



INEEL
Idaho National Engineering & Environmental Laboratory
BECHTEL BWXT IDAHO, LLC

A-35

PRA Basics for Regulatory Applications P-105

US Nuclear Regulatory Commission

Page Intentionally Left Blank

PRA Basics for Regulatory Applications P-105

Bill Galyean, INEEL

Mike Calley, INEEL

June 25 - 27, 2002

NRC Headquarters

Rockville, MD

Page Intentionally Left Blank

PRA Basics for Regulatory Applications

P-105

1. Introduction to Risk-Informed Regulation	1
2. Risk Assessment Concepts & PRA	17
3. Generic Letter 88-20 IPEs/IPEEEs	37
4. Basic PRA Techniques	45
5. Event Tree Analysis	59
6. Fault Tree Analysis	73
7. Component Failure Data	93
8. Human Reliability Analysis	111
9. Sequence Quantification	127
10. Accident Progression & Consequence Analysis	153
11. External Events	171
12. Shutdown Risk	191
13. Uncertainties in PRA	205
14. Configuration Risk Management	221
15. Introduction to Risk-Informed Decision-Making	249
16. Acronyms and Abbreviations	269

Page Intentionally Left Blank

1. Introduction to Risk-Informed Regulation

Introduction to Risk-Informed Regulation

- Purpose: Students will be introduced to the NRC PRA Policy Statement, PRA Implementation Plan, Risk-Informed Implementation Plan, concepts of risk-informed regulation, and potential PRA applications.
- Objectives:
 - ✧ Understand the NRC PRA Policy Statement
 - ✧ Understand PRA Implementation Plan
 - ✧ Understand Risk-Informed Implementation Plan
 - ✧ Understand general concepts of risk-informed regulation
 - ✧ List potential PRA applications

Timeline of NRC PRA Policy Statement, PRA Implementation Plan, and Risk-Informed Regulation Implementation Plan

	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	
PRA Policy Statement												
PRA Implementation Plan												
NRC Strategic plan, FY 2000 - 2005												
Risk-Informed Regulation Implementation Plan; SECY-00-0062, SECY-00-0213, SECY-01-0218						Updated Approximately Every 6 Months						

PRA Policy Statement

- 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 (cont.)

- 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 (cont.)

- 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
- 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

Risk-Informed Regulation Implementation Plan - Overall Objectives and Scope

- Organized to track three principal arenas in Agency's Strategic Plan: Nuclear Reactor Safety, Nuclear Materials Safety, and Nuclear Waste Safety.
- Provide clear objectives and linkages to PRA Policy Statement and to Agency's Strategic Plan.
- 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
- Informs Commission of staff progress via semi-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.
- Implementation can be by various means:
 - ✧ Prescriptive (e.g., design feature, program elements)
 - ✧ Performance-oriented
 - ✧ Risk-oriented

Applications of PRA

- Reactor operations
 - ✧ 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
 - ⤴ Others?
 - ✧ Inspection
 - ⤴ Prioritization and planning
 - ⤴ Evaluation of findings
 - ⤴ Evaluation of licensee use of PRA

Applications of PRA (cont.)

- Resource allocation
 - ✧ Inspection
 - ✧ Regulatory requirements (e.g., NEI initiative)
 - ✧ Research
 - ✧ Regulatory analysis
- Reactor design
 - ✧ Identify weaknesses in design
 - ▲ Risk-significant SSCs
 - ▲ Risk-significant accident scenarios
 - ▲ Risk-significant human actions
- Events analysis and significance
- Non-reactor issues
 - ✧ 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 -- NASA use of PRA (relied largely on FMEAs before Challenger)
- Chernobyl accident -- use of PRA for DOE reactors
- Drell report to U.S. Congress -- risk assessments of nuclear weapons systems
- Economic pressures
- Increased understanding and acceptance of methods
- Increasing availability of cheap, powerful computers

Risk Assessment Training Courses

- **P-102 Probability and Statistics for PRA - (9 days)** This course presents selected quantitative concepts from the fields of probabilistic modeling, statistics, and reliability theory that arise frequently in probabilistic risk assessment (PRA). Through lecture and workshop problems, participants are presented with mathematical techniques from probability and statistics that have applications in current PRA. The topics covered include a review of classical probability and statistics, selected distributions important to PRA, uncertainty analysis techniques, and Bayesian analysis.
- **P-105 PRA Basics for Regulatory Applications - (3 days)** This course addresses the special needs of the regulator who requires knowledge of PRA issues and insights to better evaluate the effects of design, testing, maintenance, and operating strategies on system reliability. The full range of PRA topics is presented in abbreviated form with the goal of introducing the regulatory staffs to the basic concepts and terminology of PRA as applied to the inspection process. The course uses actual plant PRAs and IPEs and stresses the uses and applications of these publications in planning audits and inspections and evaluating plant safety issues.
- **P-107 PRA for Technical Managers - (3 days)** This course introduces the NRC technical manager to PRA concepts including reactor and non-reactor applications. The course includes an introduction to PRA methods used in system modeling, accident progression analysis, accident consequence analysis, and performance assessment. In addition to furnishing a good understanding of the mechanics of a PRA, the course provides information on the more detailed training available to the technical staff, the current agency policy on the use of PRA, information on how the agency has used PRA in making decisions, and the value of and methods for using PRA to get the most benefit from available resources. A discussion of PRA strengths, limitations, and uncertainty is also included.
- **P-111 PRA Technology and Regulatory Perspectives - (9 days)** This course addresses the special needs of Regional Inspectors, Resident Inspectors, and other technical personnel who require knowledge of PRA issues and insights to better evaluate the effects of design, testing, maintenance, and operating strategies on system reliability. The course will concentrate on the use of PRA results in inspection planning, monitoring licensee performance, and reviewing licensee risk-informed submittals.

Risk Assessment Training Courses (continued)

- **P-200 System Modeling Techniques for PRA - (4 days)** This course will help develop advanced user level skills in performing event tree and fault tree analysis, with numerous practice workshops. The course covers the calculation of initiating event frequencies, component failure rate, and the use of "super components" to create fault trees. A second focus of the course is dependent failure analysis, including multiple Greek letter, binomial failure rate, basic parameter methods, and alpha factor methods for estimating common cause/common mode failure probabilities.
- **P-201 SAPHIRE Basics - (4 days)** This course provides hands-on training in the use of Systems Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE) for Windows to perform PRA on a PC. When the course is completed, the participants are able to: build fault tree models on the PC, assign reliability data, analyze the fault trees and develop minimal cut sets, calculate various importance measures, perform uncertainty analysis, analyze accident sequences, create and quantify accident sequences, and generate reports.
- **P-202 Advanced SAPHIRE - (4 days)** This course provides hands-on training in the advanced features of Systems Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE) for Windows to perform PRA on a PC. SAPHIRE allows the user to build and evaluate the models used in PRA.
- **P-203 Human Reliability Assessment - (3 days)** This course serves as an introduction to Human Reliability Assessment (HRA) including the methods used in modeling of human errors and various methods of estimating their probabilities. This course is designed to teach introductory level skills in HRA and includes a broad introduction to HRA and its applications. A discussion of HRA strengths, limitations, and results is also included.
- **P-204 External Events - (3 days)** This course deals with the analysis of external events such as fires, floods, earthquakes, high winds, and transportation accidents. The course has been developed to provide the student with information that can be used in the review of IPEEE results.

Risk Assessment Training Courses (continued)

- **P-300 Accident Progression Analysis - (3 days)** This course deals with the portion of probabilistic risk assessment typically referred to as Level 2 analysis. The course will address accident phenomenology under post-core damage conditions and will discuss development of PRA models for this severe accident regime. The emphasis of the course is on the important modeling issues and how they are dealt with, rather than how to use specific modeling software.
- **P-301 Accident Consequence Analysis - (3 days)** This course deals with the portion of PRA typically referred to as Level 3 analysis. The course addresses environmental transport of radio nuclides and the estimation of offsite consequences from core damage accidents. The emphasis of the course is on important modeling issues and how they are dealt with, rather than how to use specific modeling software.
- **P-302 Risk Assessment in Event Evaluation - (4 days)** This course covers the use of PRA techniques to assess the risk significance of initiating events and condition assessments that occur at operating reactors. The course addresses the use of simplified PRA models to estimate conditional damage probability using the Graphical Evaluation Module (GEM) of the SAPHIRE suite of programs. In addition, common cause and non-recovery probabilities will also be addressed. The course includes conventional workshops and GEM program workshops.
- **P-400 Introduction to Risk Assessment in NMSS - (3 days)** This course introduces risk assessment concepts for Nuclear Material Safety and Safeguards (NMSS) applications. The NRC's policy on the use of risk information as well as the framework for employing risk-informed regulation within NMSS is presented. Various risk assessment concepts and methodologies are introduced and discussed. Examples of the risk assessment methodologies are presented, and some of the strengths and weaknesses associated with the various methodologies are addressed. Several case studies are presented to demonstrate the risk assessment methodology used for the respective study and the risk insights gained are discussed. This course also addresses the perception, communication, and management of risk based on the results obtained from the risk assessment.

Page Intentionally Left Blank

2. Risk Assessment Concepts & PRA

Risk Assessment Concepts & PRA

- **Purpose:** Students will be introduced to the fundamental concepts which underlie risk assessment. Will include discussion of the definition of risk, approaches to risk assessment besides PRA, basic terminology used in risk analysis, and the objectives and limitations of PRA.
- **Objectives:** At the conclusion of this section, students will be able to:
 - ✧ understand basic terms used in risk assessment
 - ✧ identify types of information generated by PRA & example uses
 - ✧ enumerate the basic questions answered by PRA
 - ✧ list several strengths and limitations of PRA
- **References:** NUREG/CR-2300, NUREG-1489

What is Risk?



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

Approaches to Risk Assessment

- Maximum credible accident
- Design basis accident
- Actuarial analysis
- PRA/PSA

Maximum Credible Accident

- Requires worst-case, credible accident to be postulated
- Consequences of accident are estimated
- Example: WASH-740, which estimated offsite consequences of maximum credible accident for commercial U.S. LWR

Maximum Credible Accident (cont.)

