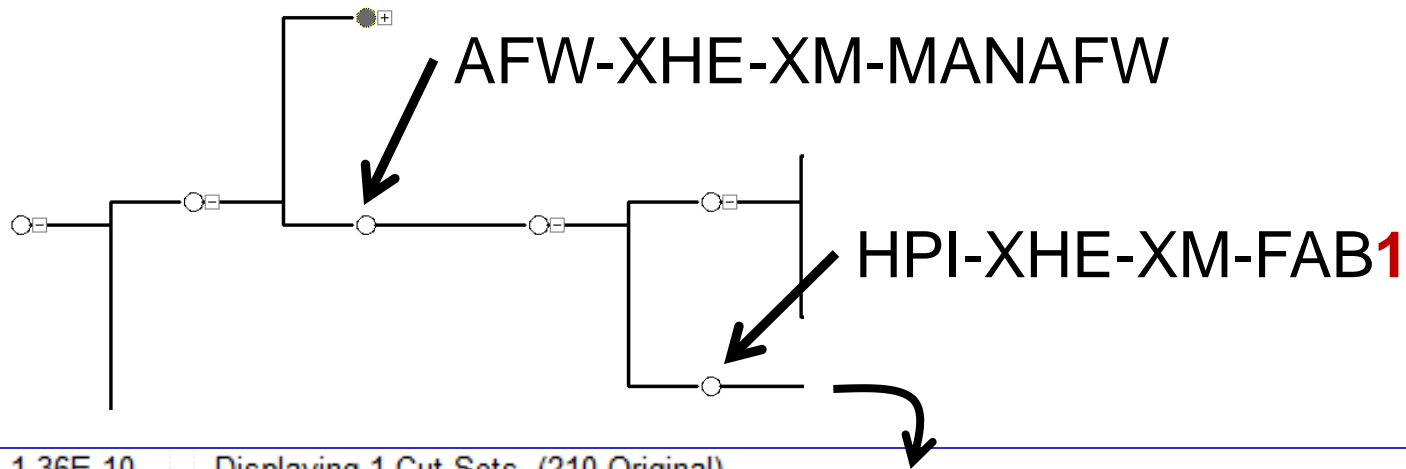
Recovery actions added by applying post-processing rules to minimal cut set

```

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

Consider dependencies between multiple HEPs

SMALL LOCA	REACTOR TRIP	AUXILIARY FEEDWATER	HIGH PRESSURE INJECTION	FEED AND BLEED
IE-SLOCA	RPS FTF-LOOP-RECOVERD	AFW FTF-LOOP-RECOVERD	HPI FTF-LOOP-RECOVERD	FAB FTF-LOOP-RECOVERD



1.36E-10	Displaying 1 Cut Sets. (210 Original)	
1.36E-10	SLOCA : 18	
6.00E-4	IE-SLOCA	SMALL LOCA
4.00E-3	AFW-XHE-XM-MANAFW	OPERATOR FAILS TO MANUALLY INITIATE AFW
6.42E-4	ESF-VCF-CF-TRNAB	CCF OF TRAIN A/B ESF ACTUATION SIGNAL
8.80E-2	HPI-XHE-XM-FAB1	OPERATOR FAILS TO INITIATE FEED AND BLEED COOLING (DE...

Sources of HRA Data

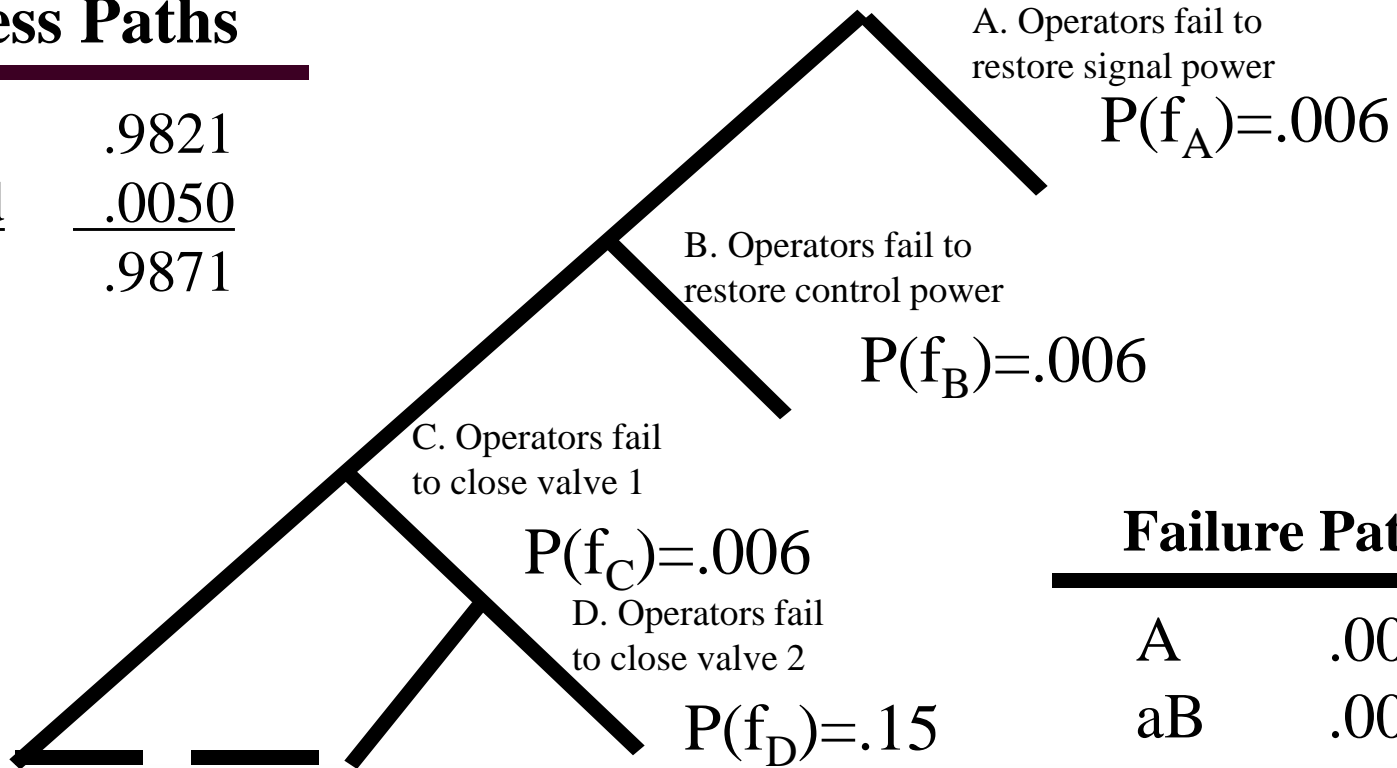
- Nuclear and allied industries
- Military
- Nuclear plant simulators
- Expert elicitation

HRA Event Tree Quantification

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

Success Paths

abc	.9821
<u>abCd</u>	<u>.0050</u>
Total	.9871



Failure Paths

A	.006
aB	.00596
<u>abCD</u>	<u>.00089</u>
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 probabilities and make human contribution to risk a principal source of uncertainty**

***** Exercise 1 *****

- **Find examples of human error modeling in the PWR SPAR model AFW fault tree used in the previous module (find "HEP" type events denoted as "XHE")**
- **Are the human error events identified, pre- or post-initiator errors?**
 - **Hint, look for failure modes of**
 - **"XR" → operator fails to restore from test or maintenance**
 - **"XL" → human error to recover**
 - **"XE" → human error failure**
 - **"XO" → operator fails to operate**
 - **"XM" → operator fails to manually actuate**

Student Exercise 2

Look in your own SPAR model or IPE...

- **If the plant is a PWR, find the value(s) of "Operator Failure to Initiate Feed & Bleed" (for when there is loss of all secondary cooling)**
 - Is this a pre- or post-initiator error?
- **If the plant is a BWR, find the value(s) of "Operator Failure to Depressurize" (for when all high pressure injection has failed)**
 - Is this a pre- or post-initiator error?
- **In class, led by the instructor, discuss**
 - Range of values discovered for these events among the SPAR or IPEs?
 - What factors (besides analyst judgment) may be legitimate reasons for the differences in the values used?



Idaho National Laboratory

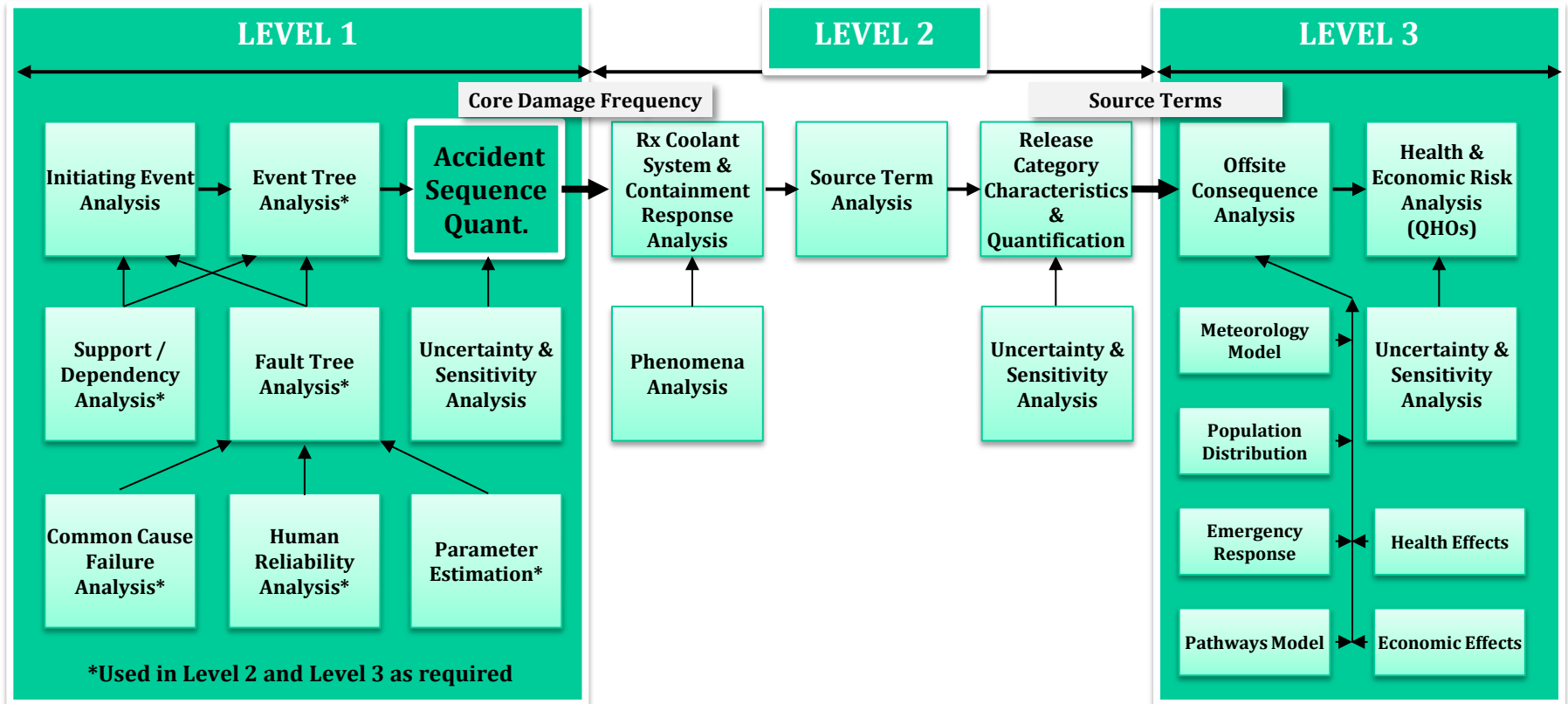
MODULE J

ACCIDENT SEQUENCE QUANTIFICATION

Accident Sequence Quantification

- **Purpose:** Introduce the students to the purpose and methods of accident sequence quantification. Students will become familiar with how the accident sequences are quantified and understand the meaning of the results.
- **Objectives:**
 - Explain how the various aspects of accident sequence quantification are accomplished, including approximations that are used.
 - Describe the major processes for accident sequence quantification
 - Describe the relationship between minimal cutsets and accident sequences, for a Fault Tree Linking approach and Event Tree with Boundary Conditions approach
 - Given minimal cutsets of varying order (number of basic events), list the defense-in-depth features associated with each which are presumed to fail to get to core damage
- **References:** NUREG/CR-2300

Principal Steps in PRA



Purpose of Accident Sequence Quantification

- **Purpose of accident sequence quantification is to provide qualitative and quantitative insights into the initiating events and associated combinations of equipment failures and/or operational errors that are the dominant contributors to core damage frequency**

Generalized Quantification Procedure

- **The following are the basic steps required to quantify accident sequences**
 1. **Identify sequences to be quantified**
 2. **Screen sequences to eliminate insignificant contributors or extremely unlikely sequences**
 3. **Solve plant logic models, with parameter values included, to obtain sequence minimal cut sets**
 - **In general, models are too large to solve completely; truncation is used to obtain approximate solution**
 - **Remaining analyses (uncertainty, sensitivity, importance) are carried out using this approximate solution**

Accident Sequence Quantification

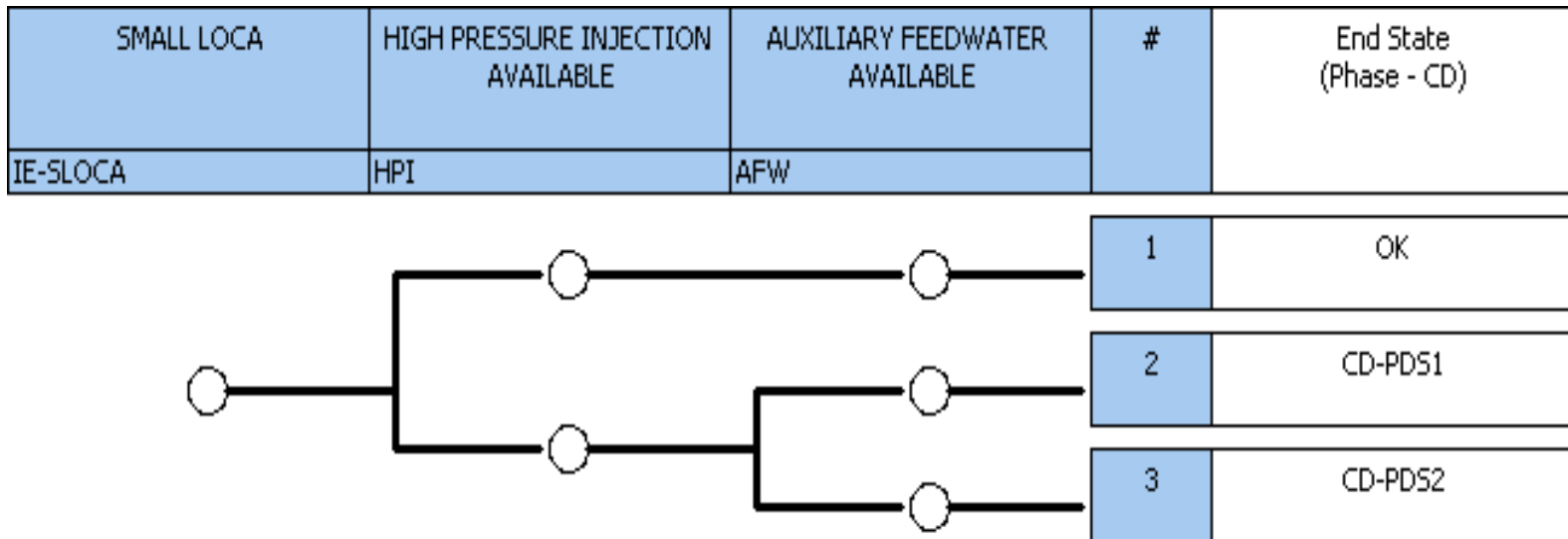
- **There are two basic approaches (for static logic models)**
 - 1. Fault Tree Linking → Fault trees are linked to their corresponding event tree top events**
 - Support system dependencies included in fault tree models
 - Tends to make fault trees complex, but simplifies event trees
 - All SPAR models (and most industry PRAs) use this
 - 2. Event Trees with Boundary Conditions → Support system dependencies explicitly included in event tree models**
 - Tends to make fault trees much simpler but complicates event trees
 - Also called the “Large Event Tree” approach
 - Briefly discussed in this class

Fault Tree Linking

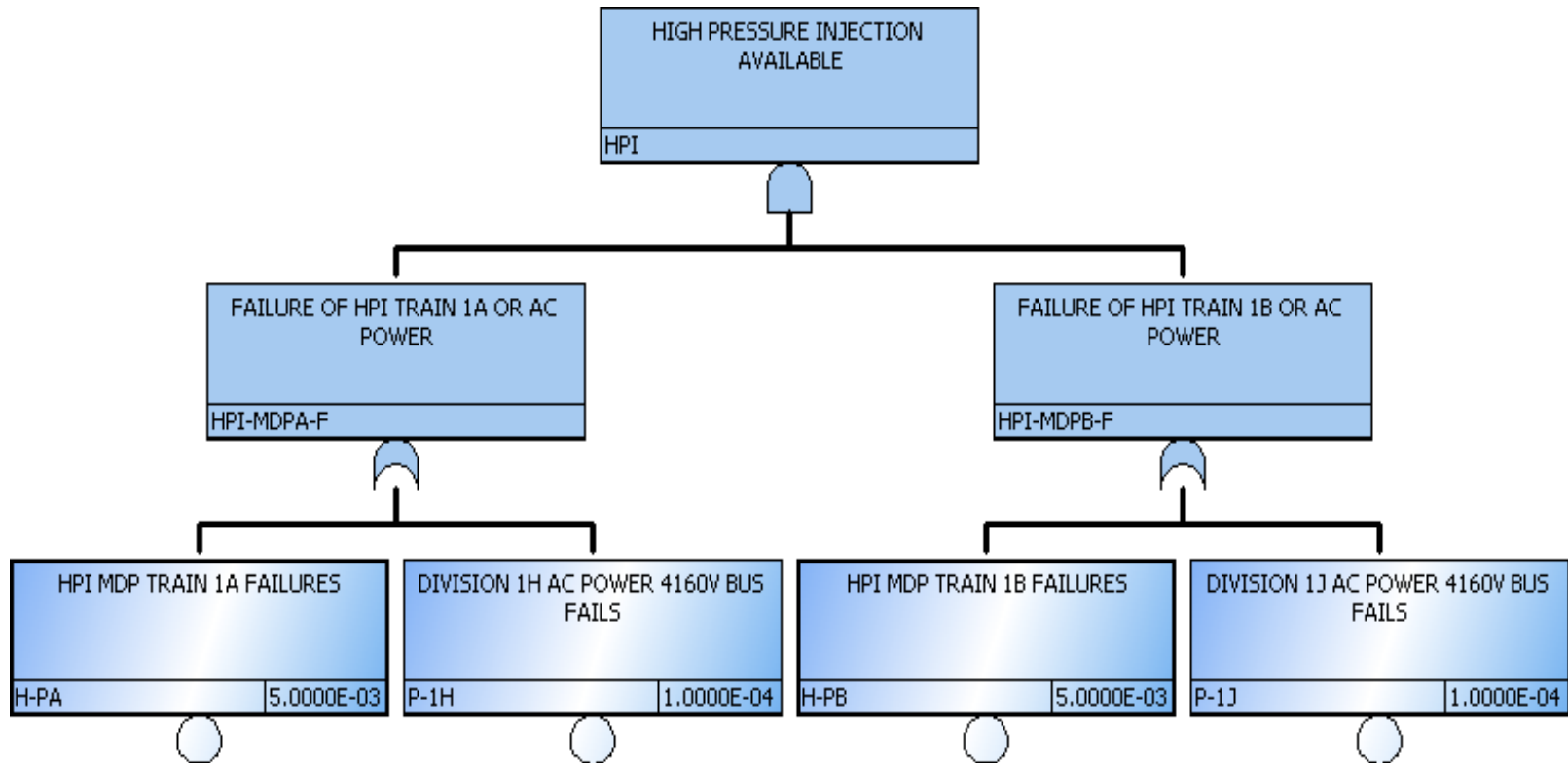
- **Fault tree linking involves development of accident-sequence fault trees, which includes inputs from**
 - An initiating event
 - Fault trees for failed systems in sequence logic
- **Process accounts for system successes in the sequence being solved.**

Simplified Example of Quantification Process

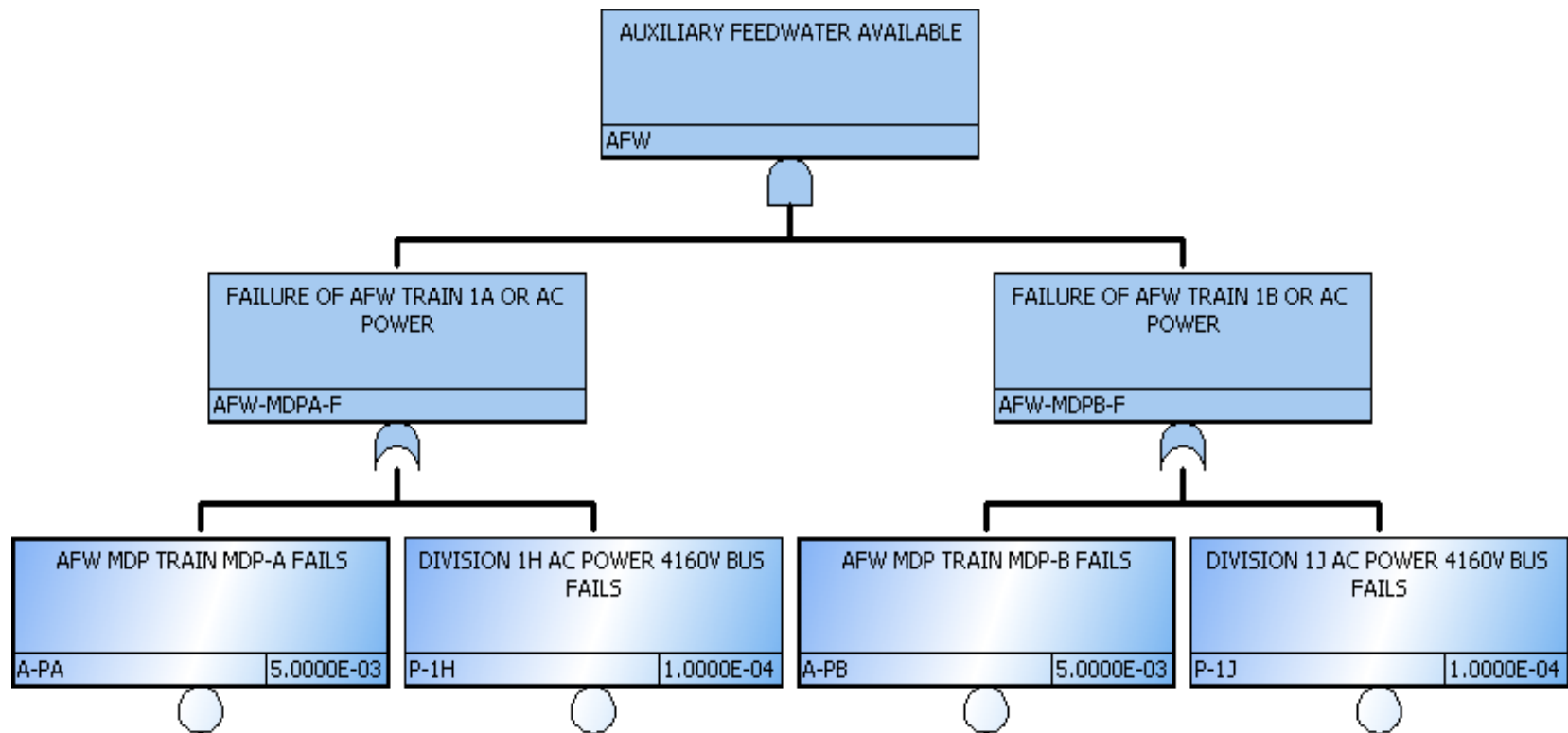
(A number of the actual event tree top events and fault tree basic events pruned for quantification illustration)



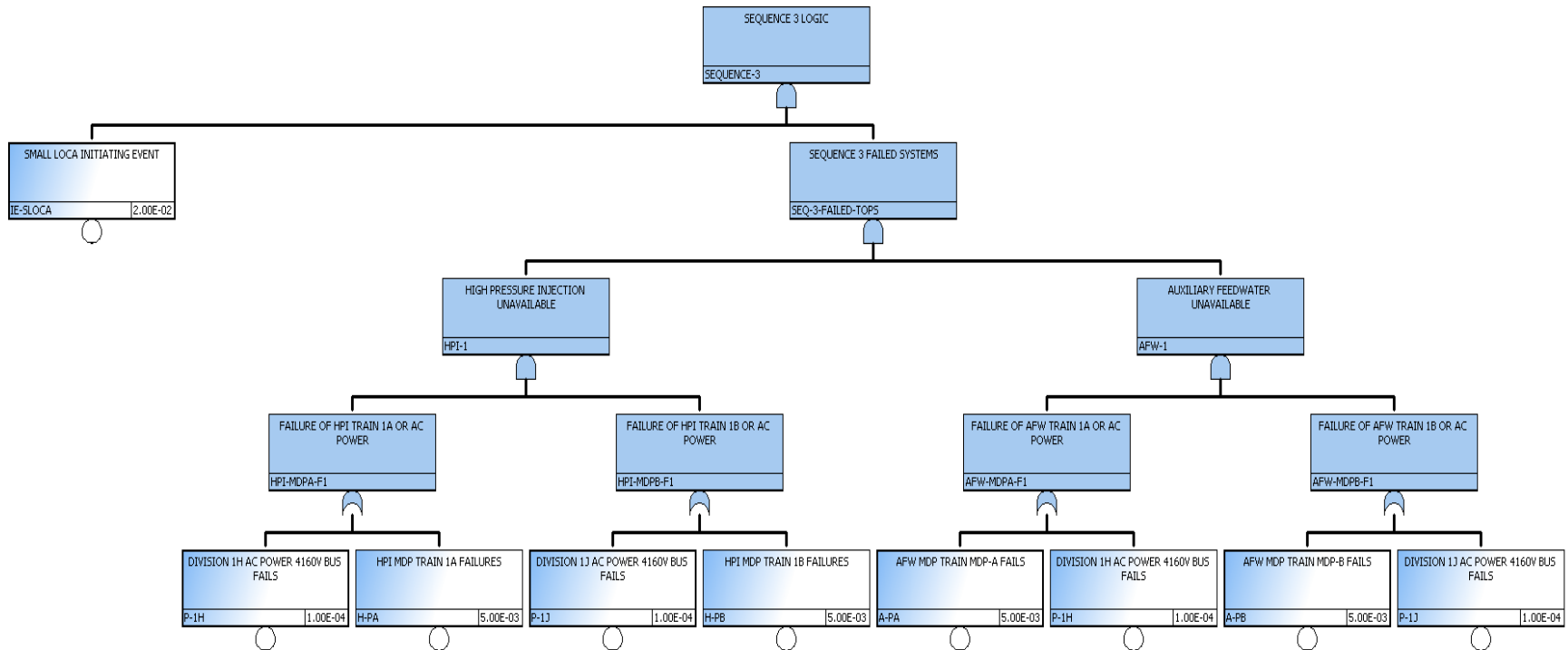
Simplified Example of Quantification Process (cont.)



Simplified Example of Quantification Process (cont.)



Simplified Example of Quantification Process (cont.)



Simplified Example of Quantification Process (cont.)

$$\text{Seq3} = \text{IE-SLOCA} * \text{System HPI Fails} * \text{System AFW Fails}$$

$$= (\text{IE-SLOCA}) * (\text{H-PA} * \text{H-PB} + \text{P-1J} * \text{H-PA} + \text{P-1H} * \text{H-PB} + \text{P-1H} * \text{P-1J}) * (\text{A-PA} * \text{A-PB} + \text{A-PA} * \text{P-1J} + \text{A-PB} * \text{P-1H} + \text{P-1H} * \text{P-1J})$$

$$= (\text{IE-SLOCA}) *$$

$$\begin{aligned} & [(\text{H-PA} * \text{H-PB} * \text{A-PA} * \text{A-PB} + \text{H-PA} * \text{H-PB} * \text{A-PA} * \text{P-1J} + \text{H-PA} * \text{H-PB} * \text{A-PB} * \text{P-1H} + \text{H-PA} * \text{H-PB} * \text{P-1H} * \text{P-1J}) \\ & + (\text{P-1J} * \text{H-PA} * \text{A-PA} * \text{A-PB} + \text{P-1J} * \text{H-PA} * \text{A-PA} * \text{P-1J} + \text{P-1J} * \text{H-PA} * \text{A-PB} * \text{P-1H} + \text{P-1J} * \text{H-PA} * \text{P-1H} * \text{P-1J}) \\ & + (\text{P-1H} * \text{H-PB} * \text{A-PA} * \text{A-PB} + \text{P-1H} * \text{H-PB} * \text{A-PA} * \text{P-1J} + \text{P-1H} * \text{H-PB} * \text{A-PB} * \text{P-1H} + \text{P-1H} * \text{H-PB} * \text{P-1H} * \text{P-1J}) \\ & + (\text{P-1H} * \text{P-1J} * \text{A-PA} * \text{A-PB} + \text{P-1H} * \text{P-1J} * \text{A-PA} * \text{P-1J} + \text{P-1H} * \text{P-1J} * \text{A-PB} * \text{P-1H} + \text{P-1H} * \text{P-1J} * \text{P-1H} * \text{P-1J})] \end{aligned}$$

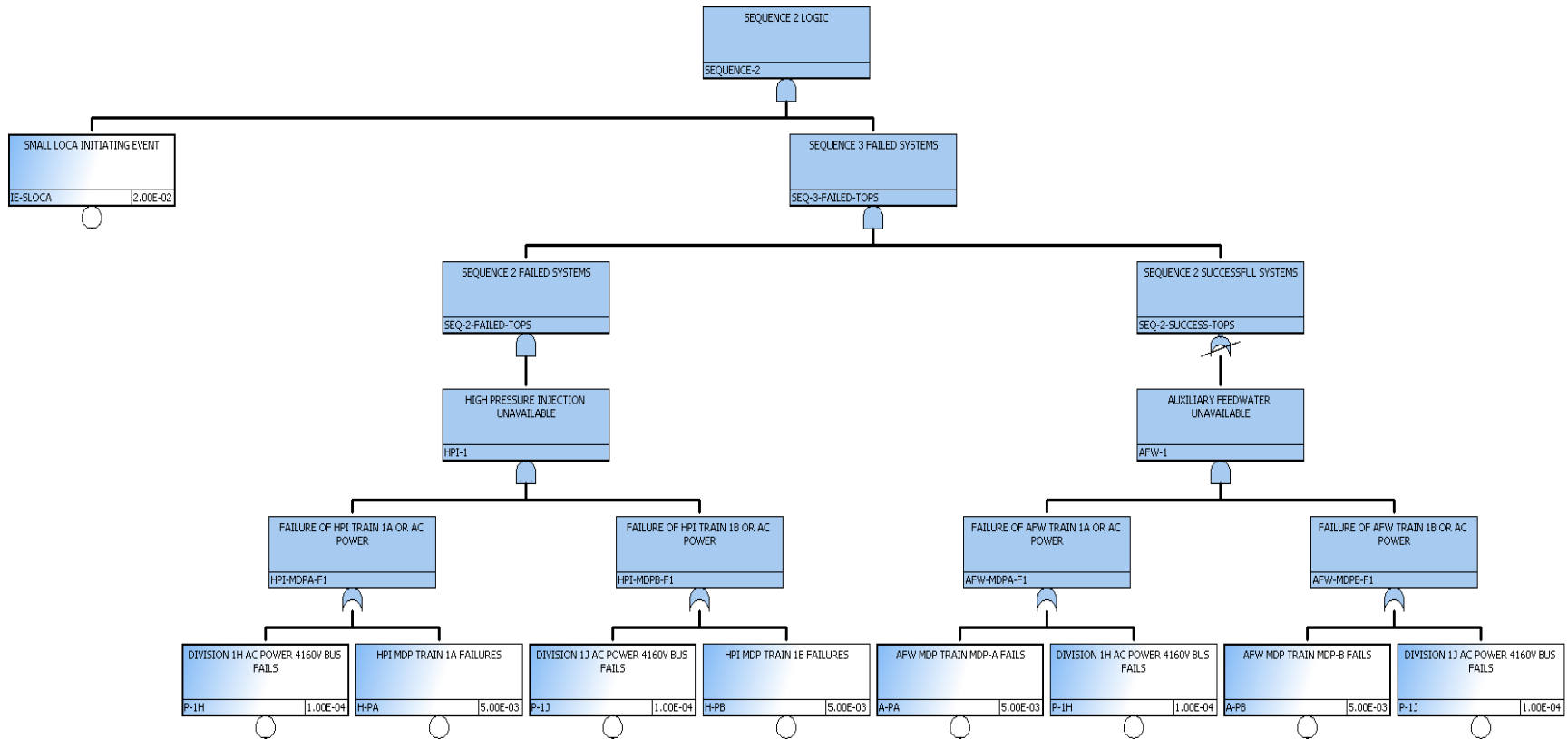
$$= \text{IE-SLOCA} * (\text{P-1H} * \text{P-1J} + \text{A-PA} * \text{H-PA} * \text{P-1J} + \text{A-PB} * \text{H-PB} * \text{P-1H} + \text{A-PA} * \text{A-PB} * \text{H-PA} * \text{H-PB})$$

$$\text{Seq3} = (2\text{E-2}/\text{Year}) * (1\text{E-4} * 1\text{E-4} + 5\text{E-3} * 5\text{E-3} * 1\text{E-4} + 5\text{E-3} * 5\text{E-3} * 1\text{E-4} + 5\text{E-3} * 5\text{E-3} * 5\text{E-3} * 5\text{E-3})$$

$$= (2\text{E-2}/\text{Year}) * (1\text{E-8} + 2.5\text{E-9} + 2.5\text{E-9} + 6.25\text{E-10})$$

$$= 3.125\text{E-10}/\text{Year}$$

Simplified Example of Quantification Process (cont.)

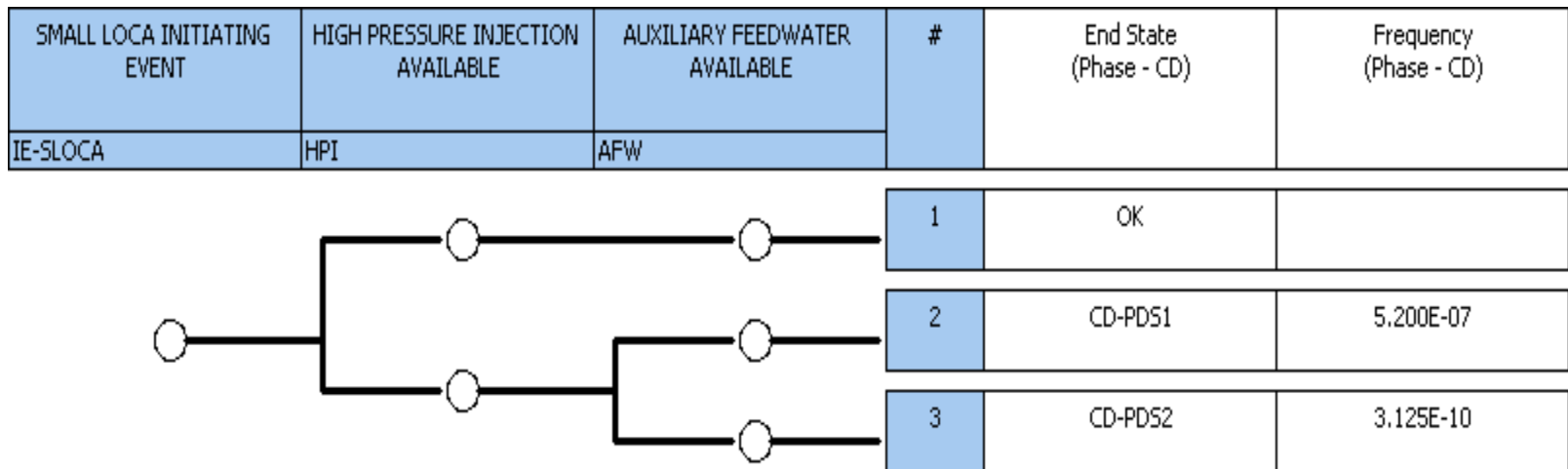


Simplified Example of Quantification Process (cont.)

