

Idaho National Engineering and Environmental Laboratory

PRA Basics for Regulatory Applications P-105

Course Presented by:

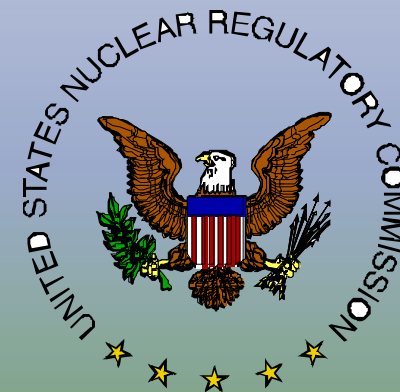
Mike Calley, INEEL

Scott Beck, INEEL

October 19 – 21, 2004

NRC Region I

King of Prussia, PA



PRA Basics for Regulatory Applications P-105

<i>Acronyms and Abbreviations</i>	3
<i>Brief Annotated Bibliography</i>	7
<i>Risk Assessment Training Courses</i>	11
1. <i>Risk Assessment Concepts & PRA</i>	17
2. <i>Basic PRA Techniques</i>	39
3. <i>Event Tree Analysis</i>	55
4. <i>Fault Tree Analysis</i>	73
5. <i>Component Failure Data</i>	95
6. <i>Human Reliability Analysis</i>	115
7. <i>Sequence Quantification</i>	135
8. <i>Accident Progression & Consequence Analysis</i>	163
9. <i>External Events</i>	183
10. <i>Shutdown Risk</i>	205
11. <i>Uncertainties in PRA</i>	221
12. <i>Introduction to Risk-Informed Regulation</i>	237
13. <i>Generic Letter 88-20 IPEs/IPEEEs</i>	251
14. <i>Configuration Risk Management</i>	265
15. <i>Introduction to Risk-Informed Decision-Making</i>	293

Idaho National Engineering and Environmental Laboratory

Acronyms and Abbreviations



Acronyms and Abbreviations (1 of 3)

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

Acronyms and Abbreviations (2 of 3)

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

Acronyms and Abbreviations (3 of 3)

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

Idaho National Engineering and Environmental Laboratory

Brief Annotated Bibliography



Bibliography (1 of 3)

U.S. NRC, 1975, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), October 1975.
Original full Level-3 PRA, NRC sponsored, project team headed by Prof. N. Rasmussen (MIT).

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

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

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

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

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

Swain, A. D. and H. E. Guttman, 1983, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application, NUREG/CR-1278, October 1983.
A Technique for Human Error Rate Prediction (THERP), basic human reliability analysis and quantification method still commonly used.

Bibliography (2 of 3)

Apostolakis, G., 1990, "The Concept of Probability in Safety Assessments of Technological Systems," Science, 250, 1359-1364.

Interesting reading with respect to how the term probability is interpreted.

U.S. NRC, 1990, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, Vol. 1-3.

Second major assessment (after WASH-1400) of NPP risks sponsored by NRC. Supporting work documented in series of NUREG/CRs (NUREG/CR-4550, Vol. 1-7, Rev. 1 – Level-1 PRAs; NUREG/CR-4551, Vol. 1-7, Rev. 1 – Level-2 portions of the PRAs).

IAEA, 1990, Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessment, IAEA-TECDOC-543.

International perspective on PRA (commonly referred to as PSA outside the U.S.).

U.S. NRC, 1993, Evaluation of Severe Accident Risks, NUREG/CR-4551, Volumes 1 - 7, Dates: various (1990 - 1993).

Most comprehensive Level-2 analysis ever performed, developed Accident Progression Event Tree (APET) method of modeling containment performance (i.e., event tree with 75 - 125 top events).

U.S. NRC, 1994, A Review of NRC Staff Uses of Probabilistic Risk Assessment, NUREG-1489, March 1994.

Survey of NRC uses of PRA, includes appendices that provide guidance on how to use PRA and on PRA methods.

Bibliography (3 of 3)

*U.S. NRC, 1997, Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance, NUREG-1560, Volumes 1, 2 & 3, December 1997.
Extracted and summarizes highlights and insights from the collective IPE results (75 IPEs covering 108 NPP units), including containment performance issues.*

*U.S. NRC, 1989, Individual Plant Examination Submittal Guidance, NUREG-1335, August 1989.
Provided guidance to licensees on how to satisfy the requirements of Generic Letter 88-20.*

*U.S. NRC, 1991, Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, NUREG-1407, June 1991.
Provided guidance to licensees on how to satisfy the requirements of Generic Letter 88-20 supplement 4.*

*U.S. NRC, 1994, Revised Livermore Seismic Hazard Estimates of 69 Nuclear Plant Sites East of the Rocky Mountains, NUREG/CR-1488, April 1994.
Revised the seismic hazard curves originally published in NUREG/CR-5250, Seismic Hazard Characterization of 69 Nuclear Power Plant Sites East of the Rocky Mountains, January 1989.*

Idaho National Engineering and Environmental Laboratory

Risk Assessment Training Courses



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

Risk Assessment Training Courses (continued)

- **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.*
- **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.*

Risk Assessment Training Courses (continued)

- **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.*
- **P-401 Introduction to Risk Assessment in NMSS Overview - (1 day)** *This course provides an overview of risk assessment concepts for Nuclear Materials Safety and Nuclear Waste Safety applications. The NRC's policy on the use of risk information as well as the framework for employing risk-informed regulation within the Office of Nuclear Material Safety and Safeguards (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. This course also addresses the topics of risk perception, risk communication, and risk management.*
- **P-406 Human Error Analysis/Human Reliability Analysis for NMSS - (2-1/2 days)** *This course serves as an introduction to Human Error Analysis/Human Reliability Analysis for Nuclear Material Safety and Safeguards (NMSS) applications. This course provides an overview of HRA, introduces the concepts and methods useful in examining human error, sensitizes staff to recognize the need and importance of HRA in their daily work, and reviews the contribution of human error to select NMSS events. As part of this overview, students are introduced to key components of HRA - error taxonomies, performance shaping factors and context, error identification, error modeling and error quantification. This course also introduces various methods used when estimating human error probabilities. A discussion of human error analysis/human reliability analysis strengths, limitations, and results is also included.*

Page Intentionally Left Blank

Idaho National Engineering and Environmental Laboratory

1. Risk Assessment Concepts & PRA



Risk Assessment Concepts & PRA

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

Several Example Approaches for Assessing Risk

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

Maximum Credible Accident (cont.)

DRAWBACKS

- *How to define “credible”*
- *Specification of worst-case accident is subjective*
- *May lead to overly conservative design or inappropriate focus*
- *likelihood of worst-case accident not quantified*
- *Implication that “worst case” is bounding for all situations might not be true*

Design Basis Accident

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

Actuarial Analysis

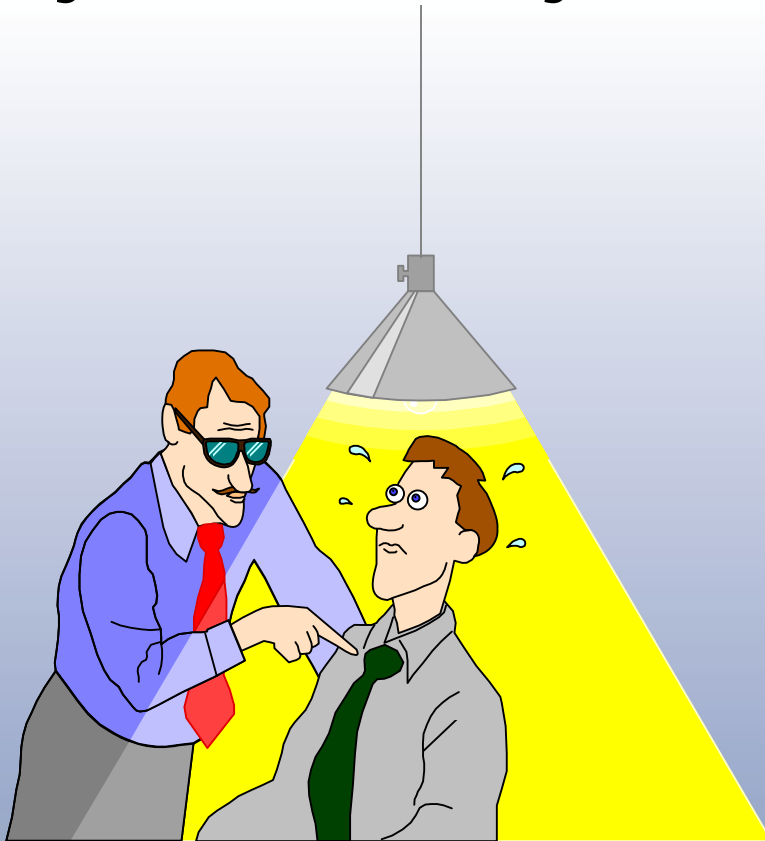
- *Estimates frequencies of accidents from statistical databases*
- *Used widely by insurance industry*
- *Requires large empirical database (which fortunately the commercial nuclear power industry does not have)*

Probabilistic Risk Assessment (PRA)

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

PRA is a Technical Analysis that systematically answers :

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



These three questions are commonly referred to as the risk triplet

Risk = Frequency (Probability) x Consequences

Traditional definition of risk

- *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 * consequence)*

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

- *Societal Risk = 93,000 accidental-deaths/year*
(based on Center for Disease Control actuarial data)
- *Average Individual Risk*
 - = *(93,000 Deaths/Year)/250,000,000 Total U.S. Pop.*
 - = *3.7E-04 Deaths/Person-Year*
 - ≈ *1/2700 Deaths/Person-Year*
- *In any given year, approximately 1 out of every 2,700 people in the entire U.S. population will suffer an accidental death*
- *Note: www.cdc.gov latest data (2001) 101,537 unintentional deaths and 284,797,000 U.S. population, thus average individual risk ≈ (101,537 deaths/year)/284,797,000 ≈ 3.6E-04 Deaths/Person-Year*

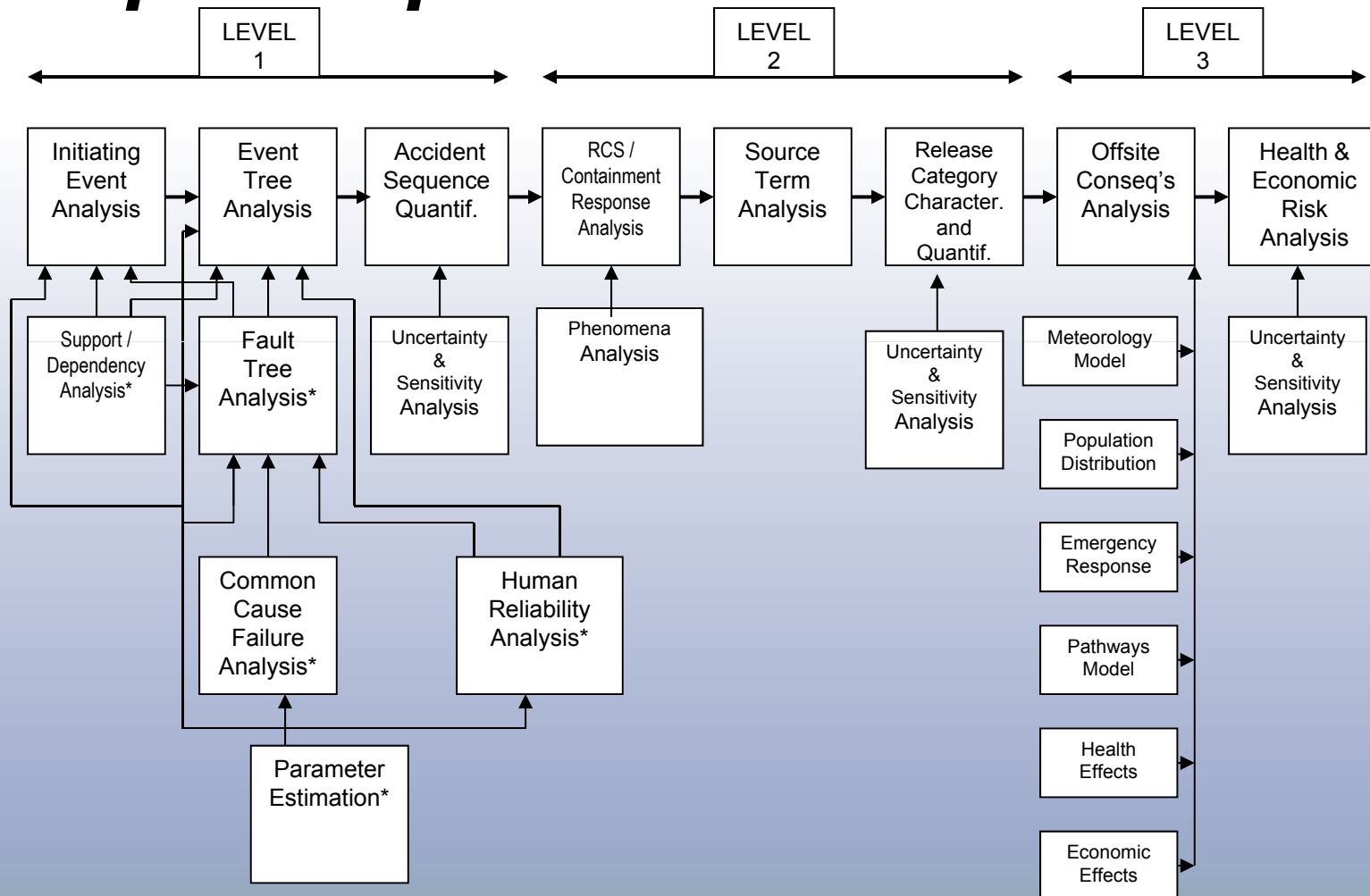
Risk Example - Death Due to Cancer

- *Societal Risk = 538,000 cancer-deaths/year
(based on Center for Disease Control actuarial data)*
- *Average Individual Risk
= (538,000 Cancer-Deaths/Year)/250,000,000 Total U.S. Pop.
= 2.2E-03 Cancer-Deaths/Person-Year
≈ 1/460 Cancer-Deaths/Person-Year*
- *In any given year, approximately 1 person out of every 460 people in the entire U.S. population will die from cancer*
- *Note: www.cdc.gov latest data (2001) 553,768 cancer deaths and 284,797,000 U.S. population, thus average individual risk ≈ (553,768 deaths/year)/284,797,000
≈ 1.9E-03 Deaths/Person-Year*