DRAWBACKS

- ✎ How to define “credible”
- ✎ Specification of worst-case accident is subjective
- ✎ May lead to overly conservative design or inappropriate focus
- ✎ No consideration given to likelihood of worst-case accident
- ✎ Can lead to belief that “worst case” is bounding

Design Basis Accident

- ⇒ Traditional, deterministic approach to nuclear safety
- ⇒ Plant designed to cope w/specified set of accidents
- ⇒ Only single, active component failures normally considered in DBA approach
- ⇒ TMI-2 accident highlighted problems of this approach

Actuarial Analysis

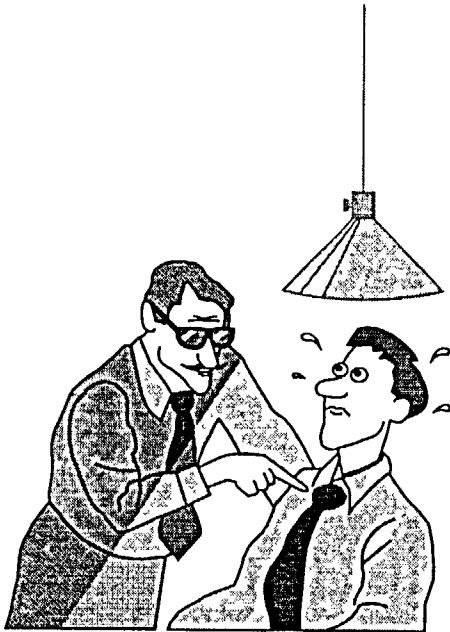
- ✎ Estimates frequencies of accidents from statistical databases
- ✎ Used widely by insurance industry
- ✎ Requires large empirical database

Probabilistic Risk Assessment (PRA)

- An analytical tool to.....
 - ✧ identify accident scenarios
 - ✧ estimate their likelihood of occurrence
 - ✧ estimate their consequences

PRA is a Technical Analysis that systematically answers:

- ✘ What can go wrong?
(accident scenario)
- ✘ How likely is it to occur?
(probability, frequency)
- ✘ What will be the outcome?
(consequences)



$$\text{Risk} = \text{Frequency (Probability)} \times \text{Consequences}$$

Traditional definition of risk

- Frequency, or rate, is the number of occurrences of some event of interest in some defined interval of time
- “Scalarizes” risk

Risk Definition

- Risk - the frequency with which a given consequence occurs

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

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

Risk Example - Death Due to Accidents

$$\text{Societal Risk} = 93,000 \frac{\text{Accidental Deaths}}{\text{Year}}$$

$$\text{Average Individual Risk} = \frac{93,000 \text{ Deaths/Year}}{250,000,000 \text{ Total U.S. Population}} = 3.7 \times 10^{-4} \frac{\text{Deaths}}{\text{Person - Year}}$$

$$\text{Average Individual Risk} \approx \frac{1}{2,700} \frac{\text{Deaths}}{\text{Person - Year}}$$

In any given year, approximately 1 out of every 2,700 people in the entire U.S. population will be in an accident that results in death

Risk Example - Death Due to Cancer

$$\text{Societal Risk} = 538,000 \frac{\text{Cancer Deaths}}{\text{Year}}$$

$$\text{Average Individual Risk} = \frac{538,000 \text{ Cancer Deaths/Year}}{250,000,000 \text{ Total U.S. Population}} = 2.2 \times 10^{-3} \frac{\text{Cancer Deaths}}{\text{Person - Year}}$$

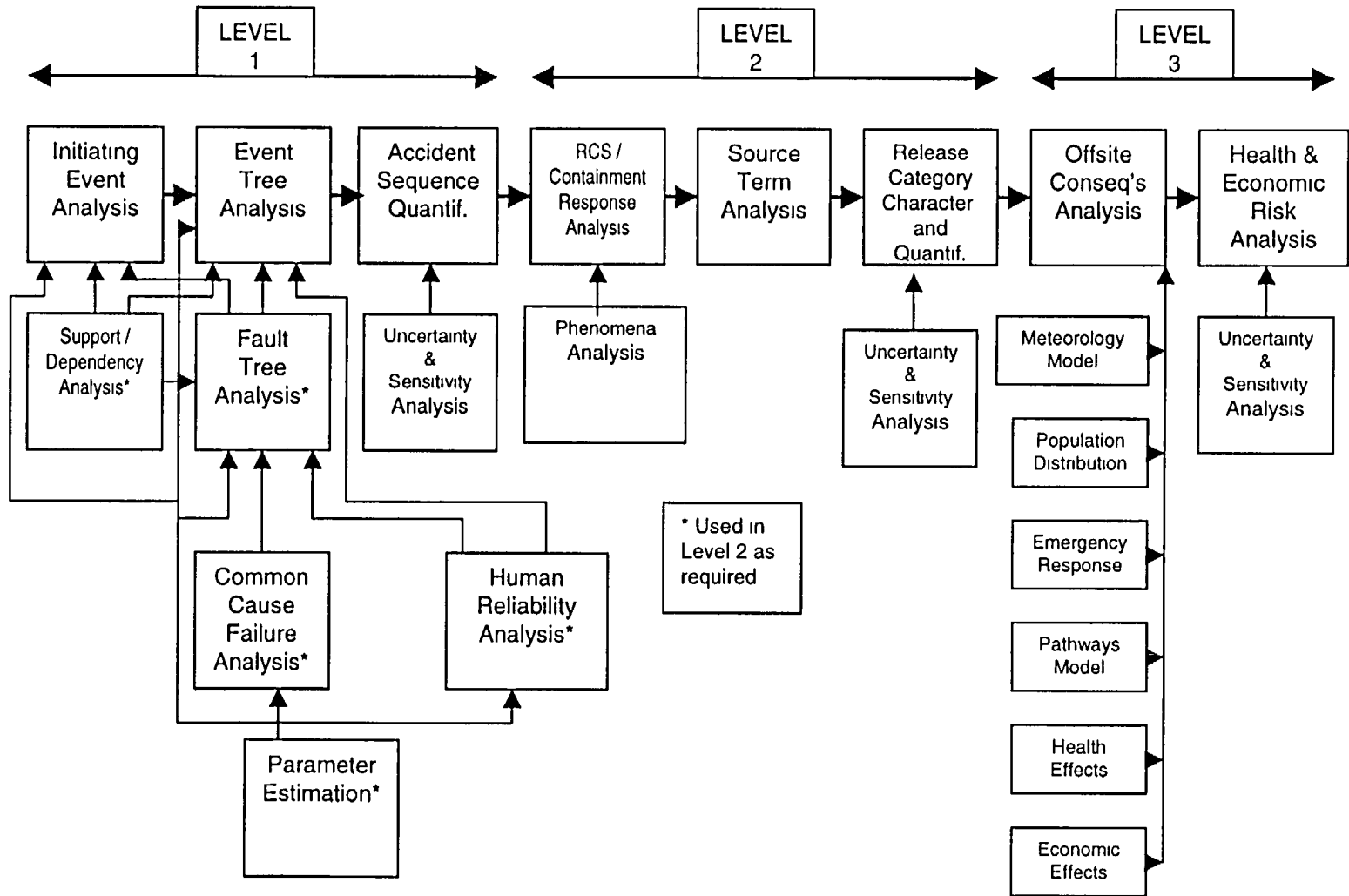
$$\text{Average Individual Risk} \approx \frac{1}{460} \frac{\text{Cancer Deaths}}{\text{Person - Year}}$$

In any given year, approximately 1 out of every 460 people in the entire U.S. population will die due to cancer