$$\begin{aligned}
 \text{Seq2} &= \text{IE-SLOCA} * \text{System HPI Fails} * [\text{System AFW Successful} - \text{typically a delete term process}] \\
 &= (\text{IE-SLOCA}) * (\text{H-PA} * \text{H-PB} + \text{P-1J} * \text{H-PA} + \text{P-1H} * \text{H-PB} + \text{P-1H} * \text{P-1J}) * [(\text{A-PA} * \text{P-1H} + \text{A-PB} * \text{P-1J})] \\
 &= (\text{IE-SLOCA}) * [(\text{H-PA} * \text{H-PB} * \text{A-PA} * \text{P-1H} + \text{H-PA} * \text{H-PB} * \text{A-PB} * \text{P-1J}) + \\
 &\quad (\text{P-1J} * \text{H-PA} * \text{A-PA} * \text{P-1H} + \text{P-1J} * \text{H-PA} * \text{A-PB} * \text{P-1J}) + \\
 &\quad (\text{P-1H} * \text{H-PB} * \text{A-PA} * \text{P-1H} + \text{P-1H} * \text{H-PB} * \text{A-PB} * \text{P-1J}) + \\
 &\quad (\text{P-1H} * \text{P-1J} * \text{A-PA} * \text{P-1H} + \text{P-1H} * \text{P-1J} * \text{A-PB} * \text{P-1J}) + \\
 &= (\text{IE-SLOCA}) * (\text{H-PA} * \text{H-PB} + \text{P-1J} * \text{H-PA} + \text{P-1H} * \text{H-PB})
 \end{aligned}$$

$$\begin{aligned}
 \text{Seq2} &= (2\text{E-2/Year}) * (5\text{E-3} * 5\text{E-3} + 1\text{E-4} * 5\text{E-3} + 1\text{E-4} * 5\text{E-3}) \\
 &= (2\text{E-2/Year}) * (2.5\text{E-5} + 5\text{E-7} + 5\text{E-7}) \\
 &= 5.2\text{E-7/Year}
 \end{aligned}$$

Simplified Example of Quantification Process (cont.)



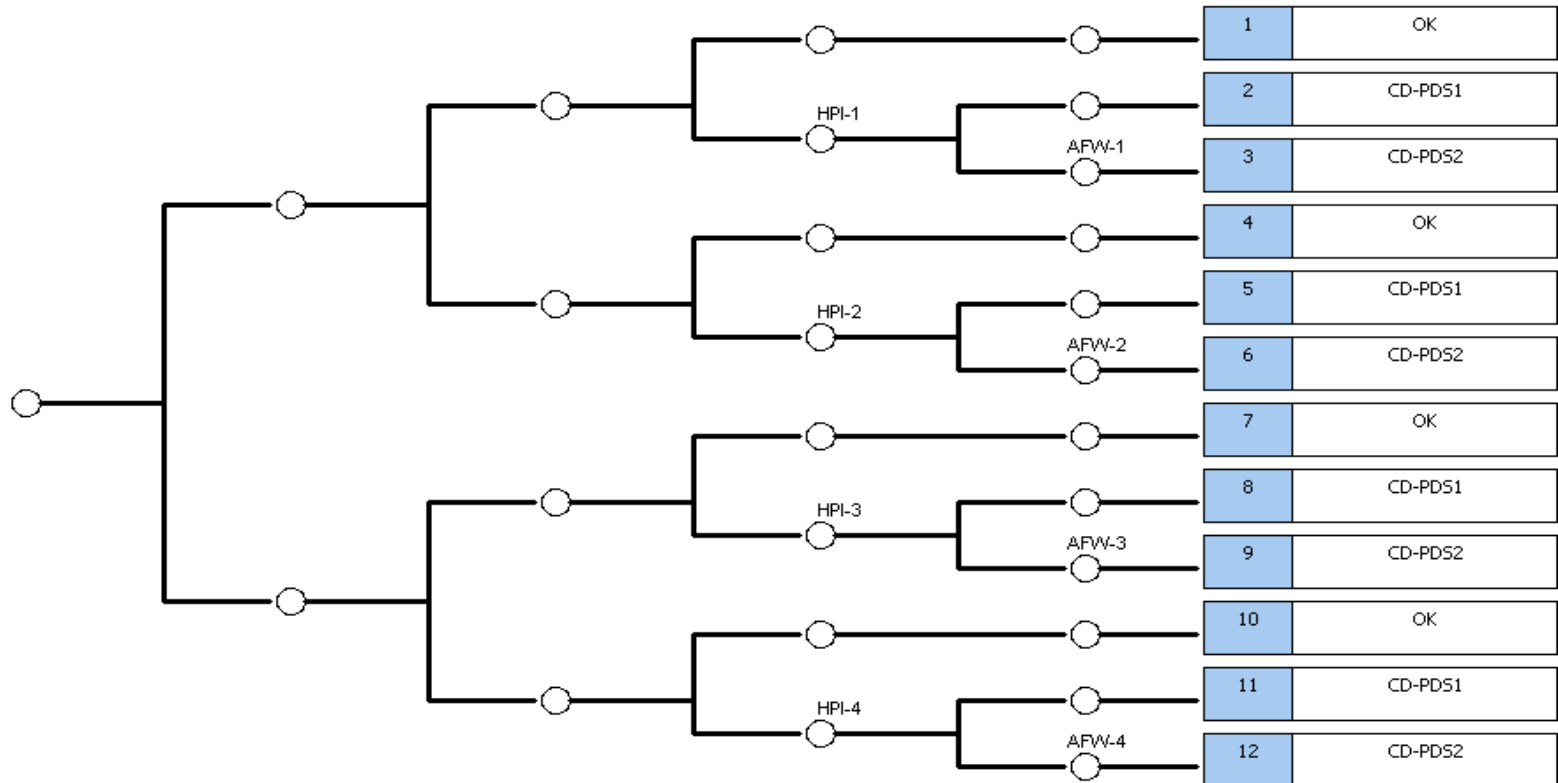
Event Trees with Boundary Conditions

- **Event trees with boundary conditions include all of the following significant intersystem dependencies in the event trees:**
 - **Front-line system to front-line system dependencies,**
 - **Front-line system to support system dependencies,**
 - **Support system to support system dependencies,**
 - **Human errors**
 - **Environmental considerations.**
- **Split fractions are determined from system logic models for conditions represented by each particular branch point or node in question**
- **The frequency of each accident-sequence path can be calculated as the product of the initiating event frequency and all split fractions along the sequence path**

Simplified Example of Large Event Tree Quantification Process

(A number of the actual event tree top events and fault tree basic events pruned for quantification illustration)

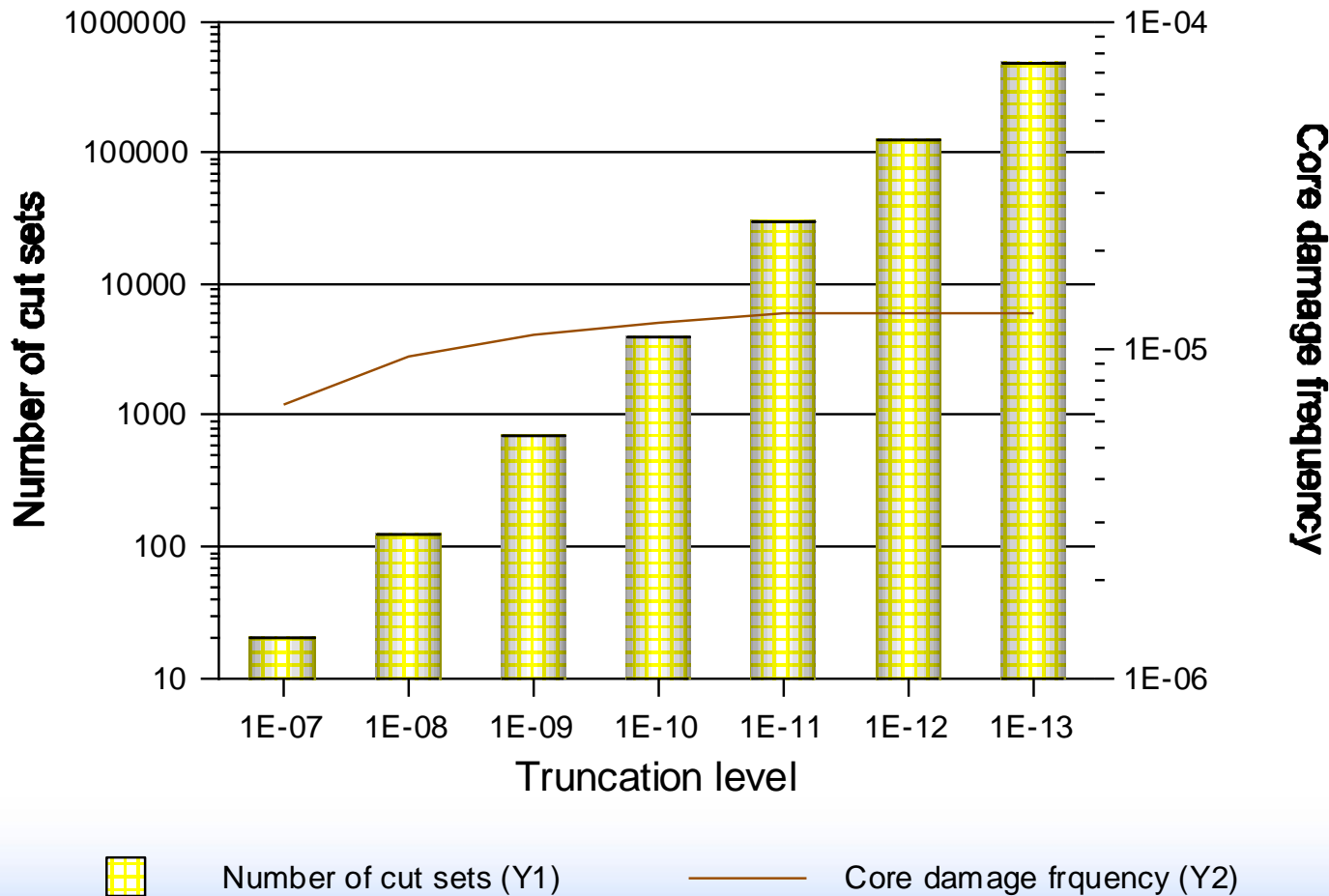
SMALL LOCA INITIATING EVENT	DIVISION 1H AC POWER	DIVISION 1J AC POWER	HIGH PRESSURE INJECTION AVAILABLE	AUXILIARY FEEDWATER AVAILABLE	#	End State (Phase - CD)
IE-SLOCA	P-1H	P-1J	HPI	AFW		



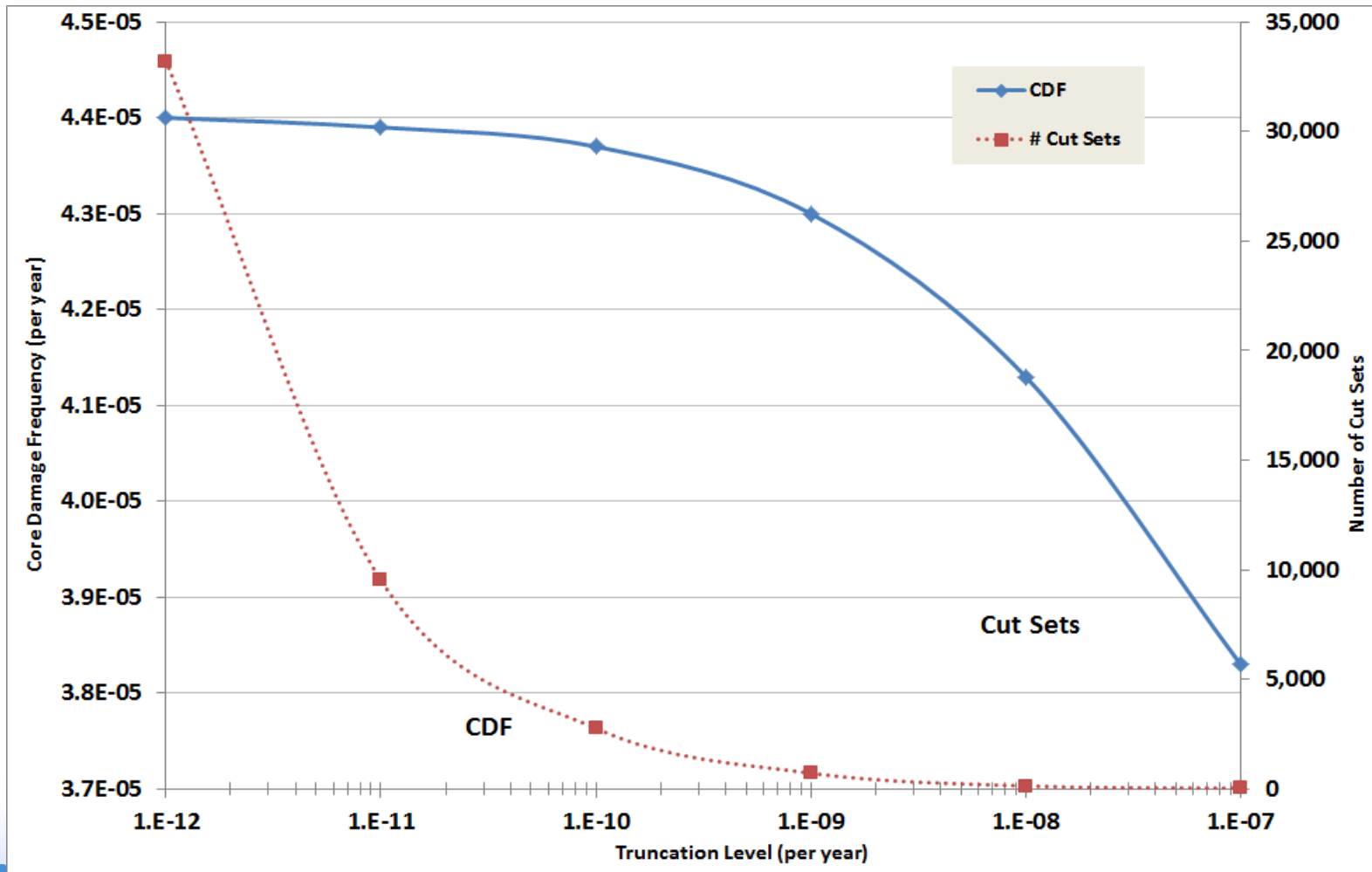
Truncation and Minimal Cut Sets

- **Truncation is practical necessity because of size of models**
 - **Eliminates some cut sets**
- **If conservative assumptions were made regarding such things as potential recovery actions or common cause failures, then a more detailed analysis can be performed to obtain less conservative values**

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



CDF and Number of Cut Sets Sensitive to Truncation Limits (PWR SPAR Model)



Quantification Results

- **Results of accident sequence quantification require careful scrutiny to ensure that errors in the analysis have not been made (test of reasonableness)**
 - **Cut sets or sequences that violate sequence success logic or otherwise do not reflect expected plant response**
 - **Cut sets or sequences containing event combinations precluded by Technical Specifications**
 - **Data input errors**
 - **Other errors**
 - **AFW fault tree's transfers were defaulted to an improper value resulting in the top two AFW cut sets being missed**
 - **Order of magnitude error in AFW failure probability**
 - **CDF too low by a factor of two**
 - **...**

Current PRA Software Codes Used by NRC and the Nuclear Plant Industry

Code and Developer:

- **CAFTA by EPRI (R&R Workstation)**
 - Fault Tree linking with Event Trees
- **RISKMAN by ABS Consulting**
 - Event Trees with Boundary Conditions
- **WinNUPRA by Scientech**
 - Fault Tree linking with Event Trees
- **RiskSpectrum by Relcon Scandpower AB in Sweden**
 - Fault Tree linking with Event Trees
- **SAPHIRE by INL**
 - Fault Tree linking with Event Trees
 - Event Trees with Boundary Conditions

***** Student Exercise *****

- **Answer the following from your plant's SPAR model or IPE**
 - **Which accident sequence quantification approach used?**
 - **Fault Tree Linking**
 - **Event Tree with Boundary Conditions**
 - **What are the two initiating events that contribute the most to the plant's CDF from a percentage contribution basis**
 - **What two classes of accidents or specific accident sequences (depends upon how results were presented) contribute the most to the plant's CDF?**



Idaho National Laboratory

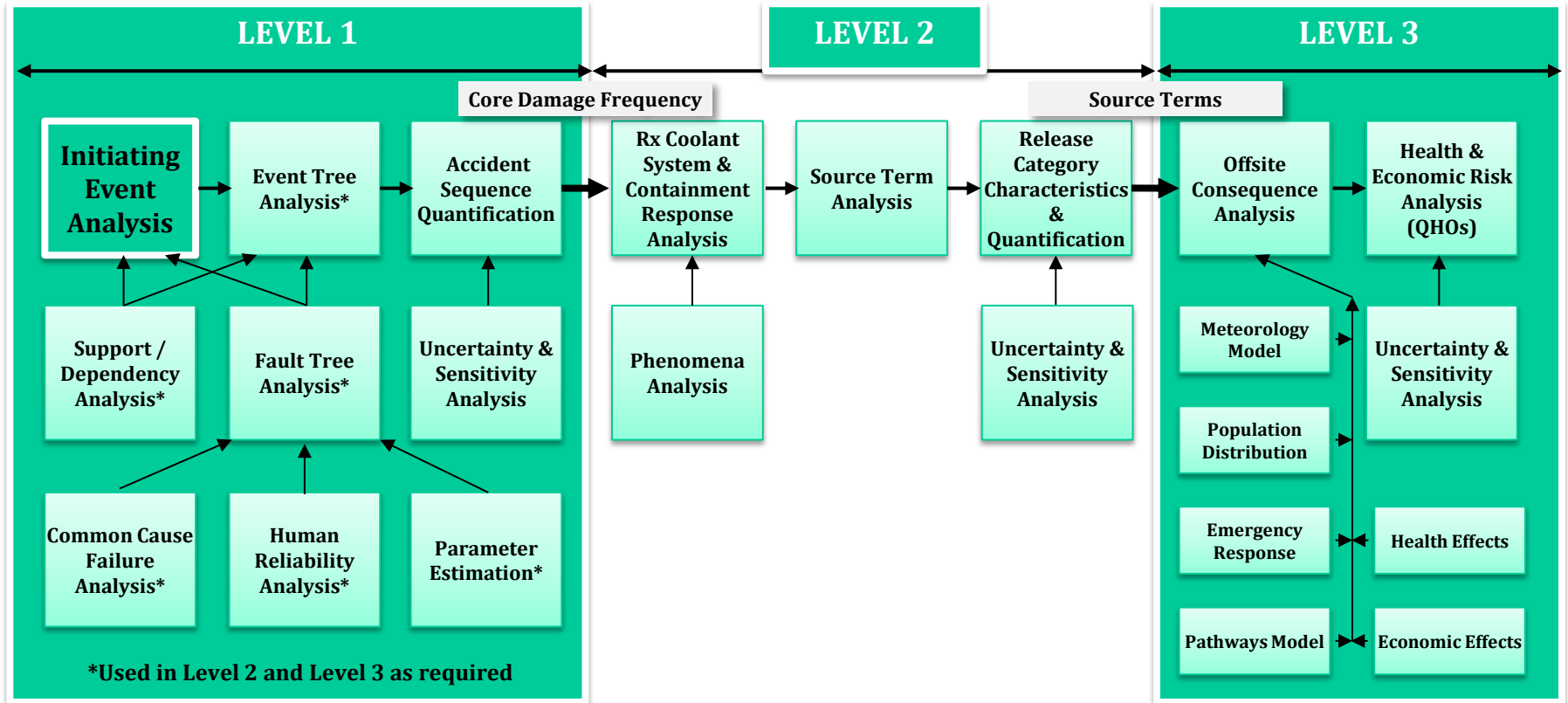
MODULE K

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:**
 1. ANSI/ANS Std. 58.21-2007 (External Events PRA Standard)
 2. NUREG/CR-6850 (fire PRA methodology)

Principal Steps in PRA



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 are of concern due to their dependent nature, that is EE can both;**
 - **Initiate a potential core damage accident**
 - **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 SSCs**
 - **Assess overall plant response to event**

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**
- **Coronal mass ejection**
- **Blizzard/Snow**
- **Drought**
- **Erosion**
- **Hail**
- **Heavy rain**
- **High temperature**
- **Low Temperature**
- **River diversion or change in lake level**
- **War**

History of External Events PRA in U.S.

- **1975 - WASH-1400 used logic models to analyze risks to public from two nuclear power plants; external events omitted from quantitative results**
- **1980s - Nuclear industry-sponsored studies of commercial nuclear plants first included assessments of external events**
 - **Oyster Creek - 1979 (first seismic PRA study)**
 - **HTGR - 1979 (first fire PRA study)**
 - **Big Rock Point - 1981 (included external events)**
 - **Zion/Indian Point - 1982 (included external events)**
 - **Browns Ferry (1983), Oconee (1984), Midland (1984), Shoreham (1986, 1988), Three Mile Island (1987), South Texas Project (1989)**

History of External Events PRA in U.S. (cont.)

- **NRC/industry-sponsored PRA Procedures Guide (NUREG/CR- 2300) includes methods for analyzing external events - 1983**
- **Extensive research sponsored by NRC and EPRI on methods for analyzing external events**
- **GL 88-20 issued - 1988, includes requirements for assessing vulnerabilities to internal floods**
- **NUREG-1150 - 1989, contains analyses of external events for Peach Bottom and Surry**
- **GL 88-20, Supplement 4 - 1991, contains IPEEE requirements for other external events**
- **NUREG-1407 issued containing IPEEE submittal guidance - 1991**
- **Originally requested IPEEE submittal date was June 1994**
- **GL 88-20, Supplement 5 revised IPEEE seismic requirements - 1995**

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 – Three Steps

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

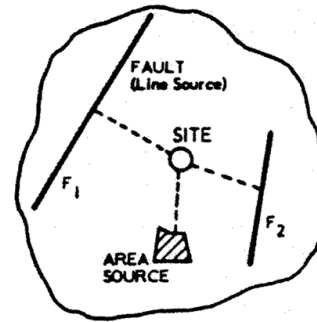
Analysis process briefly looked at in following slides



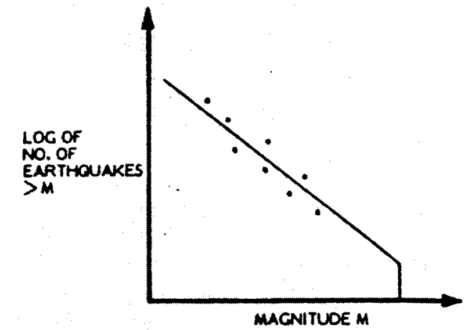
Four Steps in Seismic Hazard Curve Development

1. Identify seismic sources
2. Develop frequency-magnitude model for each source
3. Develop ground motion model for each source
4. Integrate over sources

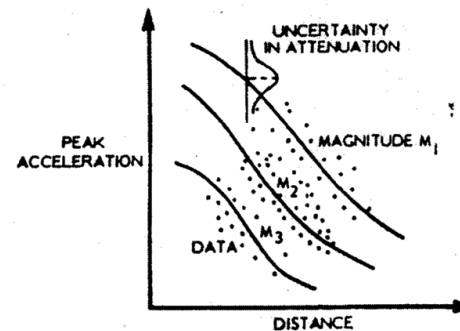
<http://earthquake.usgs.gov/hazards/>



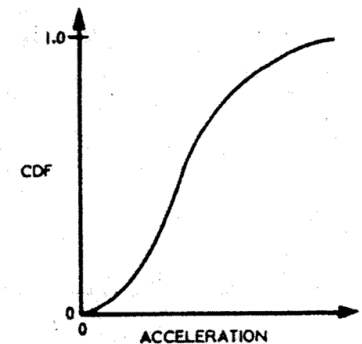
STEP 1
SOURCES



STEP 2
RECURRENCE

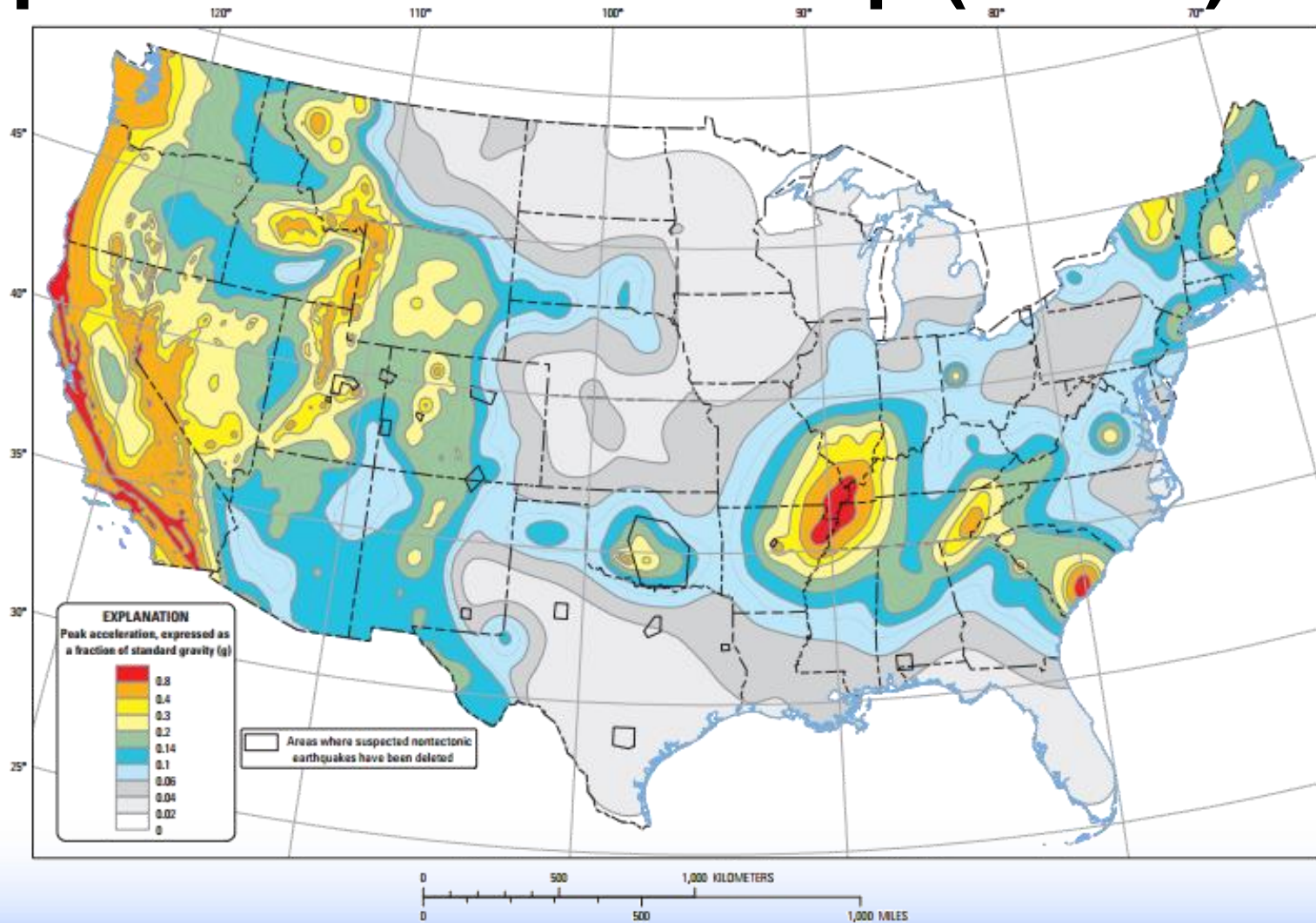


STEP 3
ATTENUATION



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

Updated US Hazard Map (USGS)



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 may be analyzed separately (i.e., as a separate and unique event)
- Failure probabilities of plant SSCs calculated based on specific g-level and fragility of SSC
- Internal events PRA re-evaluated using seismic failure probabilities (based upon g-level)
 - Core Damage (seismic) = $f(\text{earthquake}_g) * \text{Pr}(\text{failures}_g)$

$$\underbrace{\hspace{10em}}_{\text{Hazard}} \quad \underbrace{\hspace{10em}}_{\text{Fragility}}$$

Seismic Fragility Expressed in Terms of Peak Ground Acceleration

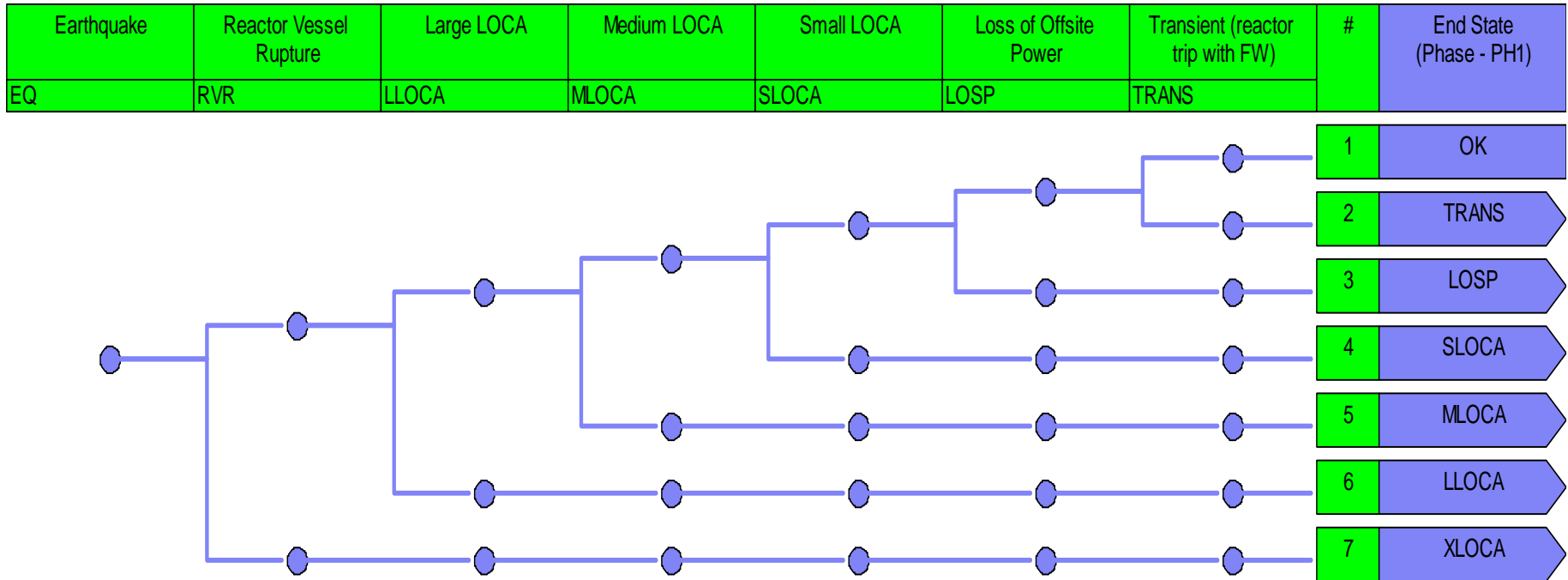
- **Fragility (A) = $A_m \beta_R \beta_U$ (lognormal model assumed)**
 - A_m = median ground acceleration capacity of SSC
 - $\beta_R \beta_U$ = Measure of the uncertainty in median fragility due to randomness and confidence, respectively (can also be labeled aleatory and epistemic, respectively)
 - A_m derived from various safety and response factors ($F_C F_{RE} F_{RS} A_{SSE}$), 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*

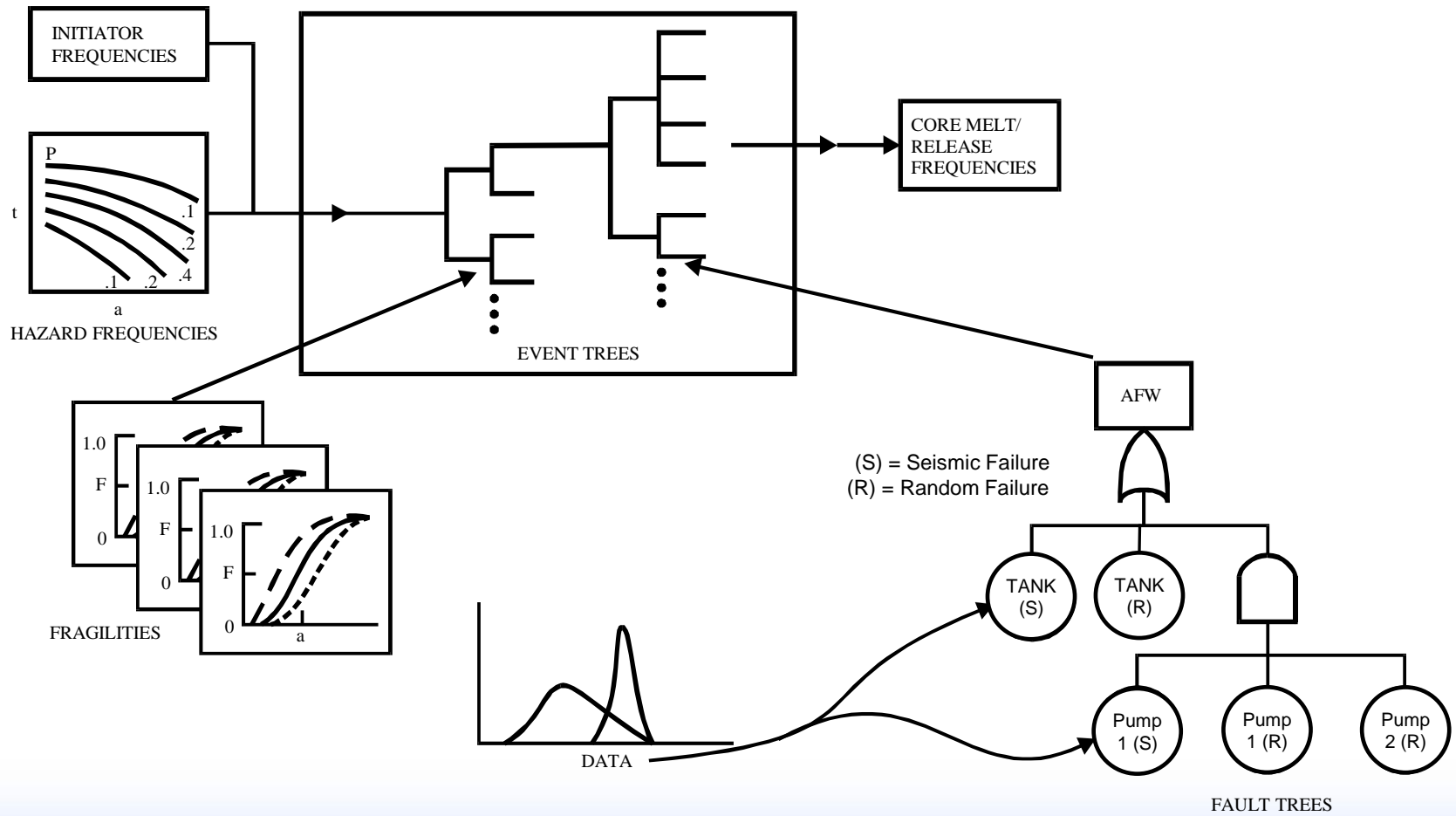
Component/Structure	Dominant Failure Mode	Median Fragility Range (g)
Concrete containment building	Shear failure	2.50-9.20
Reactor Pressure Vessel	Anchor bolt	1.04-5.70
Flat-bottom tank	Shell wall buckling	0.20-1.00
Batteries and racks	Cases and plates	0.90-5.95
Motor control centers	Chattering	0.06-4.20
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 Plant Response Estimated Given Occurrence of the External Event (Provides Link to Sequence Analysis)



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 via 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
 - Many NUREGS have been published (i.e., NUREG/CR-6931, 2128, 7010, 7150)
- **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 ($<1E-5/\text{yr}$)?