NRC Quantitative Health Objectives (QHOs)

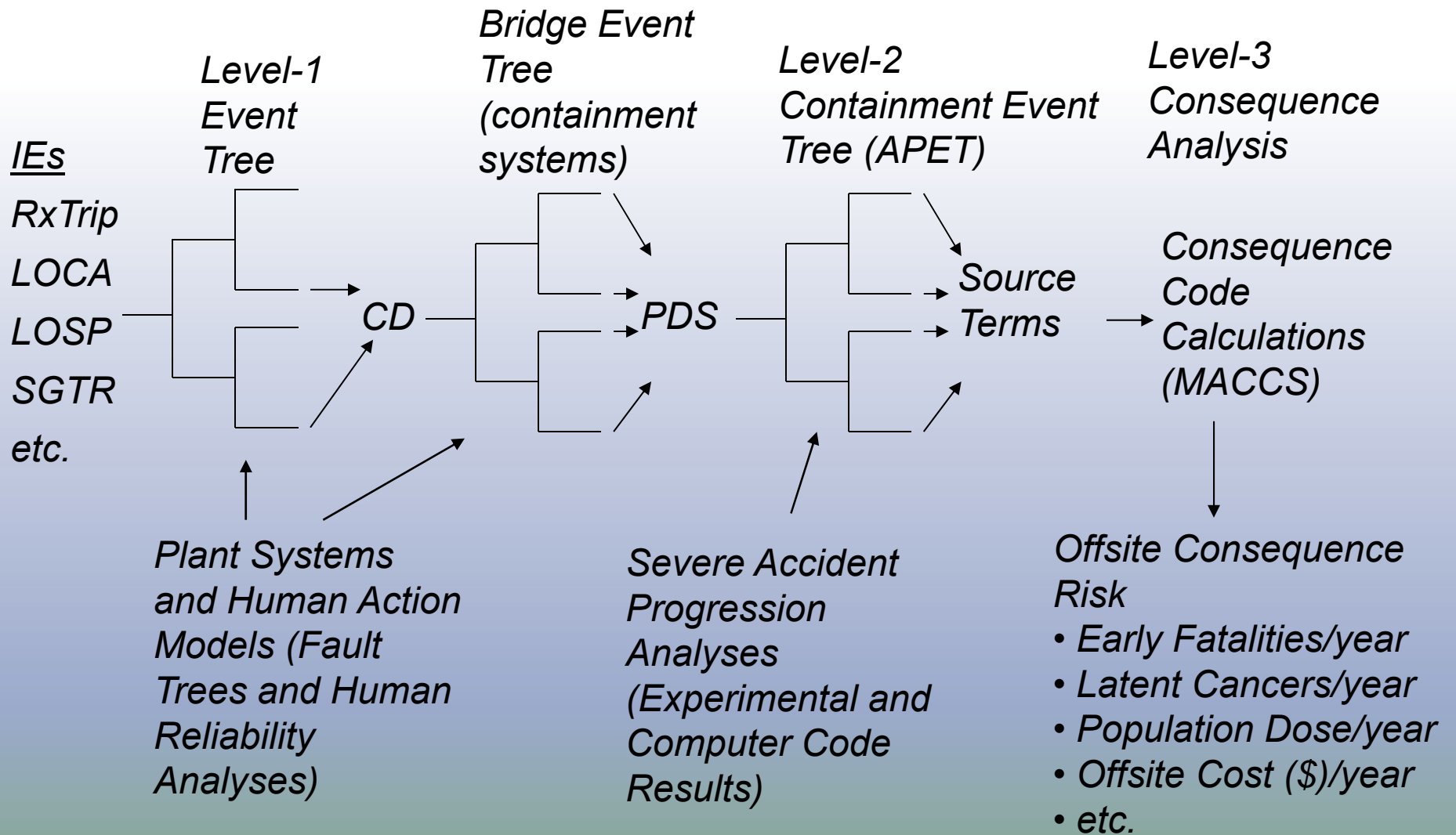
- *Originally known as the Probabilistic Safety Goals*
 - *NRC adopted two probabilistic safety goals on August 21, 1986*
- *High-level goal: incremental risk from nuclear power plant operation < 0.1% of all risks*
 - *Average individual (within 1 mile of plant) early fatality (accident) risk*
 - < $5E-7$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

Principal Steps in PRA



* Used in Level 2 as required

Overview of Level-1/2/3 PRA

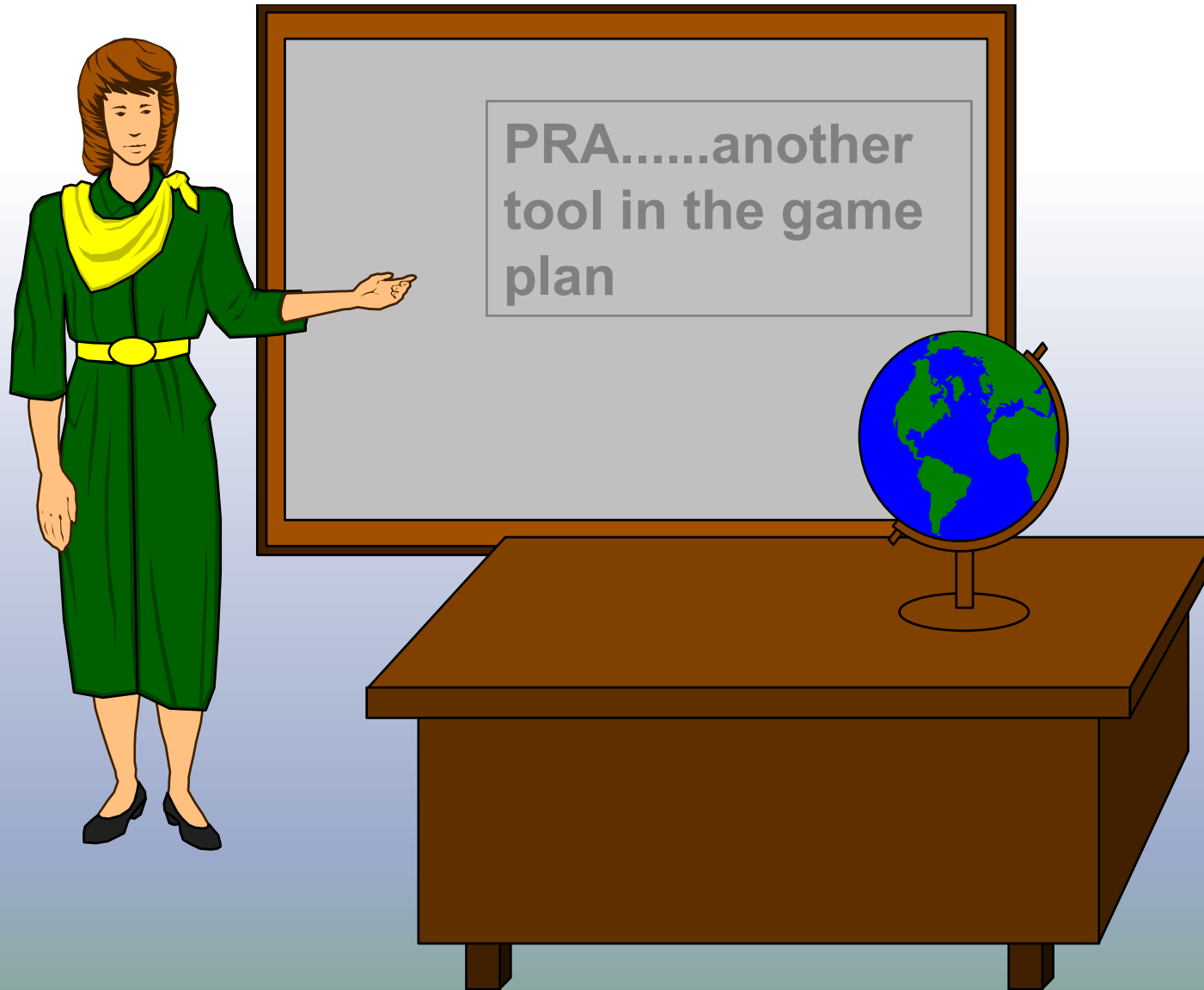


Specific Strengths of PRA

- *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

- *Inadequacy of available data*
- *Lack of understanding of physical processes*
- *High sensitivity of results to assumptions*
- *Constraints on modeling effort (limited resources)*
 - *simplifying assumptions*
 - *truncation of results during quantification*
- *PRA is typically a snapshot in time*
 - *this limitation may be addressed by having a “living” PRA*
 - *plant changes (e.g., hardware, procedures and operating practices) reflected in PRA model*
 - *temporary system configuration changes (e.g., out of service for maintenance) reflected in PRA model*
- *Lack of completeness (e.g., human errors of commission typically not considered)*



Review Risk Assessment Concepts & PRA Purpose and Objectives

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

Page Intentionally Left Blank

Idaho National Engineering and Environmental Laboratory

2. Basic PRA Techniques

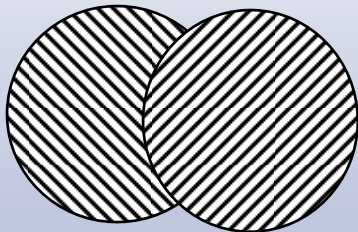


Basic PRA Techniques

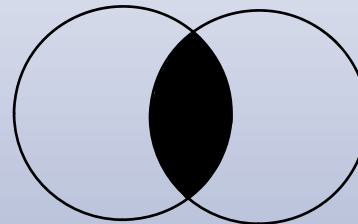
- *Purpose: Introduce/review elementary probability concepts, with focus on PRA relevant items*
- *Objectives: At the conclusion of this section, students will understand :*
 - *Basic probability operations*
 - *Difference between frequency and probability*
 - *How to calculate probability from a frequency*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

Basic Probability Concepts Used in PRAs

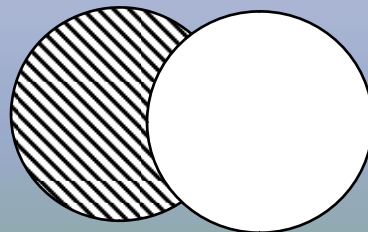
A or B
 $A + B$



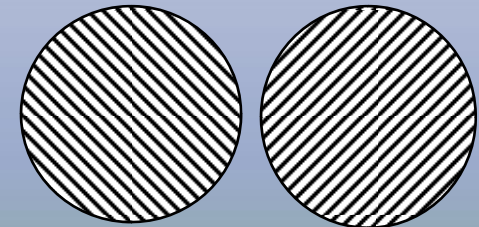
A and B
 $A * B$



A and /B
 $A * /B$



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



Each Event has a Frequency which is used to Calculate a Probability

- *Frequency*
 - *Parameter used in model for stochastic (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*
- *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 PRA Models

- *Event Frequency Models (i.e., λ and ϕ)*
 - *Lognormal*
 - *Other (e.g., Gamma, Beta, Maximum Entropy)*
 - *Event Probability Models*
 - *Binomial (used for failures on demand)*
 - $P\{r \text{ failures in } N \text{ trials} \mid \phi\} = \frac{N!}{r!(N-r)!} \phi^r (1-\phi)^{N-r}$
 - *Probability of failure for a single demand*
 - $P\{1 \text{ failure in } 1 \text{ trial} \mid \phi\} = \phi$
 - *Poisson (used for failures/events in time)*
 - $P\{r \text{ failures in } (0,t) \mid \lambda\} = \frac{(\lambda t)^r}{r!} e^{-\lambda t}$
 - *Probability of one or more failures (Poisson simplifies to exponential)*
 - $P\{T_f < t \mid \lambda\} = 1 - e^{-\lambda t} \approx \lambda t$ (for small λt ; when $\lambda t < 0.1$)
- Examples of product λt versus exact $1 - e^{-\lambda t}$*
- 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*

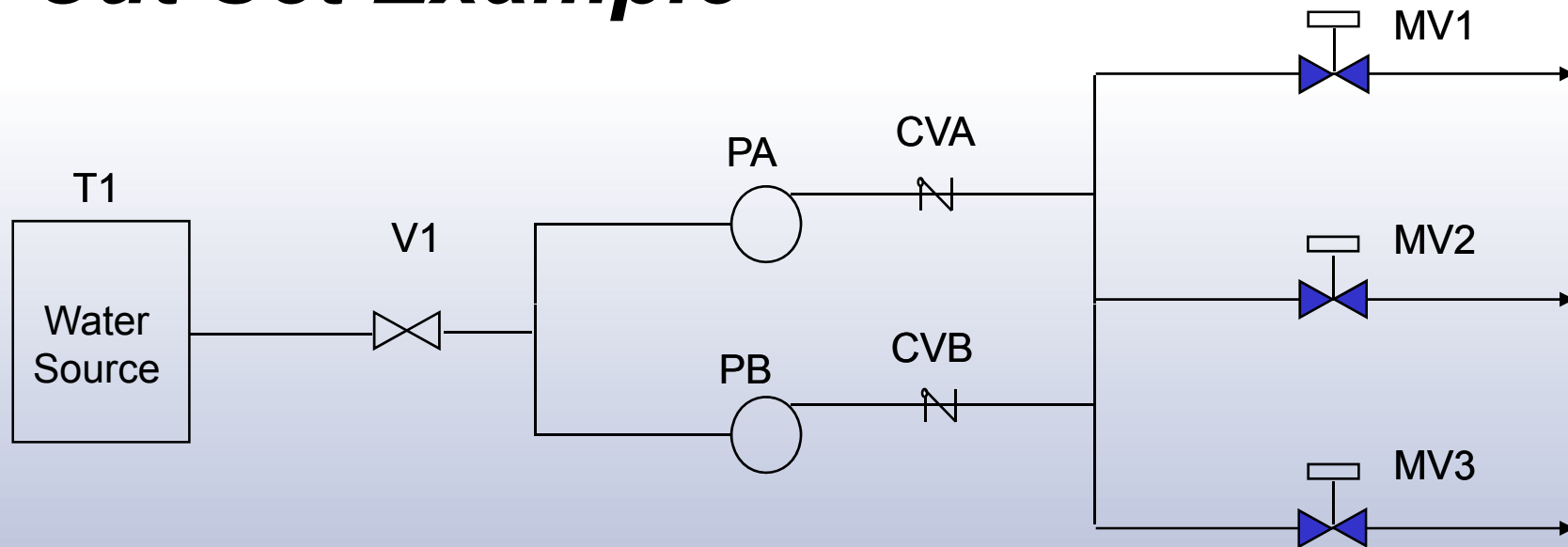
Probability and Frequency Example

- *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)*
 - $P\{\text{pump fails to start on demand}\}$
 - $P\{1 \text{ failure in 1 demand}\} = \left(\frac{1!}{1!0!}\right) (10^{-3})^1 (1-10^{-3})^0 = 10^{-3}$
 - $P\{\text{pump fails to run for 24 hrs.}\}$
 - $P\{\text{failure time} < 24 \text{ hrs}\} = 1 - e^{-(1E-4)(24)} = 2.4E-3 \approx (24)(1E-4)$

Cut Sets

- *Combination 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: ECI system success if there is flow from the tank through any one pump train through any one motor-operated valve.