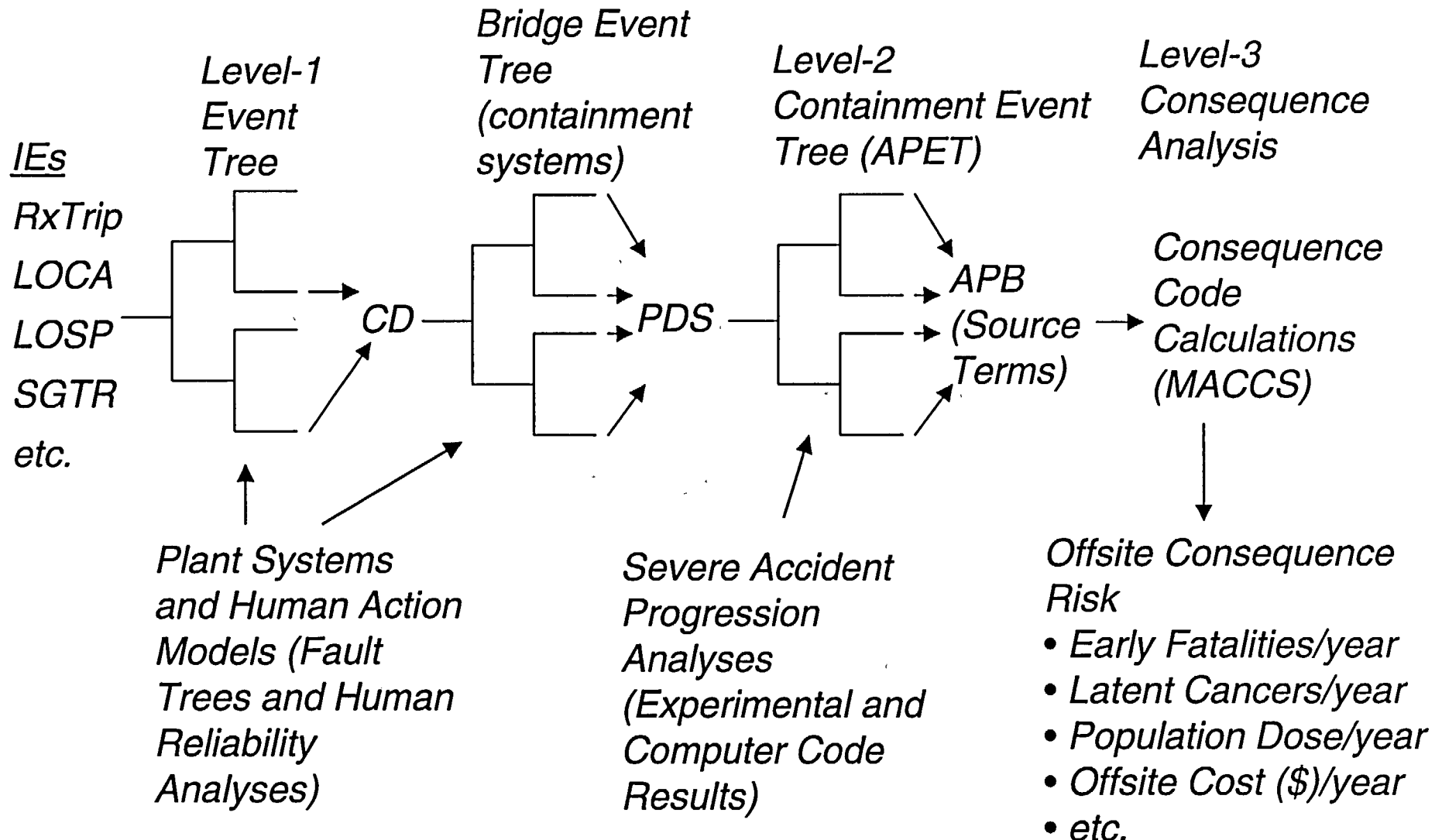
NRC Quantitative Health Objectives

- Originally known as the Probabilistic Safety Goals
 - ✧ NRC adopted the two probabilistic safety goals on August 21, 1986
- High-level goal: incremental risk from nuclear power plant operation $< 0.1\%$ of all risks
 - ✧ Average individual (within 1 mile of plant) early fatality risk $< 5E-7/\text{year}$
 - ✧ Average individual (within 10 miles of plant) latent fatality risk $< 2E-6/\text{year}$
- Lower level subsidiary goals were derived from the high-level QHOs
 - ✧ Frequency of significant core damage (CDF) $< 1E-4/\text{year}$
 - ✧ Frequency of large early release of fission products from containment (LERF) $< 1E-5/\text{year}$

Principal Steps in PRA



Overview of Level-1/2/3 PRA

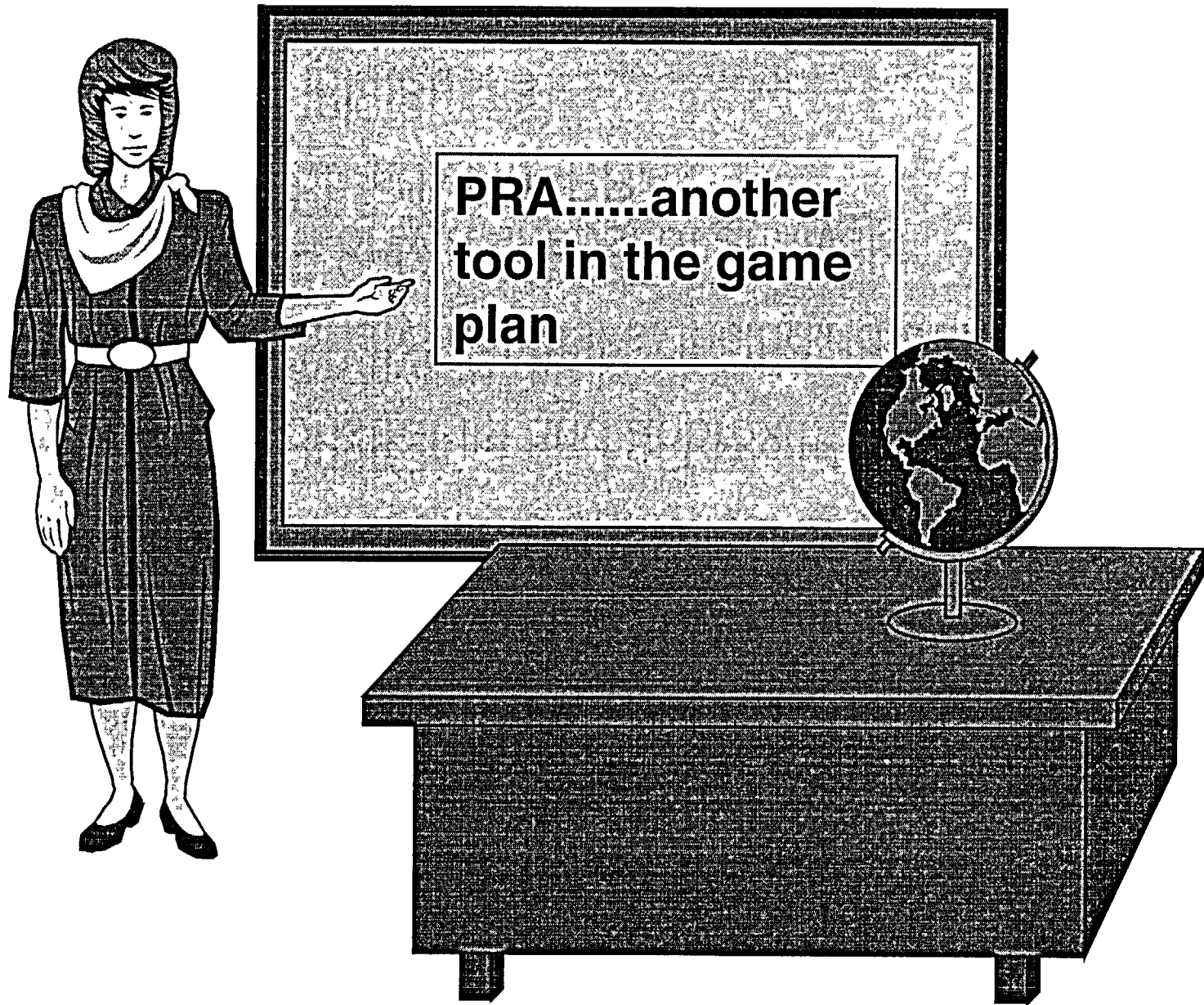


Specific Strengths of PRA

- Rigorous, systematic analysis tool
- Information integration (multidisciplinary)
- Allows consideration of complex interactions
- Develops qualitative design insights
- Develops quantitative measures for decision making
- Provides a structure for sensitivity studies
- Explicitly highlights and treats principal sources of uncertainty

Principal Limitations of PRA

- Adequacy of data base
- Level of understanding of physical processes
- Sensitivity of results to analytical assumptions
- Modeling constraints and approximations
- Bounds on analytical tasks, including truncation
- PRA is often only a snapshot analysis -- there may be a need for a “living” PRA
- Lack of completeness



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

Generic Letter 88-20 IPEs/IPEEEs

- Purpose: Students will be able to understand scope, purpose, and requirements of GL 88-20.
- Objectives: At the conclusion of this topic, students will be able to;
 - ✧ Discuss GL 88-20 (scope, purpose, & requirements)
 - ✧ Relate implications of GL 88-20 to future operation of nuclear power plants
 - ✧ Describe differences between IPE and IPEEE
- References
 - ✧ GL 88-20
 - ✧ NUREG-1335, IPE Submittal Guidance
 - ✧ NUREG-1407, IPEEE Submittal Guidance
 - ✧ NUREG-1560, IPE Insights

Purposes of IPEs/IPEEEs

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

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

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

IPEs (& IPEEEEs) 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 will use PRA to analyze external events
 - ✧ Earthquakes and fires can be analyzed via margins approach
- IPE submittal typically not a full PRA (level of detail varies widely, only full-power operation considered)
- IPEs not performed to support risk-informed, performance-based regulation

Intended NRC Staff Uses of IPE Results

- Vulnerabilities that exist due to failure to meet NRC regulations to be corrected regardless of cost
- Enhancements to safety beyond current NRC regulations to be evaluated in accordance with 10 CFR 50.109 (Backfit Rule)
- Generic vulnerabilities evaluated to determine if existing regulations are adequate

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

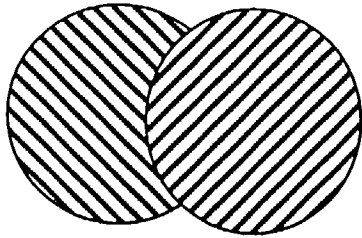
- Requires more detailed reviews of IPE models and data
 - ✧ Currently, NRC reviews IPEs to ensure requirements of GL 88-20 were met by licensee submittal
 - ✧ Current reviews **do not** validate modeling assumptions, input data, or results
 - ✧ SER issued (and sometimes TER) for each IPE (Staff Evaluation Report)

Page Intentionally Left Blank

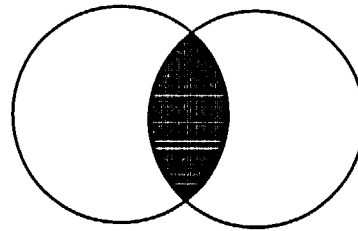
4. Basic PRA Techniques

Basic Probability Concepts

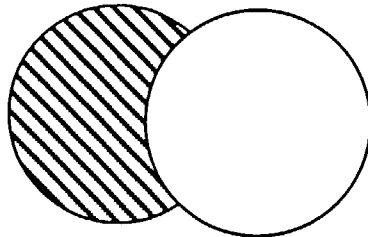
A or B
 $A + B$



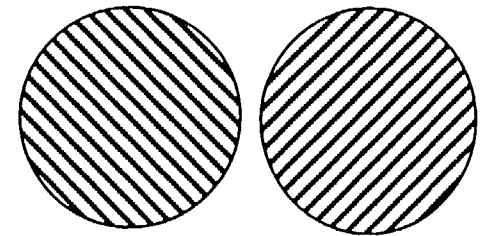
A and B
 $A * B$



A and /B
 $A * /B$



A or B
 $A + B$
*with the two
event
mutually
exclusive*



Common PRA Models

- Event Occurrence Models (Aleatory Uncertainty)