If Not:

- Does bounding analysis estimate CDF $<1E-6/\text{yr}$?

If Not:

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



Idaho National Laboratory

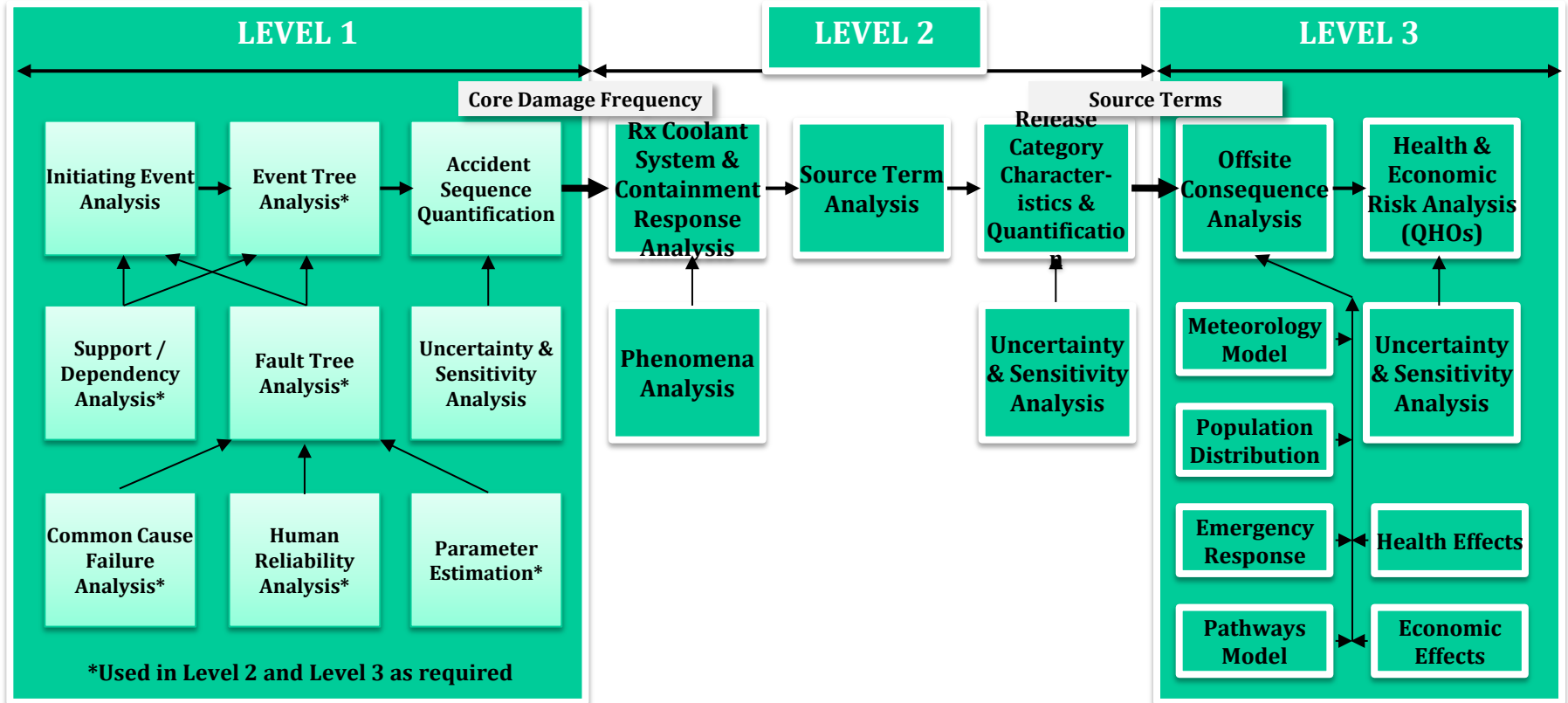
MODULE L

LEVEL 2 & 3 ANALYSIS

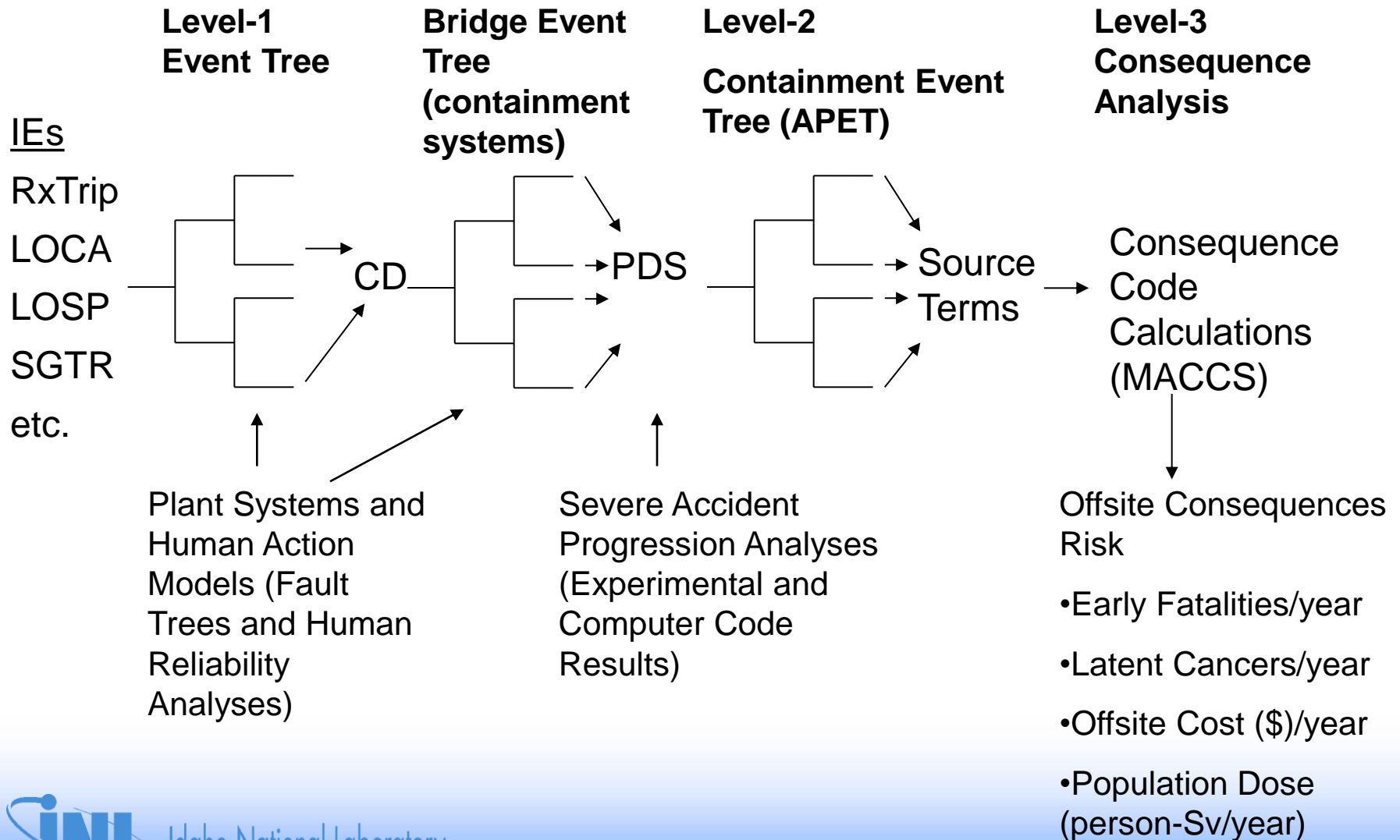
Level 2 & 3 Analysis

- **Purpose:** Introduce the students to accident progression (Level 2 PRA) and consequence analysis (Level 3 PRA).
- **Objectives:**
 - Describe the general purpose of Level 2 and 3 analyses
 - List typical types of consequences from a Level 3 PRA
- **References:** NUREG/CR-2300

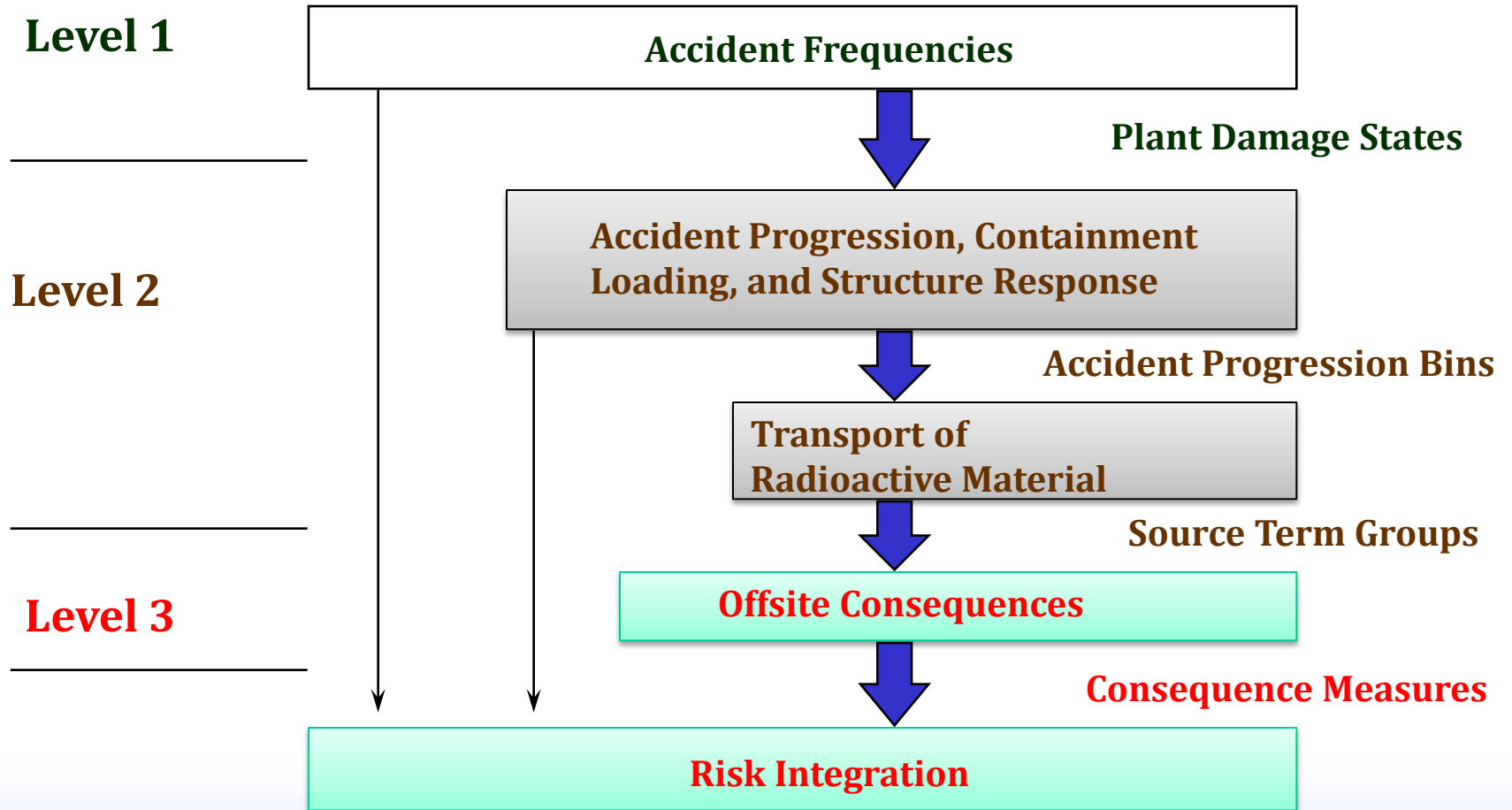
Principal Steps in PRA



Overview of Level-1/2/3 PRA



Principal Steps in PRA Process



Purpose of Level 2 & 3 Analyses

- Level 2 & 3 analyses bridge the gap between the engineering and operations associated with a reactor and the potential risk that it presents to the public
 - Level 2 (Containment) Analysis starts with the Level 1 plant damage states and calculates a set of **radionuclide source terms** released to the environment
 - Level 3 (Consequence) Analysis calculates potential ranges (probability of occurrence and magnitude) of **adverse impacts** (consequences) of an accidental release of radionuclides

Level 2 & 3 Analyses Continues the Scenario Through Public Impacts

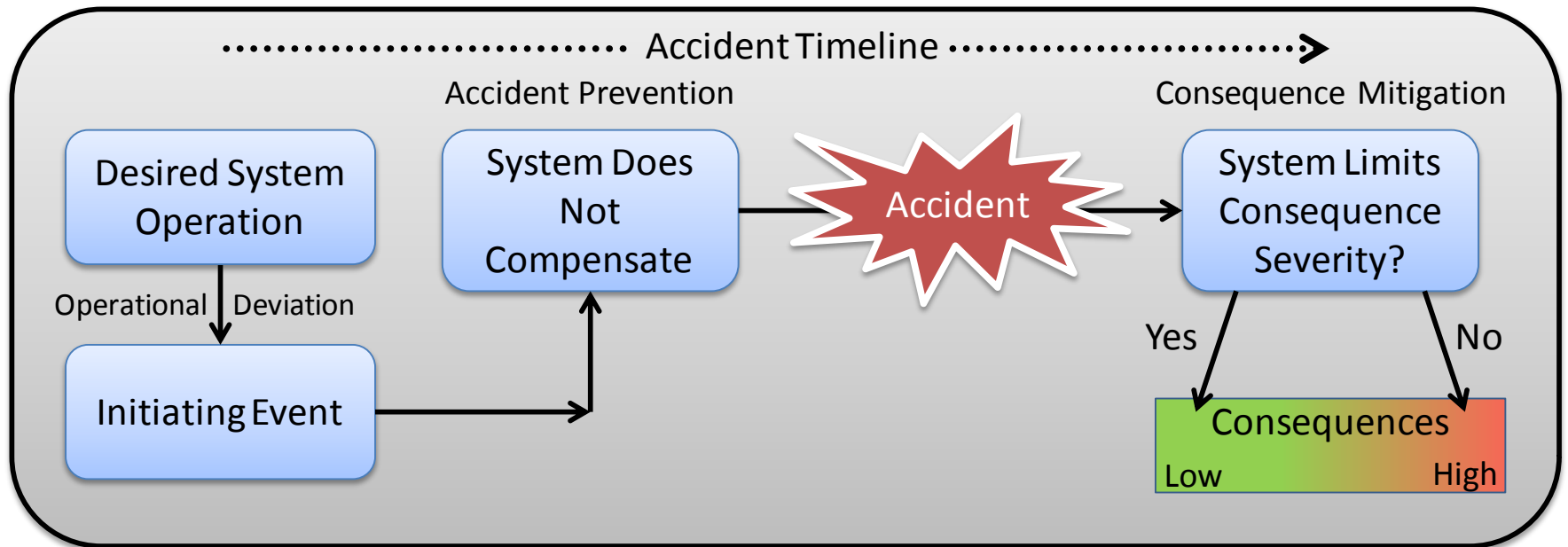


Figure 4.3 – NASA/SP-2011-3421

Level 2 Analysis Overview

- A Level 2 Analysis evaluates the radionuclide releases from accidents that result in a severely damaged core
- It considers the following items:
 - Fission product transportation, deposition, and release in the **reactor coolant system**,
 - Fission product transportation, deposition, and release in the **containment**
 - Determining source terms **from** the containment

Plant Damage State Binning

- **Plant-damage states are groups of accident sequences with certain similarities regarding**
 - **Plant response**
 - **Timing of the scenario outcomes**
 - **Equipment status**
- **Containment analyst provides guidance as to which types of sequences are aggregated into which plant-damage states**

Containment Response

- **Following core damage, we first are concerned about what happens to the containment**
- **How does the containment system deal with physical conditions resulting from the accident?**
 - **Pressure**
 - **Heat sources**
 - **Fission products**
 - **Steam and water**
 - **Hydrogen**
 - **Other noncondensable gasses**

Transportation, Deposition, and Release in Reactor Coolant System

- **The following issues concerning**
 - **Transportation through**
 - **Deposition in**
 - **Release of radionuclides**
from the reactor coolant system
- **Needed to be considered in the Level 2 analysis**
 - **Vessel pressure and inventory**
 - **Recovery of injection prior to or after vessel breach**
 - **Hydrogen released prior to or after vessel breach**
 - **Hydrogen burn prior to or after vessel breach**

Transportation, Deposition, and Release in Containment

- **Issues concerning transportation through, deposition in, and release of radionuclides from containment to be considered in Level 2 analysis**
 - **Debris coolability**
 - **Pressure increase due to hydrogen burn/detonation**
 - **Interactions between molten fuel and water**
 - **Debris-concrete interaction**
 - **Containment pressure**

Source Term from the Containment

- **Release of radionuclides from containment is dependent upon**
 - Radionuclide chemistry
 - Physical form of the fuel
 - Environment into which it is released
- **Source term specification should include**
 - Magnitude of the release
 - Release rate
 - Chemical and physical forms of the release material

Source Term from the Containment (cont.)

- **Potential release processes need to be considered:**
 - **Cladding-rupture release**
 - **Diffusion release**
 - **Leach release**
 - **Melt release**
 - **Melt/concrete release**
 - **Fragmentation release**

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

Level 3 Analysis Overview

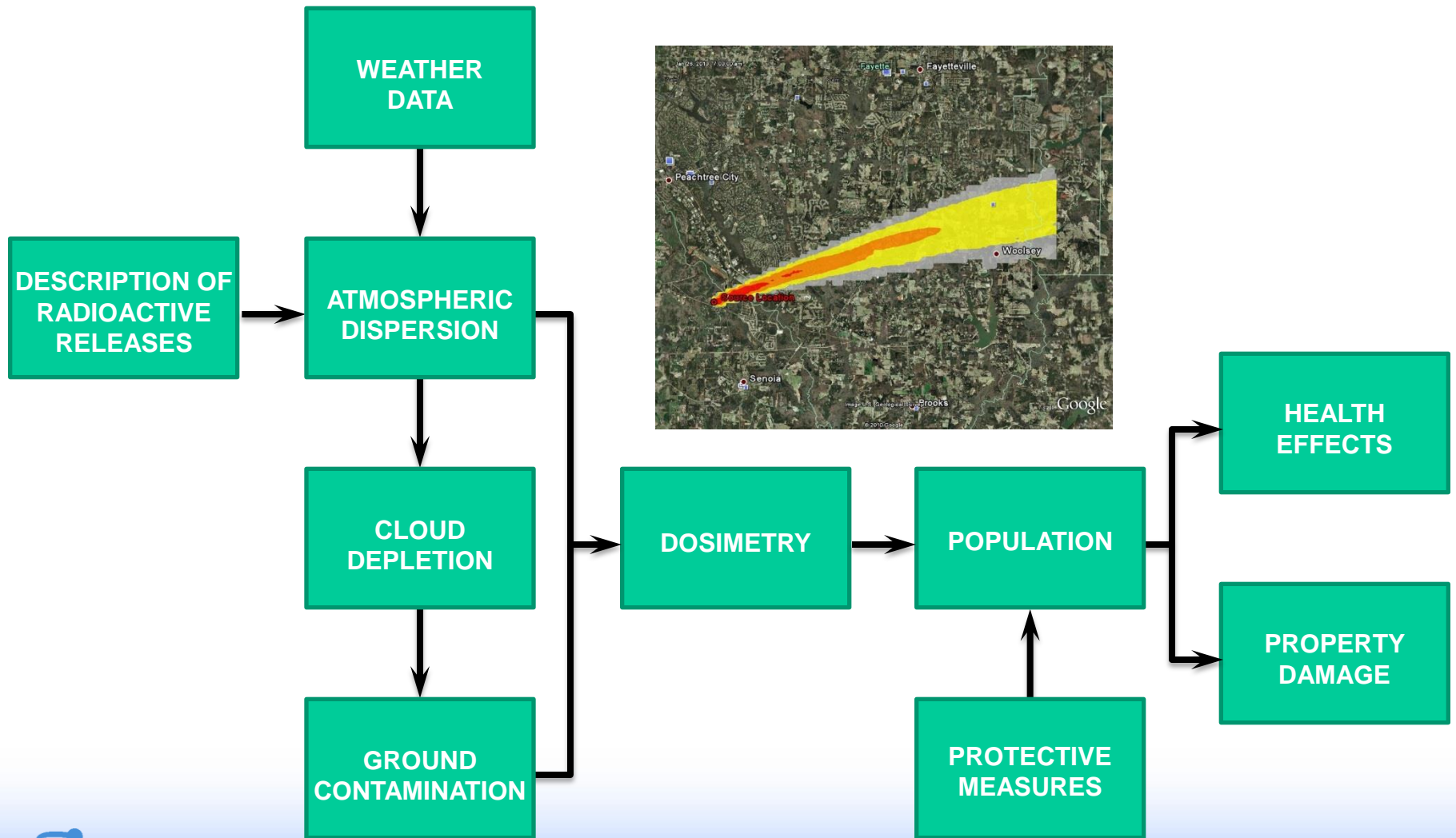
- **A Level 3 Analysis evaluates the effects of the release of radioactive materials on the surrounding population and environment**
- **Can consider the following adverse impacts (commonly referred to as "public risk")**
 - **Early and long-term deaths**
 - **Early and long-term injuries**
 - **Contamination of property, land, or water**
 - **Economic impacts**

Level 3 PRA

- **Focuses on atmospheric releases of radionuclides**
- **Conditional on the nature of the release occurring**
- **Computer codes calculate consequences**
 - **In the US (and outside)**
 - **MACCS (straight-line Gaussian plume model)**
 - **HYSPLIT (Lagrangian-based particle model)**
 - **In Europe**
 - **COSYMA (European Commission), ARANO (Finland), CONDOR (UK), LENA (Sweden), MECA2 (Spain), OSCAAR (Japan), ...**



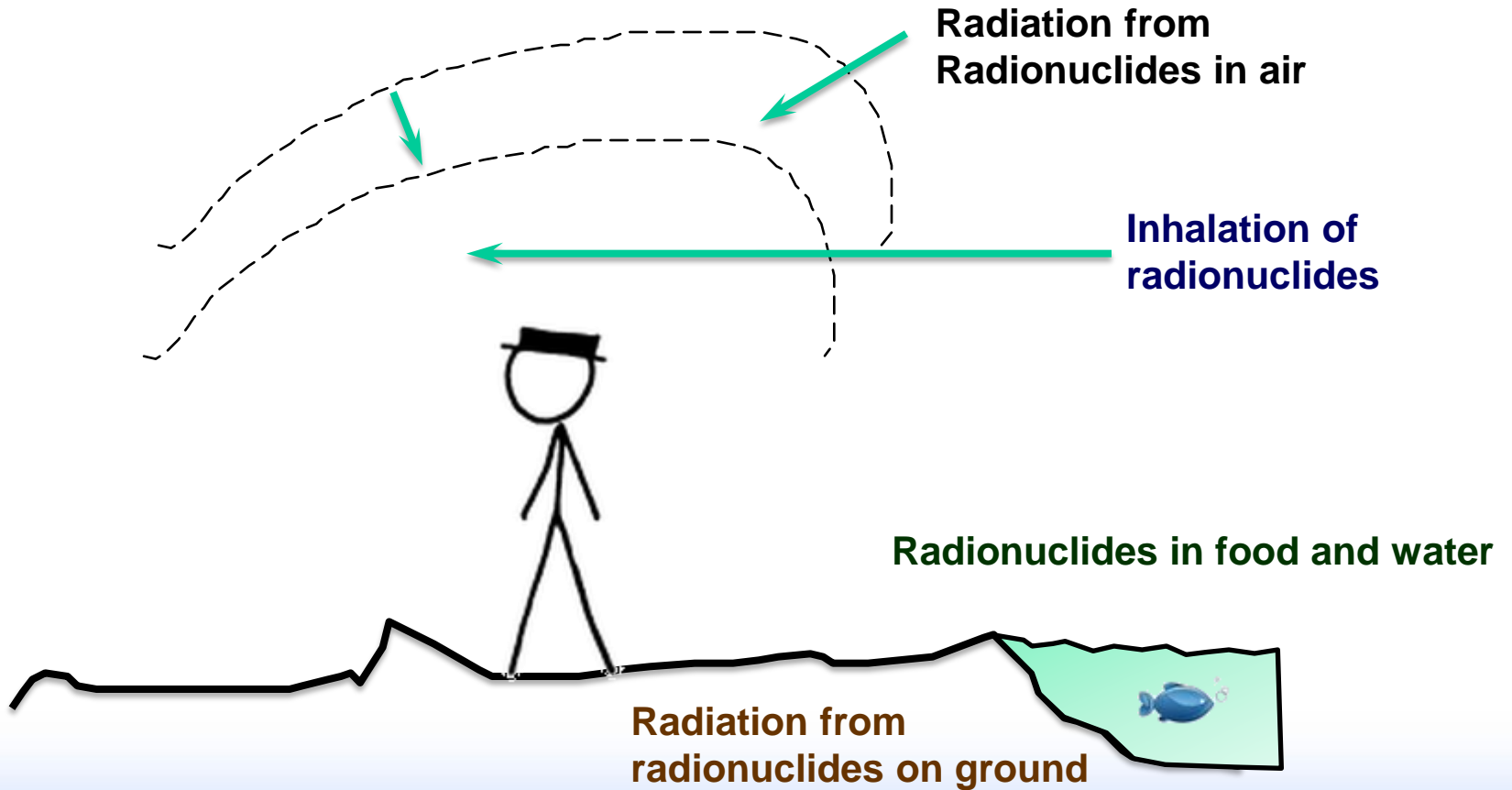
Approach for Consequence Analysis



Major Parts of a Level 3 Analysis

- **The following areas are the major considerations that must be taken into account during a level 3 analysis: atmospheric transportation and deposition model, including meteorology**
 - **Pathways model**
 - **Dosimetry model**
 - **Health effects model**
 - **Population distribution model**
 - **Emergency response model**
 - **Economic effects model**

Pathways to People



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**

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 x consequence

***** Exercise *****

- **Answer the following for your choice of a plant's IPE:**
 - **In either the summary sections in the front of the IPE, or in the plant unique design features section (often Section 6), note any particular strengths or weaknesses cited from a containment capability perspective.**



Idaho National Laboratory

Module M

**LOW-POWER and
SHUTDOWN RISK**

Low-Power and Shutdown Risk

- **Purpose:** To understand why low-power and shutdown (LP/SD) modes of operation are thought to be of concern from a risk perspective, and to become familiar with approaches to analyzing these risk.
- **Objectives:**
 - Describe how LP/SD modes can be risk-significant
 - Describe why PRA must treat separate modes of operation during LP/SD
 - Discuss the risk importance of systems available to maintain plant safety functions and the effect of maintenance outages on LP/SD risk
- **References:**
 - NUREG-1449 - Review of shutdown events
 - NUREG/CR-6143 and NUREG/CR-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.-58.22 for LPSD PRA

Low-Power and Shutdown Risk

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

LP/SD Operational Events Established the Significance of LP/SD 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 LP/SD Risk

- **Some systems may not be available since Tech. Specs. allow more equipment to be inoperable during LP/SD than at power**
- **LP/SD initiating events (by definition) impact the operable train of decay heat removal systems**
 - **IE for LP/SD 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 LP/SD**
 - **Plant instruments and indications may not be available or accurate**

NRC Staff's Evaluation of LP/SD 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 LP/SD**
 - **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**

LP/SD 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**
- **LP/SD 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	$\leq 5\%$	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 than 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 than fully tensioned

LP/SD PRA Structured Around Plant Operating State

- **PRA models (event trees and fault trees) developed for each plant operating state (POS) and each initiating event**
 - **Some PRAs imbed the POS in the IE identifier**
 - **LOSP-POS1, LOSP-POS2, LOSP-POS3, etc.**
 - **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**

Plant Operating States (PWR)

NUREG/CR-6144 POS	POS Description	Standard Technical Specification Mode (SPAR POS)	Technical Specification Mode Description
POS 1	Low power and reactor shutdown	1	Power operation
POS 2	Cooldown with SGs from operating temp to 345°F	3	Hot standby
POS 3	Cooldown with RHR from 345°F to 200°F	4 (4E)	Hot shutdown
POS 4	Cooldown with RHR below ~200°F	5 (5EF)	Cold shutdown
POS 5	Draining RCS to mid-loop	5 (5EF)	Cold shutdown
POS 6	Mid-loop operation	5 (5ER)	Cold shutdown
POS 7	Fill for refueling	6 (6)	Refueling
POS 8	Refueling	6 (6)	Refueling
POS 9	Draining RCS to mid-loop after refueling	6 (6)	Refueling
POS 10	Mid-loop operations after refueling	5 (5LR)	Cold shutdown
POS 11	Refilling RCS	5 (5LF)	Cold shutdown
POS 12	RCS heatup solid and draw bubble	5 (5LF)	Cold shutdown
POS 13	RCS heatup to 350°F	4 (4L)	Hot shutdown
POS 14	RCS heatup with SGs available above 350°F	2	Startup
POS 15	Startup and low power operations	1	Power operation

PRA's Analyze LP/SD 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 LP/SD PRA Studies

- **LP/SD risks not studied as extensively as those for power operation**
- **However, several LP/SD 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 LP/SD 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 LP/SD Models

- **10 LP/SD 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 LP/SD PRAs Have Been Developed

- **Perception continues that LP/SD operations pose less risk than full-power**
- **LP/SD 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 LP/SD 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 LP/SD 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



Idaho National Laboratory

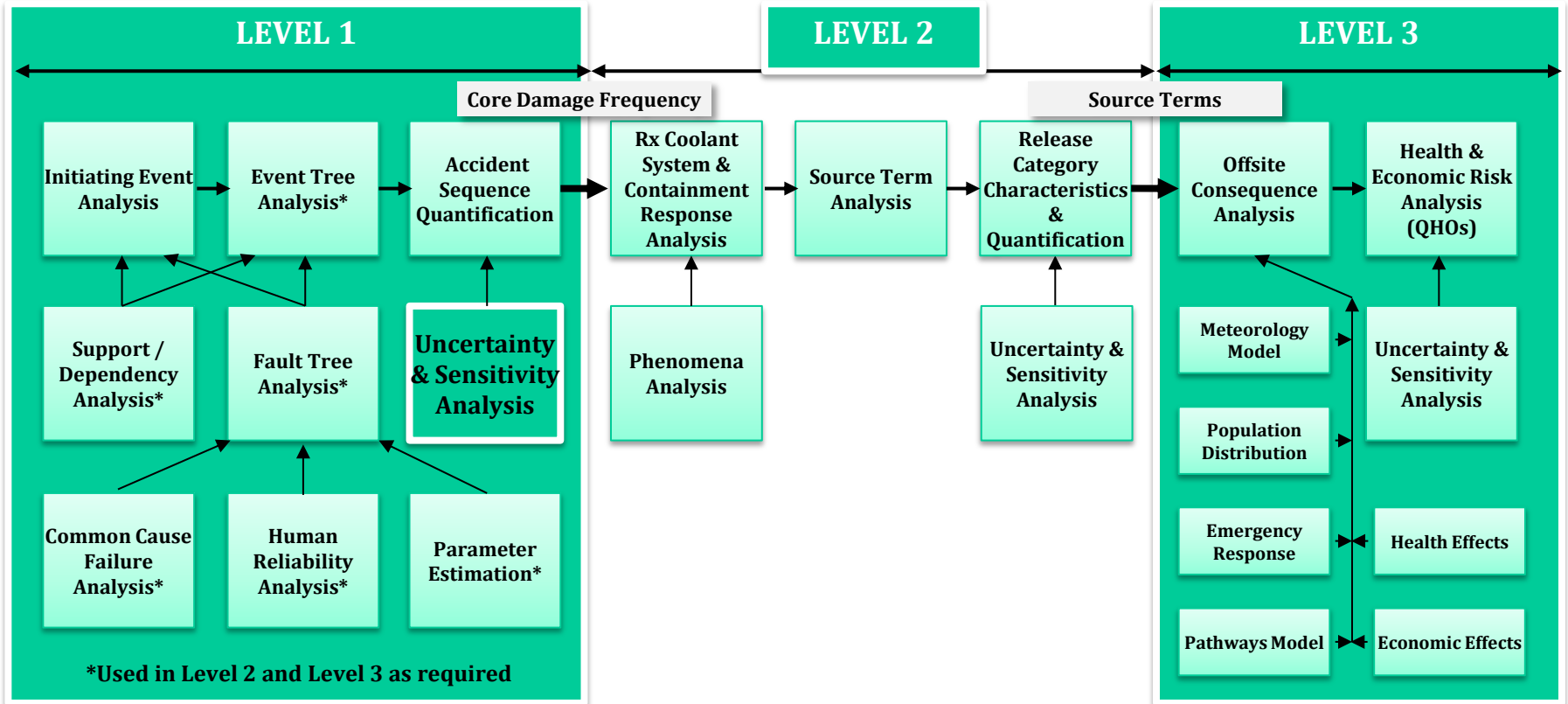
MODULE N

IMPORTANCE MEASURES

Importance Measures

- **Purpose:** Students will be introduced to concepts of quantitative importance measures. Several different types of importance measures and their meanings are presented.