ECI system components include;

T# - tank

V# - manual valve, normally open

P# - pump

CV# - check valve

MV# - motor-operated valve, normally closed

Cut Sets for ECI

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

ECI-System =

$$\begin{aligned} &T1 + \\ &V1 + \\ &PA * PB + \\ &PA * CVB + \\ &PB * CVA + \\ &CVA * CVB + \\ &MV1 * MV2 * MV3 \end{aligned}$$

Cut Sets Can Be Quantified Using Various Methods

- *Exact Solution for Cut-Sets = A + B:*
 - $P(\text{Cut-Sets}) = P(A + B) = P(A) + P(B) - P(AB)$
- *Cross terms become unwieldy for large lists of cut sets. e.g., if Cut-Sets = A + B + C, then:*
 - $P(\text{Cut-Sets}) = P(A) + P(B) + P(C) - P(AB) - P(AC) - P(BC) + P(ABC)$
- *Cut Sets typically quantified using either Rare-Event Approximation or Minimal Cut Set Upper Bound Approximation*

Rare Event Approximation

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

Minimal Cut Set Upper Bound Approximation

- $P(\text{Cut-Sets}) = 1 - (\text{product of cut set success probabilities})$
 $= 1 - [(1 - P(A)) * (1 - P(B))]$
- *Assumes cut sets are independent*
- *In general, $P\{\text{Cut-Sets}\} \leq 1 - \prod_{k=1, K} (1 - P\{\text{MCS}_k\})$*

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

	Small values for $P(A)$ & $P(B)$, A & B independent	Large values for $P(A)$ & $P(B)$, A & B independent	A & B dependent
Cut-Sets = 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

Review Basic PRA Techniques Purpose and Objectives

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

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 at least once 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

Idaho National Engineering and Environmental Laboratory

3. *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

- *Typically used to model the response to an initiating event*
- *Features:*
 - *One event tree for each initiating event*
 - *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*

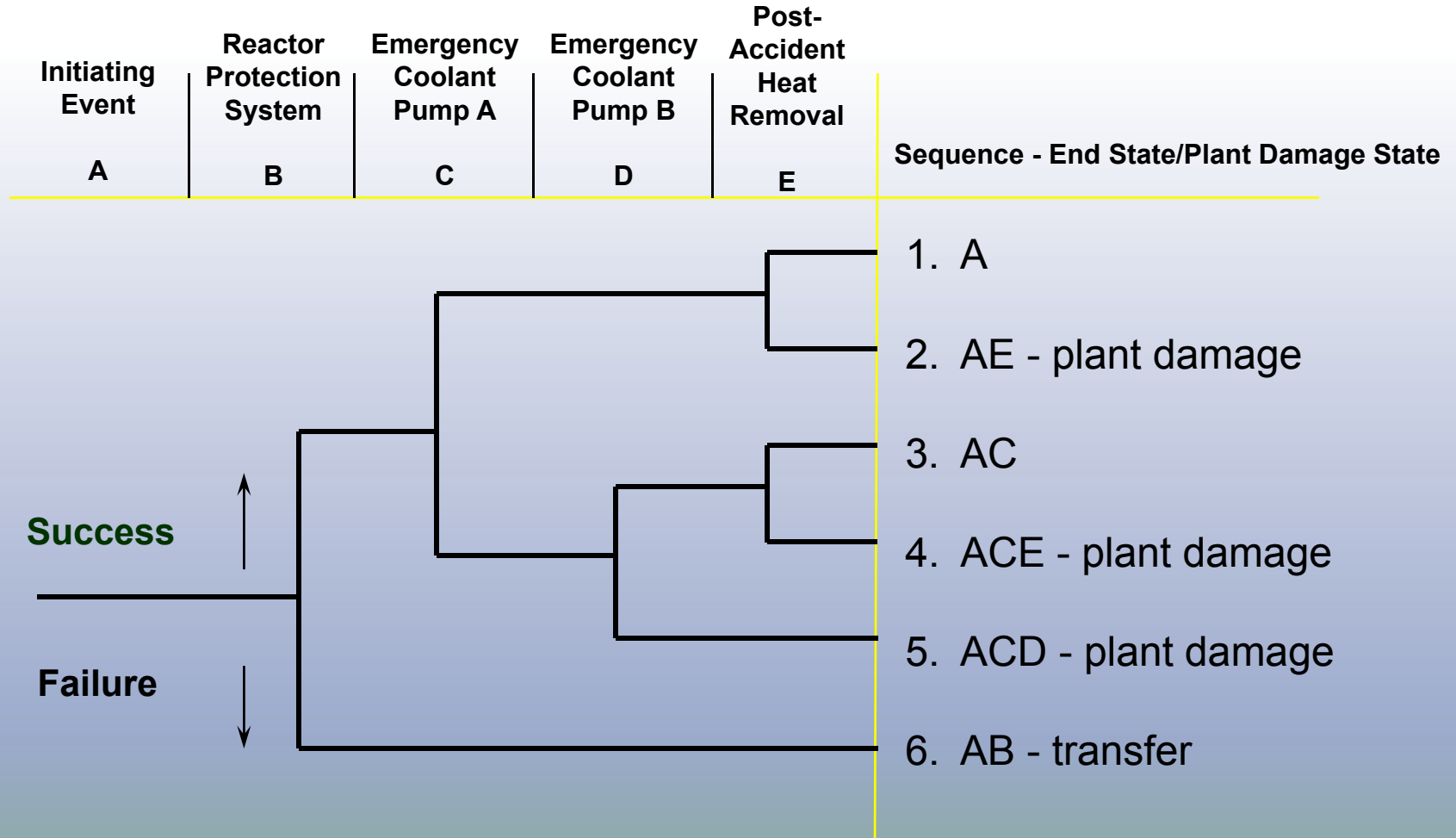
Initiating Events

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

Identification of Initiating Events

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

Simple Event Tree



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 time*
- *End States - undesired outcome*
 - *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*

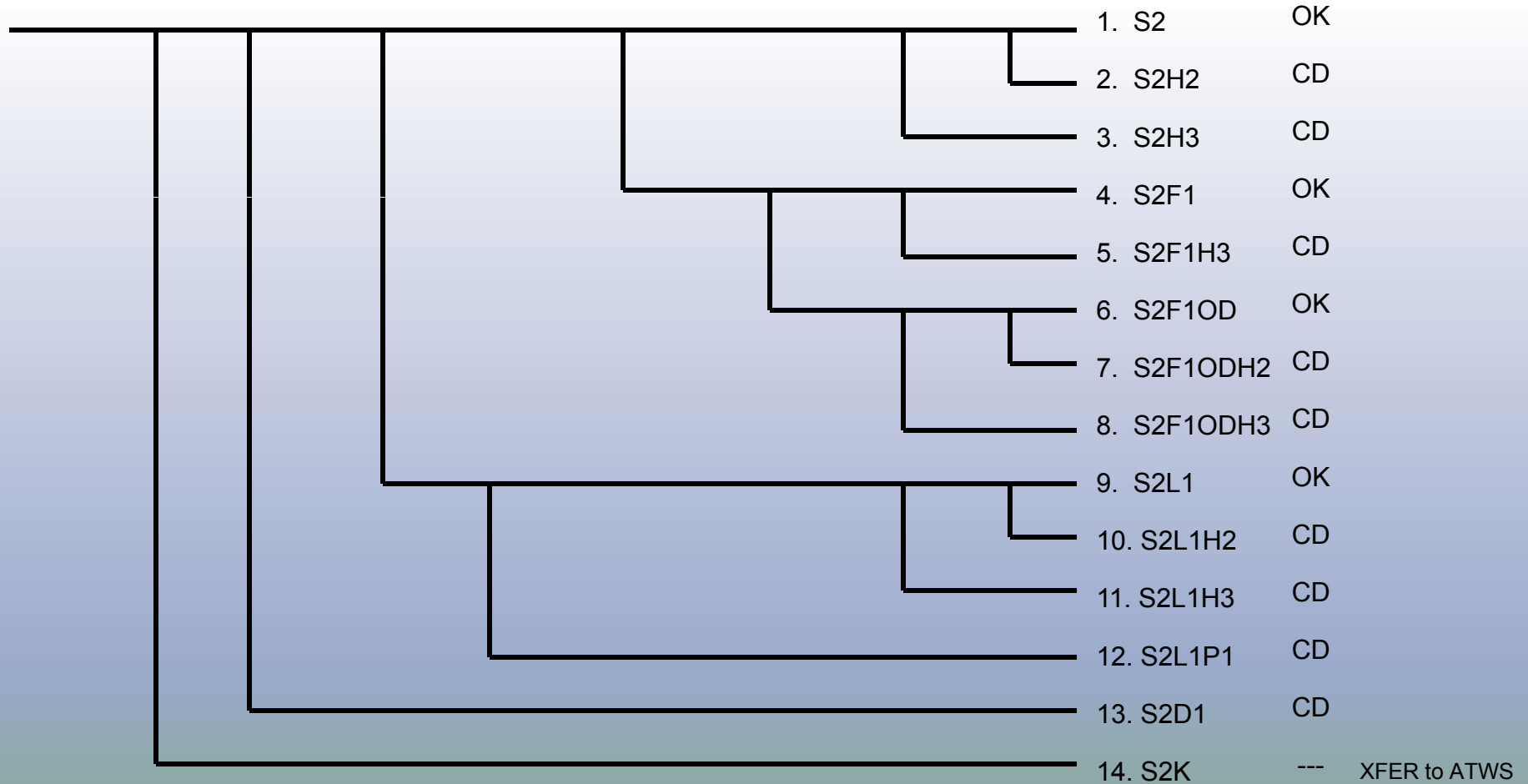
Success Criteria (cont.)

- *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*

Small LOCA	Reactor Protection System	High Pressure Injection	Auxiliary Feedwater 2/4 Steam Generators	Pressure-Operated Relief Valves Open	Containment Spray Injection	Operator Depress. Reactor Coolant System	Low Pressure Injection/ Re-circulation	High Pressure Re-circulation	Sequence	Core	Comments
S2	K	D1	L1	P1	F1	OD	H3	H2			



Event Tree for S2 - Small LOCA

Plant Damage State (PDS)

- *Core Damage (CD) designation for end state not sufficient to support Level 2 analysis*
 - *Need details of core damage phenomena to accurately model challenge to containment integrity*
- *PDS relates core damage accident sequence to:*
 - *Status of plant systems (e.g., AC power operable?)*
 - *Status of RCS (e.g., pressure, integrity)*
 - *Status of water inventories (e.g., injected into RPV?)*