- ✧ Binomial

- ▲ $P\{r \text{ failures in } N \text{ trials} \mid \phi\} = \frac{N!}{r!(N-r)!} \phi^r (1-\phi)^{N-r}$

- ▲ Probability of failure for a single demand

- $P\{1 \text{ failure in } 1 \text{ trial} \mid \phi\} = \phi$

- ✧ Poisson

- ▲ $P\{r \text{ failures in } (0, T) \mid \lambda\} = \frac{(\lambda T)^r}{r!} e^{-\lambda T}$

- ▲ Probability of one or more failures => Exponential

- $P\{T_f < t \mid \lambda\} = 1 - e^{-\lambda t} \approx \lambda t$ (for small λt)

- Model Parameter (i.e., λ and ϕ) Estimates (Epistemic Uncertainty)

- ✧ Lognormal

- ✧ Other (e.g., Gamma, Beta, Maximum Entropy)

PRA Quantify Events as Either a Probability or a Frequency

- Probability
 - ✧ Internal measure of certainty about the truth of a proposition
 - ✧ Always conditional
 - ✧ Unitless
 - ✧ Value between zero and 1.
 - ✧ Used for all events in a PRA except the initiating event
- Frequency
 - ✧ Parameter used in model for aleatory uncertainty
 - ✧ Units of per-demand or per-unit-of-time
 - ✧ Time-based frequencies can be any positive value (i.e., can be greater than one)
 - ✧ Only used for initiating events and failure rates
- Different concepts; sometimes numerically equal

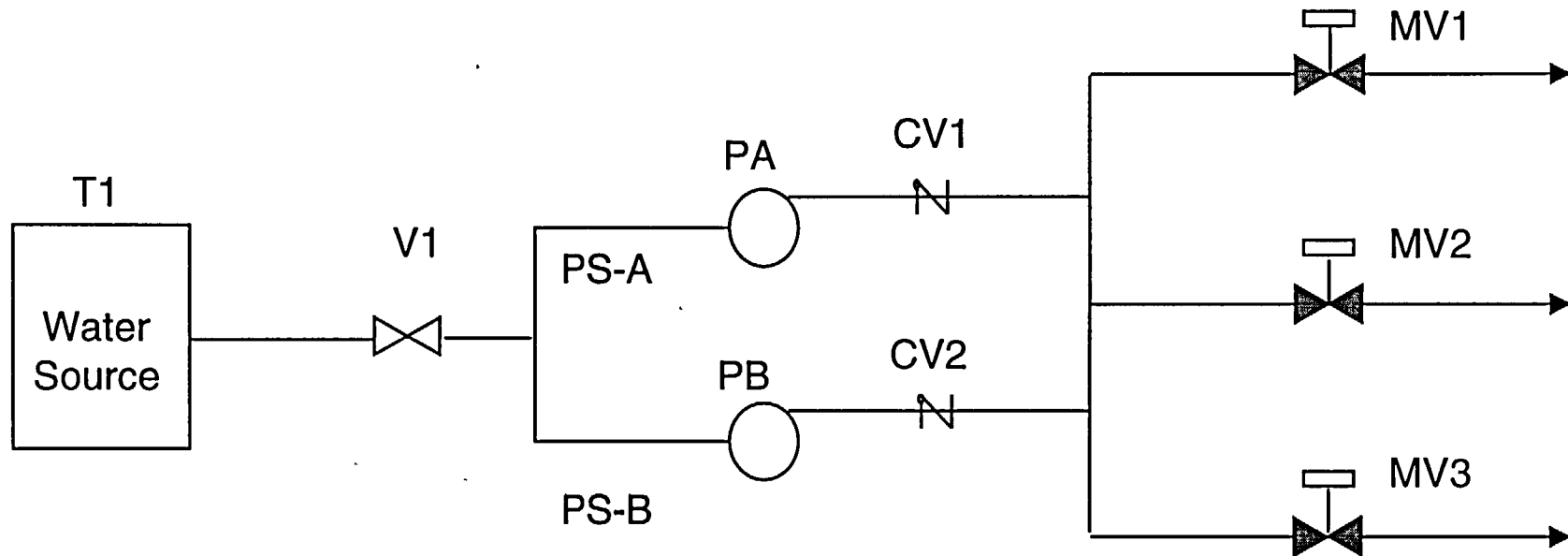
Probability and Frequency Example

- Frequencies (failure rates)
 - ✧ 1×10^{-3} failures/demand (binomial)
 - ✧ 1×10^{-4} failures/operating hours (Poisson)
- Frequencies converted to probabilities based on a specified mission (i.e., probability of successfully completing mission)
 - ✧ $P\{\text{pump fails to start on demand}\}$
 - ✧ $P\{1 \text{ failure in 1 demand}\} = \binom{1}{1} (10^{-3})^1 (1-10^{-3})^0 = 10^{-3}$
 - ✧ $P\{\text{pump fails to run for 24 hrs.}\}$
 - ✧ $P\{\text{failure time} < 24 \text{ hrs}\} = 1 - e^{-(1 \times 10^{-4})(24)} = 2.4 \times 10^{-3} = (24)(1 \times 10^{-4})$

Cutsets

- Combination of events that result in a particular outcome
- Minimal Cutsets 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 cutsets

Cutset Example



Flow from any one pump through any one MV is success

T_ tank

V_ manual valve, normally open

PS_ pipe segment

P_ pump

CV_ check valve

MV_ motor-operated valve, normally closed

Cutsets for ECI

By inspection from (P&ID):

$$\begin{aligned} ECI-Top = & T1 + \\ & V1 + \\ & PA * PB + \\ & PA * CV2 + \\ & PB * CV1 + \\ & CV1 * CV2 + \\ & MV1 * MV2 * MV3. \end{aligned}$$

Cutset Lists Are Quantified Using One of Two Approximation Methods

- Exact Solution for $Top = A + B$:
 - ✧ $P(Top) = P(A + B) = P(A) + P(B) - P(AB)$
- Cross terms become unwieldy for large lists of cutsets. e.g., if $Top = A + B + C$, then:
 - ✧ $P(Top) = P(A) + P(B) + P(C) - P(AB) - P(AC) - P(BC) + P(ABC)$
- Top events typically quantified using either Rare-Event Approximation or Minimal Cutset Upper Bound Approximation

Rare Event Approximation

- $P(\text{Top}) = \text{sum of probabilities of individual cutsets}$
 $= P(A) + P(B)$
- $P(AB)$ judged sufficiently small (rare) that it can be ignored (i.e., cross-terms are simply dropped)
- In general, $P\{\text{TopEvent}\} \leq \sum_{k=1, K} P\{\text{MCS}_k\}$

MinCut UB Approximation

- $P(\text{Top}) = 1 - \text{product of cutset success probabilities}$
$$= 1 - [(1 - P(A)) * (1 - P(B))]$$
- Assumes cutsets are independent
- In general, $P\{\text{TopEvent}\} \leq 1 - \prod_{k=1, K} (1 - P\{\text{MCS}_k\})$

Examples of Cutset Quantification Methods

Top = A + B	$P(A) = 0.01$ $P(B) = 0.03$	$P(A) = 0.4$ $P(B) = 0.6$	$B = /A, P(A) = 0.4$ $P(B) = P(/A) = 0.6$
Exact	$0.01 + 0.03 - (0.01 * 0.03)$ $= 0.0397$	$0.4 + 0.6 - (0.4 * 0.6)$ $= 0.76$	$0.4 + 0.6 - P(A*/A)$ $= 1.0$
Rare Event	$0.01 + 0.03 = 0.04$	$0.4 + 0.6 = 1.0$	$0.4 + 0.6 = 1.0$
MinCut UB	$1 - [(1-0.01) * (1-0.03)]$ $= 0.0397$	$1 - [(1-0.4) * (1-0.6)]$ $= 0.76$	$1 - [(1-0.4) * (1-0.6)]$ $= 0.76$

Probability and Frequency Questions

1. An event occurs with a frequency of 0.02 per year.
 - 1.1. What is the probability that an event will occur within a given year?
 - 1.2. What is the probability that an event will occur during the next 50 years?
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 an event (either A or B) will occur during the next year?
 - 2.2. What is the probability that an event (either A or B) will occur during the next 5 years?
3. An experiment has a probability of 0.2 of producing outcome C. If the experiment is repeated 4 times, what is the probability of observing at least one C?

Page Intentionally Left Blank

5. Event Tree Analysis

Event Tree Analysis

- **Purpose:** Students will learn purposes & techniques of event tree analysis. Students will be exposed to the concept of dominant accident sequences and learn how event tree analysis is related to the identification and quantification of dominant accident sequences.
- **Objectives:**
 - ✧ Understand purposes of event tree analysis
 - ✧ Understand currently accepted techniques and notation for event tree construction
 - ✧ Understand purposes and techniques of dominant accident sequence identification
- **References:** NUREG/CR-2300, NUREG-1489

Event Trees

- Features:
 - ✧ Related to systems/functions
 - ✧ Event sequence progression
 - ✧ End-to-end traceability of accident sequences
- Primary use
 - ✧ Identification of accident sequences which result in some outcome of interest (usually core damage and/or containment failure)
 - ✧ Basis for accident sequence quantification