- **Objectives:**
 - Identify four common quantitative importance measures
 - Calculate values for four types of importance measures given Level 1 PRA results
 - Discuss how importance measures are influenced by the value of the associated basic event, the values of other basic events, and modeling assumptions
 - Understand implications of each importance measure for plant safety & inspection activities
 - Explain why use of importance measures is considered valid for Maintenance Rule applications (i.e., binning SSCs into risk and non-risk categories)
- **References:**
 - NUREG-1489, App. C
 - NRC Inspection Manual Part 9900: Technical Guidance-Operations; Use of Probabilistic Risk Ranking Information
 - The Use of Risk Importances for Risk Based Applications and Regulation; W.E. Vesely, PSA-96
 - Some Perspectives on Risk Importance Measures, I. Wall, D. Worledge, PSA-96
 - Developing Useful Insights and Avoiding Misleading Conclusions from Risk Importance Measures in PSA Applications, K. Fleming, PSA-96

Principal Steps in PRA



What are Importance Measures

- **A means of utilizing a PRA model to measure impact of model inputs on total risk**
 - **An effective way to separate, identify, & quantify values of individual factors which affect risk**
 - **Design features**
 - **Plant operations**
 - **Test & maintenance**
 - **Human reliability**
 - **System & component failures**

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 Ratio or Risk Achievement Worth (RAW)**
 - **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)

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

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 Measure Calculation Example

- Consider these minimal cut sets:

$$\begin{aligned}
 T * A &= 1/\text{year} * 6 \times 10^{-4} && = 6 \times 10^{-4} \\
 T * B * C &= 1/\text{year} * 1 \times 10^{-2} * 3 \times 10^{-3} && = 3 \times 10^{-5} \\
 T * C * D &= 1/\text{year} * 3 \times 10^{-3} * 1 \times 10^{-3} && = 3 \times 10^{-6} \\
 &&& F(x) = 6.33 \times 10^{-4}
 \end{aligned}$$

where:

$$\begin{aligned}
 T &= 1/\text{year} \\
 A &= 6 \times 10^{-4} \\
 B &= 1 \times 10^{-2} \\
 C &= 3 \times 10^{-3} \\
 D &= 1 \times 10^{-3}
 \end{aligned}$$

- Fussell-Vesely Importance

$$\begin{aligned}
 FV_T &= 6.33 \times 10^{-4} / 6.33 \times 10^{-4} && = 1.0 \\
 FV_A &= 6.00 \times 10^{-4} / 6.33 \times 10^{-4} && = 0.948 \\
 FV_B &= 3.00 \times 10^{-5} / 6.33 \times 10^{-4} && = 0.047 \\
 FV_C &= 3.30 \times 10^{-5} / 6.33 \times 10^{-4} && = 0.052 \\
 FV_D &= 3.00 \times 10^{-6} / 6.33 \times 10^{-4} && = 0.005
 \end{aligned}$$

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

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

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 Measure Calculation Example

- Consider these minimal cut sets:

$$\begin{aligned}
 T * A &= 1/\text{year} * 6 \times 10^{-4} && = 6 \times 10^{-4} \\
 T * B * C &= 1/\text{year} * 1 \times 10^{-2} * 3 \times 10^{-3} && = 3 \times 10^{-5} \\
 T * C * D &= 1/\text{year} * 3 \times 10^{-3} * 1 \times 10^{-3} && = 3 \times 10^{-6} \\
 &&& F(x) = 6.33 \times 10^{-4}
 \end{aligned}$$

where:

$$\begin{aligned}
 T &= 1/\text{year} \\
 A &= 6 \times 10^{-4} \\
 B &= 1 \times 10^{-2} \\
 C &= 3 \times 10^{-3} \\
 D &= 1 \times 10^{-3}
 \end{aligned}$$

- Risk Reduction Ratio Importance

$$\begin{aligned}
 RRR_T &= 6.33 \times 10^{-4} / 0.0 && = \infty \\
 RRR_A &= 6.33 \times 10^{-4} / 3.3 \times 10^{-5} && = 19.18 \\
 RRR_B &= 6.33 \times 10^{-4} / 6.03 \times 10^{-4} && = 1.05 \\
 RRR_C &= 6.33 \times 10^{-4} / 6.00 \times 10^{-4} && = 1.06 \\
 RRR_D &= 6.33 \times 10^{-4} / 6.30 \times 10^{-4} && = 1.00
 \end{aligned}$$

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: $RIR_{x_i} = RAW_{x_i} = F(1) / F(x)$

Difference (or Interval): $RII_{x_i} = F(1) - F(x)$

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 ≥ 1
 - Caution when interpreting RAW for initiating events, recall initiating events are typically input as a frequency rather than a probability
- For Maintenance Rule (10 CFR 50.65), NUMARC Guide 93-01 (endorsed by NRC) uses a RAW significance criterion of 2

Risk Increase Importance Measure Calculation Example

- Consider these minimal cut sets:

$$\begin{aligned} T * A &= 1/\text{year} * 6 \times 10^{-4} && = 6 \times 10^{-4} \\ T * B * C &= 1/\text{year} * 1 \times 10^{-2} * 3 \times 10^{-3} && = 3 \times 10^{-5} \\ T * C * D &= 1/\text{year} * 3 \times 10^{-3} * 1 \times 10^{-3} && = 3 \times 10^{-6} \\ F(x) &= 6.33 \times 10^{-4} \end{aligned}$$

where:

$$\begin{aligned} T &= 1/\text{year} \\ A &= 6 \times 10^{-4} \\ B &= 1 \times 10^{-2} \\ C &= 3 \times 10^{-3} \\ D &= 1 \times 10^{-3} \end{aligned}$$

- Risk Achievement Worth Importance

$$\begin{aligned} RAW_T &= 6.33 \times 10^{-4} / 6.33 \times 10^{-4} && = 1.0 \text{ (caution interpreting RAW for IE)} \\ RAW_A &= 1.0 / 6.33 \times 10^{-4} && = 1579.78 \\ RAW_B &= 3.603 \times 10^{-3} / 6.33 \times 10^{-4} && = 5.69 \\ RAW_C &= 1.16 \times 10^{-2} / 6.33 \times 10^{-4} && = 18.33 \\ RAW_D &= 3.63 \times 10^{-3} / 6.33 \times 10^{-4} && = 5.73 \end{aligned}$$

Birnbaum (Bi)

- 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

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

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

$$Bi_{x_i} = F(1) - F(0)$$

- 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 Measure Calculation Example

- Consider these minimal cut sets:

$$\begin{aligned}
 T * A &= 1/\text{year} * 6 \times 10^{-4} && = 6 \times 10^{-4} \\
 T * B * C &= 1/\text{year} * 1 \times 10^{-2} * 3 \times 10^{-3} && = 3 \times 10^{-5} \\
 T * C * D &= 1/\text{year} * 3 \times 10^{-3} * 1 \times 10^{-3} && = 3 \times 10^{-6} \\
 &&& F(x) = 6.33 \times 10^{-4}
 \end{aligned}$$

where:

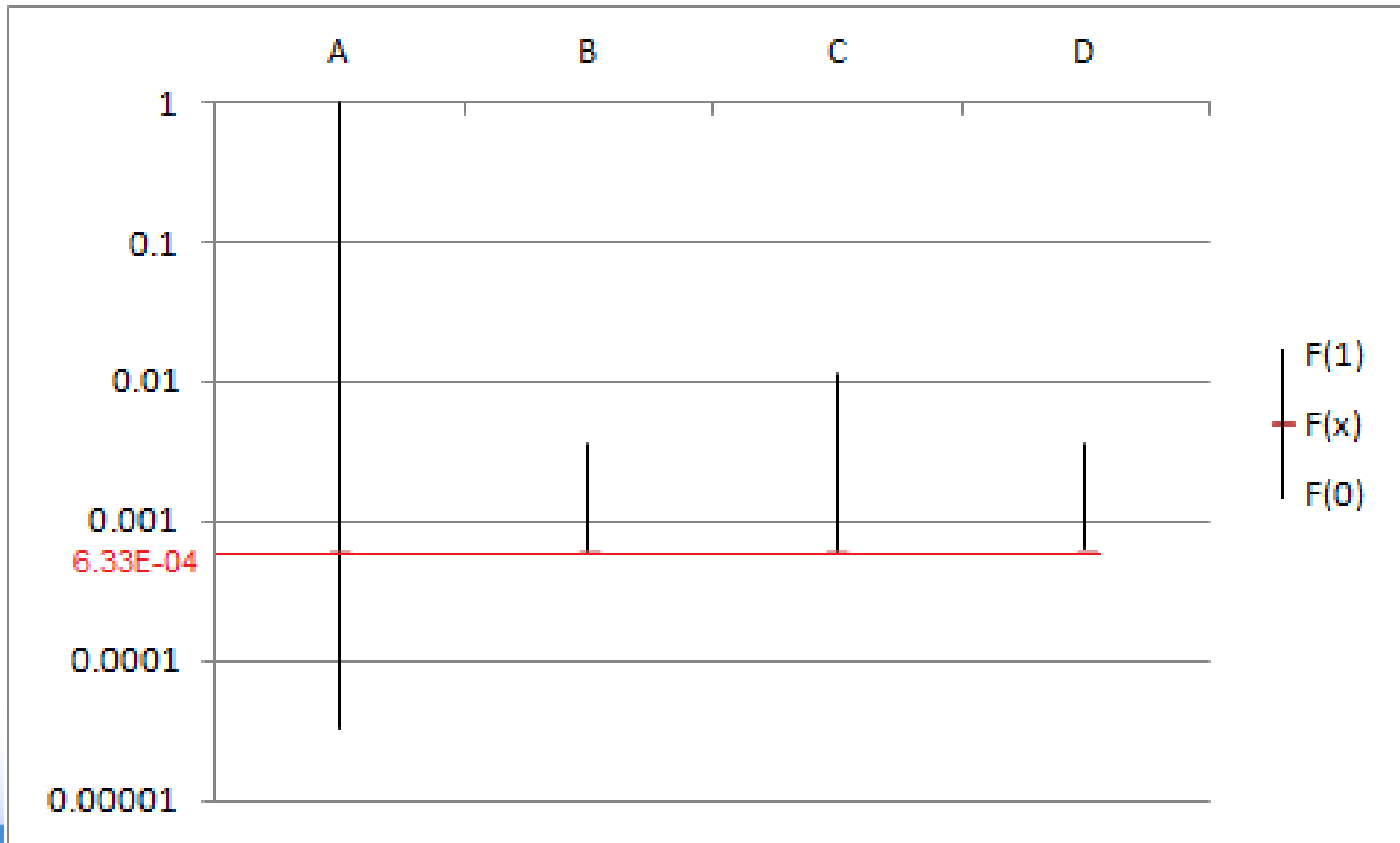
$$\begin{aligned}
 T &= 1/\text{year} \\
 A &= 6 \times 10^{-4} \\
 B &= 1 \times 10^{-2} \\
 C &= 3 \times 10^{-3} \\
 D &= 1 \times 10^{-3}
 \end{aligned}$$

- Birnbaum Importance

$$\begin{aligned}
 Bi_T &= (6.33 \times 10^{-4}) - (0) && = 6.33 \times 10^{-4} \text{ (caution interpreting } Bi \text{ for IEs)} \\
 Bi_A &= (1.0) - (3.3 \times 10^{-5}) && = 1.0 \\
 Bi_B &= (3.603 \times 10^{-3}) - (6.03 \times 10^{-4}) && = 3.0 \times 10^{-3} \\
 Bi_C &= (1.16 \times 10^{-2}) - (6.00 \times 10^{-4}) && = 1.1 \times 10^{-2} \\
 Bi_D &= (3.63 \times 10^{-3}) - (6.30 \times 10^{-4}) && = 3.0 \times 10^{-3}
 \end{aligned}$$

Birnbaum Importance Example

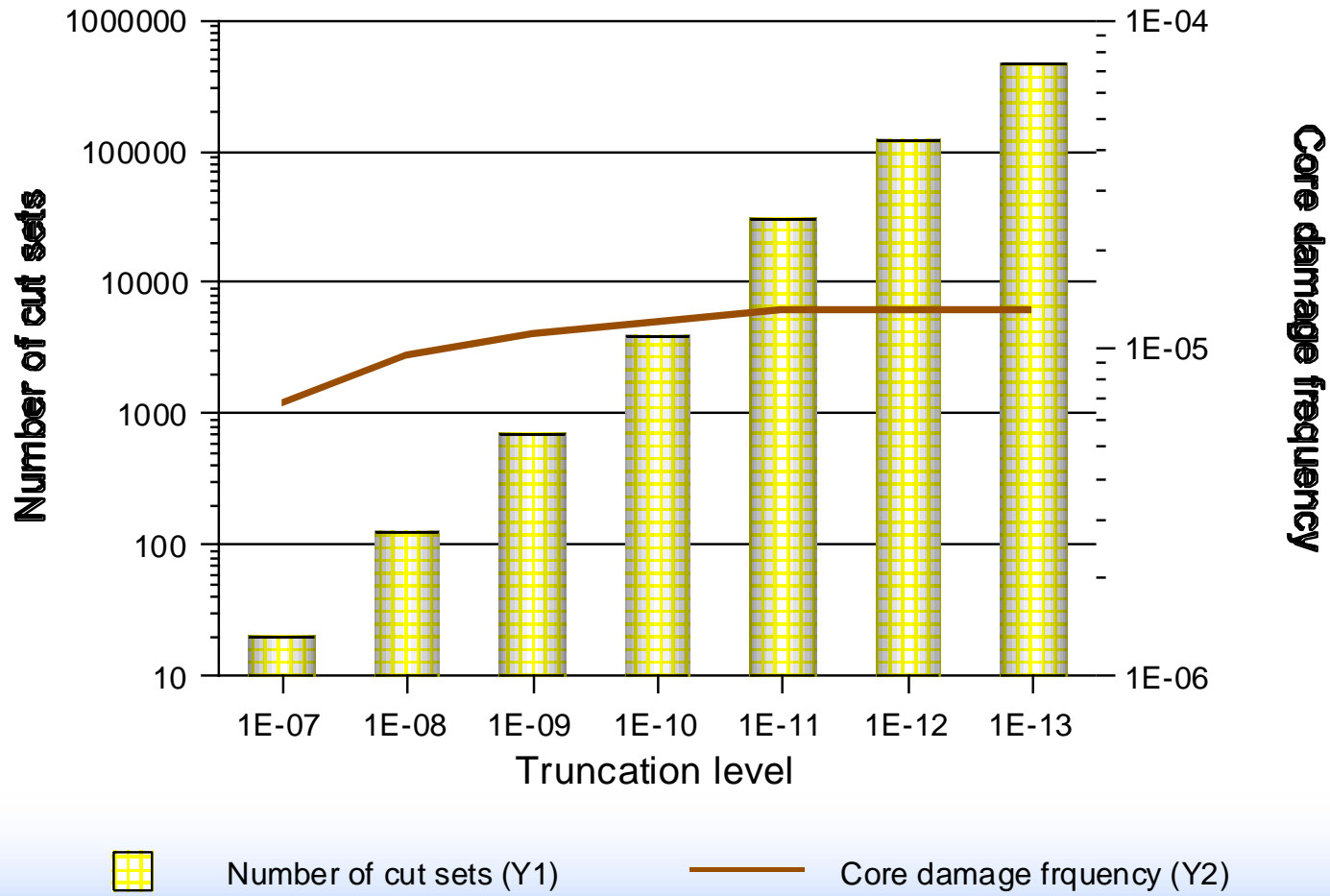
Plot of component's Birnbaums



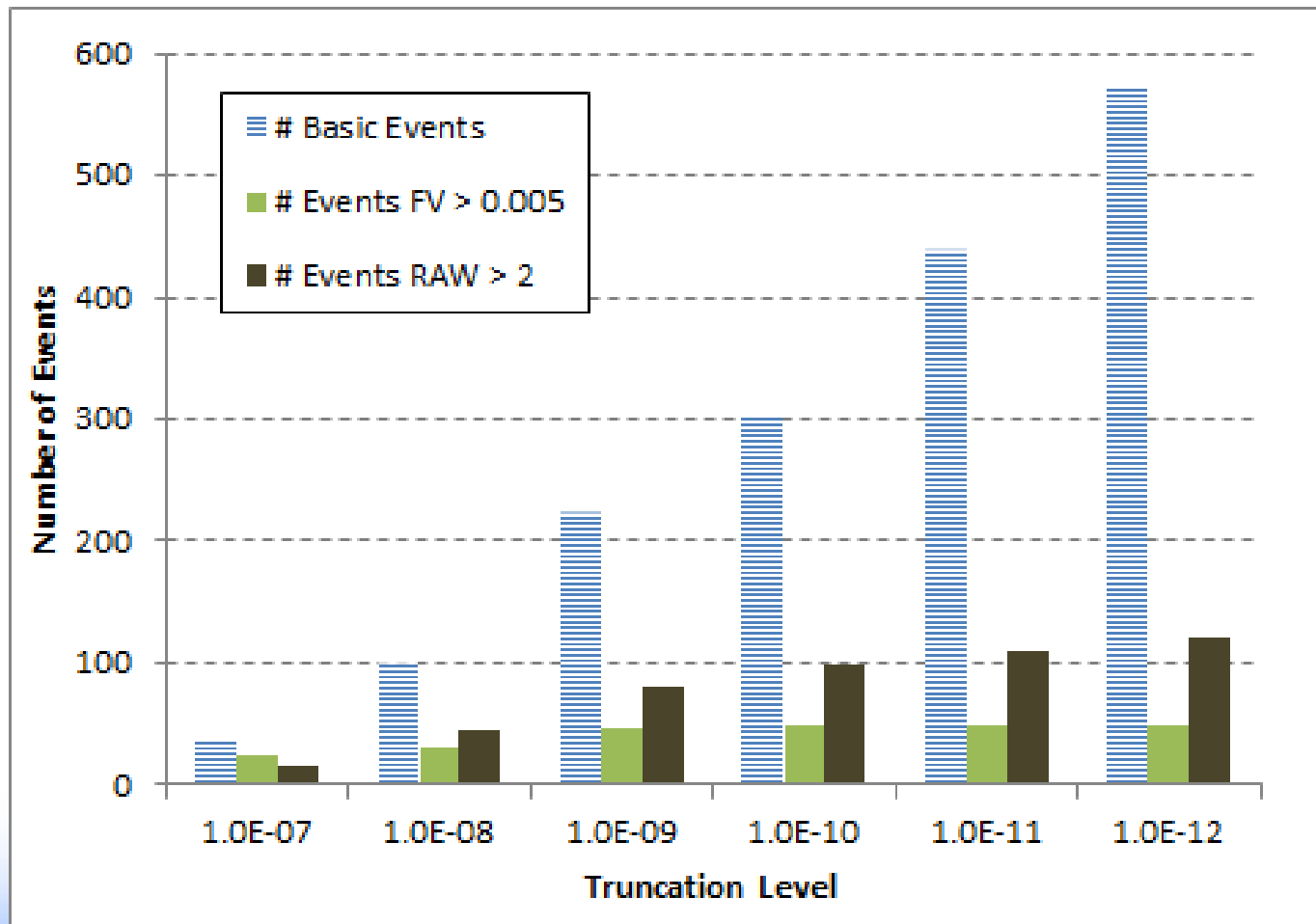
Limitations of Risk Importance Measures

- **Numerical values for the importance measures can be in suspect due to:**
 - **Exclusion of equipment or operator actions from PRA model**
 - **Parameter values used for other basic events in model (masking importance)**
 - **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 (SPAR PWR model)



Example PWR SPAR Model Importance Measures

Highlight Sequence → Right Click → View Cut Sets

Point Est.	F-V	RIR	RRR	BB	Rll	RRI	Unc (Std. Dev)	
								Data
								Plot
								Report
	Name	Count	Prob.	FV	RIR	RRR	Birnbaum	Description
<input checked="" type="checkbox"/>	ACP-BAC-LP-1AA02	1	9.60E-06	7.51E-07	1.08E+00	1.00E+00	3.00E-06	4160 VAC BUS 1AA02 FAILS
<input checked="" type="checkbox"/>	ACP-BAC-LP-1AB15	1	9.60E-06	7.51E-07	1.08E+00	1.00E+00	3.00E-06	480 VAC BUS 1AB15 FAILS
<input checked="" type="checkbox"/>	ACP-BAC-LP-1BA03	1	9.60E-06	7.51E-07	1.08E+00	1.00E+00	3.00E-06	4160 VAC BUS 1BA03 IS UNAVAILABLE
<input checked="" type="checkbox"/>	ACP-BAC-LP-1BB16	1	9.60E-06	7.51E-07	1.08E+00	1.00E+00	3.00E-06	480 VAC BUS 1BB16 FAILS
<input checked="" type="checkbox"/>	ACP-CRB-CO-1BA0...	1	3.60E-06	2.82E-07	1.08E+00	1.00E+00	3.00E-06	CIRCUIT BREAKER 1BA0309 FAILS OPEN
<input checked="" type="checkbox"/>	ACP-CRB-CO-1BB1...	1	3.60E-06	2.82E-07	1.08E+00	1.00E+00	3.00E-06	CIRCUIT BREAKER 1BB1601 FAILS OPEN
<input checked="" type="checkbox"/>	ACP-CRB-CO-AA210	1	3.60E-06	2.82E-07	1.08E+00	1.00E+00	3.00E-06	CIRCUIT BREAKER AA210 FAILS OPEN
			3.60E-06	2.82E-07	1.08E+00			
			2.16E-05	3.62E-06	1.17E+00			AB1...
			2.16E-05	3.62E-06	1.17E+00			BB1...
<input checked="" type="checkbox"/>	ACP-XHE-XM-REC4...	16	1.00E+00	2.45E-01	1.00E+00	1.32E+00	9.38E-06	FAILURE TO RESTORE 4160V BUS WITHIN 4 H...
<input checked="" type="checkbox"/>	AFW-MDP-CF-START	1	8.25E-05	3.62E-07	1.00E+00	1.00E+00	1.68E-07	CCF OF AFW MDPS TO START
<input checked="" type="checkbox"/>	AFW-MDP-FR-4002	1	5.38E-04	1.26E-02	2.44E+01	1.01E+00	8.99E-04	AFW MOTOR-DRIVEN PUMP P4-4002 FAILS T...
<input checked="" type="checkbox"/>	AFW-MDP-FS-4002	1	1.50E-03	3.52E-02	2.44E+01	1.04E+00	8.99E-04	AFW MOTOR-DRIVEN PUMP P4-4002 FAILS T...
<input checked="" type="checkbox"/>	AFW-MDP-TM-4002	4	4.00E-03	1.09E-01	2.77E+01	1.12E+00	1.03E-03	AFW MDP P4-4002 UNAVAILABLE DUE TO TE...
<input checked="" type="checkbox"/>	AFW-MOV-OO-FV5...	1	1.00E-03	2.35E-02	2.44E+01	1.02E+00	8.99E-04	FAILURE OF AFW MDP B MINFLOW MOV 5154...
<input checked="" type="checkbox"/>	AFW-TDP-FR-4001	1	4.10E-03	3.85E-03	1.93E+00	1.00E+00	3.60E-05	TURBINE DRIVEN FEED PUMP P4-001 FAILS T...
<input checked="" type="checkbox"/>	AFW-TDP-FS-4001	2	7.00E-03	6.57E-03	1.93E+00	1.01E+00	3.60E-05	TURBINE DRIVEN FEED PUMP P4-001 FAILS T...
<input checked="" type="checkbox"/>	AFW-TDP-TM-4001	1	5.00E-03	4.69E-03	1.93E+00	1.00E+00	3.60E-05	AFW TDP PUMP P4-001 IS IN TEST OR MAINT...
<input checked="" type="checkbox"/>	AFW-XHE-XM-MAN...	3	4.00E-03	4.10E-06	1.00E+00	1.00E+00	3.93E-08	OPERATOR FAILS TO MANUALLY INITIATE AFW
<input checked="" type="checkbox"/>	AFW-XHE-XM-TDPB...	4	1.00E-01	1.65E-01	2.48E+00	1.20E+00	6.32E-05	OPERATOR FAILS TO CONTROL AFW TDP AF...
<input checked="" type="checkbox"/>	CCW-HTX-CF-ALL	1	1.35E-06	2.11E-05	1.66E+01	1.00E+00	6.00E-04	COMMON CAUSE FAILURE OF CCW HEAT EXC...
<input checked="" type="checkbox"/>	CCW-HTX-PG-001	3	1.44E-05	1.74E-06	1.12E+00	1.00E+00	4.61E-06	CCW LOOP A HEAT EXCHANGER CCW-HXA IS...

Sorted by Name

Click Header to Resort



Limitations of Risk Importance Measures (cont.)

- **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 (unless just looking at FV)
- **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 should not 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 a train may have low rankings (i.e., importance measure values do not add)**
 - **Other types of measures (e.g., Differential Importance Measure, or DIM) have been designed to be aggregated if needed**

NRC Technical Guidance for Inspection Programs

- NRC Inspection Manual, Part 9900, provides technical guidance on use of probabilistic risk ranking Information
 - Some key points to consider:
 - Use of PRA is effective in identifying and ranking risk-significant SSCs to prioritize inspection activities
 - SSCs with highest rankings normally warrant greater concentration of inspection resources
 - Risk reduction, FV, and risk increase measures convey fundamentally different information regarding a SSC's importance to plant risk
 - Thus, no single measure should be used as the sole indicator
 - Risk reduction and FV measures **overall contribution to risk**
 - RAW measures risk impact of component **out-of-service**

NRC Technical Guidance for Inspection Programs (Cont.)

- **Be aware that risk ranking results will change when plant configuration and/or system lineup is not the same as that assumed during original ranking**
- **Assumptions should not be made that non-modeled SSCs, initiators, or plant operating modes are not important to risk**
- **Adequacy of the model for decision-making is important**
- **Scope of analysis should be sufficient to incorporate all necessary SSCs to be considered**
 - **E.g., Level 1 PRA would not include SSCs for preservation of containment integrity**
- **Level of detail must be sufficient to support decisions regarding safety determinations**
 - **E.g., modeling of SSCs with respect to component boundaries**

NRC Technical Guidance for Inspection Programs (Cont.)

- **Overall quality of the PRA must be adequate to support quantitative decisions**
 - **E.g., PRA should be based on realistic, best estimate assumptions and data**
 - **Conservative assumptions can elevate importance of certain SSCs and mask importance of others**
 - **Importance measures are a “relative ranking” process**
- **An appreciation of the uncertainty of PRA results provides a better understanding of the results including their precision and limitations**

***** Exercise *****

- **From your SPAR model or IPE:**
 - **What are the most risk significant items (approximately top five) to CDF from a Fussell-Vesely/Risk Reduction point of view?**
 - **What are the most risk significant items (approximately top five) to CDF from a Risk Increase/Risk Achievement Worth (RAW) point of view?**

Optional: Importance Measure Workshop

- Looking back at the ECI system minimal cut sets from Module C and assuming the probability values listed below:

$$ECI\text{-System-Failure} = T1 + V1 + PA * PB + PA * CVB + PB * CVA + CVA * CVB + MV1 * MV2 * MV3$$

Basic Event Values:

$$T1 = 1E-6$$

$$V1 = 5E-5$$

$$PA = PB = 1E-2$$

$$CVA = CVB = 1E-4$$

$$MV1 = MV2 = MV3 = 3E-3$$

$$ECI\text{-System-Failure} = T1 + V1 + PA * PB + PA * CVB + PB * CVA + CVA * CVB + MV1 * MV2 * MV3$$

$$ECI\text{-System-Failure} = (1E-6) + (5E-5) + (1E-2) * (1E-2) + (1E-2) * (1E-4) + (1E-2) * (1E-4) + (1E-4) * (1E-4) + (3E-3) * (3E-3) * (3E-3)$$

$$ECI\text{-System-Failure} = (1E-6) + (5E-5) + (1E-4) + (1E-6) + (1E-6) + (1E-8) + (2.7E-8)$$

$$ECI\text{-System-Failure} = (1.530E-4)$$

- What would the Fussell-Vesely be for basic event PA for the ECI-System cut sets?
- What would the RRR be for basic event PA for the ECI-System cut sets?
- What would the RAW be for basic event PA for the ECI-System cut sets?
- What would the Birnbaum be for basic event PA for the ECI-System cut sets?



Idaho National Laboratory

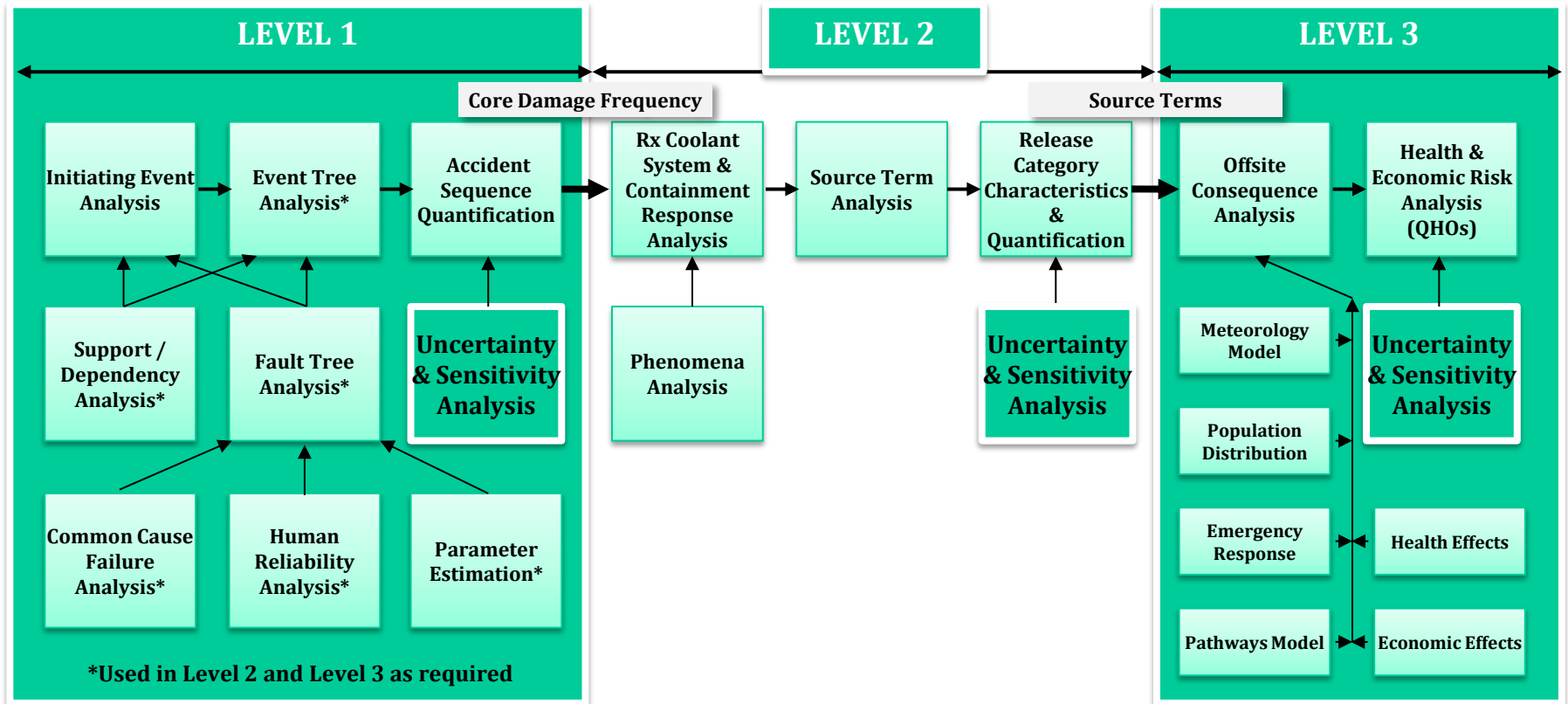
MODULE 0

UNCERTAINTY – TRADITIONAL ENGINEERING AND PROBABILISTIC

Uncertainties in PRA

- **Purpose:** To acquaint students with concept of uncertainty both from a traditional engineering and a PRA perspective. Students will understand the types of uncertainty encountered, their sources, and how they are treated
- **Objectives:** Upon completion of this module, the students;
 - Will be able to list the types of uncertainty and their sources
 - Understand how uncertainty is accounted for in PRA

Principal Steps in PRA



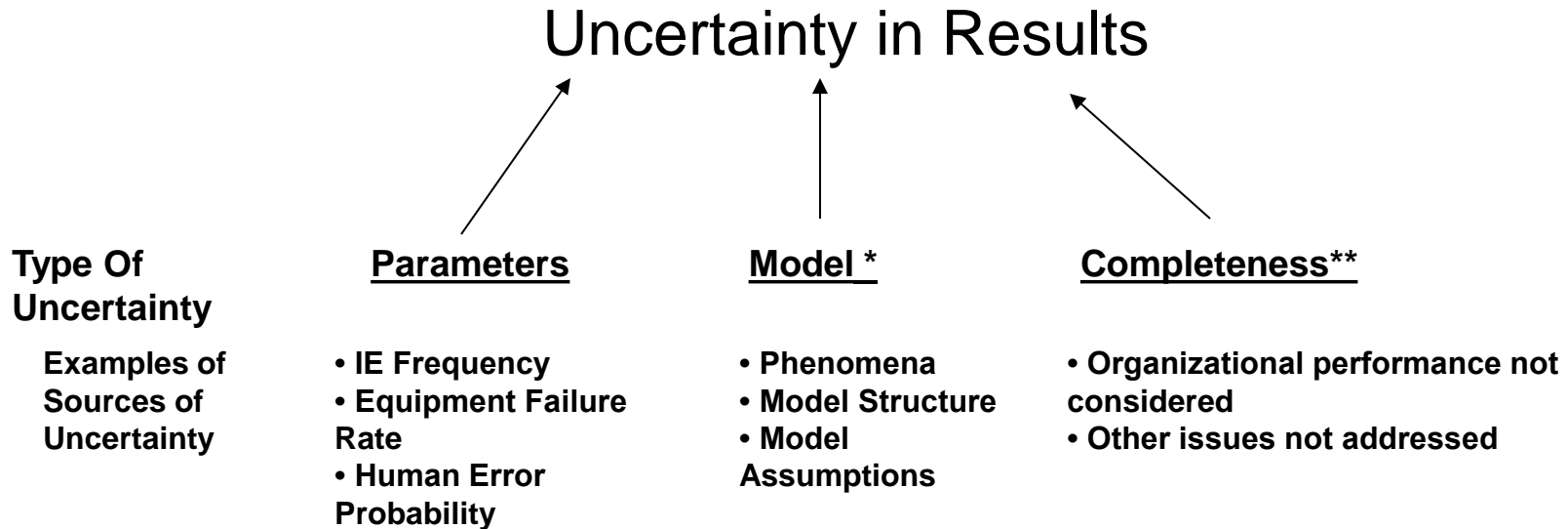
Uncertainty

- **Historically, the term "uncertainty" has been used to describe either of the following concepts**
 - **Stochastic variability in an observable quantity**
 - “1,000 hour” light bulbs do not fail exactly after 1,000 hours of use
 - **Imprecision in state-of-knowledge regarding models**
 - Their parameters
 - Their assumptions
 - How well they reflect reality

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, not all modes of operation modeled, external events not included)**

Sources of Uncertainty



* Model is approximation of reality; some models cause greater uncertainty in results than others

** Lack of completeness in models contributes to uncertainty in results

Traditional Engineering Approaches to Uncertainty

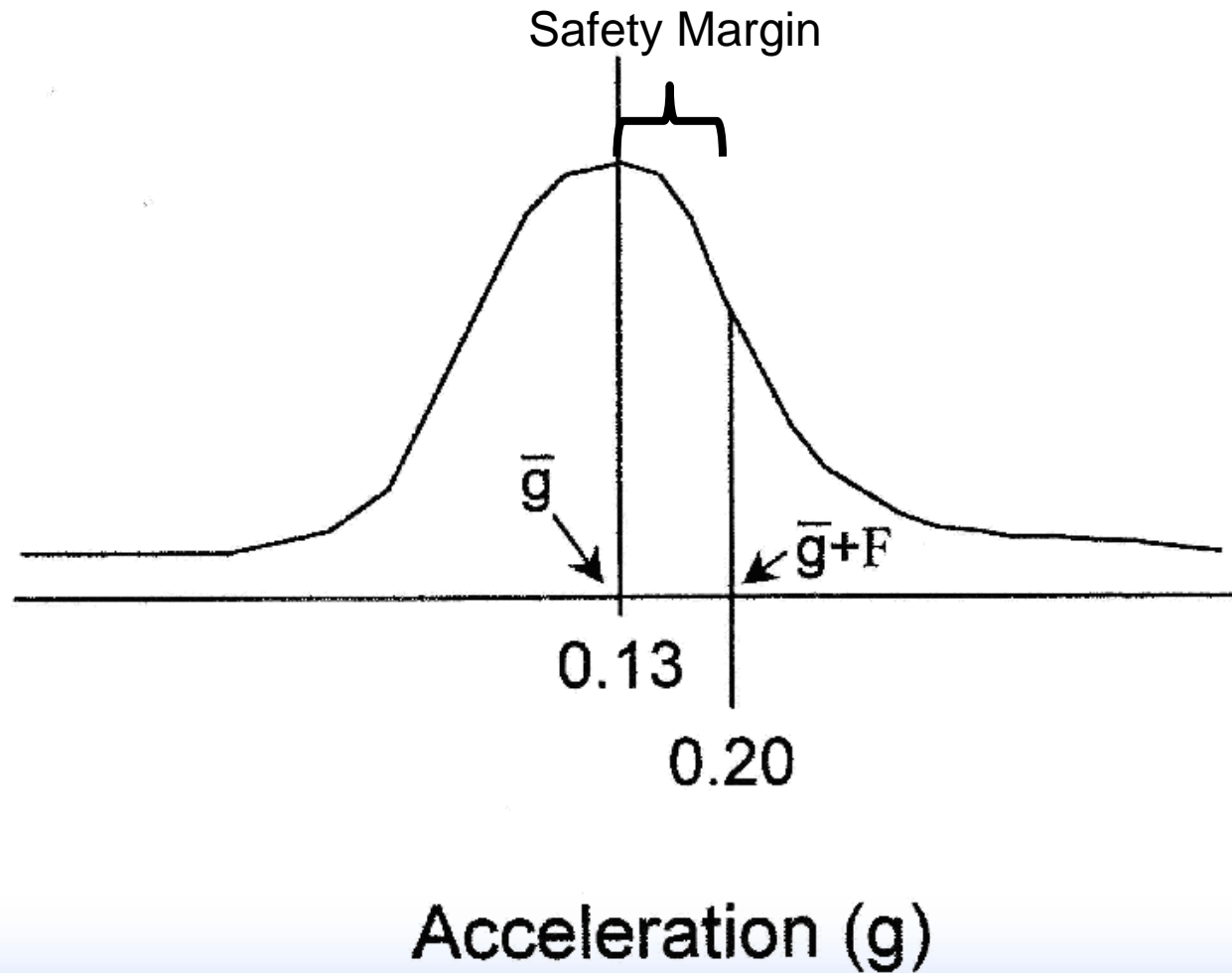
- **Traditional engineering approach involves use of defense-in-depth to establish safety margins in design basis accidents**
 - **Assumes occurrence of initiating event and single system failure**
 - **Uses conservative values for plant conditions and equipment performance to account for lack of knowledge about plant performance and phenomenological processes**

SEISMIC EXAMPLE

(Hope Creek FSAR Chapter 2)

- **Observations indicated mean value of peak horizontal acceleration is approximately 13% of gravity for recording sites where (Modified Mercalli Intensity VII) damage was sustained**
- **..on the basis of the above relationships, it is recommended that the design acceleration for Hope Creek be considered as 20% of gravity at foundation level**
- **This value is considered conservative**
 - **Equivalent to the ground motion of the mean + one standard deviation for recording sites where MMI VII damage was sustained**

Seismic Example (cont.)