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

Small LOCA Event Tree from Surry SDP Notebook

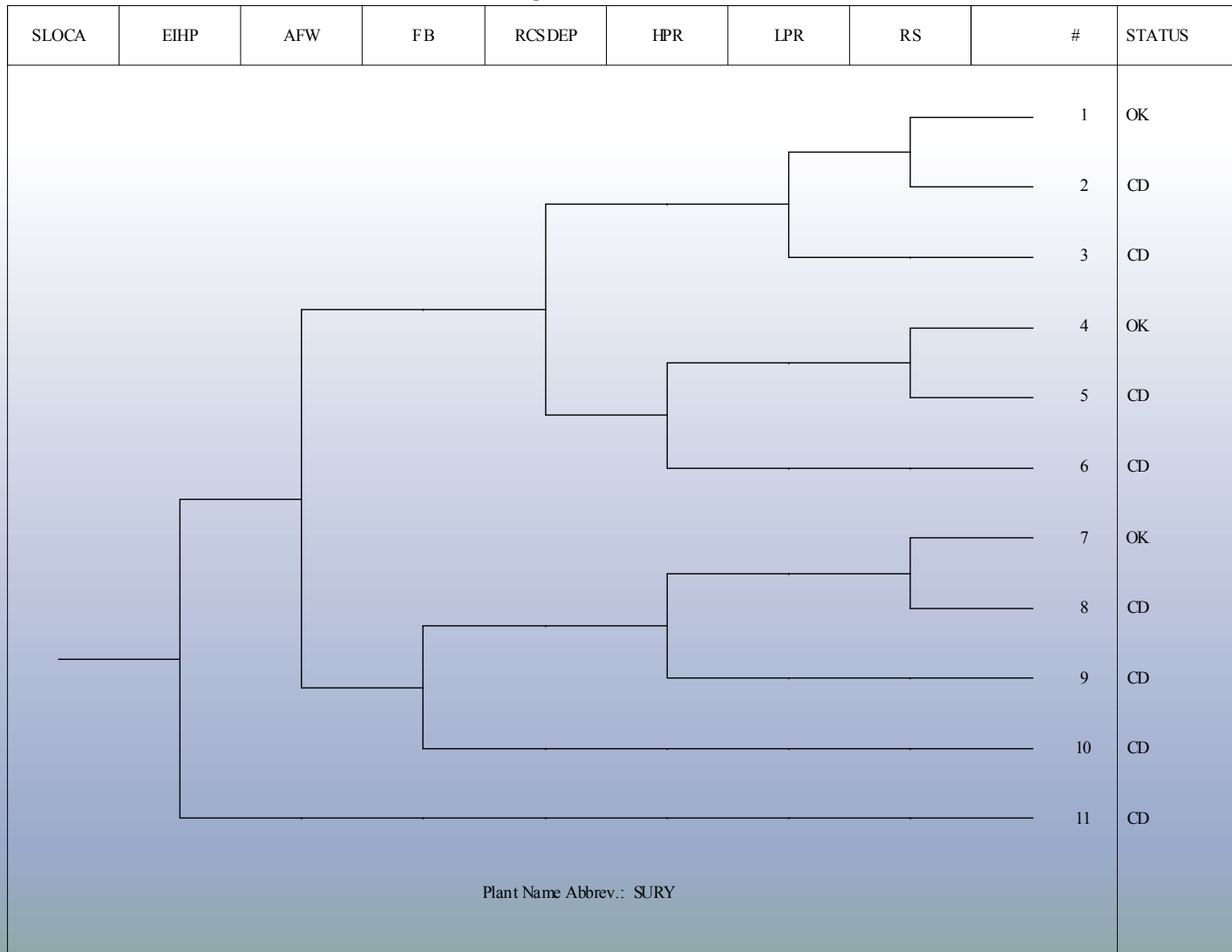


Table 3.3 SDP Worksheet for Surry Power Station, Units 1 and 2 — Small LOCA (SLOCA)

Safety Functions Needed:		Full Creditable Mitigation Capability for Each Safety Function:				
Early Inventory, High Pressure Injection (EIHP) ⁽⁴⁾		1/2 charging pump trains or use of 1 spare charging pump ⁽⁶⁾ (1 multi-train system)				
Secondary Heat Removal (AFW)		1/2 MDAFW trains (1 multi-train system) ⁽¹⁾ or 1/1 TDAFW train (1 ASD train) with 1/5 safety relief valves or 1/1 SG PORV for the associated 1/3 SGs				
RCS Cooldown/Depressurization (RCSDEP)		Operator depressurizes and cools down RCS using 1/3 ADVs and 1/2 Pzr Sprays (operator action = 3) ⁽⁵⁾				
Primary Heat Removal, Feed/Bleed (FB)		1/2 PORVs open for Feed/Bleed (operator action = 2) ⁽²⁾				
Low Pressure Recirculation (LPR)		1/2 LHSI pumps auto initiated by RMT (1 multi-train system) ⁽³⁾				
High Pressure Recirculation (HPR)		1/2 charging pump trains with 1/2 LHSI pumps auto initiated by RMT (1 multi-train system) ⁽³⁾				
Recirculation Spray (RS)		1/2 inside RS (1A or 1B) trains or 1/2 outside RS (2A or 2B) trains (2 multi-train systems)				
Circle Affected Functions		IEL	Remaining Mitigation Capability Rating for Each Affected Sequence		Recovery Credit	Results
1 SLOCA - RS (2,5,8) 3 + 6	9					
2 SLOCA - LPR (3) 3 + 3	6					
3 SLOCA - RCSDEP ⁽⁵⁾ - HPR (6) 3 + 3 + 3	9					
4 SLOCA - AFW - HPR (9) 3 + 4 + 3	10					
5 SLOCA - AFW - FB (10) 3 + 4 + 2	9					
6 SLOCA - EIHP (11) 3 + 3	6					
Identify any operator recovery actions that are credited to directly restore the degraded equipment or initiating event:						
If operator actions are required to credit placing mitigation equipment in service or for recovery actions, such credit should be given only if the following criteria are met: 1) sufficient time is available to implement these actions, 2) environmental conditions allow access where needed, 3) procedures exist, 4) training is conducted on the existing procedures under conditions similar to the scenario assumed, and 5) any equipment needed to complete these actions is available and ready for use.						

Notes:

- Use of 1/3 opposite unit's AFW trains via crosstie is possible. The crosstie function can be considered as a possible recovery action for a deficiency in the unit's AFW system. In both cases, the discharge pathways to the SGs are the same which may limit the credit that may be applicable.
- The human error probability (HEP) assessed in the PRA for establishing bleed and feed cooling is 2.66E-3. A credit of 2 is assigned based on a survey of the operation action at similar plants.
- When the RWST level reaches its low setpoint, the RMT system automatically initiates the switchover of the low pressure injection pumps to the recirculation mode. The sump suction valves open and the RWST suction valves close. The changeover to high head recirculation will also take place automatically on low RWST level. The recirculation mode transfer (RMT) system automatically initiates the switchover of the suction of the high pressure injection pump from the RWST to the low pressure injection pump discharges on low RWST level.
- Based on the licensee's comments, in case of EIHP failure secondary cooldown using the 1/3 SG ADVs and 50% AFW flow for LPI and LPR is not credited.
- The HEP assessed in the PRA for operator depressurizing and cooling down the RCS is 5.33E-3. A credit of 3 is assigned and verified through benchmarking.
- The spare charging pump can be aligned as a recovery action when the charging pump aligned to the bus is failed. A credit of 1 can be assigned for use of the spare charging pump.

Review Event Tree Analysis Purpose and Objectives

- *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*

Page Intentionally Left Blank

Idaho National Engineering and Environmental Laboratory

4. Fault Tree Analysis



Fault Tree Analysis

- **Purpose:** *Students will learn purposes & techniques of fault tree analysis. Students will learn how appropriate level of detail for a fault tree analysis is established. Students will become familiar with terminology, notation, and symbology employed in fault tree analysis. In addition, a discussion of applicable component failure modes relative to the postulation of fault events will be presented.*
- **Objectives:**
 - *Demonstrate 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, NRC Uses of 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.”

NUREG-0492

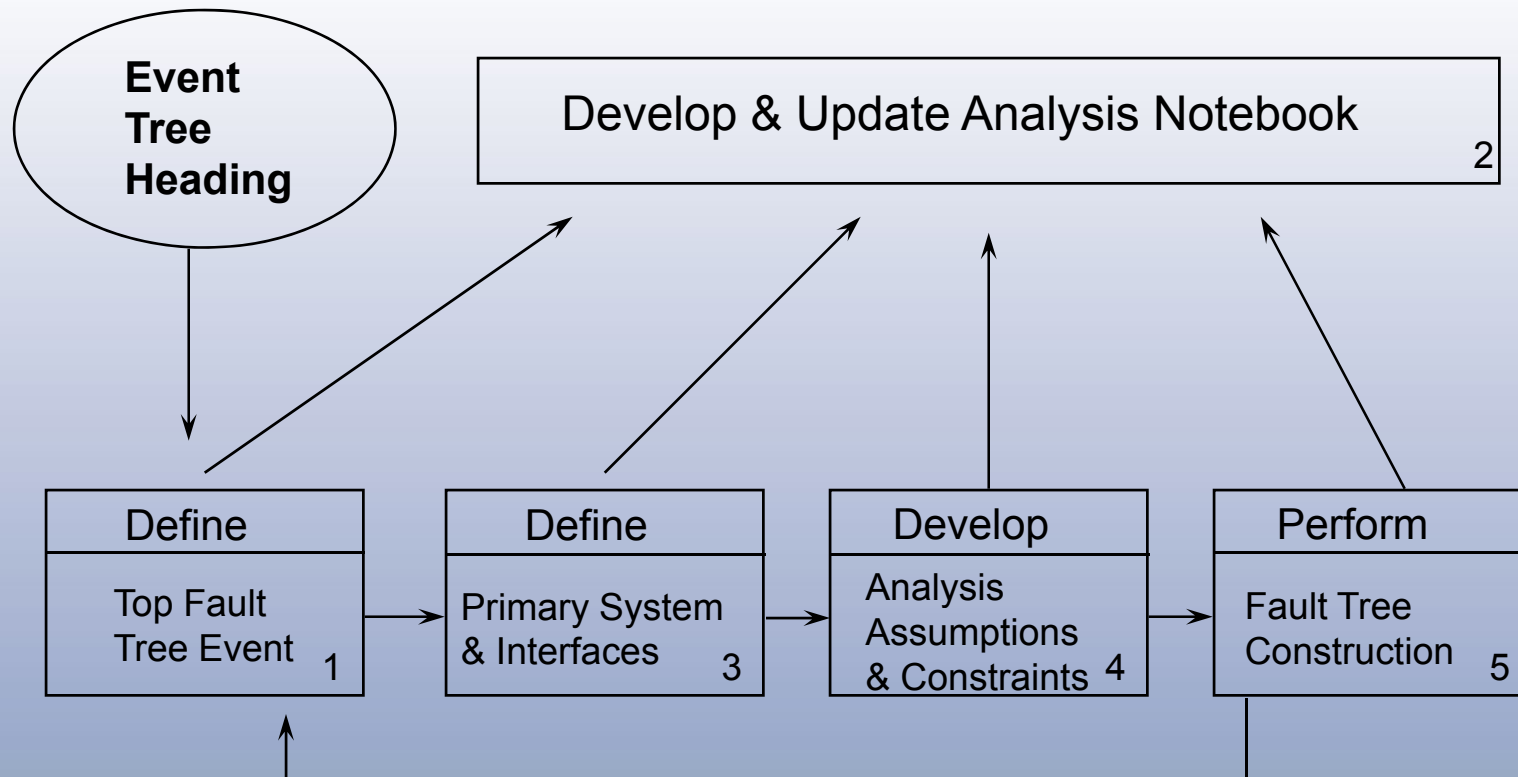
Fault Trees

- *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*
 - *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 (i.e., 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 IEs*

2. Develop & Maintain Analysis Notebook

- *Scope of analysis and system definition*
- *Notebook should include system design and operation information, technical specifications, test and maintenance data, pertinent analytical assumptions, 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*

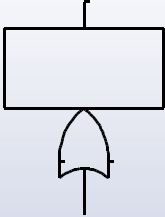
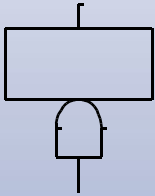
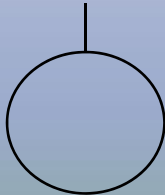
4. Develop Analysis Assumptions & Constraints

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

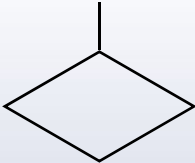

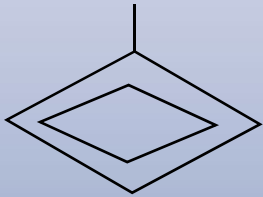
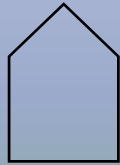
5. *Fault Tree Construction*

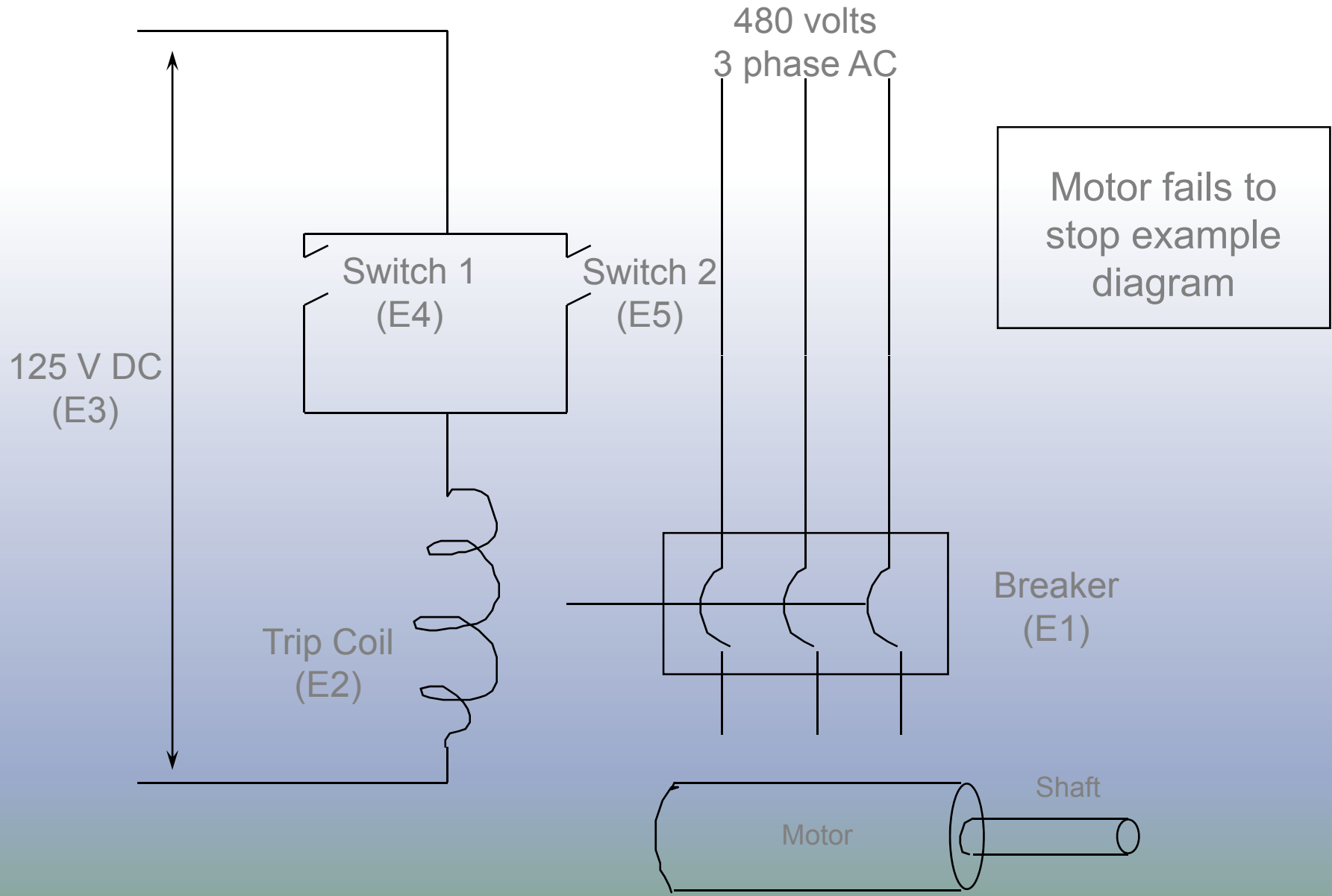
- *Step-by-step postulation of system faults*
- *Utilization of standard symbology*
- *Postulation consistent with level of resolution of data & assumptions*
- *Iterative process*