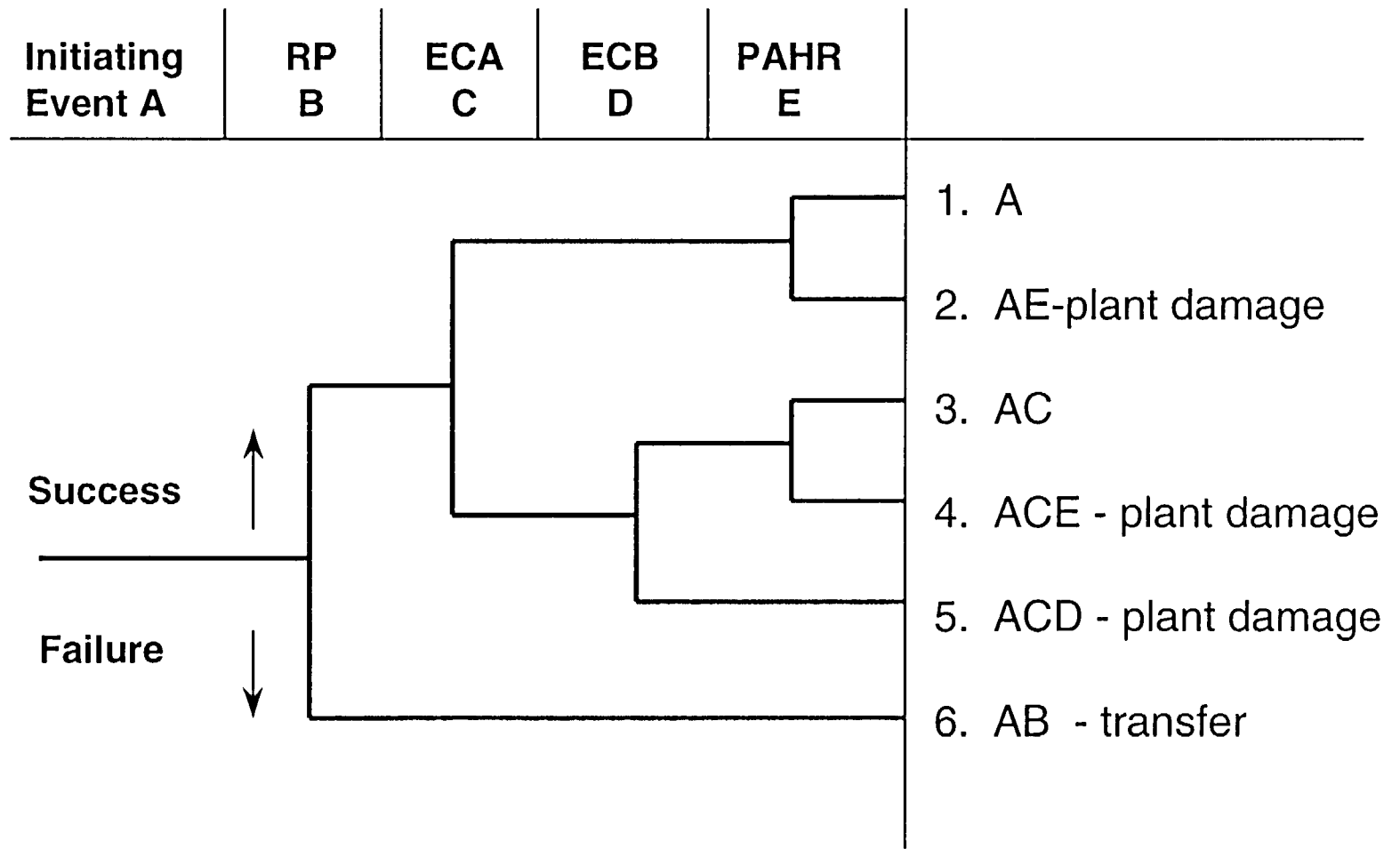
Initiating Events

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

Identification of Initiating Events

- Past operating experience, including similar stations
- Review of other PRAs
- FMEA
- Feedback from system modeling
- Master logic diagram (special type of fault tree)

Simple Functional Event Tree



Principal Steps in Event Tree Development

- Determine boundaries of analysis
- Define safety functions required for initiating event
- Determine success criteria
- Event tree heading - order & development
- Sequence delineation

Determining Boundaries

- Mission time
- End States
 - ✧ Core vulnerable
 - ✧ Containment vulnerable
 - ✧ Core damage
- Extent of operator recovery

Success Criteria

- Start with functional event tree
- Six fundamental safety functions for core & containment
 - Reactor subcriticality
 - Core heat removal
 - Core inventory makeup
 - Containment pressure suppression
 - Containment heat removal
 - Containment integrity

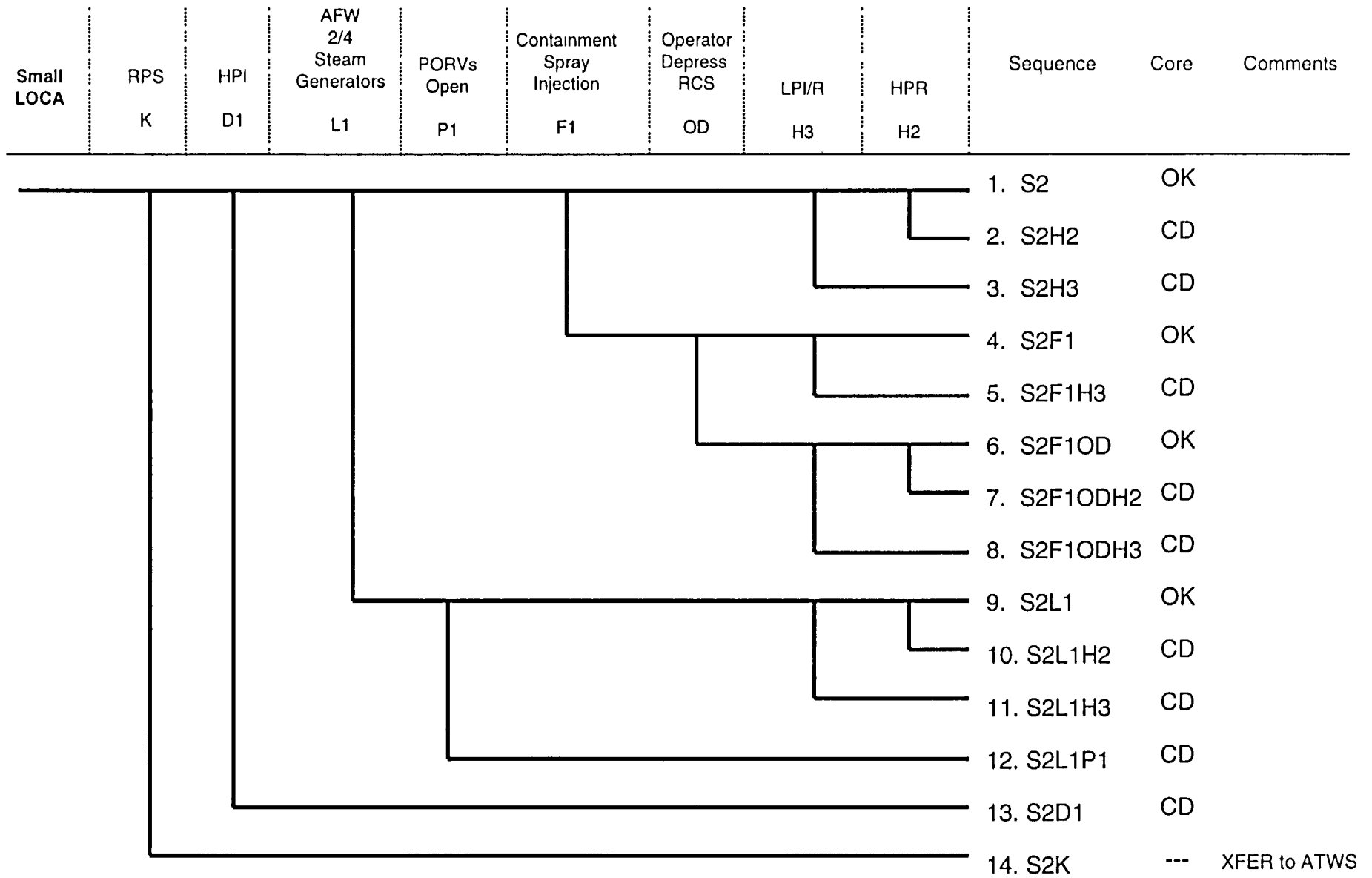
Success Criteria (cont.)

- ✓ Identify systems which can perform each function
- ✓ Identify minimum complement of equipment necessary to perform function (often based on thermal/hydraulic calculations, source of uncertainty)
 - » Calculations often best-estimate, rather than conservative
- ✓ May credit non-safety-related equipment where feasible

Event Tree Development Rules of Thumb

- One event tree per initiating event category
- Systems involved in success criteria become headings
- Logic typically binary (success/failure)
- Ordered in temporal fashion where possible
- Sequence delineation

Event Tree for S₂ - Small LOCA



Plant Damage State

- Sometimes called “Accident Class” or “End State”
- Relates core damage accident sequence to:
 - ✧ Status of system operability
 - ✧ Status of RCS
 - ✧ Status of water inventories
- Used for grouping similar accident sequences for Level 2 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

6. Fault Tree Analysis

Fault Tree Analysis

- **Purpose:** Students will learn purposes & techniques of fault tree analysis. Students will learn how appropriate level of detail for a fault tree analysis is established. Students will become familiar with terminology, notation, and symbology employed in fault tree analysis. In addition, a discussion of applicable component failure modes relative to the postulation of fault events will be presented.
- **Objectives:**
 - ✧ Demonstrate a working knowledge of terminology, notation, and symbology of fault tree analysis
 - ✧ Demonstrate a knowledge of purposes & methods of fault tree analysis
 - ✧ Demonstrate a knowledge of the purposes and methods of fault tree reduction
- **References:**
 - ✧ NUREG-0492, Fault Tree Handbook
 - ✧ NUREG/CR-2300, PRA Procedures Guide
 - ✧ NUREG-1489