ANOTHER CHAPTER 2 (SITING) EXAMPLE

- **Plume dispersion depends on time-varying parameters, limiting predictability of radionuclide concentration and position**
- **To overcome this limitation, empirically-based, conservative assumptions are made**
 - **How long atmospheric conditions exist (R.G.s 1.3 and 1.4)**
 - **For example, wind always blows toward largest population center**

THERMAL-HYDRAULIC EXAMPLE (GESSAR II Chapter 4)

- **Uncertainties in thermal-hydraulic parameters are considered in statistical analysis performed to establish fuel cladding integrity safety limit**
 - **Set limits such that at least 99.95 of fuel rods in core are **not expected** to experience boiling transition during any moderate frequency transient event**
- **... uncertainties considered and their corresponding values are shown in the following Table...**

Description of Uncertainties (GESSAR II Chapter 4)

Quantity	Std. Deviation (% of point)	Comment
Feedwater Flow	1.76	This is the largest component of total reactor power uncertainty
Feedwater Temp. Reactor Pressure	0.76 0.5	These are the other significant parameters in core power distribution
Channel Flow Area	2.5	This accounts for manufacturing and service induced variations in the free flow area within the channel
Friction Factor Multiplier	10.0	Accounts for uncertainty in the correlation representing two-phase pressure losses

PRAs Identify Two Types of Uncertainty

- **Distinction between aleatory and epistemic uncertainty:**
 - **“Aleatory”** from the Latin *alea* (dice), of or relating to 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

- **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

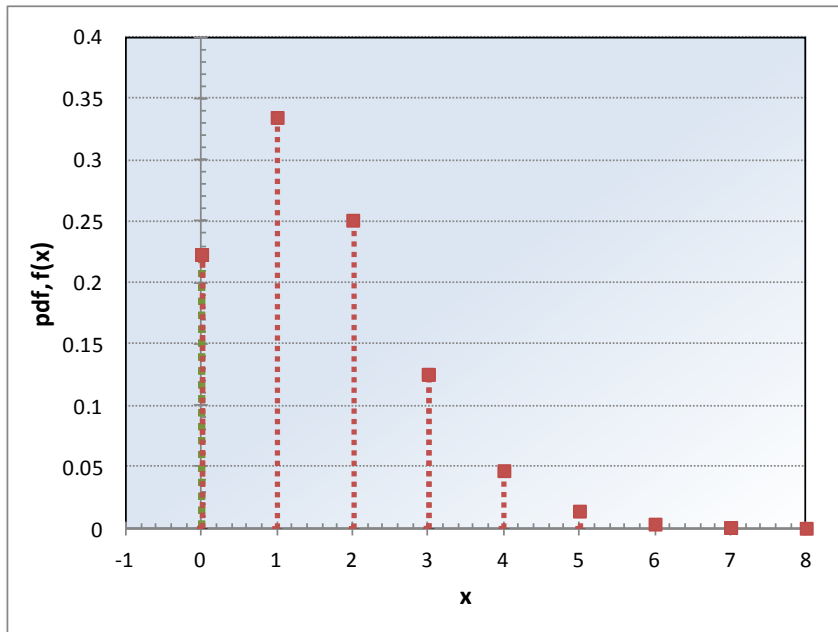
- In the Poisson model, the parameter λ is not known precisely
- Could we model uncertainty in estimate of λ using statistical confidence interval?
 - Cannot propagate confidence intervals through PRA models
 - Cannot interpret confidence intervals as probability statements about value of λ
 - Cannot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

Advantages to Bayesian Approach

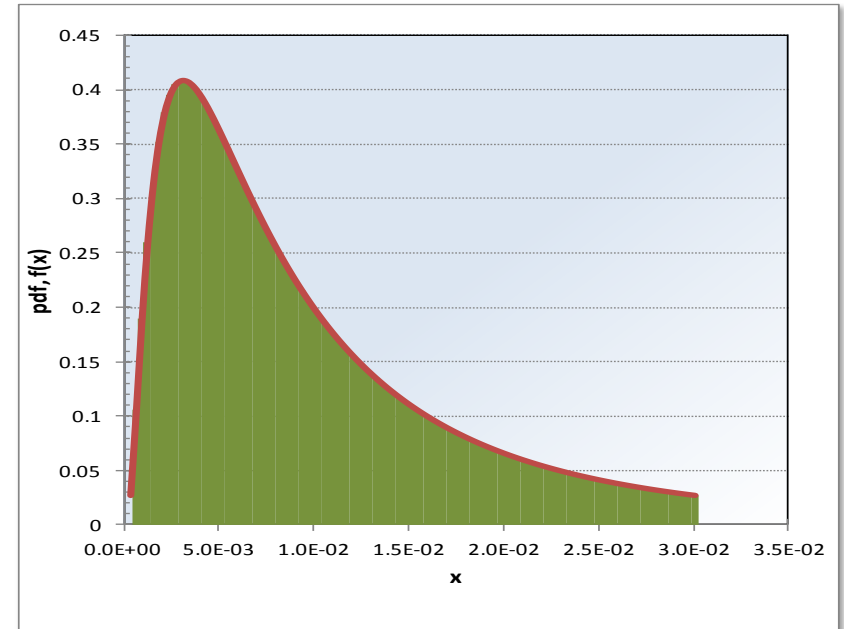
- **Allows uncertainties to be propagated easily through PRA models**
 - We describe all of our “results” as probability distributions
- **Allows probability statements to be made concerning λ and outputs that depend upon λ**
- **Provides unified, consistent framework for parameter estimation**
 - Allows 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)

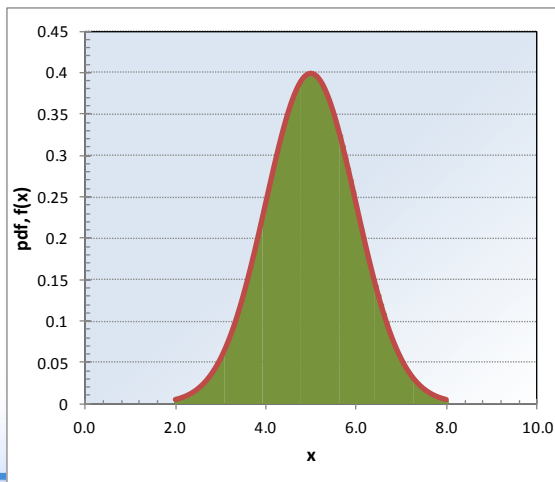


Continuous Distribution
(Lognormal with mean of 0.005)

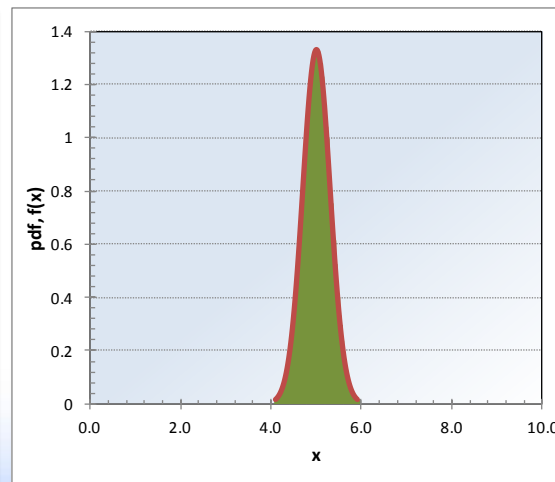
Probability Distributions Represent Uncertainty

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

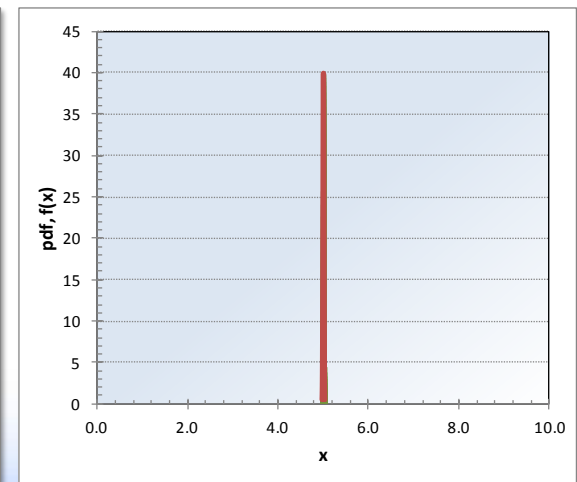
Large uncertainty



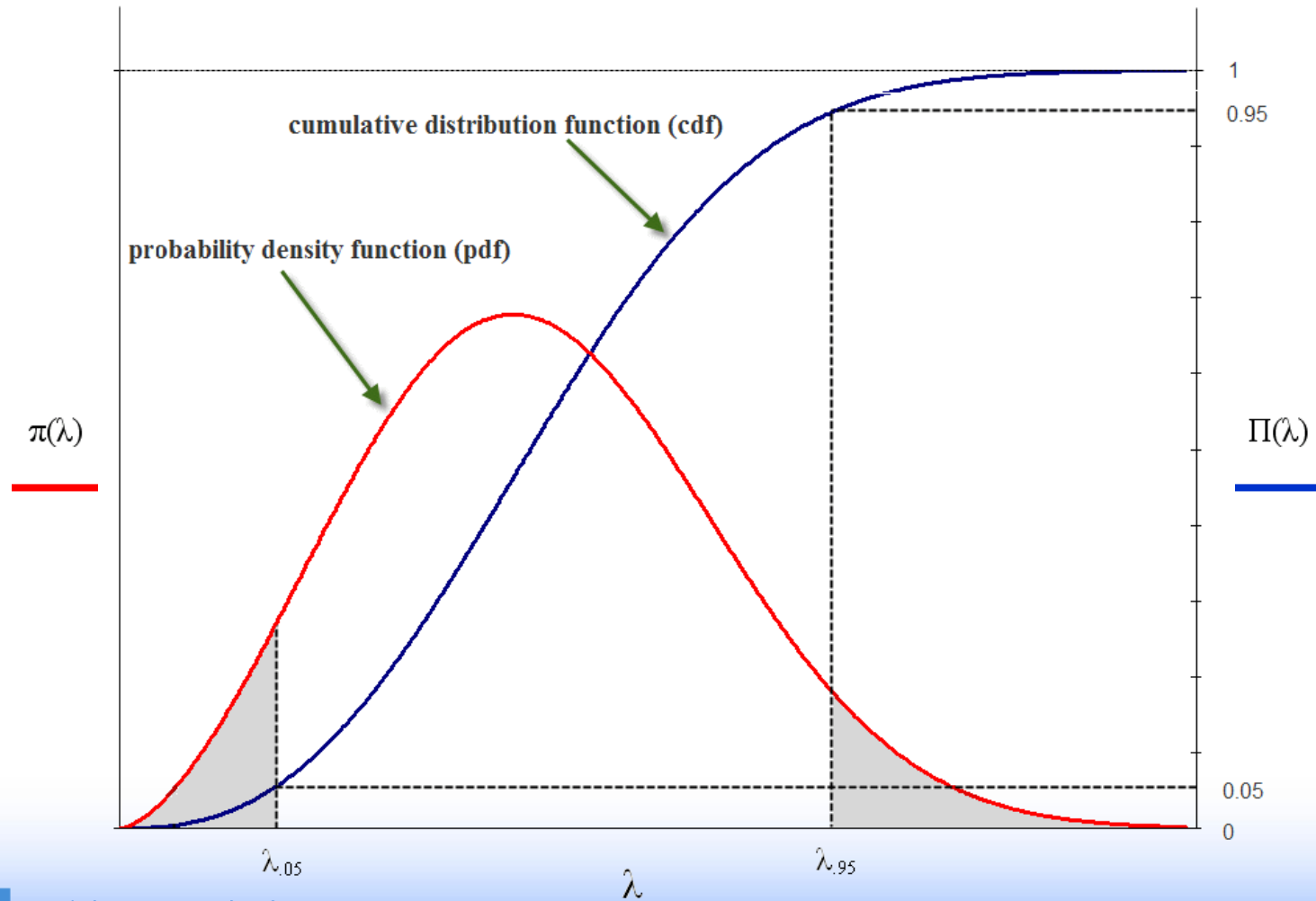
Less uncertainty



No uncertainty



Uncertainty in λ Expressed as Probability Distribution

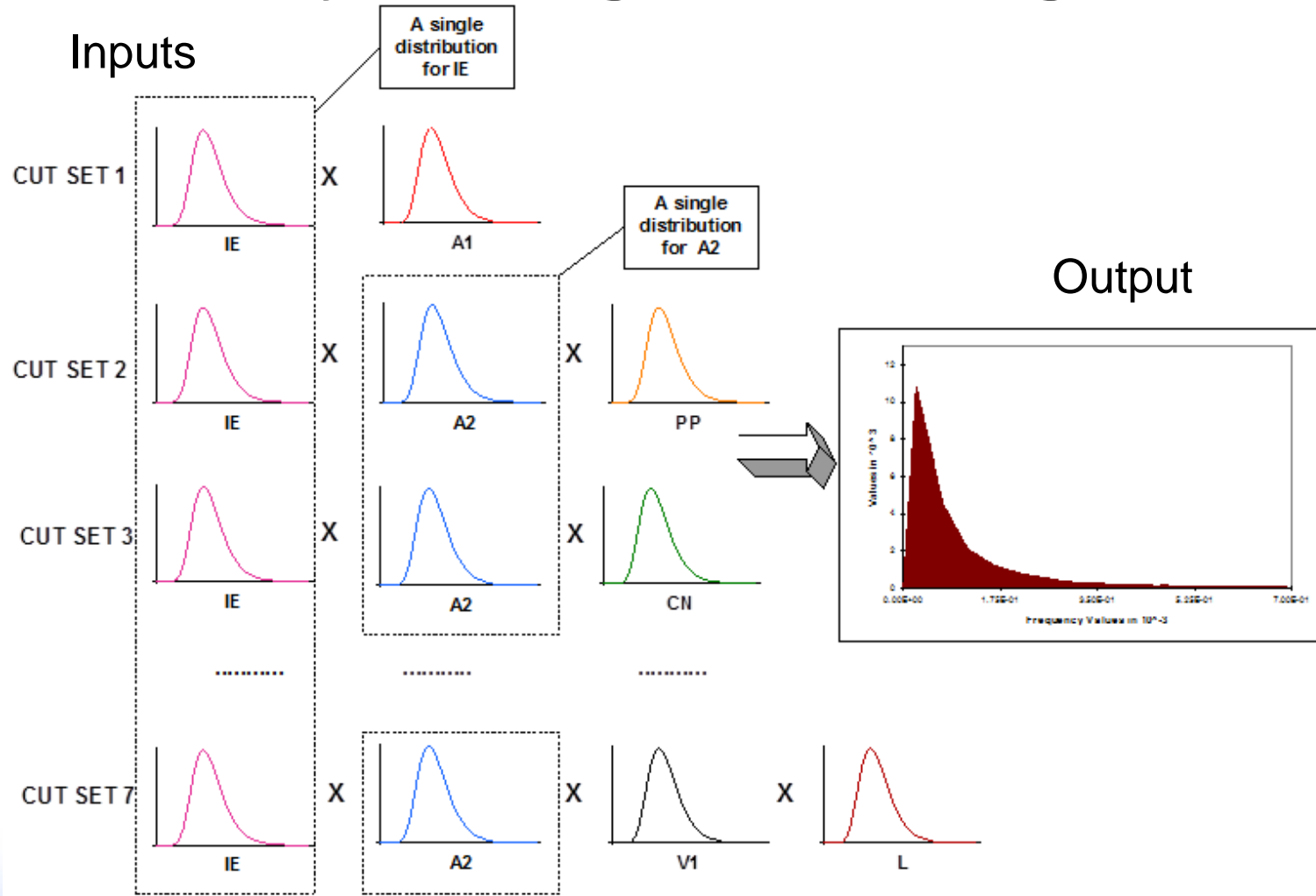


Uncertainty Propagation

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



Uncertainty Propagation through Model



Other Epistemic Uncertainties in PRA and How They are Addressed

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

Other Epistemic Uncertainties in PRA and How They are Addressed (cont.)

- **Completeness**
 - Complex errors of commission
 - Design and construction errors
 - Unexpected failure modes and system interactions
 - All modes of operation not modeled
- **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

Other Epistemic Uncertainties in PRA and How They are Addressed (cont.)

- **Errors in analysis**
 - Failure to model all trains of a system
 - Data input errors
 - Analysis errors
- **Errors in analysis may be difficult to catch and are typically addressed through peer review and validation process**
 - QA and the use of the PRA model by a community of analysts helps to find (and weed-out) errors

Uncertainty Identification

- **Tools and Techniques for identifying uncertainty**
 - Questioning attitude required to identify uncertainties
 - Comparisons between model predictions and “reality”
 - Do the results make logical sense
 - Quantitative methods
 - Uncertainty propagation through a model
 - Predictive models
 - Critical thinking

e.g., Separating “knowns” from assumptions



“Information Theory, Inference, and Learning Algorithms” D. MacKay



Idaho National Laboratory

MODULE P

**PLANT-SPECIFIC, RISK-INFORMED
APPLICATIONS**

Introduction to Risk-Informed Regulation

- **Purpose:** Students will be introduced to the NRC PRA Policy Statement, Risk-Informed and Performance-Based Plan (RPP), concepts of risk-informed regulation, potential PRA applications, the principal steps in making risk-informed regulatory decisions, including the acceptance guidance contained in the Standard Review Plans (SRP).
- **Objectives:**
 - Understand the NRC PRA Policy Statement
 - Understand Risk-Informed and Performance-Based Plan
 - Understand general concepts of risk-informed regulation
 - List potential PRA applications
 - List the major elements of the decision logic used to review submittals containing changes to the current licensing basis and the role of the new Regulatory Guides and SRPs in this process, including the numerical decision criteria related to CDF and LERF

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

- 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 (RIRIP)**

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

- **Name changed from (RIRIP) to the Risk-Informed and Performance-Based Plan (RPP) (April 26, 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**
 - Increased use by NASA; relied largely on FMEAs before Challenger
- **Chernobyl accident**
 - Increased 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**

Risk-Informed Regulatory Guides and SRPs

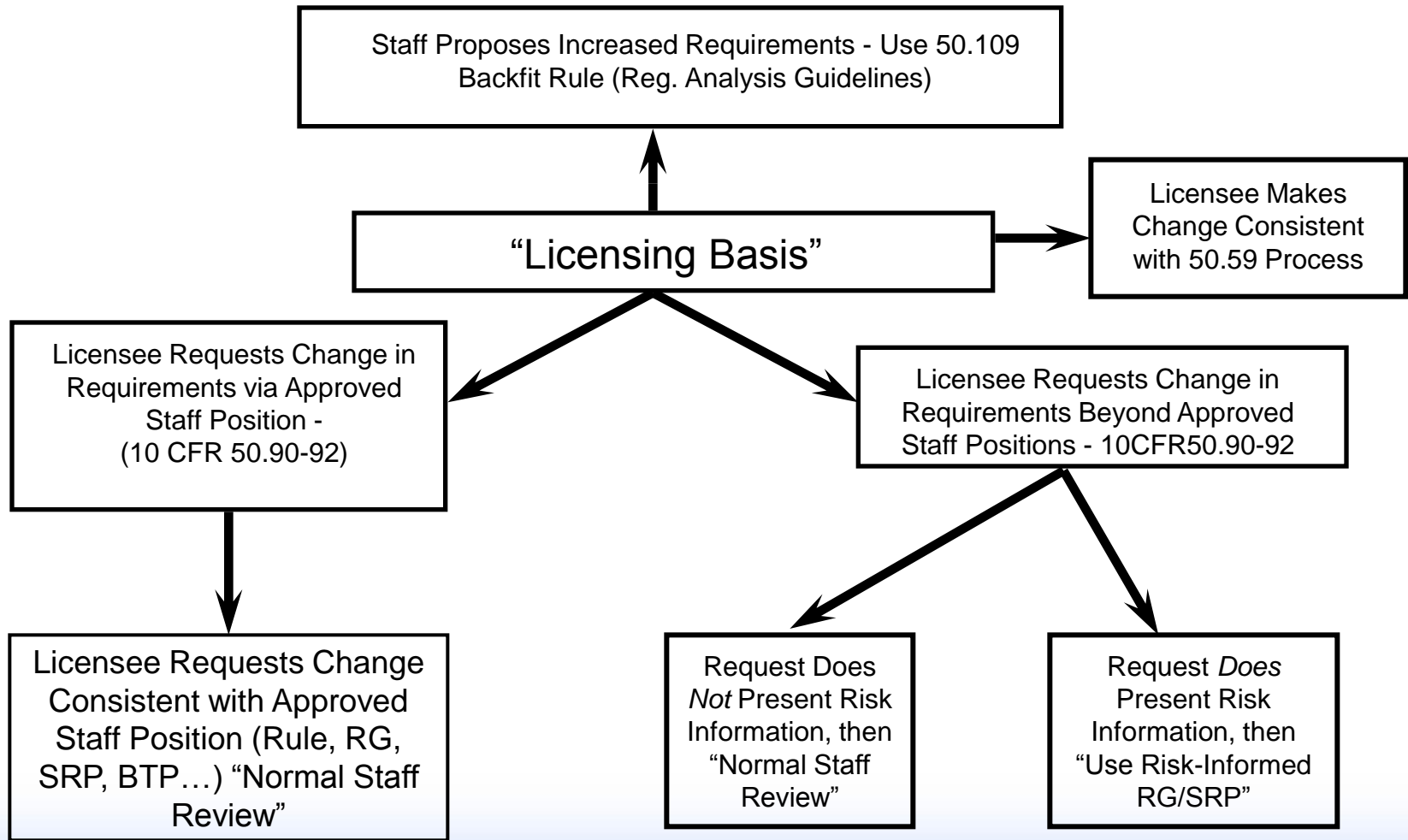
Regulatory Guide

- **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**

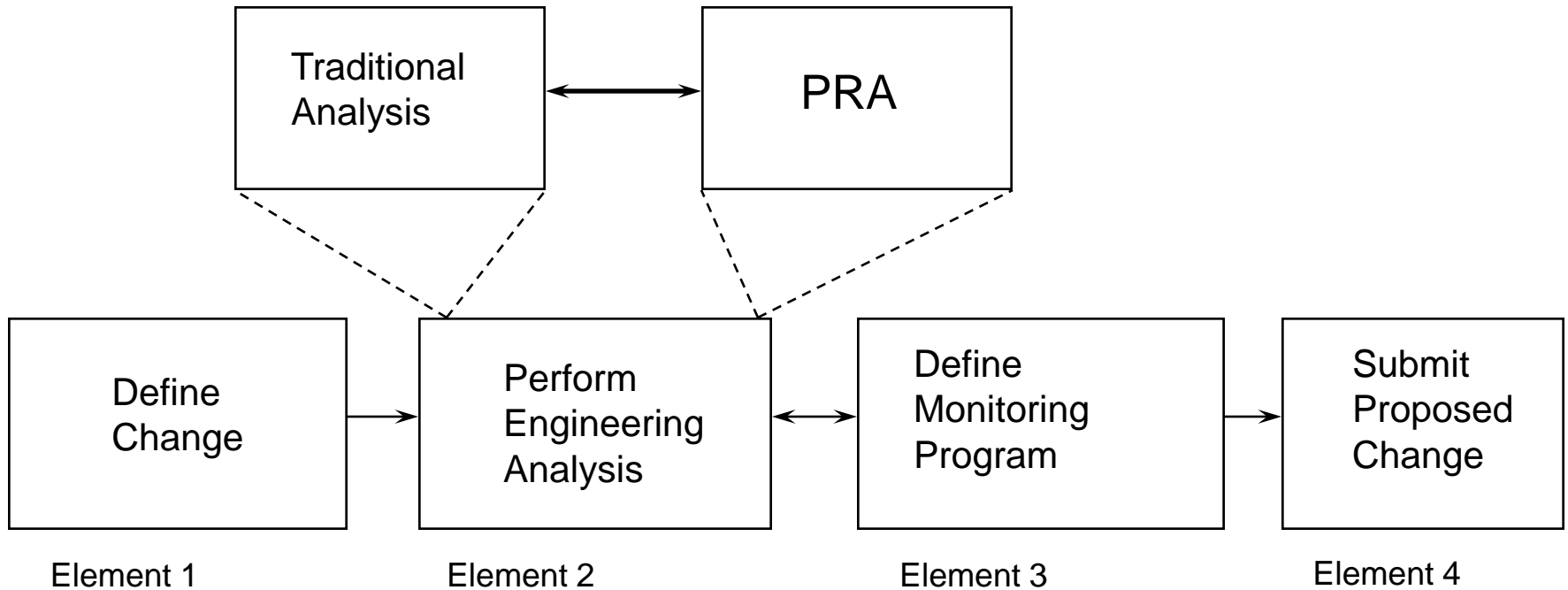
Standard Review Plan

- **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



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)

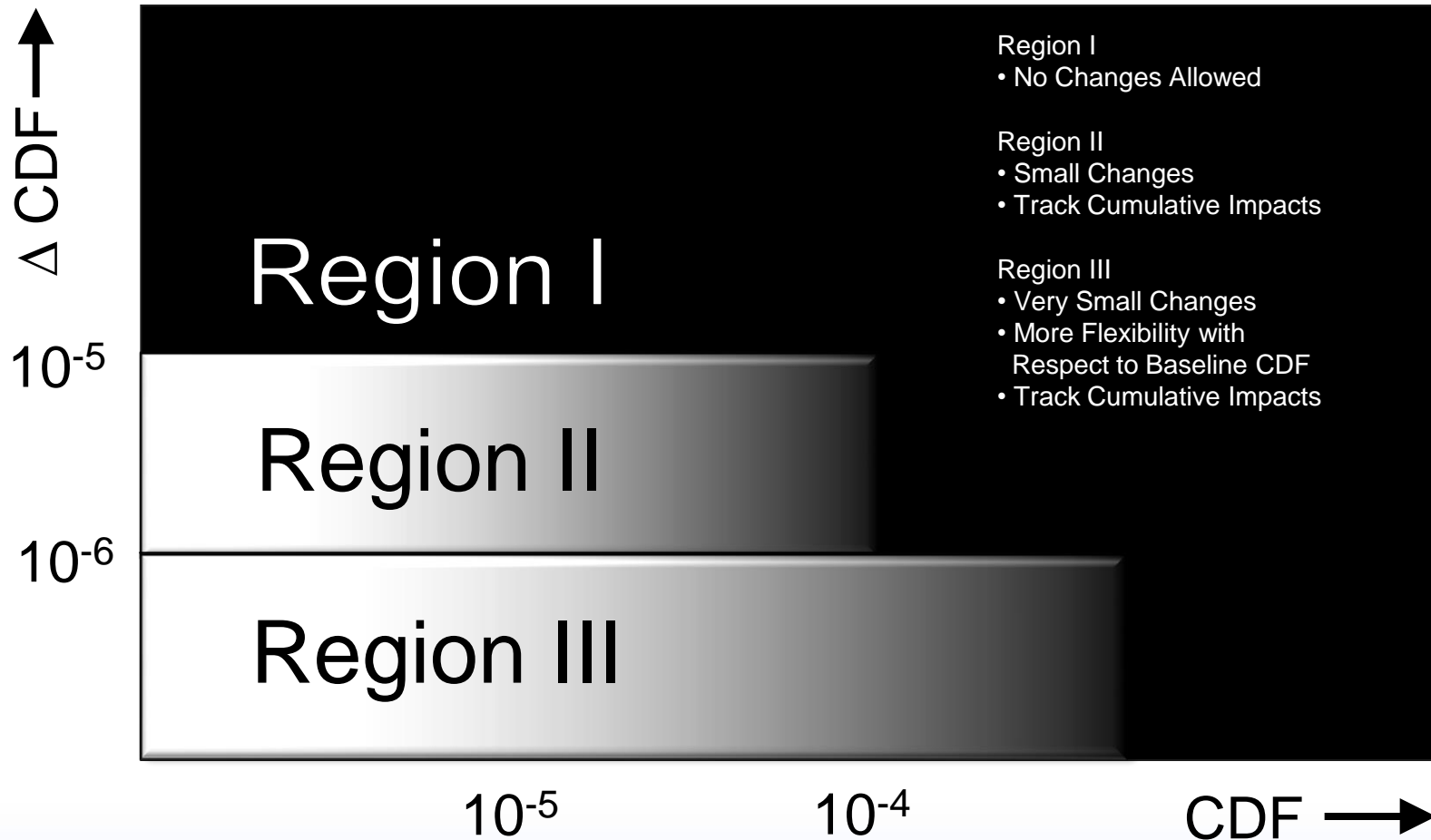


Figure 3. Acceptance Guidelines for Core Damage Frequency (CDF)

Mean Large Early Release Frequency Acceptance Guidelines (RG 1.174)

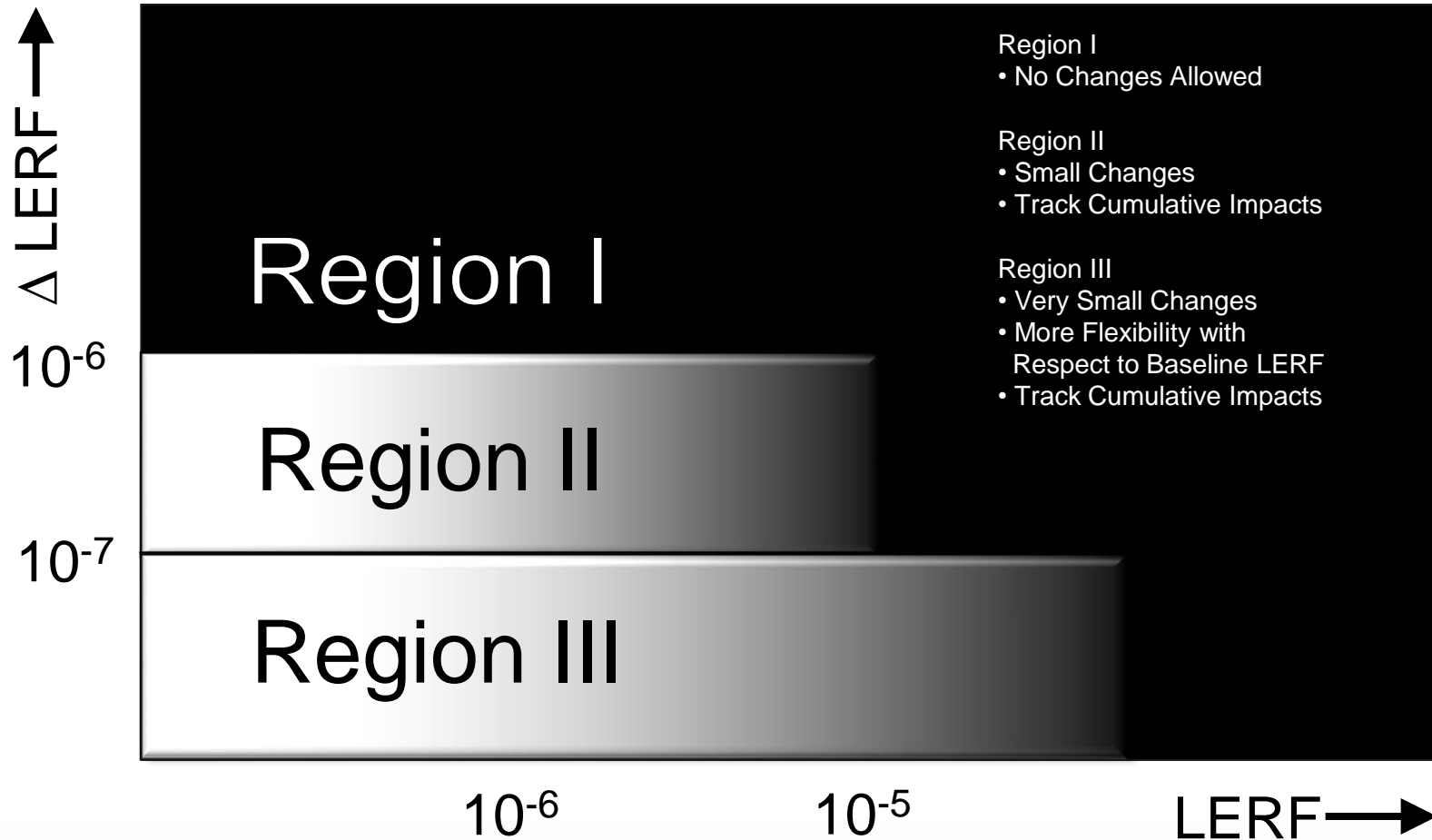


Figure 4. Acceptance Guidelines for Large Early Release Frequency (LERF)

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**



Idaho National Laboratory

MODULE Q

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:**
 - Explain why base case or nominal PRA results cannot be used for maintenance planning
 - Explain what is meant by “configuration risk management” and how it related to risk-informed regulation
 - Evaluate “risk” profiles quantitatively
- **References:**
 - NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications
 - Regulatory Guide 1.160 (rev. 3) - Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
 - Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, NUMARC 93-01 Rev. 4A, 2011

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 increased amounts of 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

Observed Preventive Maintenance Practices of Concern

- **Multiple components simultaneously out of service, as allowed (implicitly) by technical specifications**
- **Repeated entries into Action Statements to perform PM + long equipment downtimes**
- **Significant portions of power operations may be spent in Action Statements to carry out PMs**

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 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?**

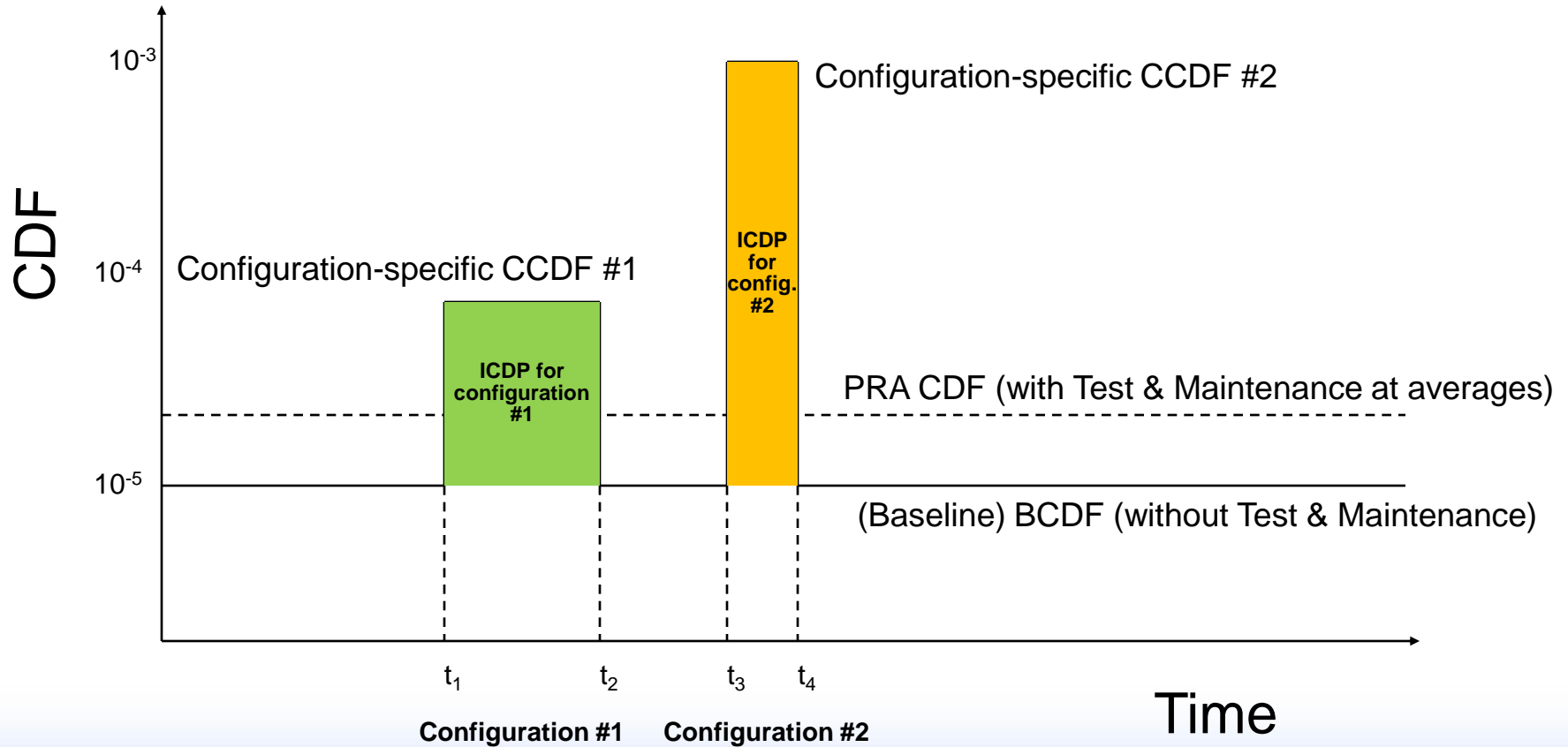
Configuration Risk Management

- **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)**

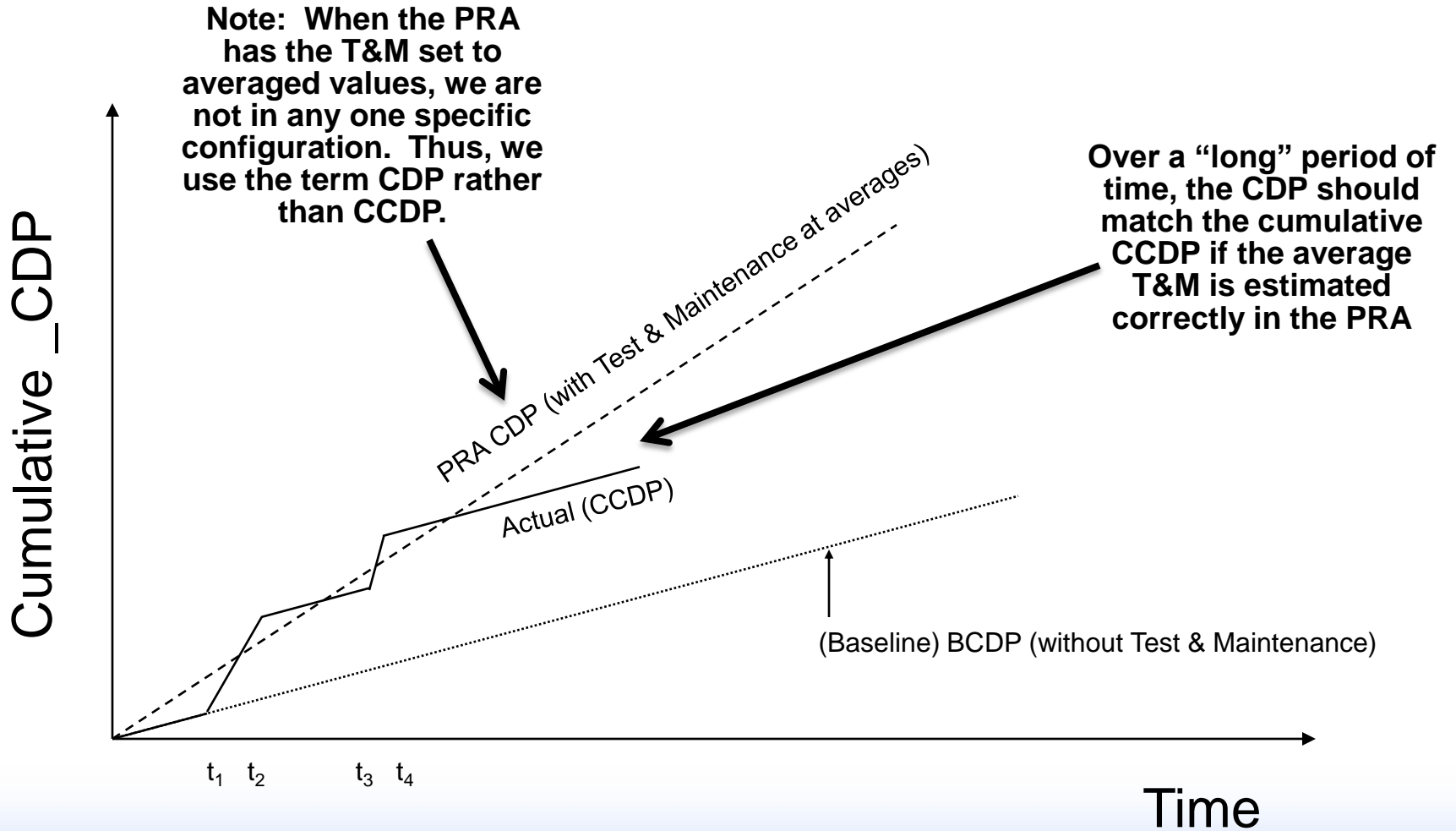
Configuration Risk Management

- 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 Δ 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)
 - $\text{ILERP} \approx \text{ILERF} * \text{duration}$
 - $\text{ILERP} = \text{CLERP} - \text{BLERP}$

Configuration CDF Profile



Cumulative CDP Profile



Configuration Risk Management

- **Includes management of:**
 - **OOS components**
 - **Instantaneous CCDF (configuration-specific CDF)**
 - **Outage time of components & systems**
 - **Configuration duration**
 - **CCDP**
 - **ICDP**
 - **Backup components**
 - **Instantaneous CCDF**
 - **Frequency of specific configuration**
 - **Cumulative CDP over time (slide Q-11)**
- (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., single permanent change to AOT acceptable if (RG 1.177):**
 - **ICDP $< 5E-7$ (called ICCDP in Reg. Guide)**
 - **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 assumes random failures of equipment (including equipment outages for testing & maintenance)**
 - Importance measures based on random, independent maintenance of components
- **PRA does not correctly 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 average risk level**
- **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 maintenance performed at shutdown
 - 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**
- **Sciencetech/NUS Safety Monitor**
 - The NRC acquired this package from Sciencetech, and has an agency-wide license covering its use
- **EPRI R&R Workstation (EOOS)**
 - 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



Risk Monitor Strengths and Limitations

- **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 Limitations

- **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 issues**
 - Effects on IE frequencies
 - Human recovery modeling
 - CCF adjustments
 - Consideration of plant features not normally modeled in PRA studies
 - Truncation limits

***** Exercise #1 *****

- **Review your SPAR model or IPE and identify component out-of-service modeling**
 - **What types of outages are modeled?**
 - **Testing**
 - **Preventive maintenance**
 - **Corrective maintenance**
 - **Any "special" events that cover multiple, simultaneous component outages?**
 - **What are the basis for the component outage probabilities?**
 - **Generic**
 - **Plant-specific**
 - **Time period covered**
 - **Sources for data collection**
 - **Definition of outage duration**

*** Exercise #2 – Preventive Maintenance Schedule Evaluation ***

- Plant X is planning preventive maintenance both on its steam-driven auxiliary feedwater (AFW) train and on one of its two diesel generators, DGB. The steam-driven AFW train preventive maintenance will require the train to be unavailable for 20 hours. The DGB preventive maintenance will require the diesel generator to be unavailable for 15 hours. The two schedules provided below are being evaluated. The Baseline CDF (without test/maintenance) is equal to $5E-6$ per year.
 - Schedule #1 maintenance activities will be performed in parallel (i.e., both preventive maintenance activities being performed within 20 total hours). The DGB and steam-driven AFW train preventive maintenance will be started at the same time, with DGB being returned to service after the first 15 hours (last 5 hours will have just the steam-driven AFW train out for maintenance). The RAW value for each maintenance configuration with respect to the Baseline CDF (w/o test/maintenance) are;
 - DGB and steam-driven AFW train out for test/maintenance - RAW = 15
 - Steam-driven AFW train out for test/maintenance - RAW = 5
 - Schedule #2 maintenance activities will be performed in series (i.e., both preventive maintenance activities being performed within 35 total hours). The DGB preventive maintenance will be performed first and then the steam-driven AFW train preventive maintenance will be performed as soon as the DGB is returned to service. The RAW value for each maintenance configuration with respect to the Baseline CDF (w/o test/maintenance) are;