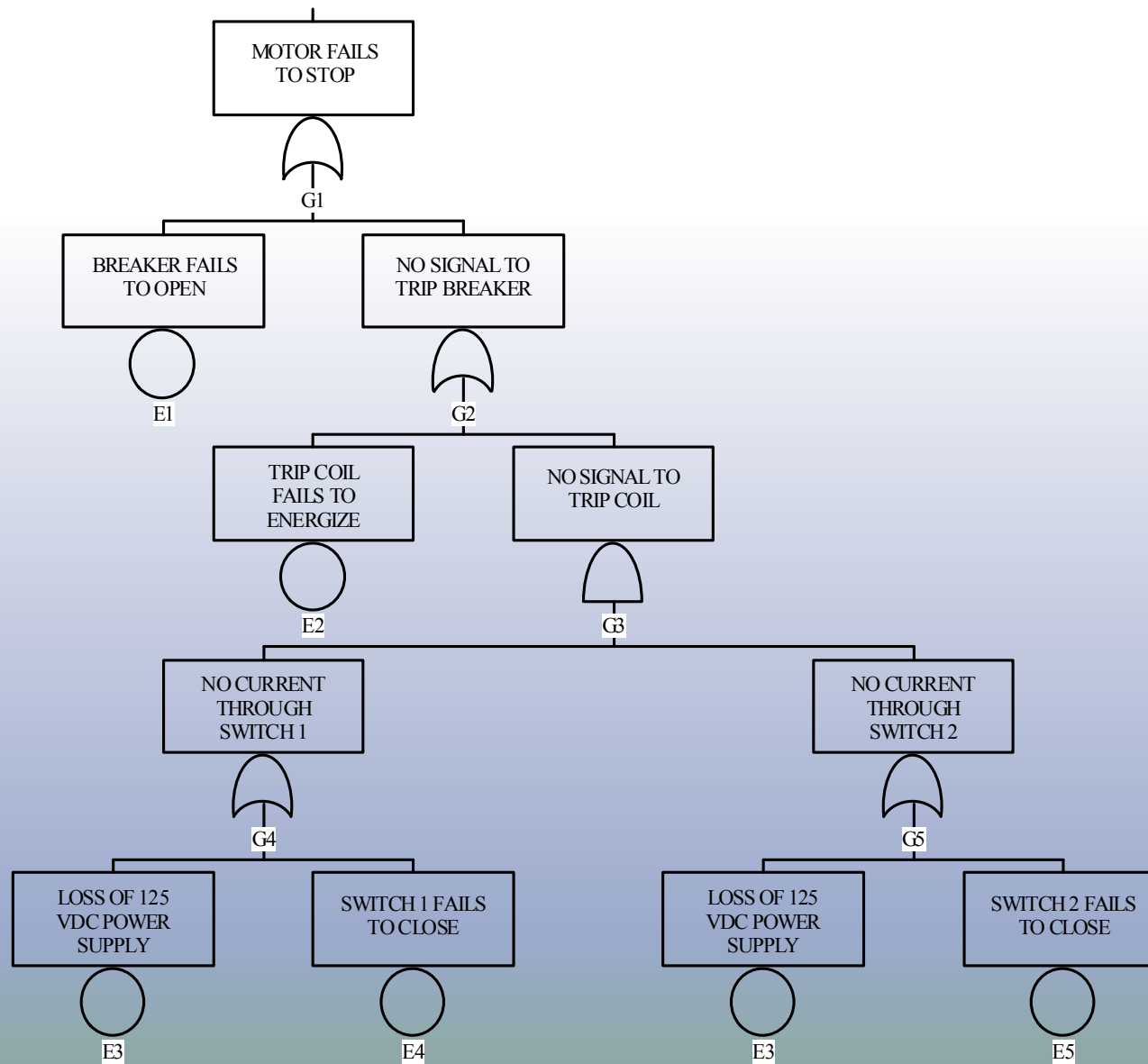
Fault Tree Symbols

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 occur.
	"AND" Gate	Logic gate providing a representation of the Boolean intersection of input events. The output will occur if all of the inputs occur.
	Basic Event	A basic component fault which requires no further development. Consistent with level of resolution in databases of component faults.

Fault Tree Symbols (cont.)

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





Boolean Fault Tree Reduction

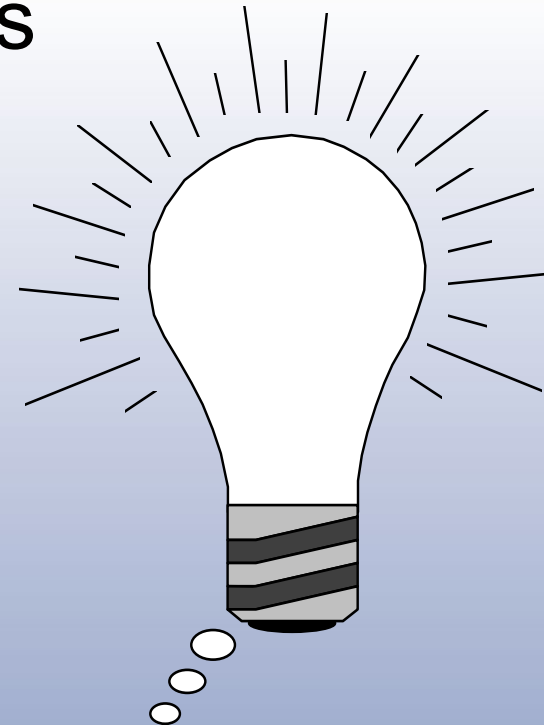
- *Express fault tree logic as Boolean equation*
- *Apply rules of Boolean algebra to reduce terms*
- *Results in reduced form of Boolean equation*

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”)*

$$G1 = E1 + G2$$

$$G2 = E2 + G3$$

$$G3 = G4 * G5$$

$$G4 = E3 + E4$$

$$G5 = E3 + E5$$

- *Back-substitute*

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

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

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

- *Expand terms in parentheses and brackets*

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

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

Reduction of Example Fault Tree (cont.)

- Reduce terms using rules of Boolean algebra

*Idempotent Law applies to $E3 * E3 = E3$*

*Law of Absorption applies to $E3 + (E3 * "Y") = E3$*

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

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

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

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

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

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

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

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

- Quantify the minimal cut sets to calculate probability of the top gate which is Motor Fails to Stop; For example using rare event

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

Review Fault Tree Analysis Purpose and Objectives

- *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*

Page Intentionally Left Blank

Idaho National Engineering and Environmental Laboratory

5. Component Failure Data



Component Failure Data

- *Purpose: Students will be introduced to sources of hardware data and equipment failure modes, including common cause failure, that are modeled in PRAs.*
- *Objectives: Students will be able to:*
 - *Understand failure modes typically modeled in PRA and how each failure mode is quantified.*
 - *Understand what is meant by the terms*
 - *Generic data*
 - *Plant-specific data*
 - *Bayesian updating*
 - *Describe what is meant by common-cause failure, why it is important, and how it is included in PRA*
- *References:*
 - *NUREG/CR-2300*
 - *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.*

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
- t_{OOS} = total time out of service
- t_{total} = total time

Component Failure Modes

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

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) – archival only (no longer maintained)*
- *Institute of Nuclear Power Operations Equipment Performance Information Exchange (EPIX) – replaced NPRDS*

Plant-Specific Data Sources

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

Plant-Specific Data Issues

- *Combining data from different sources can result in:*
 - *double counting of the same failure events*
 - *inconsistent component boundaries*
 - *inconsistent definition of “failure”*
- *Plant-specific data is 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*

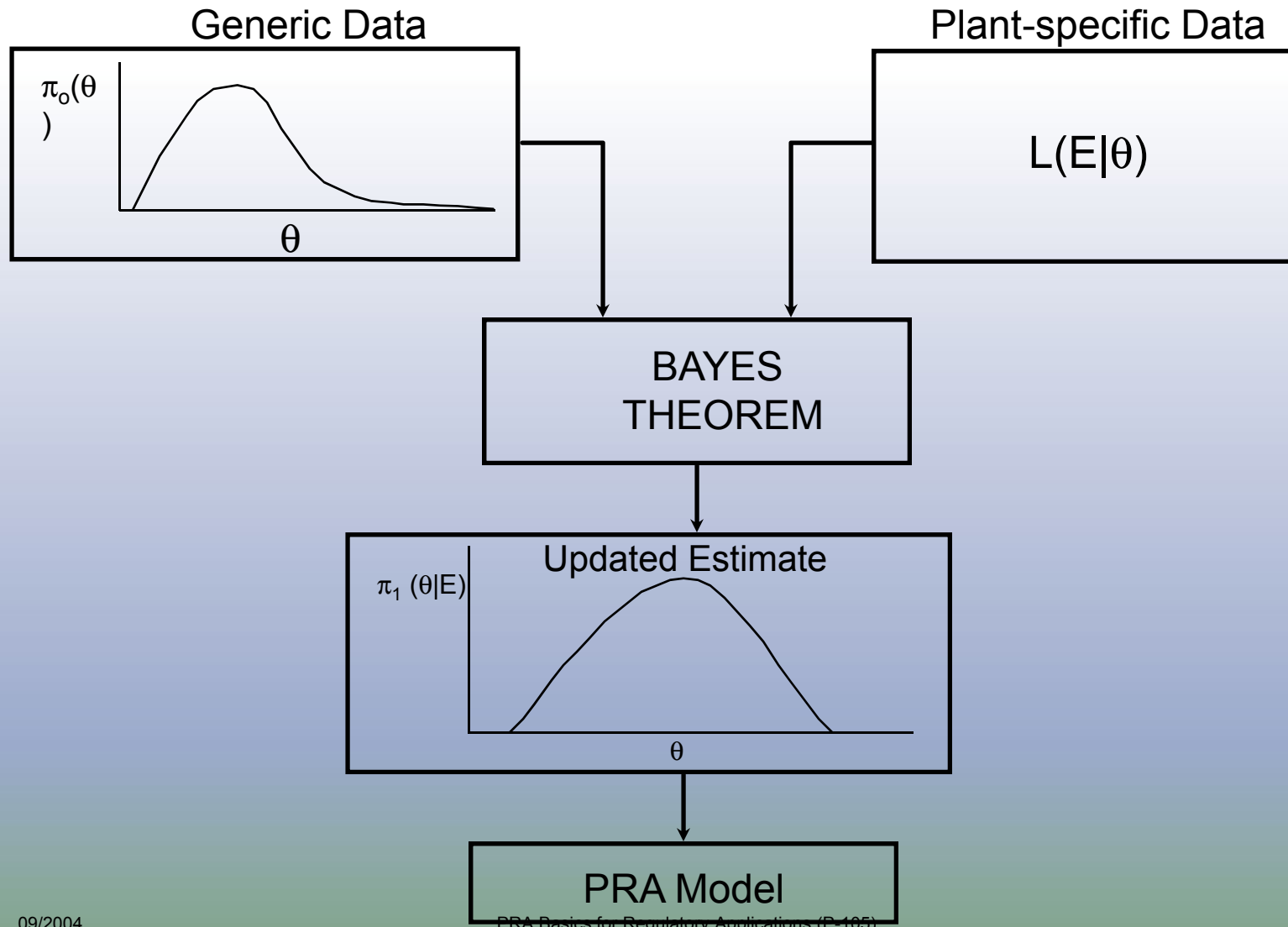
Bayes' Theorem is Basis for Bayesian Updating of Data