Fault Tree Analysis Definition

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

NUREG-0492

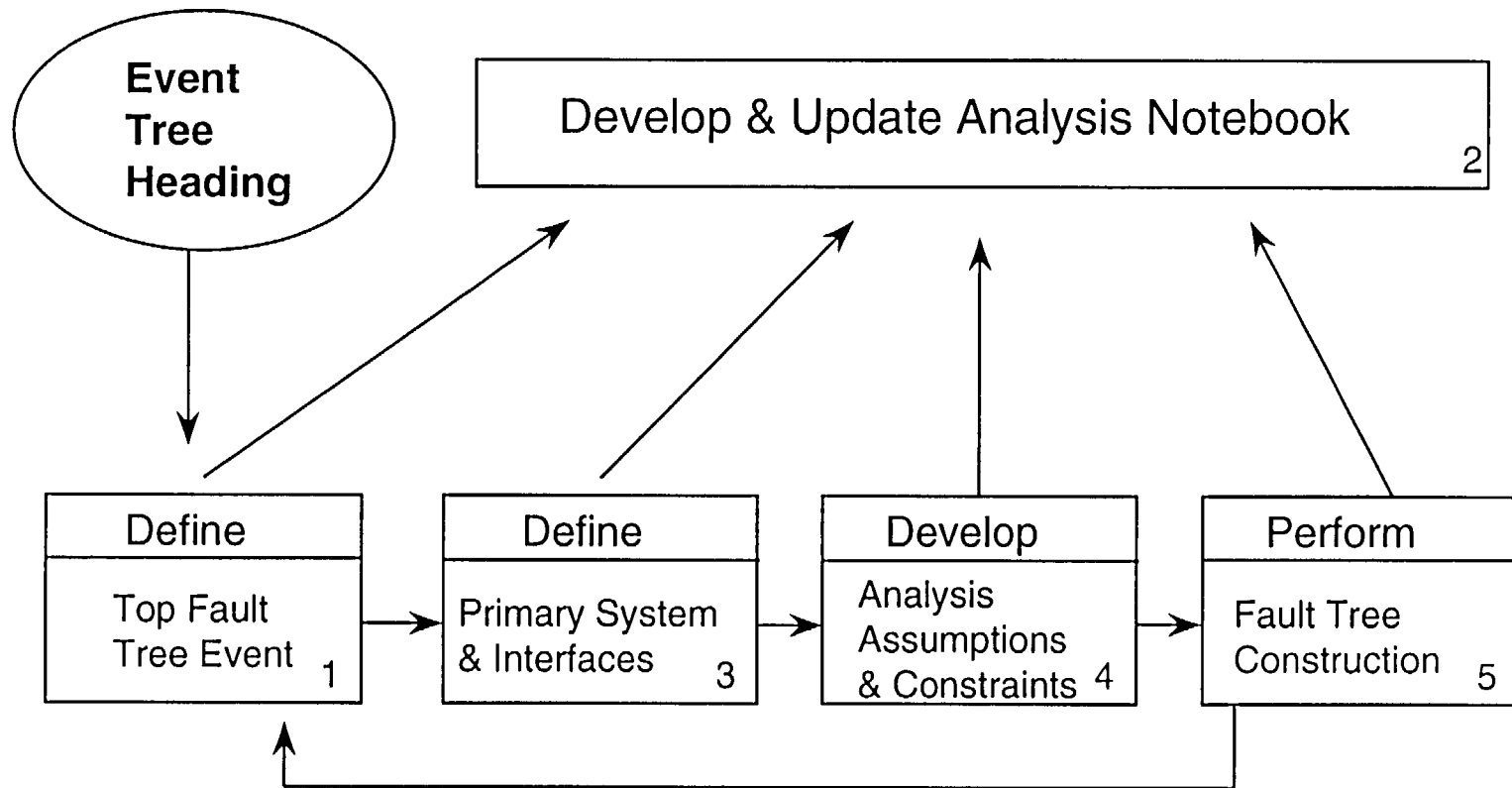
Fault Trees

- Deductive analysis (event trees are inductive)
- Starts with undesired event definition
- Used to estimate system unreliability
- Explicitly models multiple failures

Purpose of Fault Tree Analysis

- Identify ways in which a system can fail
- Models can be used to find:
 - ✧ Interrelationships between fault events
 - ✧ System “weaknesses”
 - ✧ System unreliability (failure probability)

Fault Tree Development Process



1. Define Top Event

- Undesired event or state of system
 - ✧ Based on success criterion for system

2. Develop & Maintain Analysis Notebook

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

3. Define Primary System & Interfaces

- “A collection of discrete elements which interact to perform, in total or in part, a function or set of functions”
- System boundary definition depends on:
 - ✧ Information required from analysis
 - ✧ Level of resolution of data
- Clear documentation of system boundary definition is essential

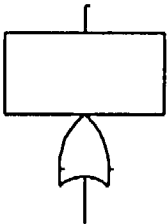
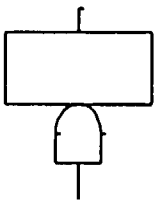
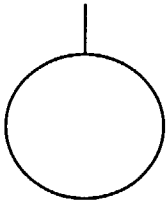
4. Develop Analysis Assumptions & Constraints

- Analytical assumptions must be developed to compensate for incomplete knowledge
- Rationale for assumptions should be specified and, wherever possible, supported by engineering analysis


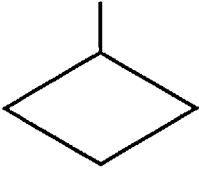
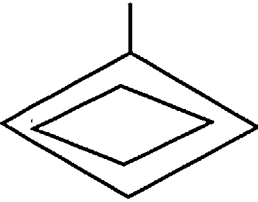
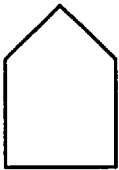
5. Fault Tree Construction

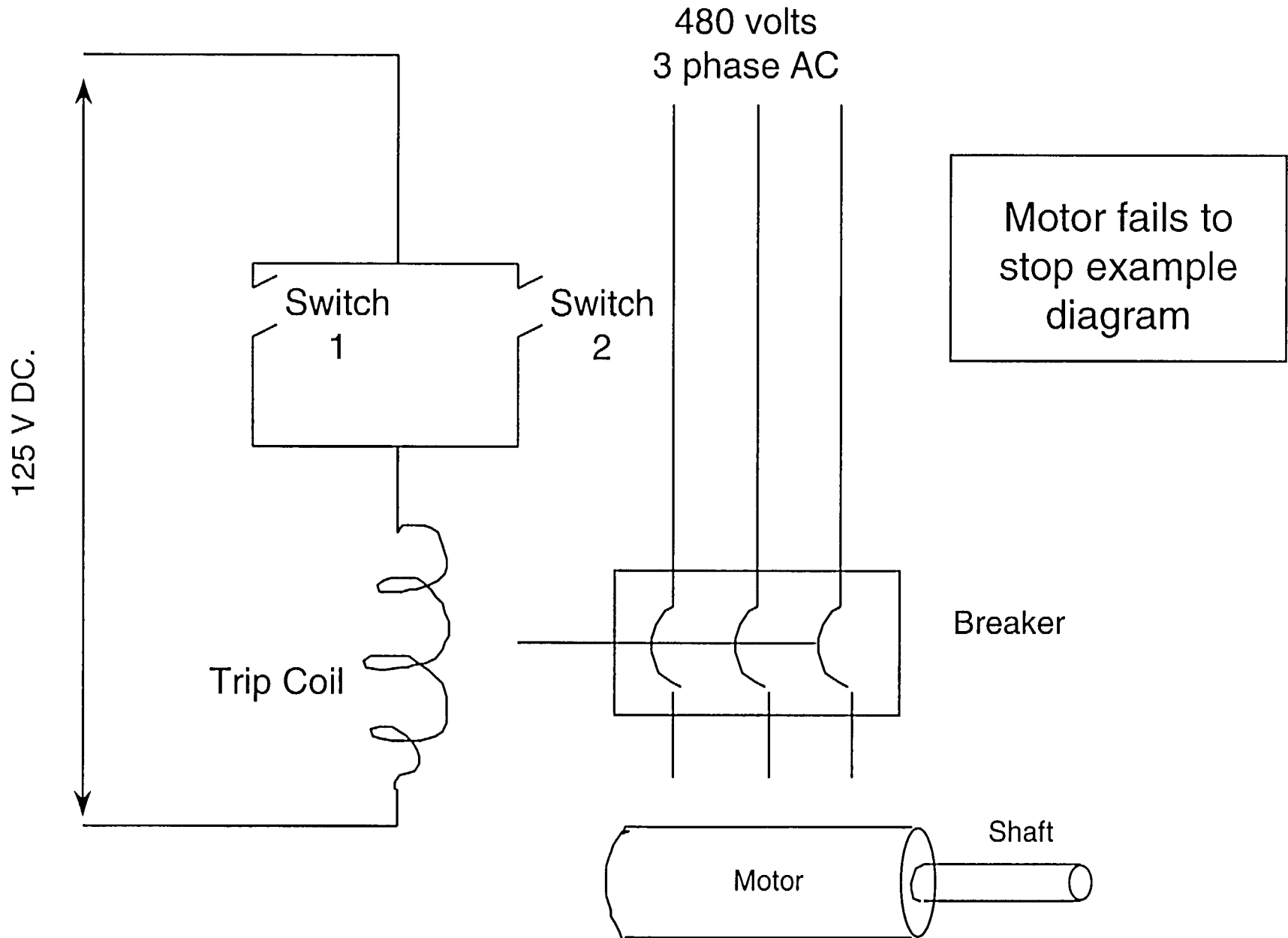
- Step-by-step postulation of system faults
- Utilization of standard symbology
- Postulation consistent with level of resolution of data & assumptions
- Iterative process