 - DGB out for test/maintenance - RAW = 8
 - Steam-driven AFW train out for test/maintenance - RAW = 5

***** Exercise #2 – Preventive Maintenance Schedule Evaluation *** (cont.)**

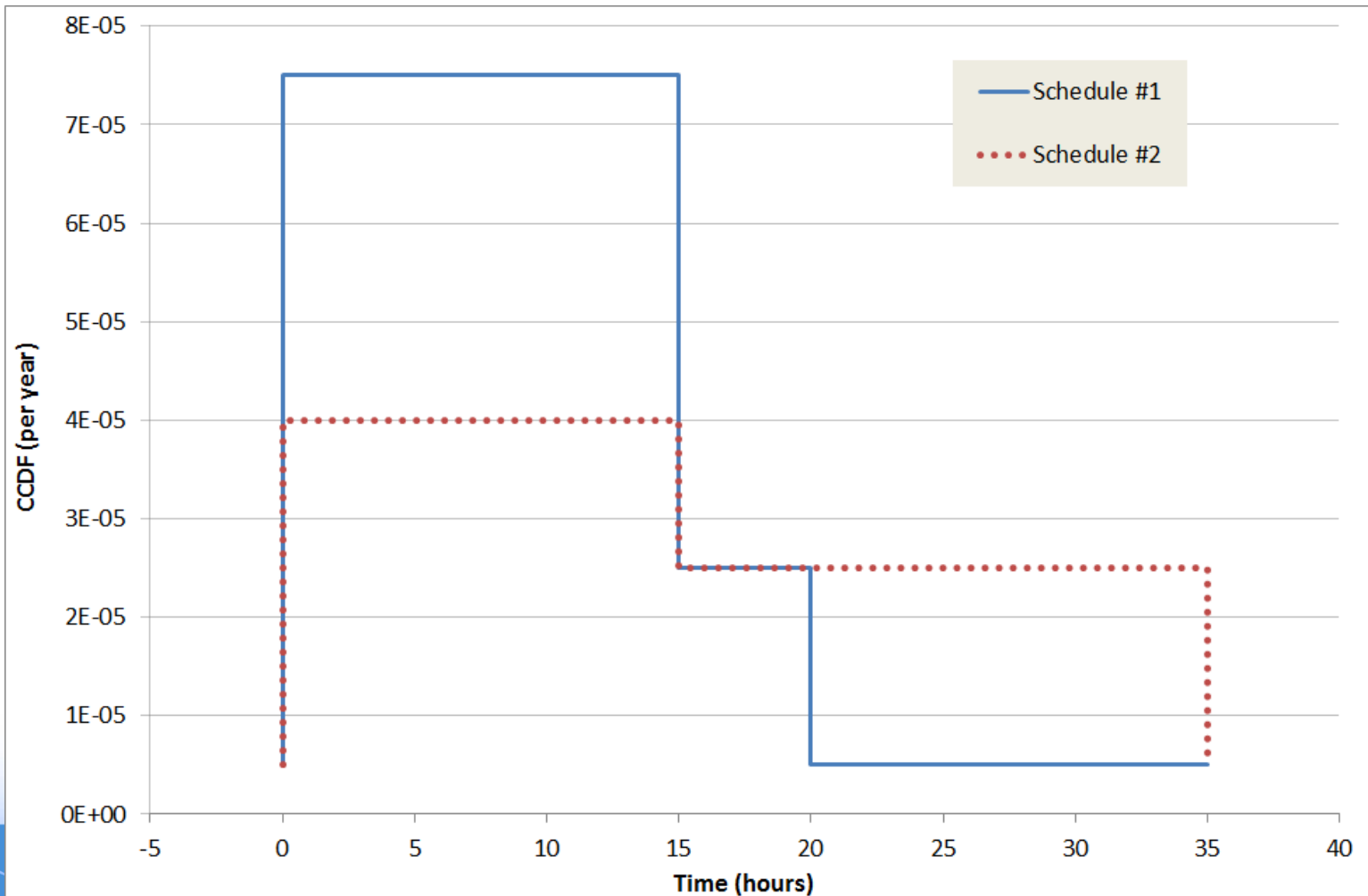
- **Draw a CDF profile for Schedule #1, indicating the Baseline CDF and Configuration-specific CDF for the configurations of this schedule.**
 - **What is the highest instantaneous CDF for Schedule #1?**
 - **What is the total incremental core damage probability (ICDP) for Schedule #1?**
- **Draw a CDF profile for Schedule #2, indicating the Baseline CDF and Configuration-specific CDF for the configurations of this schedule.**
 - **What is the highest instantaneous CDF for Schedule #2?**
 - **What is the total ICDP for Schedule #2?**
- **Based on the Configuration-specific CDF and ICDP results for the two schedules, which schedule appears to be better for performing the preventive maintenance on the DGB and steam-driven AFW train? Why?**

Schedule #1 Workspace

Schedule #2 Workspace

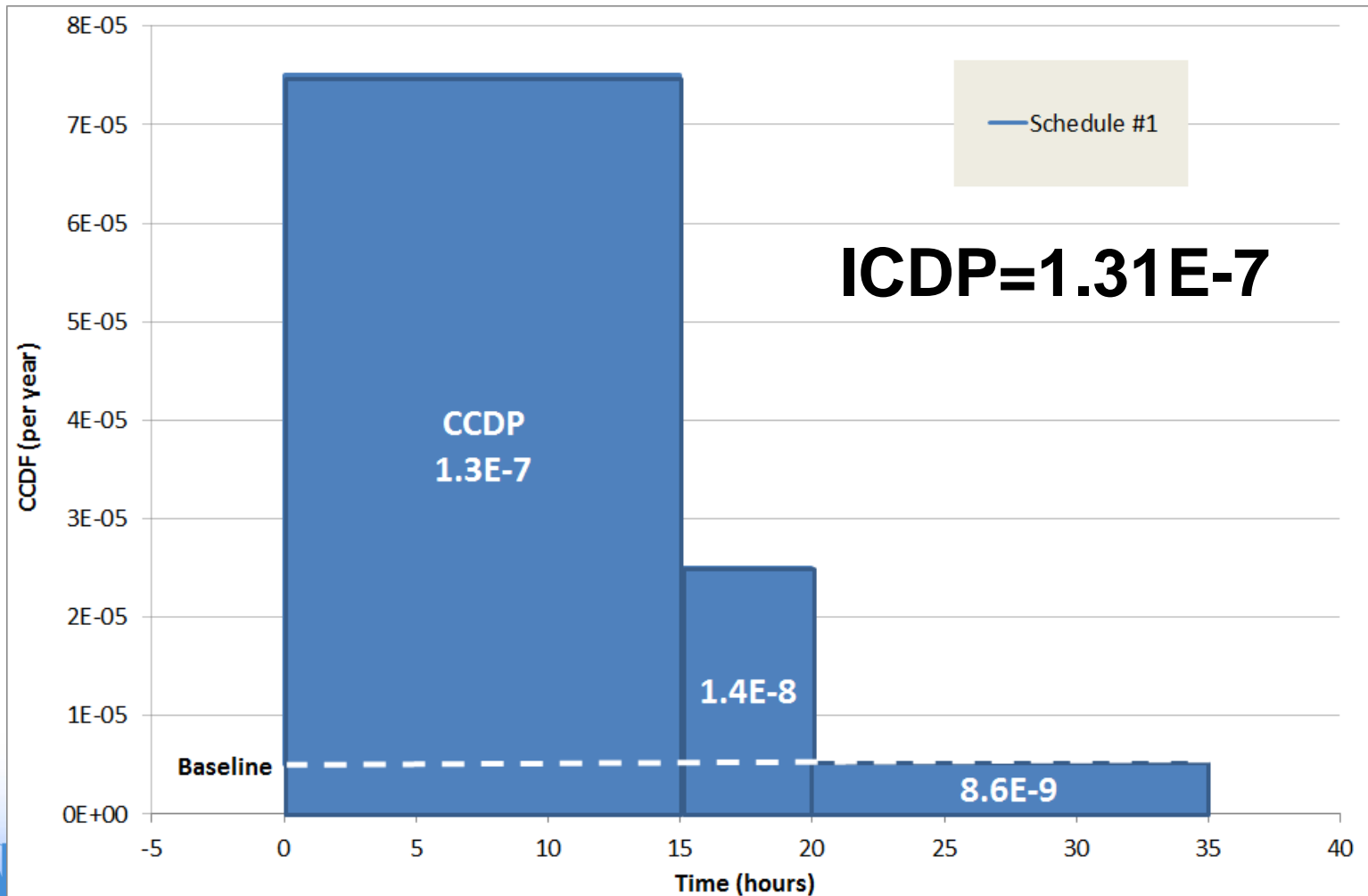
Answers to Exercise #2

CDF risk profile



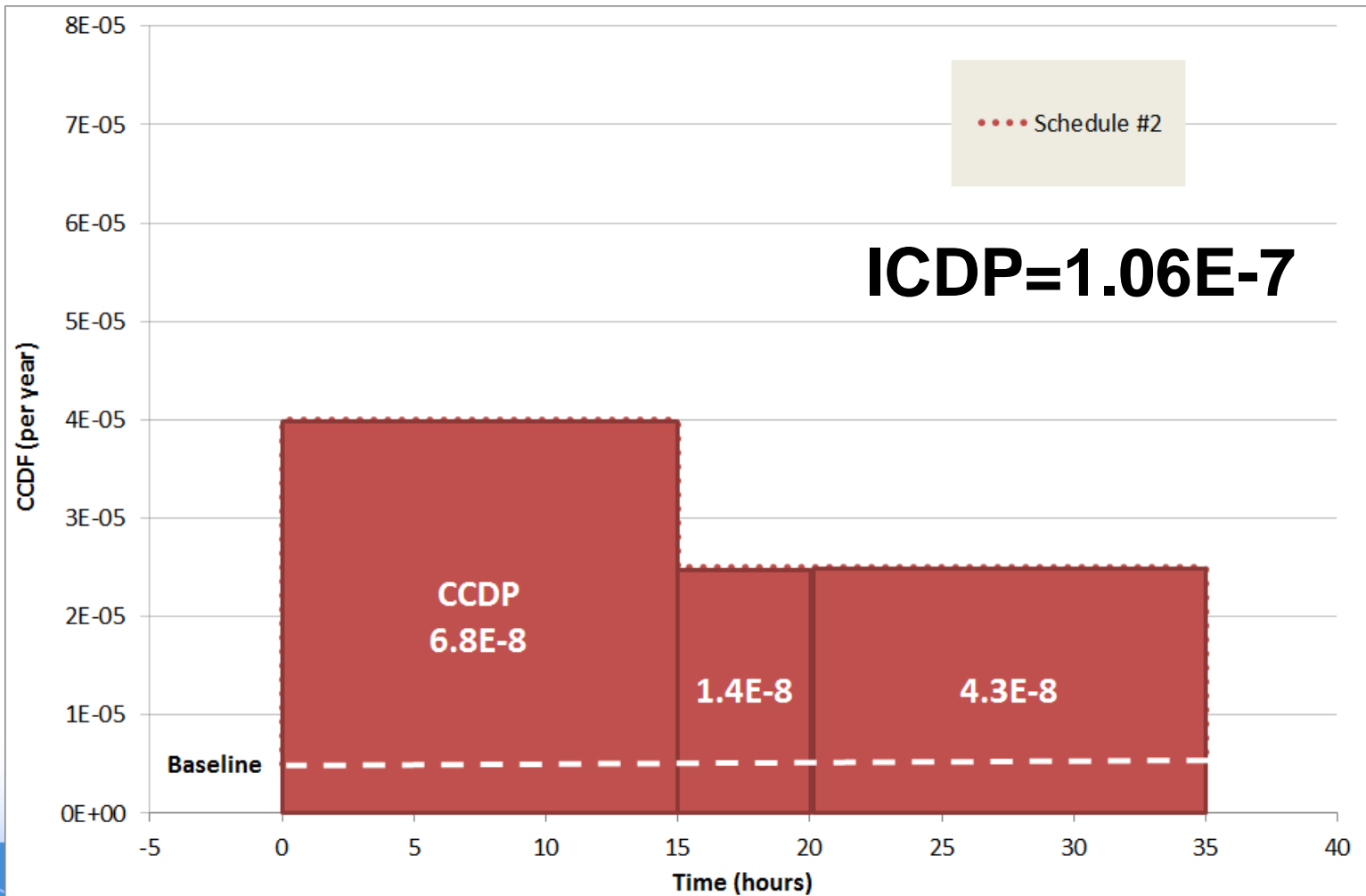
Answers to Exercise #2

CCDP profile (schedule 1)



Answers to Exercise #2

CCDP profile (schedule 2)





Idaho National Laboratory

MODULE R

MAINTENANCE RULE IMPLEMENTATION

Maintenance Rule Implementation

- **Purpose:** To acquaint students with ways in which PRA typically supports licensee implementation of the Maintenance Rule.
- **Objectives:**
 - Explain the purposes of the Maintenance Rule and identify areas in which PRA can support the rule's implementation
 - Explain how performance goals/criteria are established using the "EPRI Method"
- **References:**
 - 10 CFR 50.65, Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
 - Regulatory Guide 1.160, Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
 - NUMARC 93-01, Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
 - EPRI Technical Bulletin 96-11-01, "Monitoring Reliability for the Maintenance"
 - EPRI Technical Bulletin 97-3-01

Maintenance Rule History

- **1985: Davis Besse loss of all feedwater event**
- **1985-86: Maintenance and Surveillance Program (MSP)**
 - **NUREG-1212, “Status of maintenance in the U.S. Nuclear Power Industry 1985,” June 1986**
 - **Found lack of performance trending, lack of risk consideration, and ineffective root cause correction actions**
- **1988: Policy Statement on Maintenance of Nuclear Power Plants**
- **1990: Process-oriented and performance-based rulemaking packages developed**
- **1991: Performance-based rule adopted (5-year grace period)**
- **1996: Rule implemented**

Maintenance Rule History (cont.)

- **NRC published 10 CFR 50.65 on July 10, 1991**
- **Nuclear industry developed NUMARC 93-01 in May 1993**
- **NRC conducted nine pilot site visits from September 1994 to March 1995**
 - **Verify the usability and adequacy of draft NRC maintenance rule procedure**
 - **Determine strengths and weaknesses of the implementation of the rule at each site that used NUMARC 93-01 guidance**
 - **NUREG-1526 “Lessons Learned from Early Implementation of the Maintenance Rule at Nine Nuclear Power Plants,” issued June 1995**
- **Series of public meetings with NRC staff and industry representatives**
- **Revision 2 to NUMARC 93-01 in April 1996**
- **Rule becomes effective July 10, 1996**

Maintenance Rule Description

- **Performance-Based Rule**
- **Objectives of 10 CFR 50.65 (commonly referred to as the maintenance rule)**
 - **Require monitoring of the overall continuing effectiveness of licensee maintenance programs to ensure that**
 - **Safety-related and certain nonsafety-related structures, systems, and components (SSCs) are capable of performing their intended functions**
 - **For nonsafety-related equipment, failures will not occur that prevent the fulfillment of safety-related functions, and failures resulting in scrams and unnecessary actuations of safety-related systems are minimized**
 - **Additional objectives of the maintenance rule are to require licensees**
 - **To assess the impact of equipment maintenance on the capability of the plant to perform key plant safety functions**
 - **To use the results of the assessment before undertaking maintenance activities to manage the increase in risk caused by those activities**

Maintenance Rule Paragraphs

- Paragraph (a)(1)

- Monitor performance or condition of SSCs against licensee-established goals in a manner sufficient to provide reasonable assurance that such SSCs are capable of fulfilling their intended functions.
- Goals are to be established commensurate with safety and, where practical, take into account industry wide operating experience.
- When the performance or condition of an SSC does not meet established goals, appropriate corrective action must be taken.
- (a)(1) SSCs

Set Performance
Goals and see if
meeting these

- Paragraph (a)(2)

- Monitoring as specified in paragraph (a)(1) is not required when it has been demonstrated that the performance or condition of an SSC is being effectively controlled through the performance of appropriate preventive maintenance, such that the SSC remains capable of performing its intended function.
- (a)(2) SSCs

Relax
monitoring if
meeting goals

Maintenance Rule Paragraphs (cont.)

- Paragraph (a)(3)

- Performance and condition monitoring activities and associated goals and preventive maintenance activities be evaluated at least every refueling cycle provided the interval between evaluations does not exceed 24 months.
- Evaluations shall take into account, where practical, industry wide operating experience.
- Adjustments shall be made where necessary to ensure that the objective of preventing failures of SSCs through maintenance is appropriately balanced against the objective of minimizing unavailability of SSCs due to monitoring or preventive maintenance.

- Paragraph (a)(4)

- Before performing maintenance activities (including but not limited to surveillances, post-maintenance testing, and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to SSCs that a risk-informed evaluation process has shown to be significant to public health and safety.

Maintenance Rule Paragraphs (cont.)

- Paragraph (b)

- Scope of the monitoring program include safety-related and nonsafety-related SSCs

- Safety-related SSCs that are relied upon to remain functional during and following design basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposure comparable guidelines in §50.34(a)(1), or §50.67(b)(2), or §100.11 of this chapter, as applicable.

- Nonsafety related SSCs:

- That are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures (EOPs), or
 - Whose failure could prevent safety-related SSCs from fulfilling their safety-related function, or
 - Whose failure could cause a reactor scram or actuation of a safety-related system.

Track safety- and
nonsafety-related
SSCs if applicable

How PRA Supports Maintenance Rule Implementation

- **Establishing safety significance of SSCs covered by rule**
- **Establishing performance criteria and goals [(a)(1), (a)(2)]**
- **Evaluating balancing of SSC unavailability and reliability [(a)(3)]**
- **Assessing impact on plant risk when SSCs are removed from service for maintenance [(a)(4)]**

Safety Significance of SSCs

- **Safety Significance Categories**
 - NUMARC 93-01 establishes two safety significance categories
 - Risk-significant
 - Non-risk-significant
 - **Statements of Consideration for the rule**
 - More risk-significant
 - Less risk-significant
 - **NRC determined preferred terminology**
 - High safety significance
 - Low safety significance
 - Licensees may elect to define other categories or even define more than two – must define and use consistently

Safety Significance of SSCs (cont.)

- **Safety Significance Ranking Methodology**
 - NUMARC 93-01 recommends the use of three (3) importance measures
 1. Risk reduction worth (RRW), $RRW > 1.005$
 - Equivalent to Fussell-Vesely (FV) > 0.005
 2. Core damage frequency (CDF) contribution, included in cut sets that, when ranked in decreasing order, cumulatively account for about 90% of the CDF
 3. Risk achievement worth (RAW), $RAW \geq 2.0$
- **SSCs above cut-off levels for each importance measure are candidates for high safety significance**
- **Expert panel's role is also to consider and compensate for SSCs not in the PRA as well as PRA uncertainties...**

Factors to be Considered in Use of PRA Importance Measures

- **SSC importance vs PRA basic event importance**
 - AFW Motor-driven pump A vs AFW-MDP-FS-A180
- **Sequence truncation level used in PRA**
- **Core damage frequency importance vs large early release frequency importance**
- **Avoid reliance on just one measure of importance**

Some Relevant Statistics – Brunswick IPE

PWR SPAR

Truncation limit: $1\text{E}-10/\text{yr}$
CDF: $6.34\text{E}-6/\text{yr}$
No. basic events: 1543
No. events after truncation: 291
No. events w/F-V > 0.001: 150
No. events w/RAW > 2: 147

Truncation limit: $1\text{E}-12/\text{yr}$
CDF: $4.4\text{E}-5/\text{yr}$
No. basic events: 1,150
No. events after truncation: 572
No. events w/F-V > 0.005: 48
No. events w/RAW > 2: 120

CDF Contribution

No. events in top cut sets
Highest F-V not included
Highest RAW not included
No. events w/F-V > 0.005 not included
No. events w/RAW > 2 not included

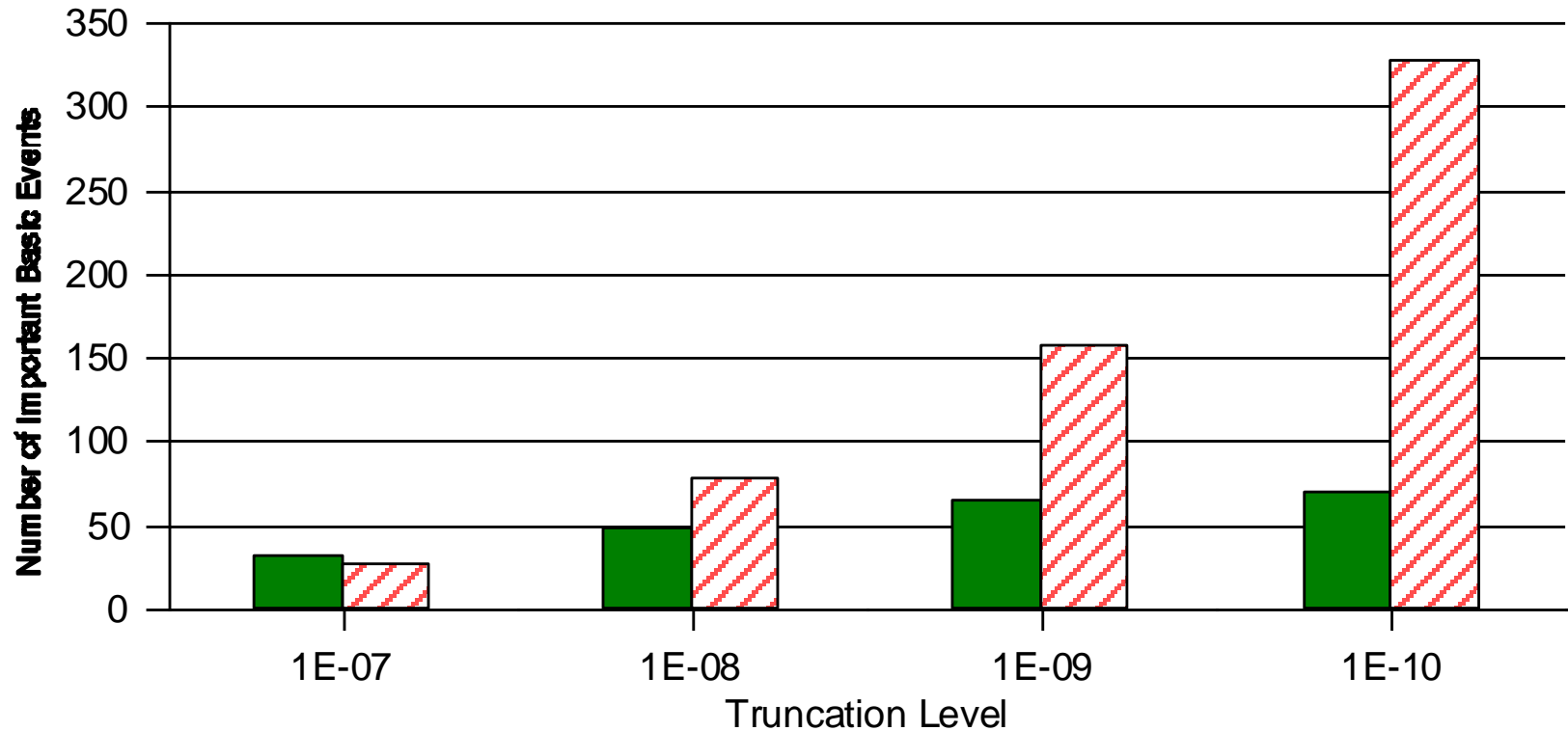
Top 90% Cut Sets

184
0.00194
33.3
0
36

Top 99% Cut Sets

281
0.000133
3.67
0
3

Truncation Limits Affect Importance Rankings



$FV > 0.005$



$RAW > 2$

SSC Performance Criteria

- **For high safety significance SSCs and standby low safety significance SSCs**
 - **Train-level unavailability and/or unreliability performance criteria**
 - **Unavailability measure - hours unavailable divided by hours plant was at power**
 - **Unreliability measure - number of failures over specified number of demands**
- **Implications of exceeding SSC performance criteria**
 - **SSCs become candidate for category (a)(1), criteria become goals to be met before SSC can be moved back to (a)(2)**

Unavailability Performance Criteria

- **PRA information**
 - **Plant-specific historical data**
 - **Time period covered**
 - **Generic estimate**
- **Other information**
 - **System engineer's experience/judgement**
 - **Industry-wide experience**
- **Final choice**
 - **Plant-specific data**
 - **95% of plant-specific data**
 - **Other**

Unreliability Performance Criteria

- **PRA information**
 - **Plant-specific historical data**
 - **Time period covered**
 - **Generic estimates often used**
- **Other information**
- **Final Choice**
 - **Generally 0, 1 or 2 failures over 2- to 3-year period**
 - **Relation to PRA values**
 - **Estimated or actual demands over 2- to 3-year period used to evaluate against value in PRA**

Performance Criteria Expected to be Commensurate with Safety

- **PRA values used to establish criteria - expectation is met**
- **If PRA values not used**
 - **Unavailability criteria**
 - **Sensitivity analysis if higher than PRA data**
 - **Unreliability criteria**
 - **EPRI approach**
 - **Sensitivity analysis**
 - **Others**
- **Acceptable increase in CDF/LERF not established by NRC**
 - **Not all SSCs expected to perform at limits**

Methods for Establishing Reliability Goals/Criteria

- EPRI method for reliability on **demand** (EPRI Technical Bulletin 96-11-01)
 - This is used for basic events with $\text{Pr}(\text{fails to start})$, $\text{Pr}(\text{fails on demand})$, $\text{Pr}(\text{fails to open})$, etc.