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

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

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

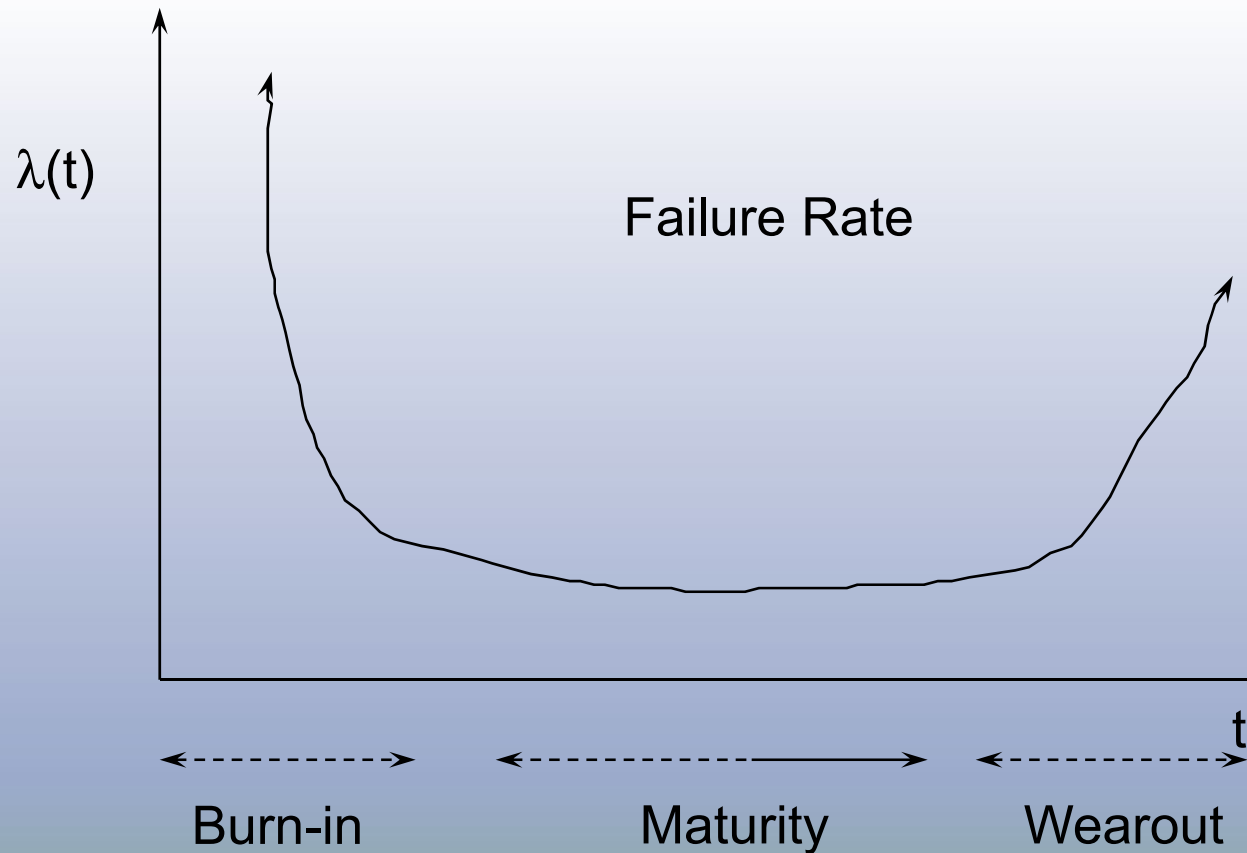
Bayesian Updating



Component Data Not Truly Time Independent

- *PRA 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 aging of equipment does occur*
 - *Failure rate (λ) = $\lambda(t)$*
 - *“Bathtub” curve*

The “Bathtub” Curve



The “Bathtub” Curve (cont.)

- *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, 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 (CCFs)

- *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

- *Three parametric models used*
 - *Beta factor (original CCF model)*
$$\beta = \frac{\text{Number of common cause failures}}{\text{Total number of failures}}$$
 - *Multiple Greek Letter (MGL) model (expanded on beta-factor)*
 - *Alpha factor model (addressed uncertainty concerns in MGL)*
- *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
 - $\beta = 10 \text{ CCF} \div 47 \text{ total failures} \approx 2.1E-1$
 - Motor-driven pump fail to start = $3.0E-3$ per demand
- Cut set: HPI-MDP-FS-A * HPI-MDP-FS-B
 - Independent failure $\approx 3E-3 * 3E-3 = 9E-6$
- Cut set: HPI-MDP-CF-CCFAB
 - $\text{CCF} = 3E-3 * \beta = 6E-4$

Review Component Failure Data Purpose and Objectives

- *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*

Page Intentionally Left Blank

Idaho National Engineering and Environmental Laboratory

6. Human Reliability Analysis



Human Reliability Analysis

- *Purpose: To expose the student to how human actions are treated in a PRA.*
- *Objectives - the student will be able to:*
 - *Explain the role of HRA within the overall context of PRA*
 - *Describe common error classification schemes used in HRA*
 - *Describe how human interactions are incorporated into system models*
 - *Identify strengths and limitations of HRA*
- *References:*
 - *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:

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

Categories Of Human Error

- *Errors can occur throughout the accident sequence*
 - *Pre-initiator errors (latent errors that may occur in or out of the main control room)*
 - *Failure to restore*
 - *Miscalibration*
 - *Often 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 (cont.)

- *Errors can occur throughout the accident sequence (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 RCS in accordance with the EOPs)*
 - *Recovery actions (consideration of actions that may be taken to recover from a fault depending upon actions required and amount of time available)*

Types Of Human Error

- *Generally, two types of human errors are defined:*
 - *Errors of omission --Failure to perform a required action or step, e.g., failure to monitor makeup tank level*
 - *Errors of commission-- Action performed incorrectly or wrong action performed, e.g., opening the wrong valve, turning off SI*
- *Normally only 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*

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	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

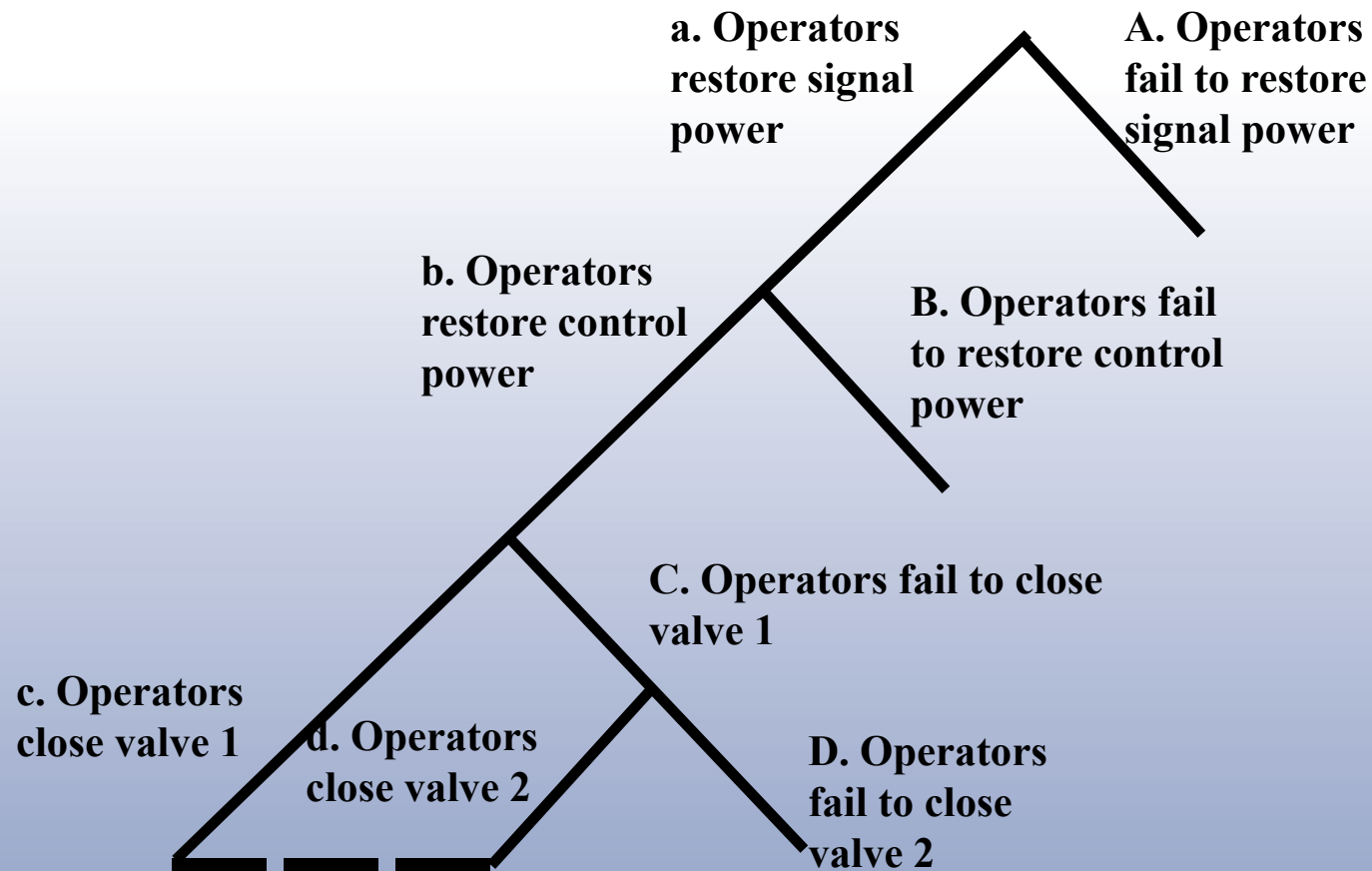
How Human Actions Are Incorporated Into PRA Model

- *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*

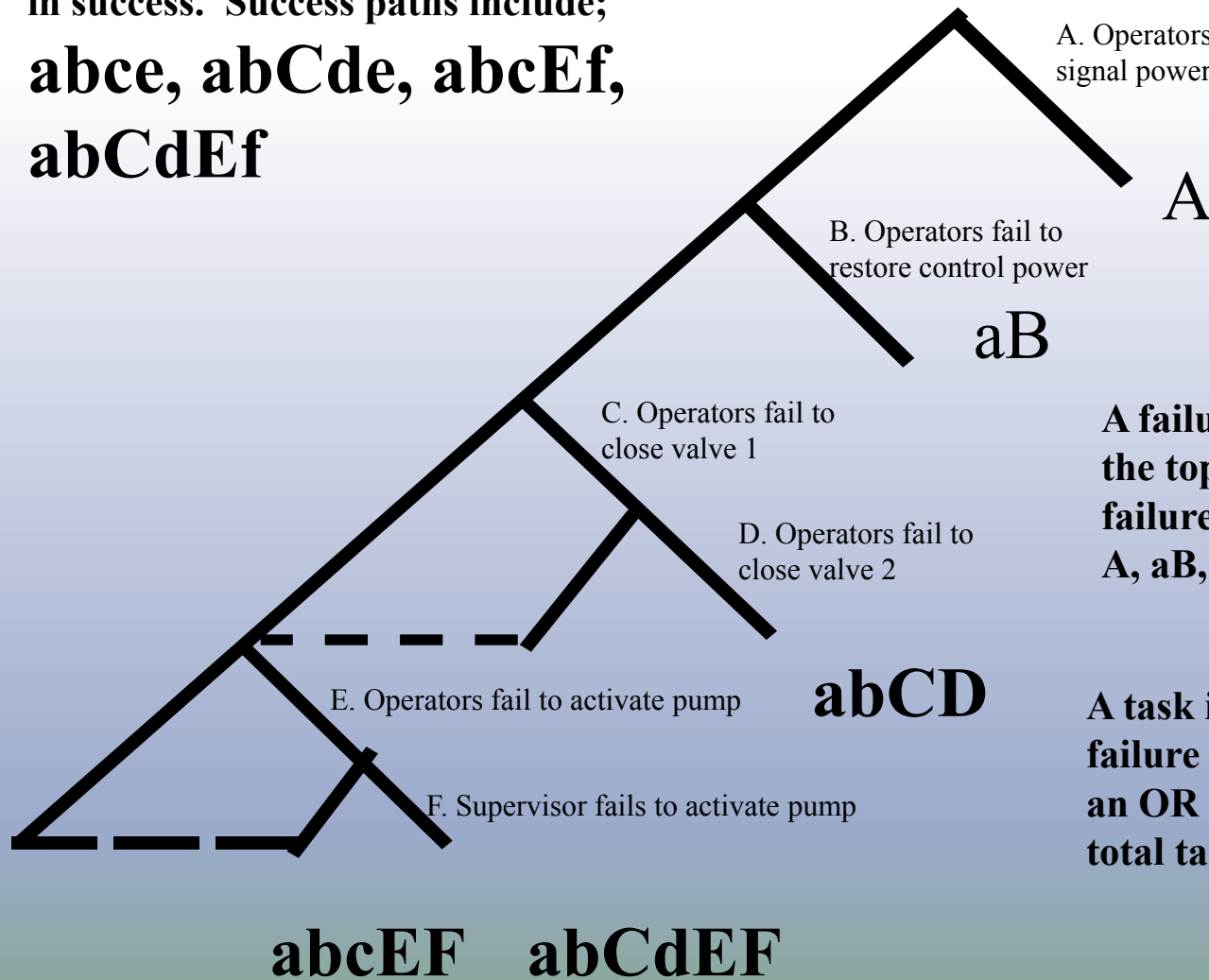
Sources of HRA Data

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

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



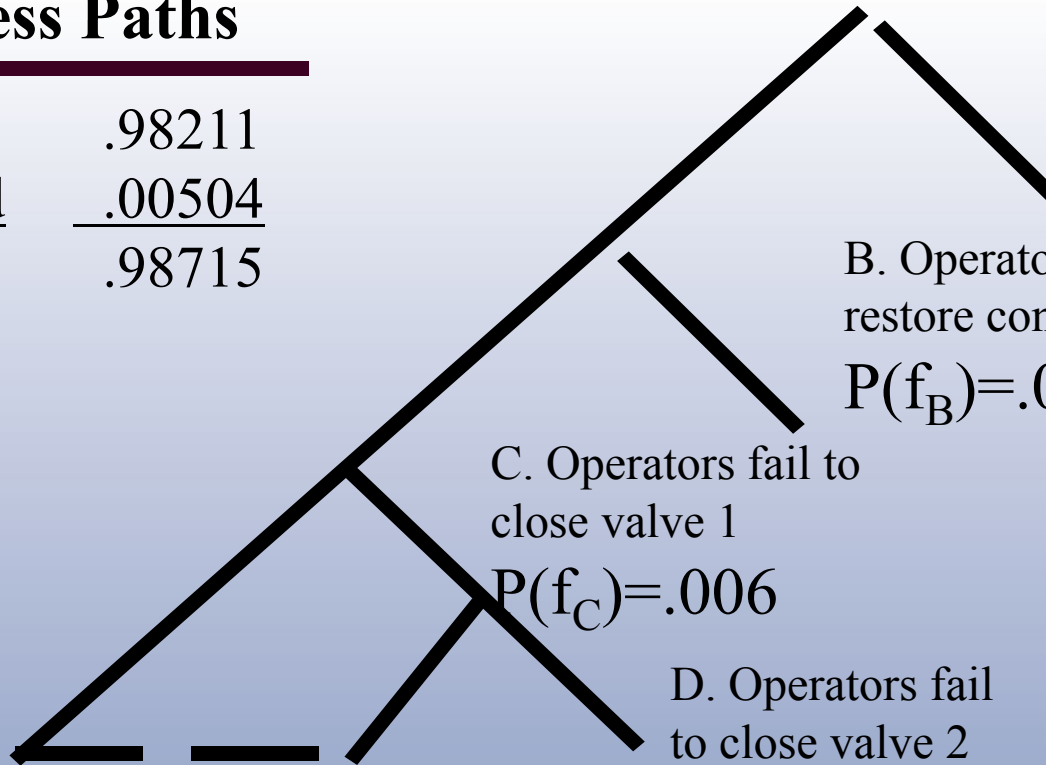
A failure path is a path starting at the top of the tree and ends in failure. Failure paths include;
A, aB, abCD, abcEF, abCdEF