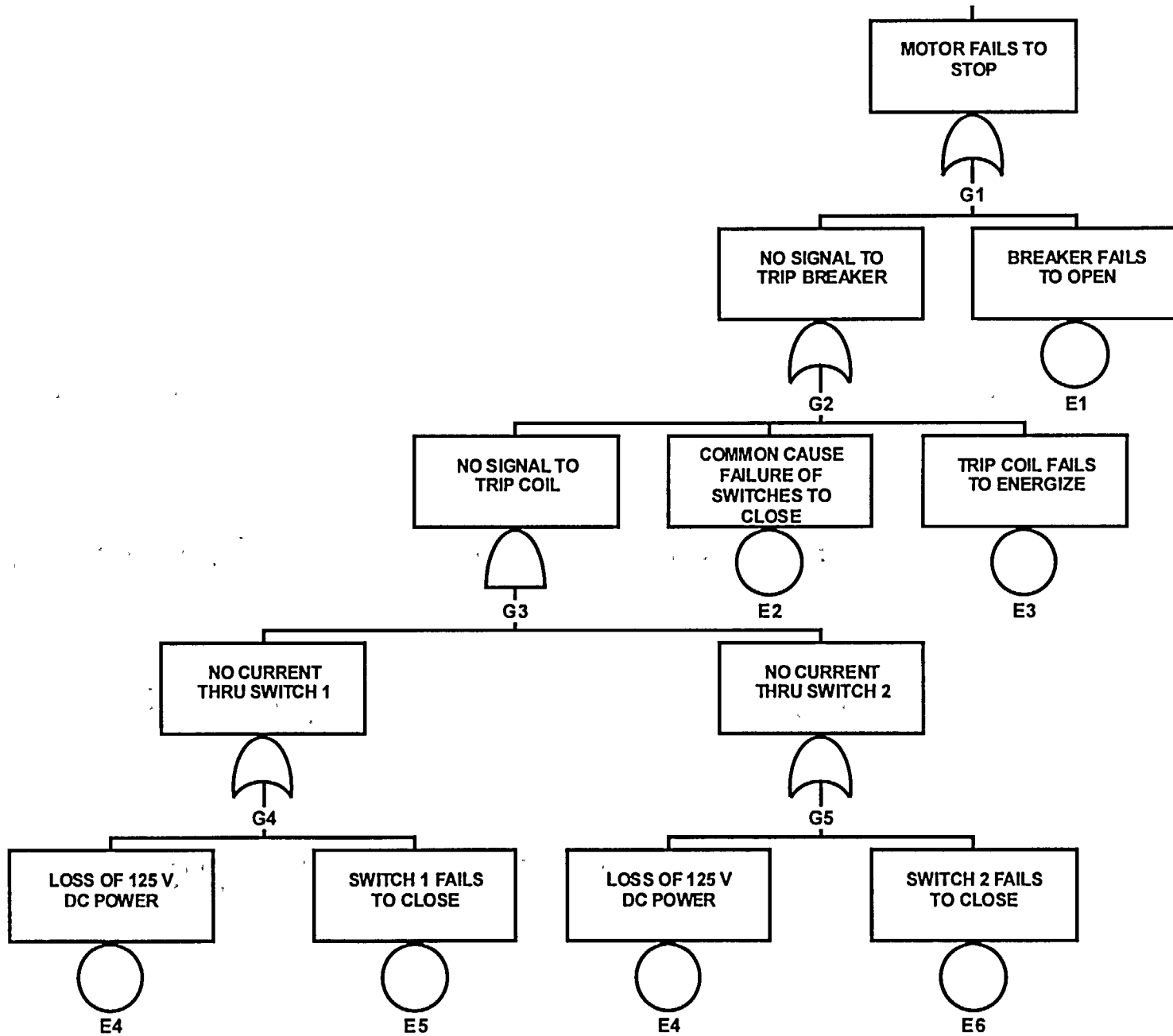
Fault Tree Symbols

Symbol		Description
	"OR" Gate	Logic gate providing a representation of the Boolean union of input events. The output will occur if at least one of the inputs exists.
	"AND" Gate	Logic gate providing a representation of the Boolean intersection of the input events. The output will occur if all of the inputs co-exist.
	Basic Event	A basic component fault which requires no further development. Consistent with level of resolution in databases used to quantify FT

Fault Tree Symbols (cont.)

Symbol		Description
	Transfer Gate	A transfer symbol to connect various portions of the fault tree
	Undeveloped Event	A fault event whose development is limited due to insufficient consequence or lack of additional detailed information
	Undeveloped Transfer Event	A fault event for which a detailed development is provided as a separate fault tree and a numerical value is derived
	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.





Boolean Fault Tree Reduction

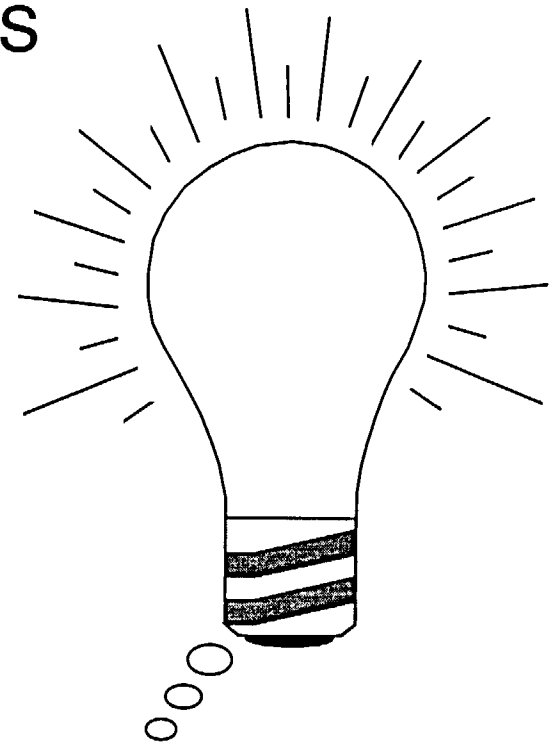
- Express fault tree logic as Boolean equation
- Apply rules of Boolean algebra to reduce terms
- Results in reduced form of Boolean equation

Rules of Boolean Algebra

Mathematical Symbolism	Engineering Symbolism	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

Minimal Cutset

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



Reduction of Example Fault Tree

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

$$G1 = G2 + E1$$

$$G2 = E2 + G3 + E3$$

$$G3 = G4 * G5$$

$$G4 = E4 + E5$$

$$G5 = E4 + E6$$

- Back-substitute

$$G3 = (E4 + E5) * (E4 + E6)$$

$$G2 = E2 + [(E4 + E5) * (E4 + E6)] + E3$$

$$G1 = E2 + [(E4 + E5) * (E4 + E6)] + E3 + E1$$

Reduction of Example Fault Tree (cont.)

- Expand parentheses

$$G1 = E2 + E4 * E4 + E4 * E6 + E5 * E4 + E5 * E6 + E3 + E1$$

- Reduce terms

$$E4 * E4 = E4$$

$$E4 + (E4 * \text{"X"}) = E4$$

$$G1 = E2 + [E4 * E4] + E4 * E6 + E5 * E4 + E5 * E6 + E3 + E1$$

$$G1 = E2 + E4 + E4 * E6 + E5 * E4 + E5 * E6 + E3 + E1$$

$$G1 = E2 + [E4 + E4 * E6] + E5 * E4 + E5 * E6 + E3 + E1$$

$$G1 = E2 + E4 + E5 * E4 + E5 * E6 + E3 + E1$$

$$G1 = E2 + [E4 + E5 * E4] + E5 * E6 + E3 + E1$$

$$G1 = E2 + E4 + E5 * E6 + E3 + E1$$

- Reduced equation is list of minimal cutsets (separated by "+")

$$G1 = E1 + E2 + E3 + E4 + E5 * E6$$

- $Pr(G1) \approx Pr(E1) + Pr(E2) + Pr(E3) + Pr(E4) + [Pr(E5) * Pr(E6)]$

7. Component Failure Data

Component Failure Data

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

Component Failure Modes

- Demand failure
 - ✧ $Q_d = p$
 - ✧ Need number of failures and valid demands to estimate p
- Mission time failure (failure to run)
 - ✧ $Q_r \approx \lambda_h t_m$
 - ✧ Need number of failures and run time to estimate λ_h
- Standby failure
 - ✧ $Q_s \approx \lambda_s t/2$
 - ✧ Need number of failures and time in standby to estimate λ_s
- Test and maintenance unavailability
 - ✧ $Q_m = \lambda_m d_m$
 - ✧ Need Out-of-Service (OOS) time to estimate Q_m
 - ✧ Need maintenance frequency for λ_m

Definition of Terms

- Q = Failure probability (unreliability or unavailability)
- p = Failure rate (per demand)
- λ_s = Failure rate (per hour) standby
- λ_h = Failure rate (per hour) operating
- t_m = mission time
- t_i = surveillance test interval
- λ_m = maintenance frequency
- d_m = maintenance duration

Data Sources for Parameter Estimation

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

Typical Generic Data Sources

- NUREG-1150 supporting documents (NUREG/CR-4550 series, pre-1987)
- WASH-1400 (pre-1975)
- 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-5496 loss of offsite power (1980-1996)
- Institute of Nuclear Power Operations Nuclear Plant Reliability Data System (NPRDS)
 - ✧ Being replaced with EPIX

Plant-Specific Data Sources

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

Plant-Specific Data Issues

- Combination of data sources
- Adequacy of sample size
- Accuracy/uniformity of reporting
- Difficulty in interpreting “raw” failure data