- The approach uses three steps
 1. Assume failure probability in PRA/IPE is correct
 2. Estimate number of demands over next evaluation period
 3. Calculate number of failures using binomial distribution such that, if PRA value is correct, there is only a 5% chance (or less) of seeing more than that number of failures
 - Assumes the binomial is an adequate aleatory model

Example: Methods for Establishing Reliability Goals/Criteria (cont.)

- Example 1 – reliability on demand:
 - Probability of **exactly x** failures in 24 demands given $p = 0.03$ using Binomial
 - $\Pr(x = 0, \text{ given } p = 0.03, N = 24) = 0.48$
 - $\Pr(x = 1, \text{ given } p = 0.03, N = 24) = 0.36$
 - $\Pr(x = 2, \text{ given } p = 0.03, N = 24) = 0.13$
 - $\Pr(x = 3, \text{ given } p = 0.03, N = 24) = 0.03$
 - Probability of **“up to and including” x** failures in 24 demands given $p = 0.03$ using Binomial
 - $\Pr(x = 0, \text{ given } p = 0.03, N = 24) = 0.48$
 - $\Pr(x \leq 1, \text{ given } p = 0.03, N = 24) = 0.48 + 0.36 = 0.84$
 - $\Pr(x \leq 2, \text{ given } p = 0.03, N = 24) = 0.48 + 0.36 + 0.13 = \mathbf{0.97}$
- Thus, performance criterion (Maintenance Preventable Failures, or MPF) could be set at 2 or fewer failures over next evaluation period
 - A conservative approach would be to set criterion of 1 or fewer failures over next evaluation period

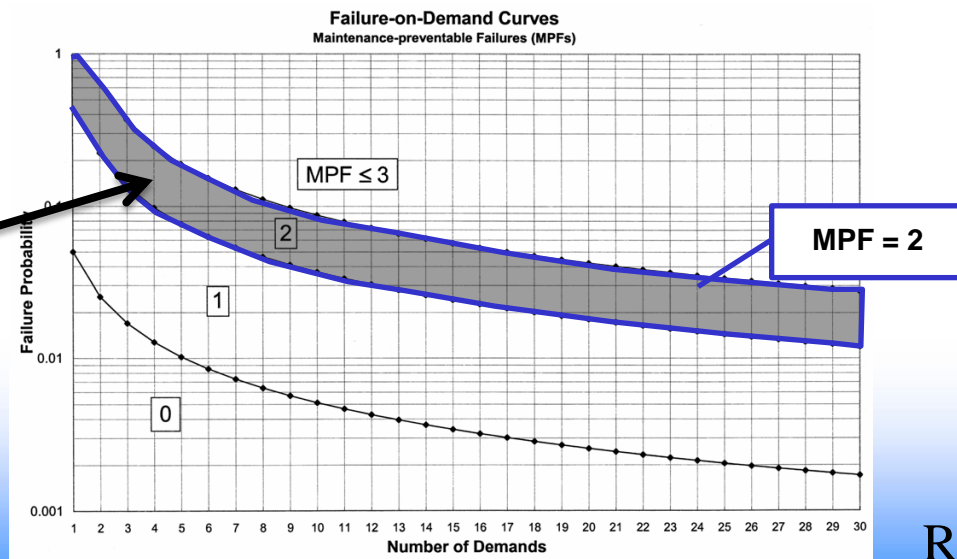
Methods for Establishing Reliability Goals/Criteria (cont.)

- Example 2 – reliability on demand:
 - Probability of **exactly x** failures in 30 demands given $p = 0.01$ using Binomial
 - $\Pr(x = 0, \text{ given } p = 0.01, N = 30) = 0.74$
 - $\Pr(x = 1, \text{ given } p = 0.01, N = 30) = 0.22$
 - $\Pr(x = 2, \text{ given } p = 0.01, N = 30) = 0.033$
 - Probability of **“up to and including” x** failures in 30 demands given $p = 0.01$ using Binomial
 - $\Pr(x = 0, \text{ given } p = 0.01, N = 30) = 0.74$
 - $\Pr(x \leq 1, \text{ given } p = 0.01, N = 30) = 0.74 + 0.22 = 0.96$
- Therefore, performance criterion could be set at 1 or fewer failures over the next evaluation period
 - A conservative approach would be to set performance criterion of 0 failures over the next evaluation period

Methods for Establishing Reliability Goals/Criteria (cont.)

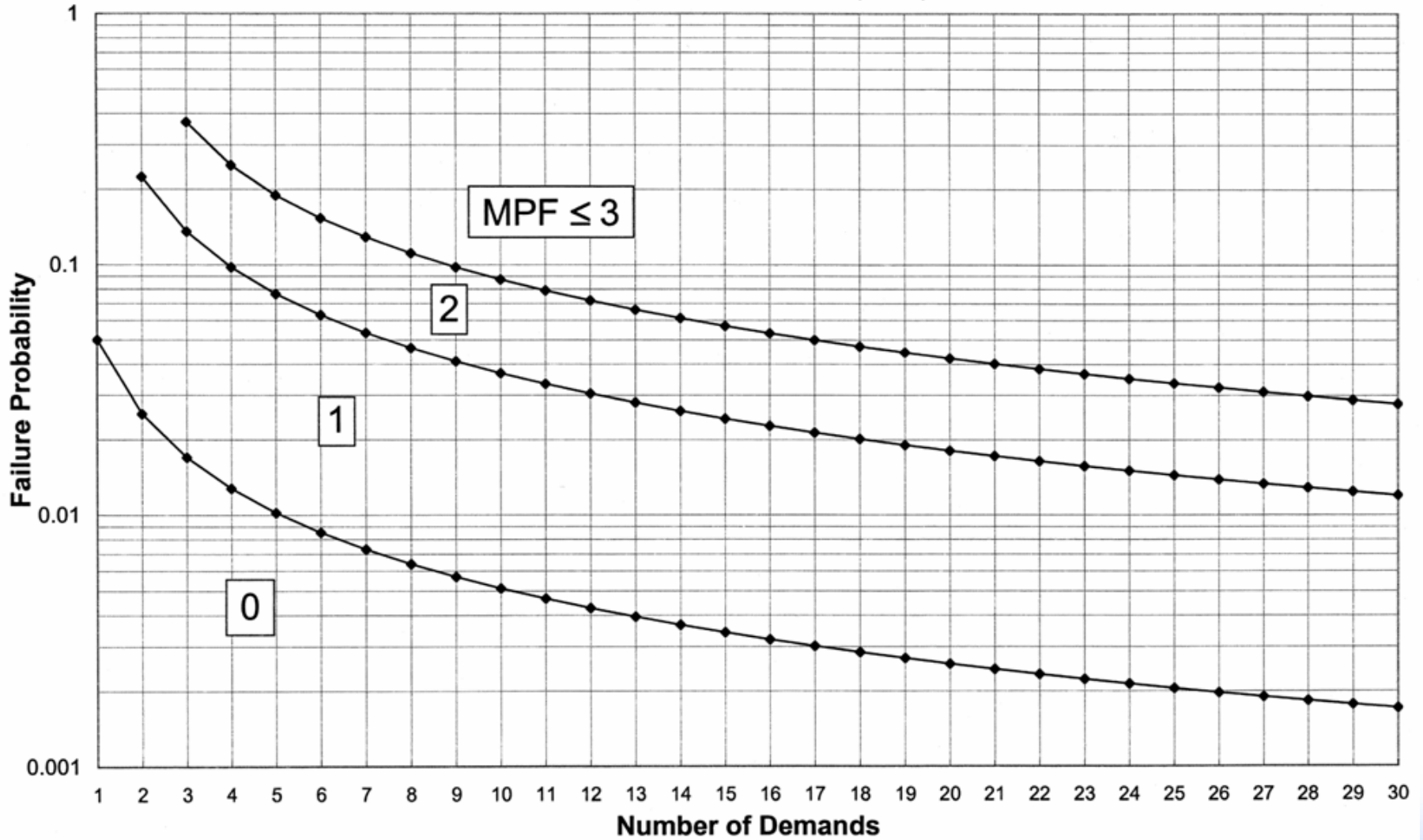
- These calculations for “demand” type failures can be reduced to a lookup on a plot
- Need to know
 1. How many demands (N) in the next evaluation period
 2. What is the demand failure probability (p) from the PRA
- Example (full chart on next slide)
 - N=24 & p=0.03

All points in this region represent $MPF \leq 2$



Failure-on-Demand Curves

Maintenance-preventable Failures (MPFs)



Methods for Establishing Reliability Goals/Criteria (cont.)

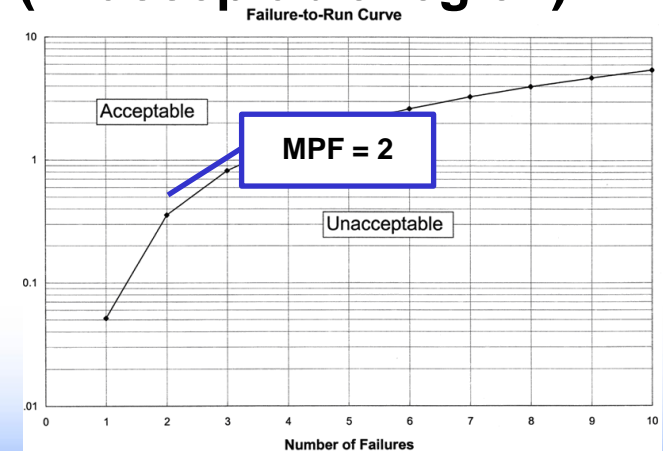
- EPRI method for reliability of **normally running** SSCs (EPRI Technical Bulletin 97-3-01)
 - This is used for basic events with $\text{Pr}(\text{fails to run})$, $\text{Pr}(\text{fails to operate over time})$, etc.
- The approach uses three steps
 1. Assume failure rate in PRA/IPE is correct
 2. Estimate total running time over next evaluation period
 3. Calculate number of failures, using Poisson distribution, such that, if PRA value is correct, there is approximately a 5% chance of seeing more than that number of failures
 - Assumes Poisson is adequate aleatory model

Methods for Establishing Reliability Goals/Criteria (cont.)

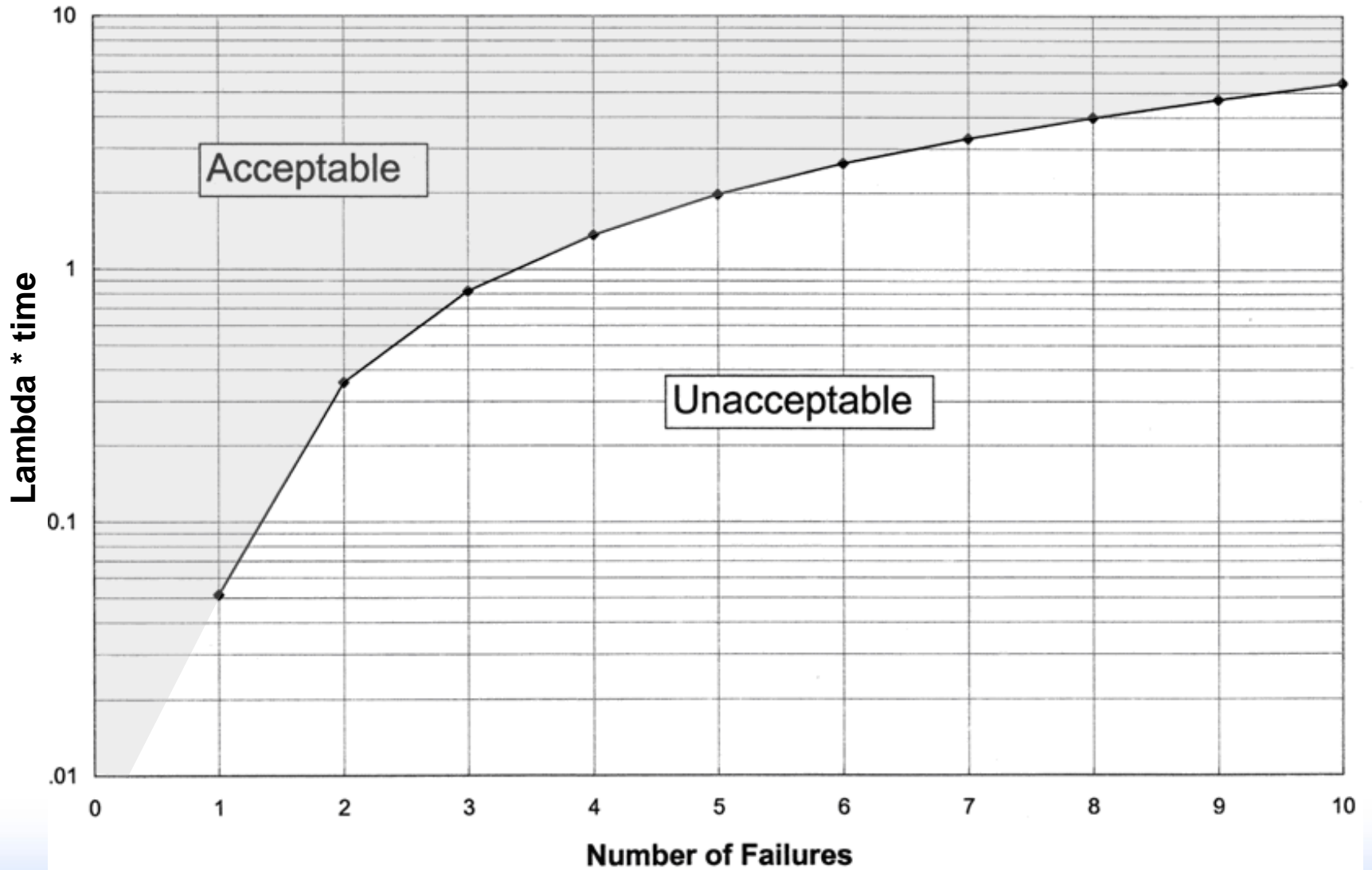
- **Example 3 – reliability on normally running:**
 - Probability of **exactly x** failures in 10,000 hours given that the failure rate (λ) = 5E-5/hour using Poisson
 - $\Pr(x = 0, \text{ given } \lambda = 5\text{E-}5/\text{hour, } t = 10,000 \text{ hrs}) = 0.61$
 - $\Pr(x = 1, \text{ given } \lambda = 5\text{E-}5/\text{hour, } t = 10,000 \text{ hrs}) = 0.30$
 - $\Pr(x = 2, \text{ given } \lambda = 5\text{E-}5/\text{hour, } t = 10,000 \text{ hrs}) = 0.08$
 - Probability of “**up to and including**” x failures in 10,000 hours given that the failure rate (λ) = 5E-5/hour using Poisson
 - $\Pr(x = 0, \text{ given } \lambda = 5\text{E-}5/\text{hour, } t = 10,000 \text{ hrs}) = 0.61$
 - $\Pr(x \leq 1, \text{ given } \lambda = 5\text{E-}5/\text{hour, } t = 10,000 \text{ hrs}) = 0.91$
 - $\Pr(x \leq 2, \text{ given } \lambda = 5\text{E-}5/\text{hour, } t = 10,000 \text{ hrs}) = 0.99$
- **Therefore, performance criterion could be set at 2 or fewer failures over the next evaluation period**
 - A conservative approach would be to set performance criterion at 1 or fewer failures over the next evaluation period

Methods for Establishing Reliability Goals/Criteria (cont.)

- These calculations for “running” type failures can be reduced to a lookup on a plot
- Need to know
 1. How many hours of operation (time) expected in the next evaluation period
 2. What is the failure rate (λ) from the PRA
 3. Find $\lambda \cdot \text{time}$ & perform lookup (in acceptable region)
- Example (full chart on next slide)
 - Time=10,000 hr & $\lambda=5E-5$
 - Time $\cdot\lambda = 0.5$



Failure-to-Run Curve



Balancing of Unavailability and Unreliability

- **Track SSC unavailability and unreliability**
- **Compare with performance criteria**
- **If performance criteria are approached or exceeded**
 - **Reduce preventive maintenance (if unavailability criterion is exceeded with no failures)**
 - **Increase preventive maintenance (if failure criterion is exceeded with low unavailability)**

Assessing Plant Risk From Maintenance

- **Configuration management**
 - **Work week schedule guidance**
 - 12-week rolling schedule
 - Days of week schedule for SSCs
 - Plant risk matrix or plant status monitor required by Maintenance Rule
 - Operator experience/judgment

Plant Risk Matrix

- **Goal-Assess plant risk given all planned/unplanned SSC maintenance outages**
- **Originally was at least a 2-dimensional matrix covering high safety significance SSC maintenance outages**
 - PRA based
 - Yes or no for planned outages of 2 SSCs, based on PRA estimate of plant risk
 - Guidance for 3 or more planned SSC outages
- **Now industry uses Risk Monitors**

For Additional Information

- **Maintenance Rule Implementation Inspection Reports (for plants already inspected)**
- **NUREG-1526, Lessons Learned from Early Implementation of the Maintenance Rule at Nine Nuclear Power Plants**
- **Maintenance Rule Guideline Book**



Idaho National Laboratory

Module S

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 Δ CDF
 - How MSPI includes both unavailability and unreliability
 - How MSPI uses importance measures
- **References**
 - NEI 99-02, Rev. 7, August 2013
 - 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 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 unreliability and unplanned unavailability uses industry mean values.
 - Component planned unavailability plant specific representative of current maintenance practices.
- **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 (Monitored) 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**

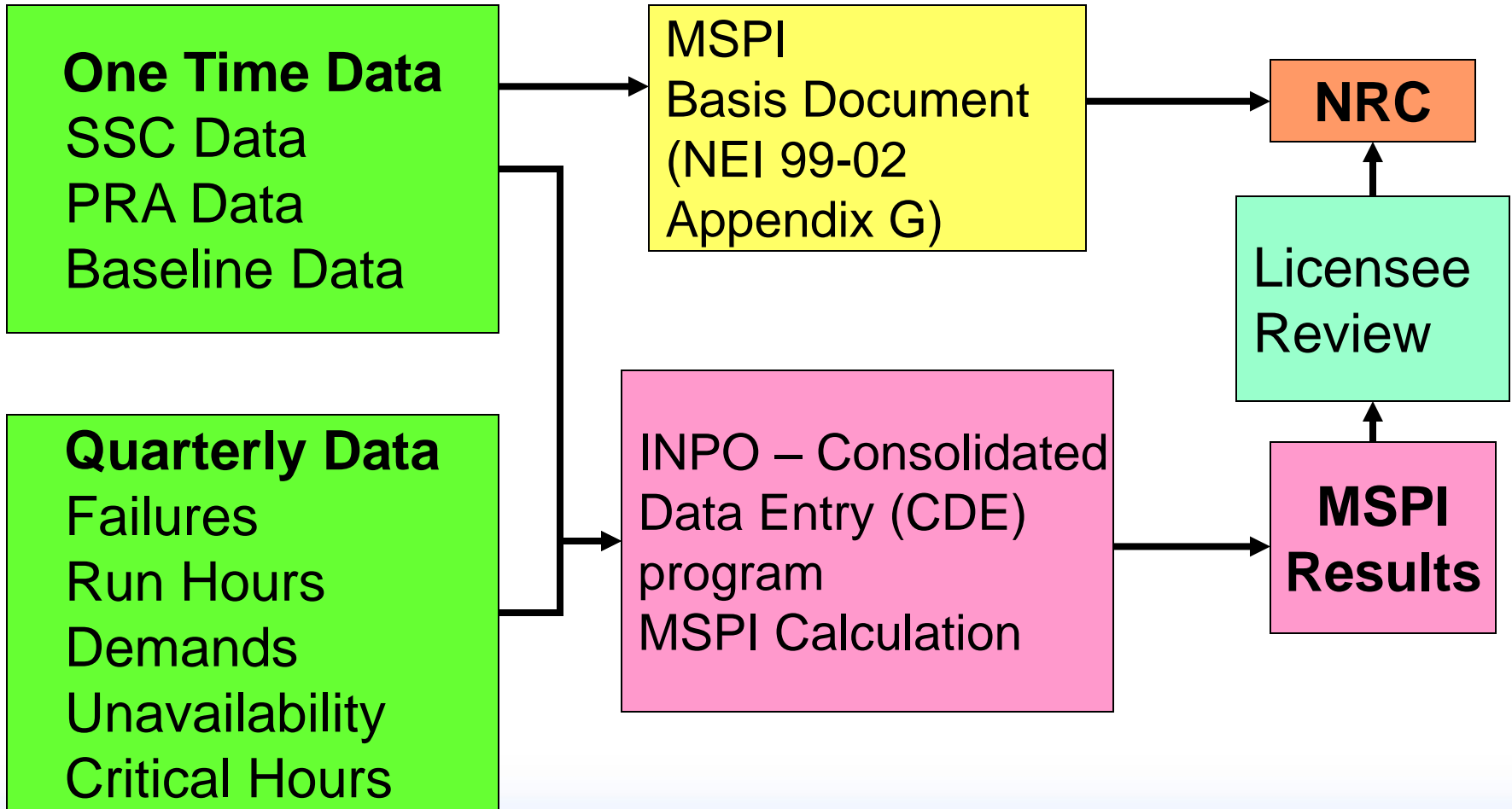
Development Timeline

- **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



Guidance Documents

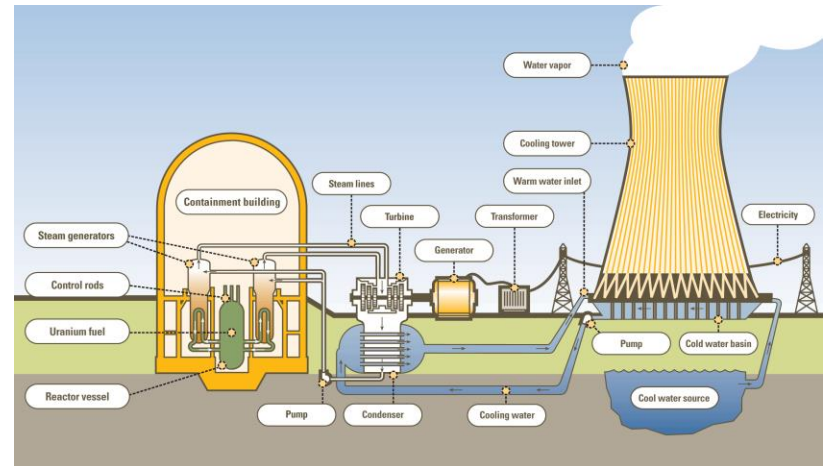
- **NEI 99-02 Section 2.2**
 - Basic Definitions
- **NEI 99-02 Appendix F**
 - Details of Calculation Methods
 - Detailed Definition of Inputs
- **NUREG-1816**
 - Technical bases
 - Description of pilot program
 - Recommended enhancements
 - MSPI limitations

MSPI Concept

$$\text{MSPI} \rightarrow \Delta\text{CDF} = \text{CDF}_1 - \text{CDF}_0$$



$\text{CDF}_1 = \text{Actual Performance}$



$\text{CDF}_0 = \text{Industry Baseline Performance}$

How To Calculate MSPI

- Includes unavailability and unreliability in single risk measure
- $MSPI = UAI + URI$
 - UAI is Unavailability Index
 - URI is Unreliability Index
- $MSPI \approx \Delta CDF = CDF_1 - CDF_0$
 - CDF_1 is actual plant performance
 - 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 Unavailability Index 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 UAI_t

- $$UAI_t = Bi_{UA_{PRA}} \times \Delta UA$$
$$= Bi_{UA_{PRA}} \times (UA_t - UA_{BLt})$$

where:

UA = train unavailability

UA_t = observed train unavailability

UA_{BLt} = baseline train unavailability

= $UA_{BLplanned} + UA_{BLunplanned}$

$UA_{BLplanned}$ = from “plant operational characteristics”

$UA_{BLunplanned}$ → Table 1 in NEI 99-02

$Bi_{UA_{PRA}}$ = Birnbaum importance of PRA basic event representing unavailability of train (i.e., AFW-MDP-TM)

Calculating UAI_t

- Relationship to Fussell-Vesely importance

$$FV_{UAPRA} = \frac{p_{UAPRA} \times Bi_{UAPRA}}{CDF}$$

where:

FV_{UAPRA} = train-specific Fussell-Vesely value for unavailability (i.e., AFW-MDP-TM)

p_{UAPRA} = train-specific unavailability (i.e., AFW-MDP-TM)

Bi_{UAPRA} = train-specific Birnbaum value for unavailability (i.e., AFW-MDP-TM)

CDF = plant PRA total core damage frequency

- Thus, can replace Bi since $Bi_{UA} = CDF * FV_{UA} / p_{UA}$

Calculating UAI_t

- Substitute into equation for UAI_t we end up with

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

where:

CDF = plant specific core damage frequency

$FV_{UA_{PRA}}$ = train-specific Fussell-Vesely value for unavailability

UA_{PRA} = plant specific PRA value of unavailability for the train

UA_t = actual unavailability of train t, defined as:

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

UA_{BLt} = total historical baseline unavailability value for the train (plant operational planned and unplanned)

Birnbaum Importance and Δ CDF

- More on Birnbaum importance

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

- Δ CDF $\approx \Sigma Bi_{UAPRA}(x) \Delta p_x$
- Thus, UAI is approximately the increase in CDF caused by increase in unavailability of monitored systems

Calculating URI

$$URI = \sum_{j=1}^n Bi_{\max} (UR_{PRA,j})(UR_{BC,j} - UR_{BL,j})$$

Bi_{\max} = maximum Birnbaum importance of all basic events for given component (i.e., AFW-MDP-FR, AFW-MDP-FS)

UR_{PRA} = unreliability from PRA [i.e., P(AFW-MDP-FS)]

UR_{BC} = “Bayesian-corrected” unreliability (plant-specific) i.e., incorporated data accumulated such as # of failures and # of demands

UR_{BL} = Industry baseline unreliability [probability from Appendix F NEI99-02]

n = number of failure modes of a component

Calculating URI

- Using relationship between Fussell-Vesely and Birnbaum importance gives

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

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

Calculating URI

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

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

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

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 NEI 99-02)

RUNNING

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

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_{BLt} = historical baseline values of unreliability for the component's failure modes [i.e., MDP fails to run]
[Appendix F of NEI99-02]

Color Scale for MSPI

- **MSPI = UAI + URI**
- **MSPI is calculated for each monitored system and compared to risk thresholds**
 - **MSPI $\leq 10^{-6}$ GREEN**
 - **$10^{-6} < \text{MSPI} \leq 10^{-5}$ WHITE**
 - **$10^{-5} < \text{MSPI} \leq 10^{-4}$ 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 could be expected to see 2 or 4 failures in three year period.
 - It is not appropriate a system should be placed in WHITE band due to expected variation.
- **Avoid this by capping most risk-significant failure at 5×10^{-7} (from risk-informed Tech. Specs.)**
 - This ensures one failure beyond expected alone doesn't result in $MSPI > 1.0 \times 10^{-6}$

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 $MSPI < 1.0 \times 10^{-6}$**
- **Appendix E to NUREG-1816 or Appendix F of NEI99-02 gives formula for finding maximum allowed failures, even if MSPI is still GREEN**

*** Exercise – MSPI ***

Assume the following data were observed for AFW-MDP-3A at North Anna Unit 1 during the last 3 years:

Planned Outage Hours	Unplanned Outage Hours	Historical Planned Unavailability	Demands (n)	Failures (x)
63.76	18.7	2.61E-3	12	1

The capacity factor for the past 3 years was 92%. Calculate, UAI, URI, and MSPI for the A train of AFW, using this data, and the tables below, taken from NEI-99-02, App. F. Use the importance measures and basic event probabilities from the North Anna IPE material in Vol. 2 of the course materials. We will make the simplifying assumption that AFW-MDP-3A is the only component that will factor into the calculation, with failure to start being the only failure mode considered for URI.

In calculating URI, the Bayesian-corrected unreliability is calculated as (ref. NEI-99-02, App. F)

$$UR_{BC} = \frac{x + a}{a + b + n}$$

The values of a and b and the baseline unreliability are taken from Table 4 below (ref. NEI-99-02, App. F).

*** Exercise – MSPI *** - update table rev 7

Table 1. Historical Unplanned Unavailability Train Values
(Based on ROP Industry wide Data for 1999 through 2001)

SYSTEM	UNPLANNED UNAVAILABILITY/TRAIN
EAC	1.7 E-03
PWR HPSI	6.1 E-04
PWR AFW (TD)	9.1 E-04
PWR AFW (MD)	6.9 E-04
PWR AFW (DieselD)	7.6 E-04
PWR (except CE) RHR	4.2 E-04
CE RHR	1.1 E-03
BWR HPCI*	3.3 E-03
BWR HPCS	5.4 E-04
BWR FWCI	Use plant specific Maintenance Rule data for 2002-2004
BWR RCIC	2.9 E-03
BWR IC	1.4E-03
BWR RHR	1.2 E-03
Support Cooling	Use plant specific Maintenance Rule data for 2002-2004

Table 4. Industry Priors and Parameters for Unreliability

Component	Failure Mode	a ^a	b ^a	Industry Mean Value ^b URBLC
Circuit Breaker	Fail to open (or close)	4.99E-1	6.23E+2	8.00E-4
Hydraulic-operated valve	Fail to open (or close)	4.98E-1	4.98E+2	1.00E-3
Motor-operated valve	Fail to open (or close)	4.99E-1	7.12E+2	7.00E-4
Solenoid-operated valve	Fail to open (or close)	4.98E-1	4.98E+2	1.00E-3
Air-operated valve	Fail to open (or close)	4.98E-1	4.98E+2	1.00E-3
Motor-driven pump, standby	Fail to start	4.97E-1	2.61E+2	1.90E-3
	Fail to run	5.00E-1	1.00E+4	5.00E-5
Motor-driven pump, running or alternating	Fail to start	4.98E-1	4.98E+2	1.00E-3
	Fail to run	5.00E-1	1.00E+5	5.00E-6
Turbine-driven pump, AFWS	Fail to start	4.85E-1	5.33E+1	9.00E-3
	Fail to run	5.00E-1	2.50E+3	2.00E-4
Turbine-driven pump, HPCI or RCIC	Fail to start	4.78E-1	3.63E+1	1.30E-2
	Fail to run	5.00E-1	2.50E+3	2.00E-4
Diesel-driven pump, AFWS	Fail to start	4.80E-1	3.95E+1	1.20E-2
	Fail to run	5.00E-1	2.50E+3	2.00E-4
Emergency diesel generator	Fail to start	4.92E-1	9.79E+1	5.00E-3
	Fail to load/run	4.95E-1	1.64E+2	3.00E-3
	Fail to run	5.00E-1	6.25E+2	8.00E-4



Idaho National Laboratory

MODULE T

SIGNIFICANCE DETERMINATION PROCESS (SDP)

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 identified**
 - **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”**
 - **IMC 2201, “Security and Safeguard Inspection Program for Commercial Power Reactors”**

SDP Purpose (cont.)