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

Preview of Quantification: Plug HEP data into the model and calculate paths and total HEP

Success Paths

abc	.98211
abCd	.00504
Total	.98715



A. Operators fail to restore signal power
 $P(f_A) = .006$

B. Operators fail to restore control power
 $P(f_B) = .006$

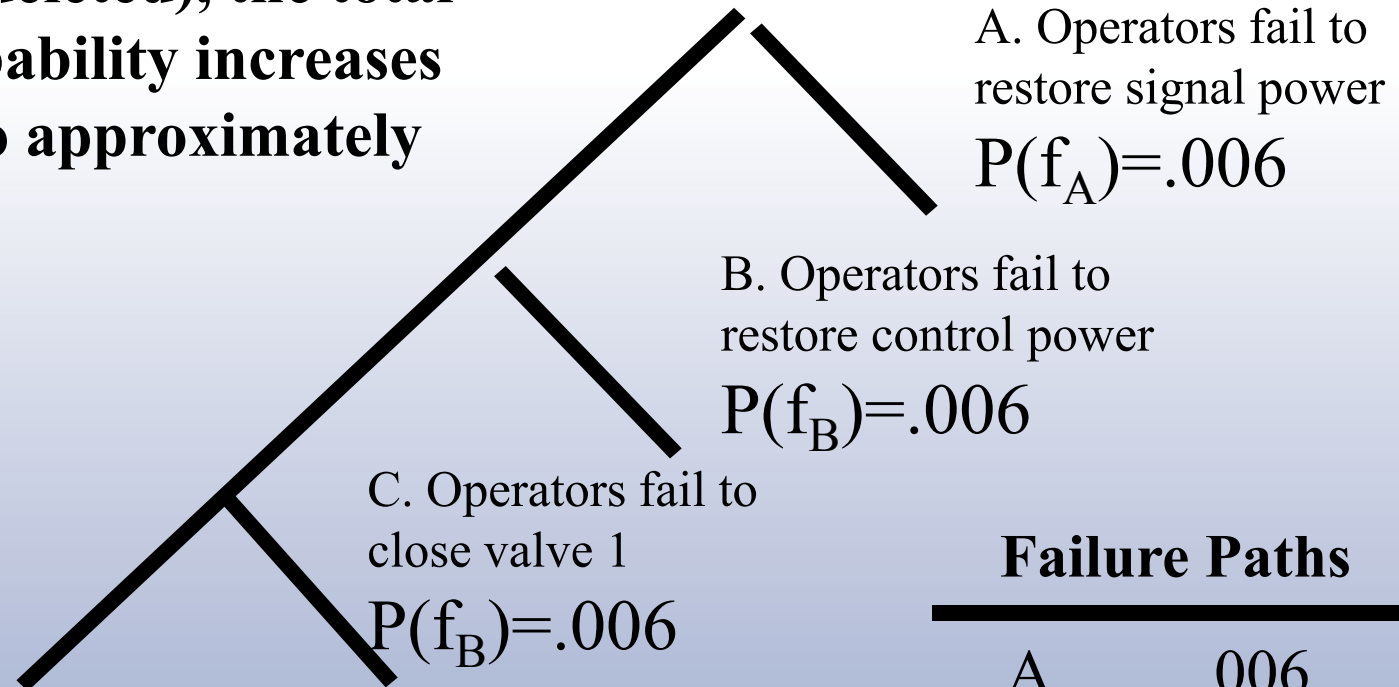
C. Operators fail to close valve 1
 $P(f_C) = .006$

D. Operators fail to close valve 2
 $P(f_D) = .15$

Failure Paths

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

When there is no recovery for C (D is deleted), the total failure probability increases from .013 to approximately .018.



Failure Paths

A	.006
aB	.00596
<u>abC</u>	<u>.00593</u>
Total	.01789

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*

Review Human Reliability Analysis Purpose and Objectives

- *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*

Idaho National Engineering and Environmental Laboratory

7. Sequence Quantification



Sequence Quantification

- *Purpose: This topic will provide students with an understanding of the quantitative basis of PRA. Elements of accident sequence quantification and importance analysis will be presented.*
- *Objectives: At the conclusion, students will be able to:*
 - *Describe the major processes for accident sequence quantification*
 - *Explain the concepts of importance analysis*
- *References: NUREG/CR-2300, NUREG-1489 (App. C)*

Quantification Inputs

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

Parameter Inputs for Sequence Quantification

- *Initiating event frequencies*
 - λ_{IE}
- *Demand failures*
 - $Q_d = p$
- *Standby failures*
 - $Q_s \approx \lambda_s t / 2$
- *Mission time failures (failure to run)*
 - $Q_r \approx \lambda_h t_m$
- *Test and maintenance unavailability*
 - $Q_m = \lambda_m d_m$
- *Common-cause parameters*
 - β

Fault-Tree Linking Approach to Accident Sequence Quantification

- *Link fault tree models on sequence level using event trees*
- *Evaluate each sequence for minimal cut sets (Boolean reduction)*
- *Quantify sequence minimal cut sets with data*
- *Add operator recovery actions and common cause failures*
- *Determine dominant accident sequences*
- *Perform sensitivity, importance, and uncertainty analysis*

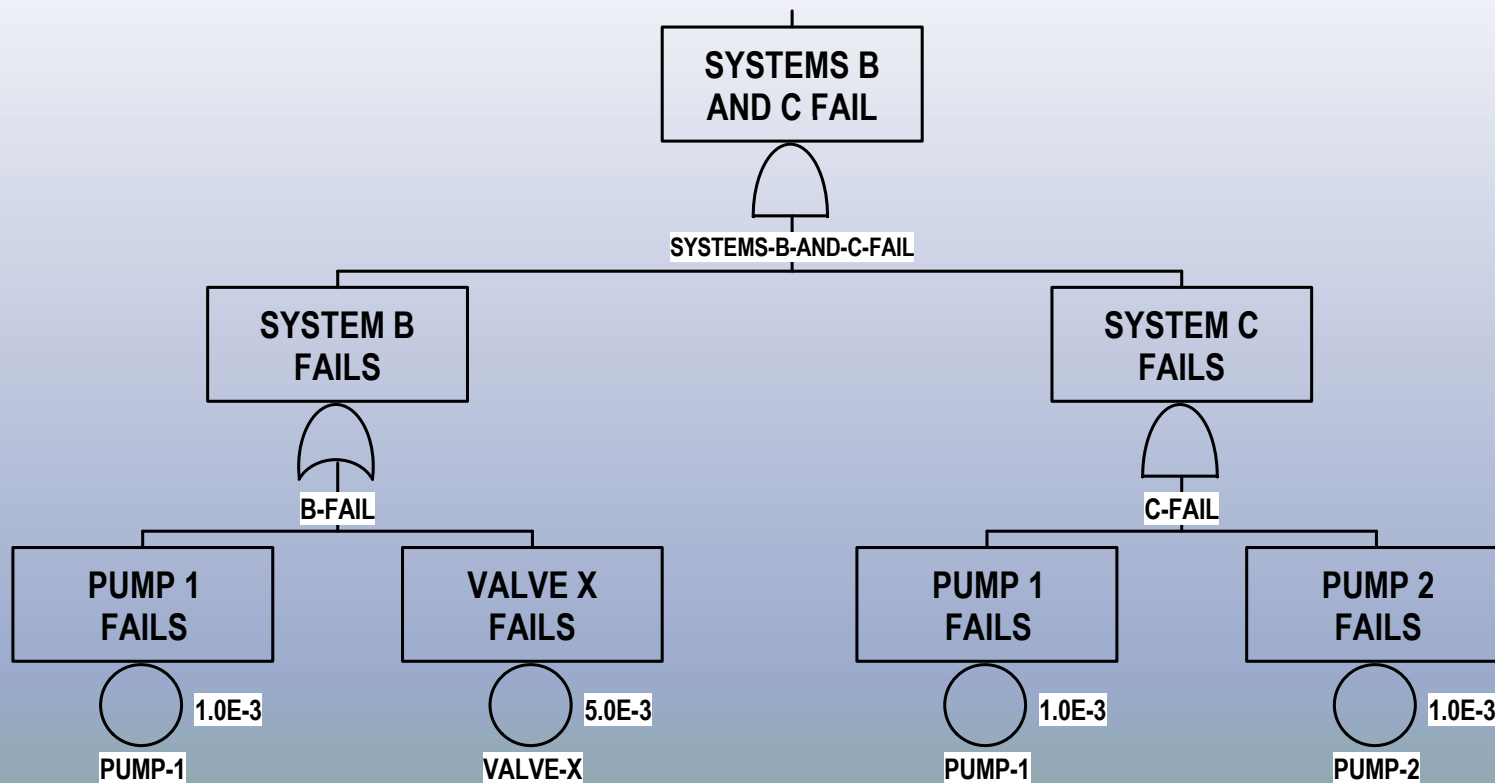
Example of Quantification Process

Transient	System A	System B	System C	Sequence Class
T	A	B	C	
				OK
				OK
				Core damage
				Core damage

.....Let's look at Sequence **TBC** (#3)

Example of Quantification Process (cont.)

T = 10 transients (demands) / year



Example of Quantification Process (cont.)

$$\begin{aligned}\text{Systems B AND C Fail} &= \text{System B Fails} * \text{System C Fails} \\ &= (\text{Pump 1} + \text{Valve X}) * (\text{Pump 1} * \text{Pump 2}) \\ &= (\text{Pump 1} * \text{Pump 1} * \text{Pump 2}) + (\text{Valve X} * \text{Pump 1} * \text{Pump 2}) \\ &= (\text{Pump 1} * \text{Pump 2}) + (\text{Valve X} * \text{Pump 1} * \text{Pump 2}) \\ &= \text{Pump 1} * \text{Pump 2} \\ &= (1\text{E-}3) (1\text{E-}3) \\ &= 1\text{E-}6 \text{ (Probability)}\end{aligned}$$

$$\begin{aligned}\text{Sequence TBC} &= T * \text{System B Fails} * \text{System C Fails} \\ &= 10/\text{Year} * 1\text{E-}6 \\ &= 1\text{E-}5/\text{Year} \text{ (Frequency)}\end{aligned}$$

Recovery Analysis

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

Summary of Sequence $T_2L_1P_1$

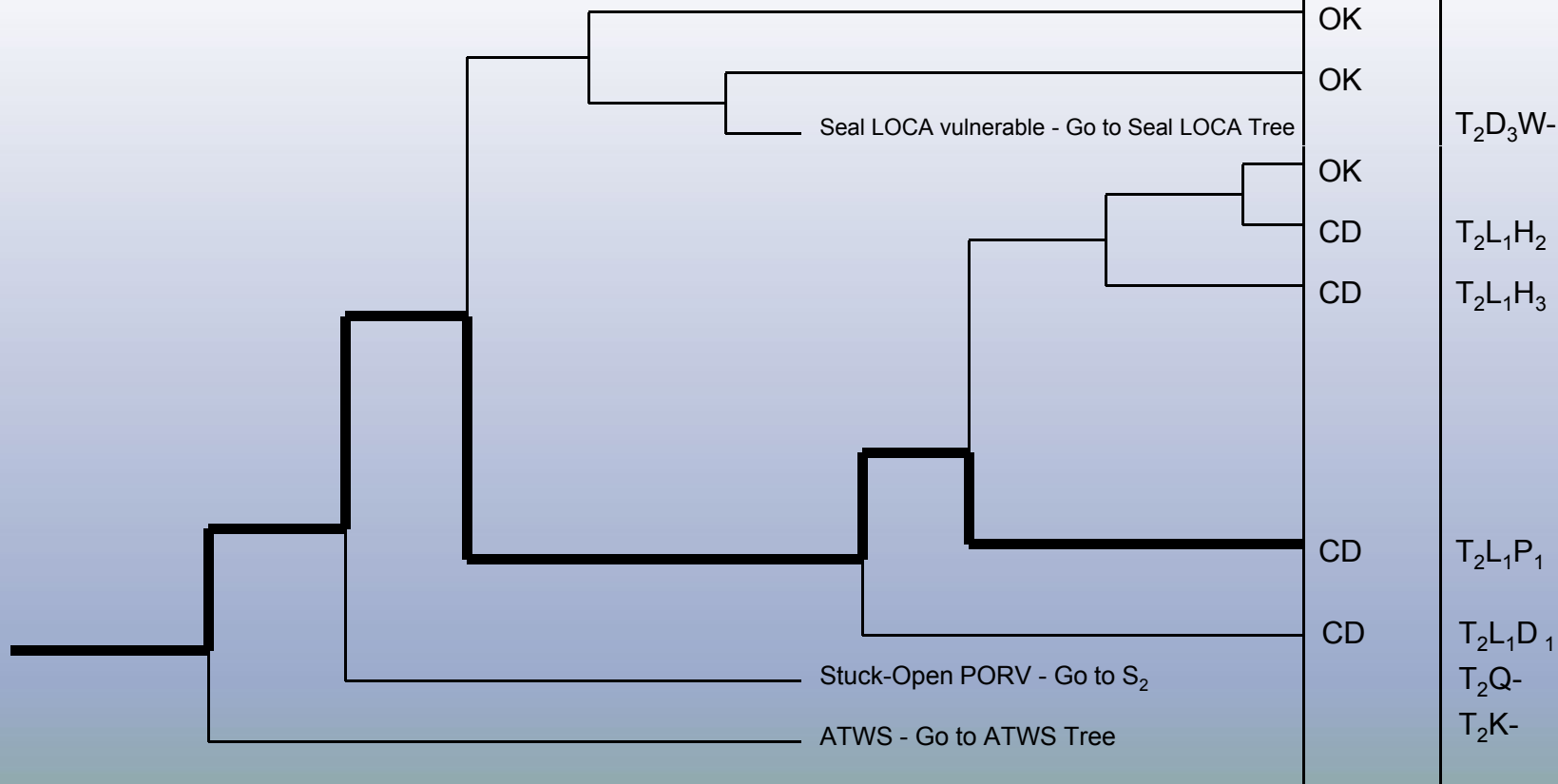
- *This sequence is initiated by a loss of main feedwater (T2), followed by failure of the auxiliary feedwater (AFW) system, and failure of feed and bleed cooling due to the inability to open both power operated relief valves (PORVs).*
- *The loss of main feedwater initiator places a demand on auxiliary feedwater to remove core decay heat. Failure of the AFW system causes a demand for feed and bleed cooling. Failure to initiate feed and bleed and various failures which prevent one of the two PORVs from opening contribute to this sequence. Success criteria require that two PORVs open for successful feed and bleed.*
- *The dominant contributors to AFW failure are common cause failure of the air-operated steam generator level control valves and the common cause failure of all three AFW pumps due to steam binding. The dominant contributor to failure of feed and bleed is operator failure to open PORVs, followed by mechanical failures of the PORV block valves and PORVs.*