Bayes' Theorem is Basis for Bayesian Updating of Data

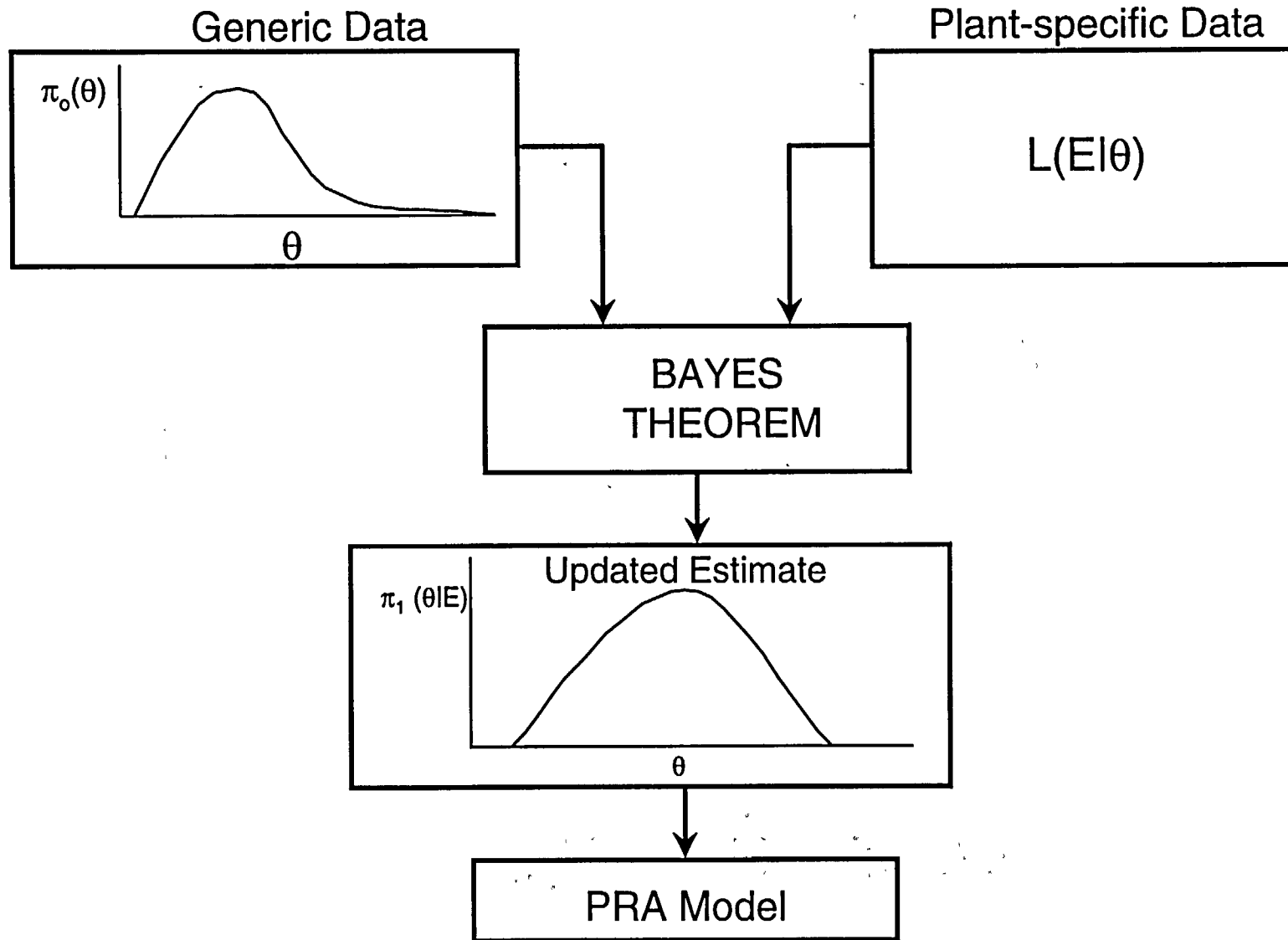
- Typical use: sparse plant-specific data combined with generic data using Bayes' Theorem:

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

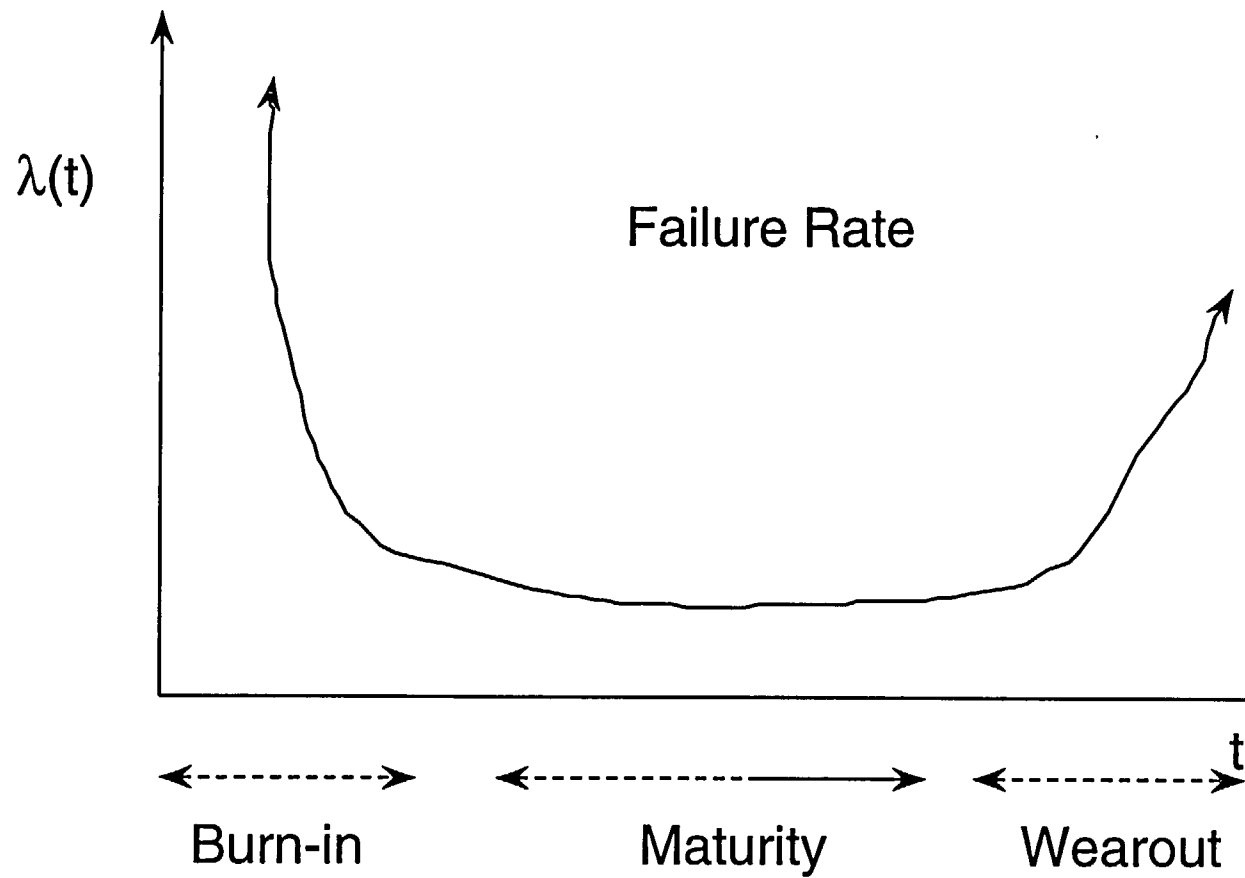
Bayes' Theorem (cont.)

- $\pi_0(\theta)$ is prior distribution (generic data)
- $L(E|\theta)$ is likelihood function (plant-specific data)
- $\pi_1(\theta|E)$ is posterior distribution (updated estimate)

Bayesian Updating



The “Bathtub” Curve



The “Bathtub” Curve (cont.)

- Most PRAs assume constant failure rates -- in “flat” portion of bathtub curve
 - ✧ May not be all that bad of an assumption considering quality level of equipment, maintenance, and testing requirements
 - ✧ However, this assumption does imply that aging (increasing failure rate) may not be modeled in the PRA

Definition of Dependent Failures

- Three general types of dependent failures:
 - ✧ Certain initiating events (e.g., fires, floods, earthquakes, service water loss)
 - ✧ Intersystem 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)
 - ✧ Intercomponent 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 (i.e., the residual dependencies not explicitly modeled) and is treated parametrically

Common Cause Failures

- Conditions which may result in failure of more than one component, subsystem, or system
- Concerns:
 - ✧ Defeats redundancy and/or diversity
 - ✧ Data suggest high probability of occurrence relative to multiple independent failures

Common Cause Failure Mechanisms

- Environment
 - ✧ Radioactivity
 - ✧ Temperature
 - ✧ Corrosive environment
- Design deficiency
- Manufacturing error
- Test or Maintenance error
- Operational error

Common Cause Modeling in PRA

Various Parametric Models are Used

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

- Beta factor (subset of multiple Greek letter method)
- Similar for three or more failures
- Apply to cut sets containing same failure mode for sample component type
 - ✧ Diesel generators
 - ✧ MOVs, AOVs, PORVs, SRVs
 - ✧ Pump
 - ✧ Batteries

Beta Factor Example

- High pressure pumps
 - ✧ $\beta = 10 \text{ CCF} \div 47 \text{ total failures} \approx 2.1\text{E-1}$
 - ✧ Motor-driven pump fail to start = 3.0E-3 per demand
- Cut set: HPI-MDP-FS-A * HPI-MDP-FS-B
- Independent failure $\approx 3\text{E-3} * 3\text{E-3} = 9\text{E-6}$
- $\text{CCF} = 3\text{E-3} * \beta = 6\text{E-4}$

8. 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:
 - ✧ 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).
 - ✧ EPRI-NP-3583, Systematic Human Action Reliability Program, 1984

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, or 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.

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
 - ✧ As a contribution or cause to initiating events

Categories Of Human Error (cont.)

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

Types Of Human Error

- Generally, two types of human errors are defined:
 - ✧ Errors of omission -- Failure to perform a required action or step, e.g., failure to monitor makeup tank level
 - ✧ Errors of commission-- Action performed incorrectly or wrong action performed, e.g., opening the wrong valve, turning off SI
- Normally only the first type is modeled due to uncertainty in being able to identify errors of commission, and lack of modeling and quantification methods to address such errors
 - ✧ ATHEANA research program is directed at errors of commission

HRA Process

- 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.)

❖ 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

Performance Shaping Factors (PSFs)

- Are people-, task-, environmental-centered influences which serve to 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

Evaluating PSFs

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	Unkept facility, lack of procedures, compliance, 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

How Human Actions Are Incorporated Into PRA Model

- Most human errors appear as fault tree basic events
- Some errors modeled in event trees (e.g., BWR failure to depressurize)
- Recovery actions added manually to results of model solution

Sources of HRA Data

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

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 (several 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

Page Intentionally Left Blank