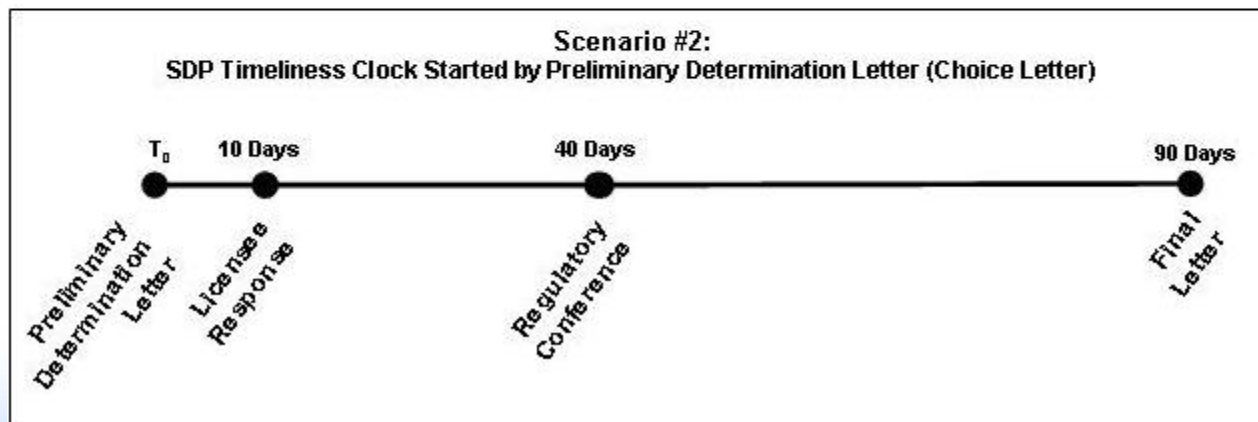
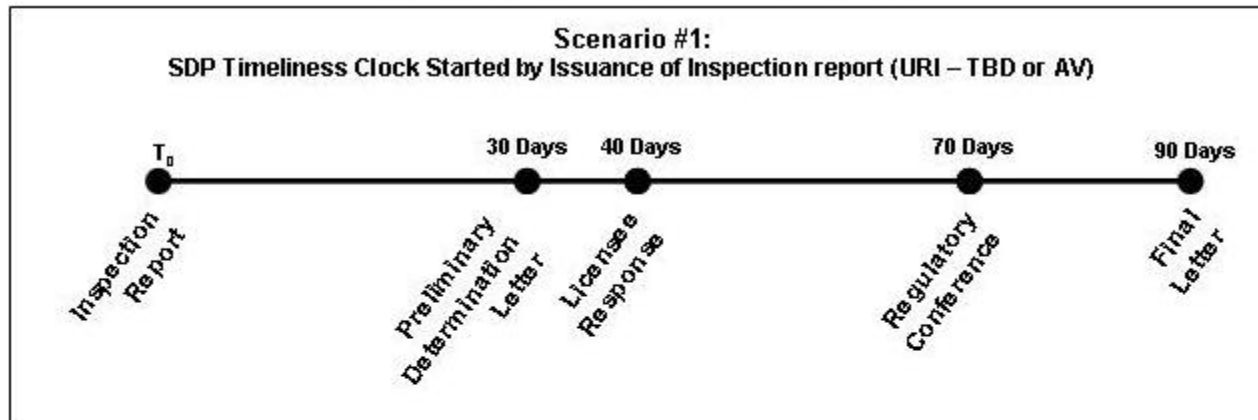
- **SDP Purpose**
 - **A risk-informed process**
 - **To use the results of the safety significance of findings, combined with the results of the risk-informed performance indicator (PI) program**
 - **To determine a licensee’s level of safety performance, and to define the level of NRC engagement with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

SDP Objectives

- **SDP Objectives:**
 - **Characterize significance** of inspection findings for the Reactor Oversight Process (ROP), using risk insights as appropriate
 - Provide all stakeholders an **objective and common framework** for communicating the potential safety 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



URI=unresolved issue, AV=apparent violation

SDP Types

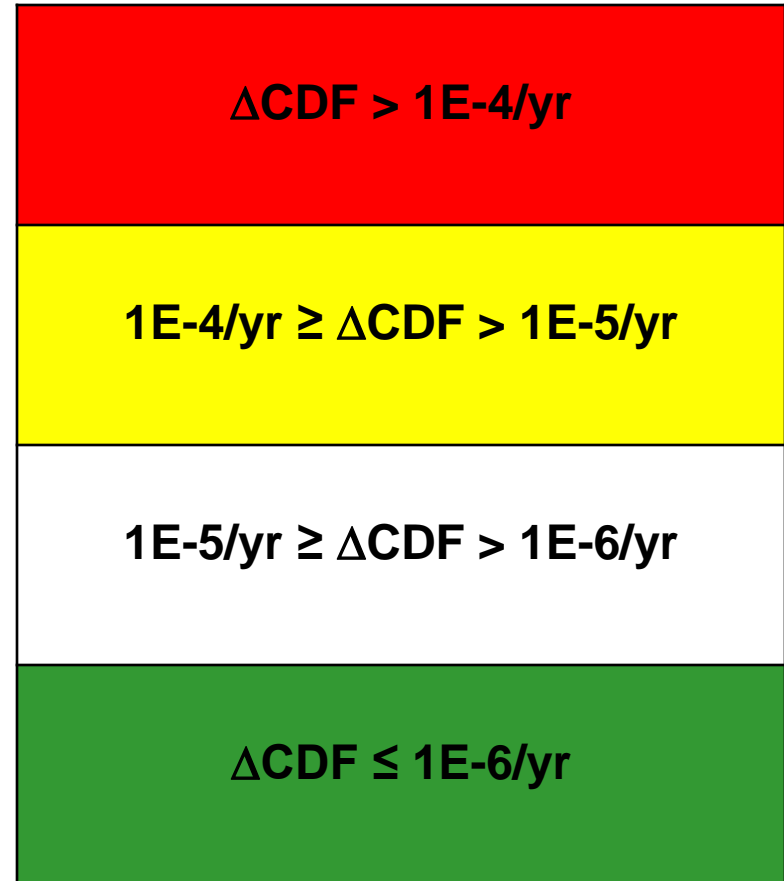
- **Different SDPs**
 - **0609 App A** **The SDP for Findings At-Power**
 - **0609 App B** **Emergency Preparedness SDP**
 - **0609 App C** **Occupational Radiation Safety SDP**
 - **0609 App D** **Public Radiation Safety SDP**
 - **0609 App F** **Fire Protection SDP**
 - **0609 App G** **Shutdown Operations 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**

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 Δ CDF that is 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



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

Definitions

- **Inspection findings are assigned a color representing finding significance**
- **Definitions include quantitative & 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 $10^{-4}\Delta\text{CDF}$ or $10^{-5}\Delta\text{LERF}$. 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 $10^{-4} \Delta\text{CDF}$ or greater than 10^{-6} and less than or equal to $10^{-5}\Delta\text{LERF}$. 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 $10^{-5}\Delta\text{CDF}$ or greater than 10^{-7} and less than or equal to $10^{-6}\Delta\text{LERF}$. 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 $10^{-6}\Delta\text{CDF}$ or $10^{-7}\Delta\text{LERF}$. 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 is to support identification of safety cornerstone(s) affected by 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 appropriate SDP appendix for further evaluation**
 - **If more than one cornerstone was affected and results in direction to more than one SDP appendix, 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, inspector and management should initially identify one cornerstone based on reasonable judgment of the situation**

SDP Example (at-power)

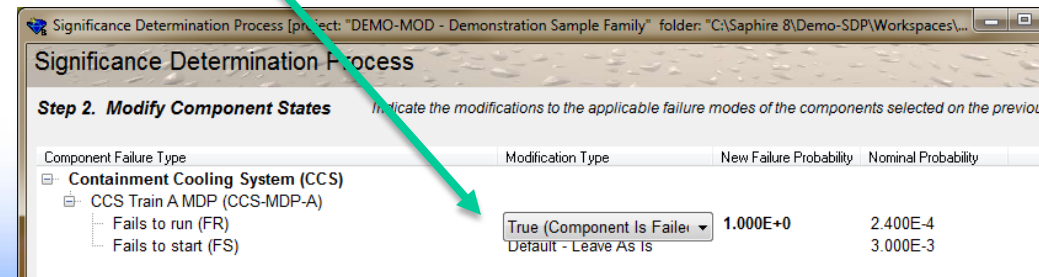
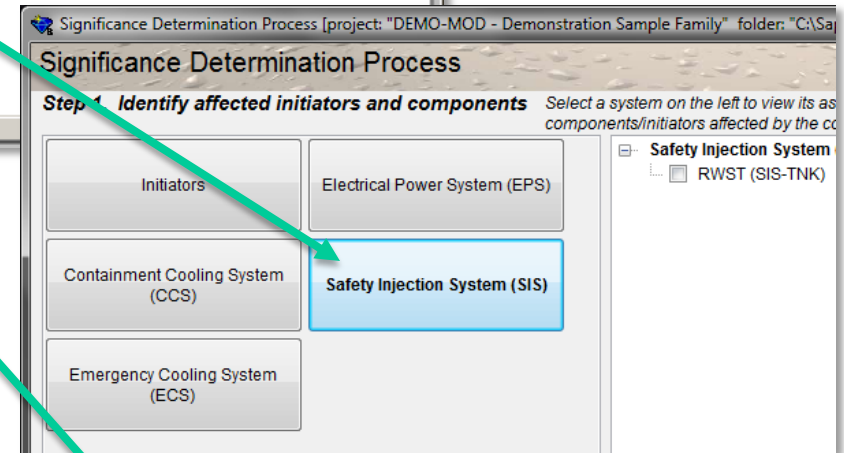
- **IMC 0609 Appendix A – The Significance Determination Process (SDP) for Findings At-Power**
 - **Appendix A is divided into two functional parts**
 1. **Screening tool that uses a series of logic questions to determine whether or not the finding can be characterized as having low safety significance (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 SAPHIRE SDP Workspace

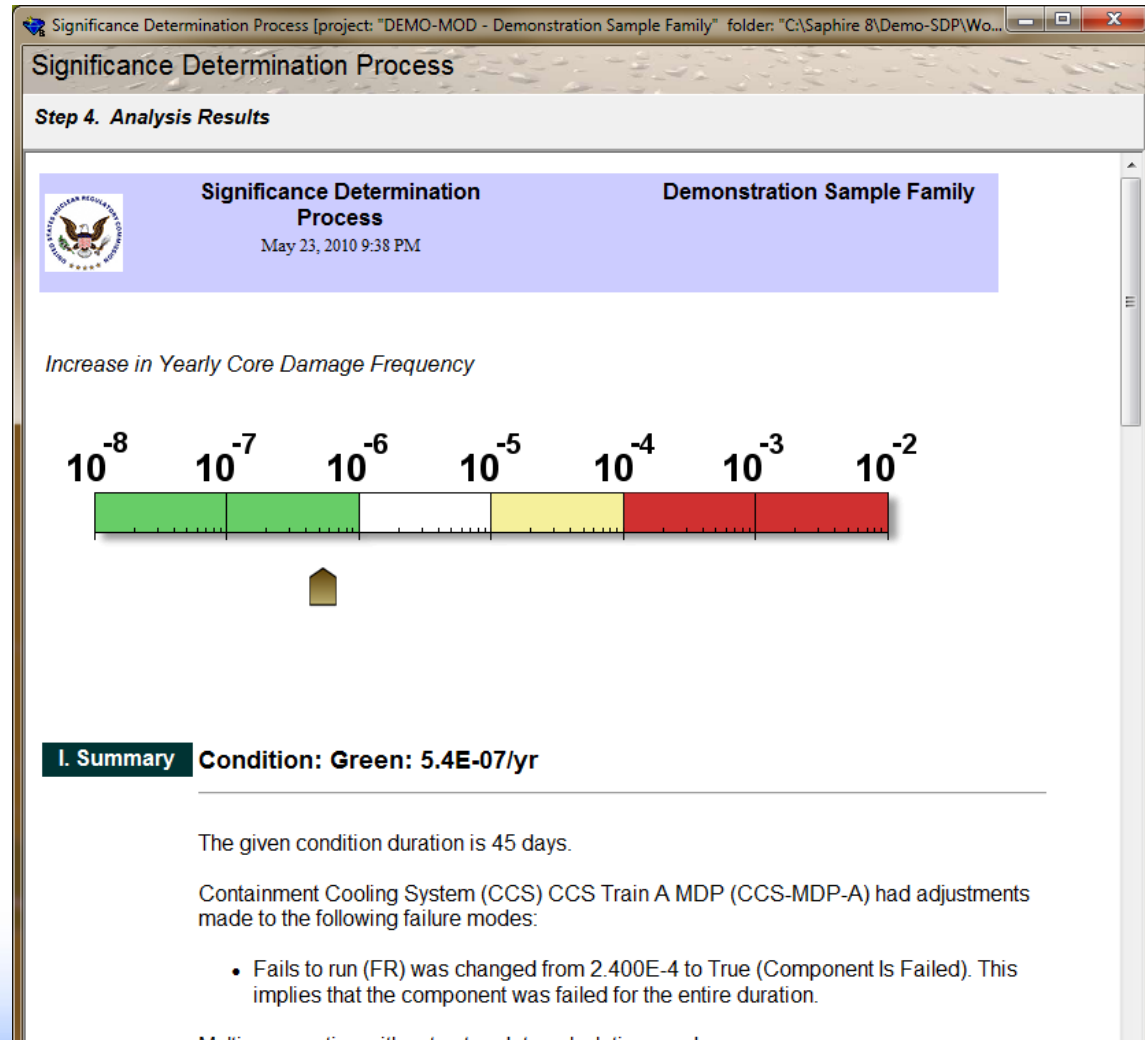
Start a SDP

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



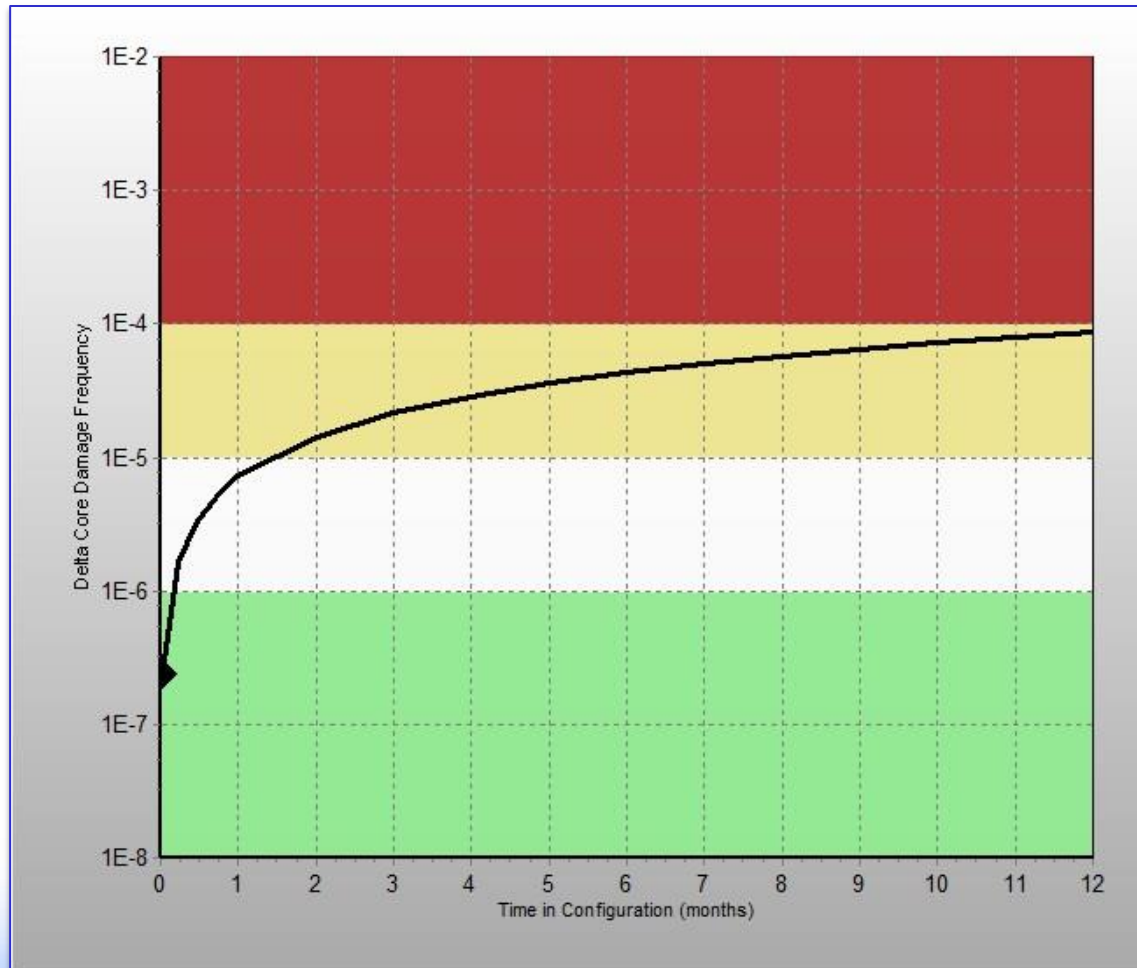
SDP – Detailed Risk Evaluation

4. Calculate!



SDP - Detailed Risk Evaluation

Example SPAR model Results



Final Risk Significance of Inspection Finding

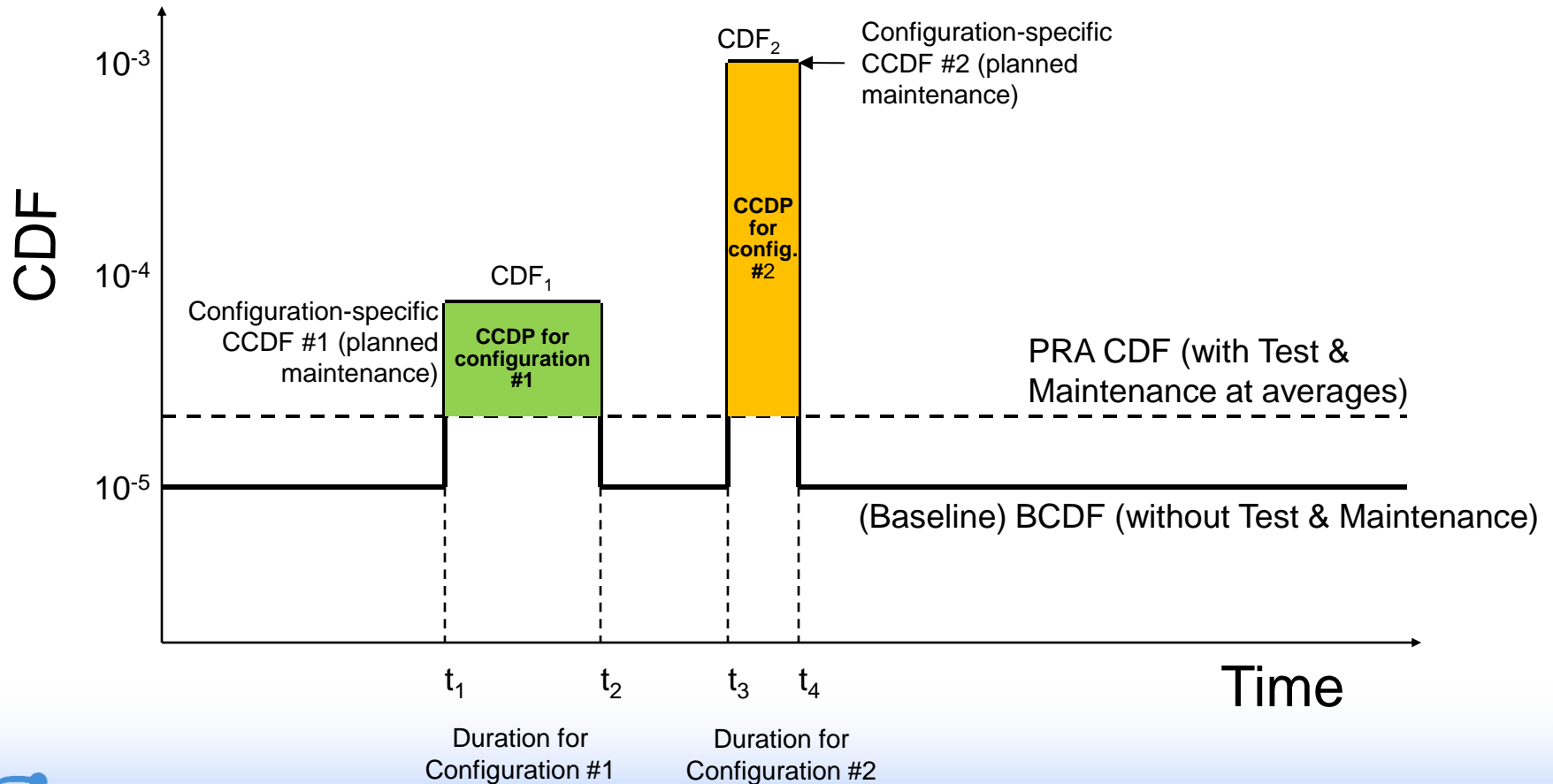
- **SDP Evaluation:**
 - **Cannot** assess impact of **degraded** equipment reliability
 - Set up to analyze conditions that exist for a period of time, not set up for initiating event assessments (where an IE has occurred)
 - Initiating event assessment results in CCDP “spike,” which is different type 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)**
 - = $(CCDF - CDF) * \text{duration}$
 - = $ICDF * \text{duration}$; or
 - = $CCDP - BCDP$
 - **Incremental Large Early Release Probability (ILERP), also referred to as incremental conditional large early release probability (ICLERP)**
 - = $(CLERF - LERF) * \text{duration}$
 - = $ILERF * \text{duration}$; or
 - = $CLERP - BLERP$

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

Conditional Core Damage Probability (CCDP)



Final Risk Significance of Inspection Finding

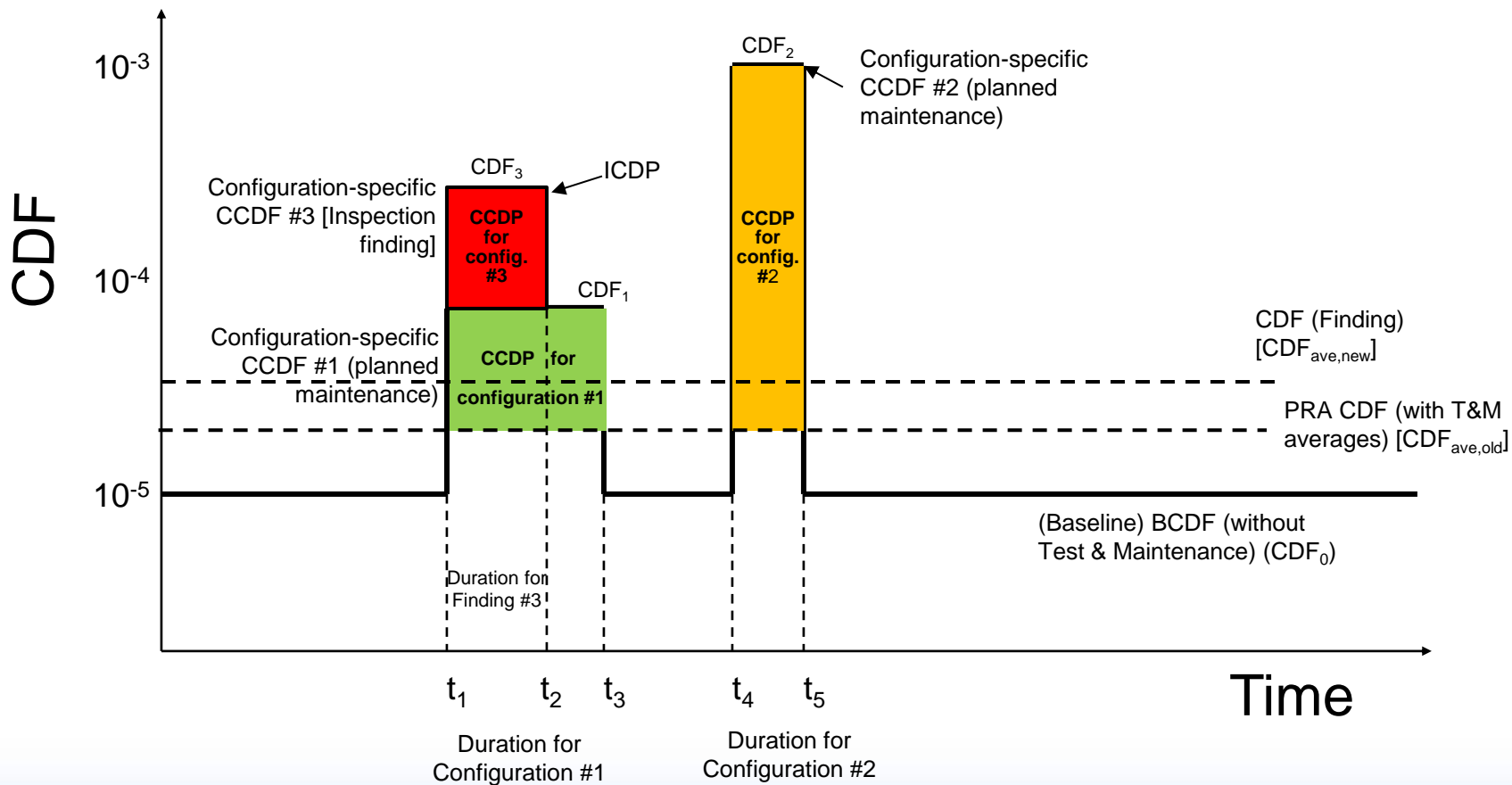
- **SDP Results (cont.)**
 - The result of SDP is a difference or change in a probability
 - Probability of core damage given a degraded condition for a specified duration minus the probability of core damage given no degraded condition for the same specified duration
 - It turns out that, **numerically**, 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 ΔCDF is $> 10^{-4}/\text{yr}$
 - **Yellow** if ΔCDF is $> 10^{-5}/\text{yr}$ and $\leq 10^{-4}/\text{yr}$
 - **White** if ΔCDF is $> 10^{-6}/\text{yr}$ and $\leq 10^{-5}/\text{yr}$
 - **Green** if ΔCDF is $\leq 10^{-6}/\text{yr}$

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)

$$CDF_{ave,new} - CDF_{ave,old} = ICDP/1 \text{ yr (SDP color)}$$



Algebra for CDF Profile (optional)

$$CDF_{ave,old} = \frac{CDF_o(t_1 + t_4 - t_3 + t_{end} - t_5)}{t_{end}} + \frac{CDF_1(t_3 - t_1)}{t_{end}} + \frac{CDF_2(t_5 - t_4)}{t_{end}}$$

$$CDF_{ave,new} = \frac{CDF_o(t_1 + t_4 - t_3 + t_{end} - t_5)}{t_{end}} + \frac{CDF_3(t_2 - t_1)}{t_{end}} + \frac{CDF_1(t_3 - t_2)}{T_{end}} + \frac{CDF_2(t_5 - t_4)}{t_{end}}$$

$$\begin{aligned} CDF_{ave,new} - CDF_{ave,old} &= \frac{CDF_3 t_2 - CDF_3 t_1 + CDF_1 t_3 - CDF_1 t_2 - CDF_1 t_3 + CDF_1 t_1}{t_{end}} \\ &= \frac{CDF_3(t_2 - t_1) - CDF_1(t_2 - t_1)}{t_{end}} = \frac{(CDF_3 - CDF_1)(t_2 - t_1)}{t_{end}} = \frac{ICDP}{t_{end}} \end{aligned}$$

SDP for External Initiators

- **SDP treats only fires (internal and external) and internal floods**
 - Licensee performance cannot impact frequency of other external events such as earthquakes and severe weather
- **External events treated in separate PRA analysis (see External Events Module)**
 - IPEEE did not require PRA for external events
 - If PRA performed, separate accident sequences generated that start with fire, flood, etc.
 - Core damage requires external IE and failure of one or more systems and/or operator actions

SDP for External Initiators (cont.)

- **SDP Phase 1 screens findings for events that increase likelihood of external IEs**
 - **Such events are analyzed by risk analyst in Phase 3 (not covered by Phase 2 SDP)**
- **Inspector may be able to identify external event sequences for analysis in Phase 3, using IPEEE or other licensee analysis**
- **If finding affects fire barrier or fire suppression feature, Appendix F is used by inspector for Phase 1 screening analysis**

SDP for Containment Integrity

- IMC 0609, App. H contains guidance
- Significance criteria for Δ LERF are order of magnitude less than for Δ CDF
 - **Red** if Δ LERF is $> 10^{-5}/\text{yr}$
 - **Yellow** if Δ LERF is $> 10^{-6}/\text{yr}$ and $\leq 10^{-5}/\text{yr}$
 - **White** if Δ LERF is $> 10^{-7}/\text{yr}$ and $\leq 10^{-6}/\text{yr}$
 - **Green** if Δ LERF is $\leq 10^{-7}/\text{yr}$
- Finding that is "Green" for Δ CDF could be "White" for Δ LERF

SDP for Containment Integrity (cont.)

- **Only some core damage sequences have significant LERF potential**
 - ISLOCA
 - SGTR
 - Sequences where reactor vessel fails at high pressure
- **Bear in mind that a "large early release" is one likely to cause acute fatalities offsite**
 - Well in excess of 10 CFR 100 release

SDP for Containment Integrity (cont.)

- SDP considers two types of findings, Type A and Type B
- Type A findings
 - Findings that **affect CDF** → CDF SDP performed
 - LERF considerations may adjust final risk significance
 - Use Appendix H, Figure 5.1 and Table 5.1 – 5.2
- Type B findings
 - Findings **that do not affect** CDF → CDF SDP not performed
 - Use Appendix H, Figure 6.1 and Table 6.1 – 6.2

SDP for Shutdown Conditions

- **Described in 0609 Appendix G**
- **Monitors five safety functions defined in NUMARC 91-06**
 - **Core decay heat removal**
 - **RCS inventory control**
 - **Power availability**
 - **Containment control**
 - **Reactivity control**
- **Phase 1 checklists (Attachment 1) are specific to plant operating state, as requirements vary among states, and states are not of equal risk significance**
- **Items screening to Phase 2 require more detailed analysis**
 - **Analysis specific to plant type (e.g., BWR versus PWR)**

SDP using SPAR + SAPHIRE

- **Discuss SAPHIRE/SDP**
- **Plant Risk Information e-Book (PRIB)**
- **Show SAPHIRE/SDP Outputs**

Acronyms and Abbreviations

AC	Alternating current	ET	Event tree
ACRS	Advisory Committee on Reactor Safeguards	FCI	Fuel-coolant interaction
ADS	Automatic depressurization system	FIVE	Fire-Induced Vulnerability Evaluation
ADV	Atmospheric dump valve	FMEA	Failure modes and effects analysis
AEOD	Office for Analysis and Evaluation of Operational Data	FSAR	Final Safety Analysis Report
AFW	Auxiliary feedwater	FT	Fault tree
AOP	Abnormal Operating Procedure	F-V	Fussell-Veseley (importance)
AOT	Allowed outage time	FW	Feedwater
AOV	Air-operated valve	GE	General Electric
APB	Accident progression bin	GL	Generic Letter
APET	Accident progression event tree	GSI	Generic Safety Issue
ASEP	Accident Sequence Evaluation Program	HCLPF	High confidence, low probability of failure
ASP	Accident Sequence Precursor	HCR	Human Cognitive Reliability
ATHEANA	A Technique for Human Event Analysis	HEP	Human error probability
ATWS	Anticipated transient without scram	HHSI	High-head safety injection
BC	Boundary condition	HLW	High-level waste
BNL	Brookhaven National Laboratory	HPCI	High-pressure coolant injection
BTP	Branch Technical Position	HPCS	High-pressure core spray
BWR	Boiling water reactor	HPI	High-pressure injection
BWROG	BWR Owners' Group	HPR	High-Pressure re-circulation
BWST	Borated water storage tank	HPSI	High-pressure safety injection
CCDF	Configuration (or conditional) core damage frequency	HRA	Human reliability analysis
CCDP	Conditional core damage probability	HVAC	Heating, ventilation, and air conditioning
CCF	Common-cause failure	HTGR	High-Temperature Gas Reactor
CCI	Core-concrete interaction	HX	Heat exchanger
CCW	Component Cooling Water	ICDF	Incremental core damage frequency
CDF	Core damage frequency	ICDP	Incremental core damage probability
CDF	Cumulative Density Function	ICCDP	Incremental conditional core damage probability
CDFM	Conservative Deterministic Failure Margin	ILERF	Incremental large early release frequency
CDP	Core damage probability	ILERP	Incremental large early release probability
CE	Combustion Engineering	ICLERP	Incremental conditional large early release probability
CEOG	Combustion Engineering Owners' Group	IE	Initiating event
CFR	Code of Federal Regulations	IMC	Inspection Manual Chapter
CLB	Current licensing basis	INL	Idaho National Laboratory
CRD	Control rod drive	INPO	Institute for Nuclear Plant Operations
CSIP	Charging/safety injection pump	IPE	Individual Plant Examination
CST	Condensate storage tank	IPEEE	Individual Plant Examination for External Events
CW	Circulating water	IREP	Interim Reliability Evaluation Program
DBA	Design basis accident	ISA	Integrated Safety Analysis
DC	Direct current	ISI	In-service inspection
DCH	Direct containment heating	ISLOCA	Interfacing system loss-of-coolant accident
DF	Decontamination factor	IST	In-service testing
DFSD	Dominant functional sequence diagram	JCO	Justification for Continued Operation
DHR	Decay heat removal	LB	Licensing basis
ECCS	Emergency core-cooling system	LCO	Limiting Condition for Operation
EDG	Emergency diesel generator	LER	Licensee Event Report
EOOS	Equipment Out of Service System	LERF	Large early release frequency
EOP	Emergency Operating Procedure	LERP	Large early release probability
EPA	Environmental Protection Agency	LLNL	Lawrence Livermore National Laboratory
EPIX	Equipment performance and information exchange system	LLW	Low-level waste
EPRI	Electric Power Research Institute	LOCA	Loss-of-coolant accident
ESF	Engineered safeguards feature	LOOP	Loss of offsite power
ESW	Emergency service water	LOSP	Loss of offsite power
ESWGR	Emergency switchgear	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	RRW	Risk reduction worth
LPSI	Low-pressure safety injection	RSS	Reactor Safety Study
LPZ	Low population zone	RVC	Relief valve re-close
LWR	Light water reactor	RWST	Refueling water storage tank
MAAP	Modular Accident Analysis Program	S/D	Shutdown
MACCS	MELCOR Accident Consequence Code System	SAR	Safety Analysis Report
MCS	Minimal cut set	SBO	Station blackout
MDP	Motor-driven pump	SDC	Shutdown cooling
MGL	Multiple Greek letter	SDP	Significance Determination Process
MOV	Motor-operated valve	SER	Safety Evaluation Report (Staff Evaluation Report for IPE/IPEEE)
MSIV	Main steam isolation valve	SG	Steam generator
MSP	Maintenance and Surveillance Program	SGTR	Steam generator tube rupture
MSPI	Mitigating System Performance Index	SHARP	Systematic Human Action Reliability Procedure
NCV	Non-cited violation	SI	Safety injection
NEI	Nuclear Energy Institute	SIF	Seal injection flow
NMSS	Office of Nuclear Materials Safety and Safeguards	SIT	Safety injection tank
NOED	Notice of Enforcement Discretion	SLOCA	Small loss-of-coolant accident
NPP	Nuclear Power Plant	SNL	Sandia National Laboratory
NPRDS	Nuclear Plant Reliability Data System	SPAR	Standardized Plant Analysis Risk
NRC	Nuclear Regulatory Commission	SRA	Senior Reactor Analyst
NRR	Office Nuclear Reactor Regulation	SRI	Senior Resident Inspector
NUMARC	Nuclear Management and Resources Council	SRP	Standard Review Plan
OOS	Out of service	SRV	Safety/relief valve
ORAM	Outage Risk Assessment and Management	SSC	Systems, structures, and components
ORNL	Oak Ridge National Laboratory	SSET	Support state event tree
OSHA	Occupational Safety and Health Administration	STG	Source term group
P&ID	Piping and instrumentation diagram	SW	Service water
PA	Performance assessment	SWGR	Switch gear
PCC	PRA Coordinating Committee	TBCCW	Turbine building closed cooling water
PCS	Power conversion system	TDP	Turbine-driven pump
PDS	Plant damage state	TER	Technical Evaluation Report
PM	Preventive maintenance	THERP	Technique for Human Error Rate Prediction
PORV	Power-operated relief valve	TRC	Time reliability correlation
POS	Plant operating state	USI	Unresolved Safety Issue
PRA	Probabilistic risk assessment	VCT	Volume control tank
PRT	Plant response tree	WOG	Westinghouse Owners' Group
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		
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		
RPS	Reactor protection system		
RPV	Reactor pressure vessel		