Identifiers for T_2 Event Tree

Event Identifier	Description	System Identifier
D ₁	Failure of charging pump system with 1 of 4 success requirements	HPI
D ₃	Failure of charging pump system in seal injection flow mode	SIF
H ₂	Failure of charging pump system in the high pressure recirculation mode	HPR
H ₃	Failure of low pressure injection/recirculation	LPI/LPR
K	Failure of reactor protection system	RPS
L ₁	Failure of auxiliary feedwater required for transients with reactor trip	AFW
P ₁	Failure of both pressurizer PORVs to open for feed & bleed	PRV
Q ₁	Failure of any relief valve to reclose	RVC
W	Failure of component cooling water to the thermal barrier of all reactor coolant pumps	CCW

Event Tree for T_2 - Loss of Main Feedwater

Initiator	RPS	RVC	AFW	SIF	CCW	HPI	PRV	LPI/ LPR	HPR	STATUS	SEQUENCE
T_2	K	Q_1	L_1	D_3	W	D_1	P_1	H_3	H_2		



Term Descriptions

T ₂	Loss of main feedwater	7.2E-1/reactor year
STEAM-BINDING	Steam-binding of all AFWS pumps	1.0E-5
PPS-SOV-FT-334	PORV 334 fails to open	6.3E-3
PPS-SOV-FT-340A	PORV 340A fails to open	6.3E-3
AFW-TDP-FS-1AS	AFWS turbine pump fails to start	3.0E-2
AFW-TDP-FR-1AS6H	AFWS turbine pump fails to run 6 hours	3.0E-2
AFW-TDP-TM-1AS	AFWS turbine pump unavailable test and maintenance	1.0E-2
AFW-AOV-CC	AFWS AOV fails to open	1.0E-3
BETA-AFW	Common cause failure factor of 2 motor pumps	5.6E-2
BETA-8AOV	Common cause failure factor of 8 AOVs	3.4E-2
AFW-MDP-FS	AFWS motor pump fails to start	3.0E-3
HPI-XHE-FO-FDBLD	Operator fails to initiate feed and bleed	2.2E-2
AFW-ACT-FA-TRNA	AFWS Train A actuation fails	1.6E-3
AFW-ACT-FA-TRNB	AFWS Train B actuation fails	1.6E-3

Dominant Contributors to Sequence $T_2L_1P_1$

Minimal Cut Set

Minimal Cut Set Frequency

T_2 * (AFW-AOV-CC * BETA-8AOV) * HPI-XHE-FO-FDBLD	5.4E-7
T_2 * STEAM-BINDING * HPI-XHE-FO-FDBLD	1.6E-7
T_2 * (AFW-AOV-CC * BETA-8AOV) * PPS-SOV-FT-334	1.6E-7
T_2 * (AFW-AOV-CC * BETA-8AOV) * PPS-SOV-FT-340A	1.6E-7
T_2 * AFW-TDP-FS-1AS * (AFW-MDP-FS * BETA-AFW) * HPI-XHE-FO-FDBLD	8.0E-8
T_2 * AFW-TDP-FR-1AS6H * (AFW-MDP-FS * BETA-AFW) * HPI-XHE-FO-FDBLD	8.0E-8
T_2 * STEAM-BINDING * PPS-SOV-FT-334	4.6E-8
T_2 * STEAM-BINDING * PPS-SOV-FT-340A	4.6E-8
T_2 * AFW-ACT-FA-TRNA * AFW-ACT-FA-TRNB * HPI-XHE-FO-FDBLD	4.1E-8
T_2 * AFW-TDP-TM-1AS * (AFW-MDP-FS * BETA-AFW) * HPI-XHE-FO-FDBLD	2.7E-8
Total $T_2L_1P_1$	1.3E-6

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*
- *Three are encountered most commonly:*
 - *Fussell-Vesely*
 - *Risk Reduction*
 - *Risk Increase or Risk Achievement*

Fussell-Vesely Importance

- *Measures overall contribution of an event to risk*
- *Calculated by adding up frequencies of cut sets containing event of interest and dividing by total*

$$FV_x = \sum \text{Cut sets with event } x / F(x)$$

or

$$FV_x = [F(x) - F(0)] / F(x)$$

where,

F(x) is risk with event x at nominal failure probability, and

F(0) is risk when event x is never failed (failure probability = 0)

- *Range is from 0 to 1*

Fussell-Vesely Importance (cont.)

- Consider these minimal cut sets:

$$A = 6 \times 10^{-4} = 6 \times 10^{-4}$$

$$B * C = 1 \times 10^{-2} * 3 \times 10^{-3} = 3 \times 10^{-5}$$

$$C * D = 3 \times 10^{-3} * 1 \times 10^{-3} = 3 \times 10^{-6}$$

$$F_{(x)} = 6.33 \times 10^{-4}$$

where,

$$A = 6 \times 10^{-4}$$

$$B = 1 \times 10^{-2}$$

$$C = 3 \times 10^{-3}$$

$$D = 1 \times 10^{-3}$$

- Fussell-Vesely Importance

$$FV_A = 6.0 \times 10^{-4} / 6.33 \times 10^{-4} = 0.948$$

$$FV_B = 3.0 \times 10^{-5} / 6.33 \times 10^{-4} = 0.047$$

$$FV_C = 3.3 \times 10^{-5} / 6.33 \times 10^{-4} = 0.052$$

$$FV_D = 3.0 \times 10^{-6} / 6.33 \times 10^{-4} = 0.005$$

Risk Reduction Importance

- *Measures amount by which the risk would decrease if event's failure probability were set to 0 (never fails)*
- *Calculated as either ratio or difference between baseline risk and risk with event failure probability at 0*
 - Ratio: $RRR(x) = F(x)/F(0)$*
 - Difference (or Interval): $RRI(x) = F(x) - F(0)$*
 - where,*
 - $F(x)$ is risk with event x at nominal failure probability, and*
 - $F(0)$ is risk when event x is never failed (failure probability = 0)*
- *Ratio - Range is from 1 to ∞*
- *Gives 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 (cont.)

- Consider these minimal cut sets:

$$A = 6 \times 10^{-4} = 6 \times 10^{-4}$$

$$B * C = 1 \times 10^{-2} * 3 \times 10^{-3} = 3 \times 10^{-5}$$

$$C * D = 3 \times 10^{-3} * 1 \times 10^{-3} = 3 \times 10^{-6}$$

$$F_{(x)} = 6.33 \times 10^{-4}$$

where,

$$A = 6 \times 10^{-4}$$

$$B = 1 \times 10^{-2}$$

$$C = 3 \times 10^{-3}$$

$$D = 1 \times 10^{-3}$$

- Risk Reduction Ratio Importance

$$RRR_A = 6.33 \times 10^{-4} / 3.3 \times 10^{-5} = 19.18$$

$$RRR_B = 6.33 \times 10^{-4} / 6.03 \times 10^{-4} = 1.05$$

$$RRR_C = 6.33 \times 10^{-4} / 6.00 \times 10^{-4} = 1.06$$

$$RRR_D = 6.33 \times 10^{-4} / 6.30 \times 10^{-4} = 1.00$$

Risk Increase Importance

- *Measures amount by which the risk would increase if event's failure probability were set to 1 (e.g., component taken out of service)*
- *Calculated as either ratio or difference between the risk with event failure probability at 1 and baseline risk*
 - Ratio: $RAW(x)$ or $RIR(x) = F(1)/F(x)$*
 - Difference (or Interval): $RII(x) = F(1) - F(x)$*
 - where,*
 - $F(x)$ is risk with event x at nominal failure probability, and*
 - $F(1)$ is risk when event x is always failed (failure probability = 1)*
- *Ratio measure referred to as risk achievement worth (RAW)*
- *RAW - Range is ≥ 1*
- *For Maintenance Rule (10 CFR 50.65), NUMARC Guide 93-01 (endorsed by NRC) uses a RAW significance criterion of 2*

Risk Increase Importance (cont.)

- Consider these minimal cut sets:

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

where,

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

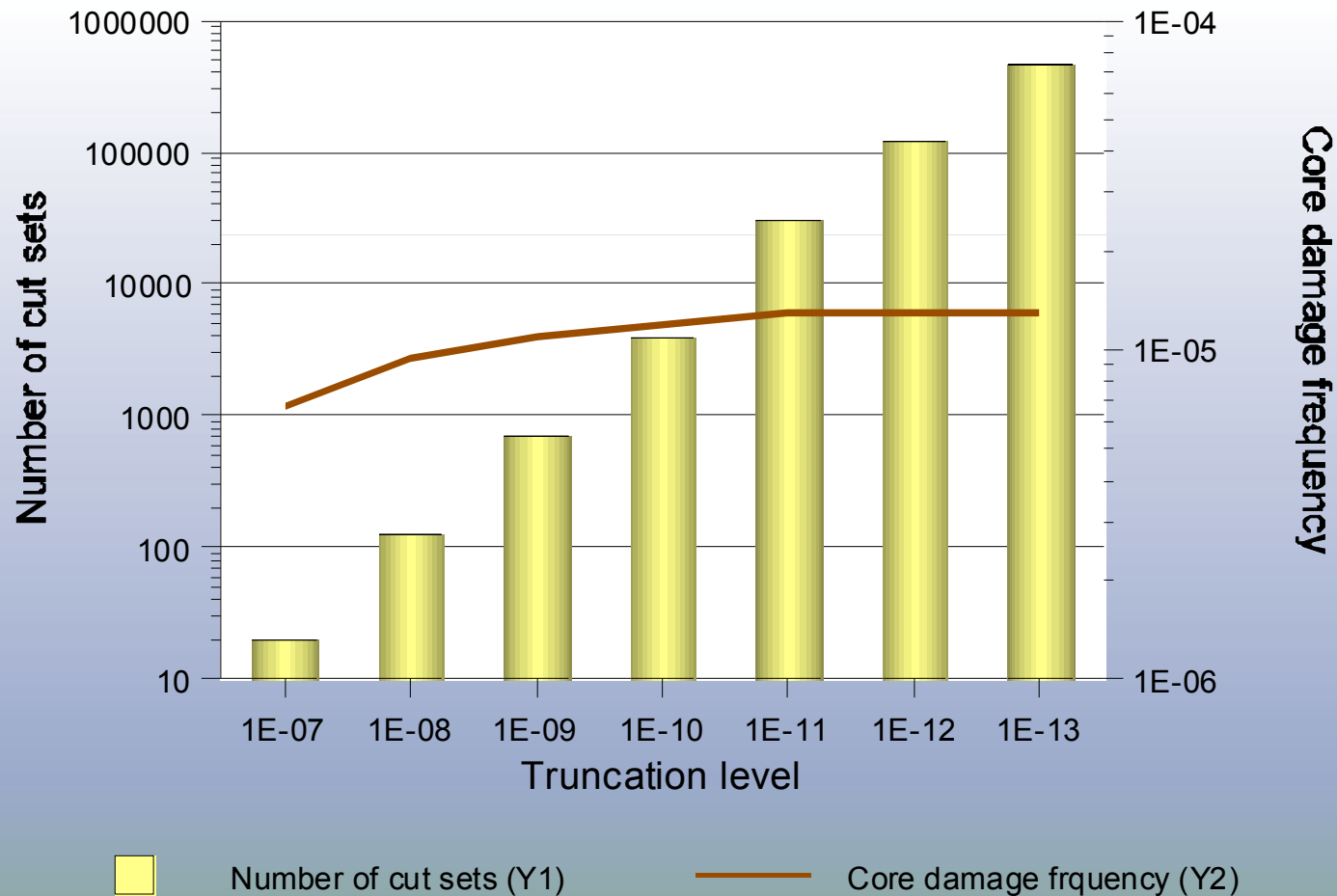
- Risk Achievement Worth Importance

$$\begin{aligned}
 RAW_A &= 1.0 / 6.33 \times 10^{-4} && = 1579.78 \\
 RAW_B &= 3.603 \times 10^{-3} / 6.33 \times 10^{-4} && = 5.69 \\
 RAW_C &= 1.16 \times 10^{-2} / 6.33 \times 10^{-4} && = 18.33 \\
 RAW_D &= 3.63 \times 10^{-3} / 6.33 \times 10^{-4} && = 5.73
 \end{aligned}$$

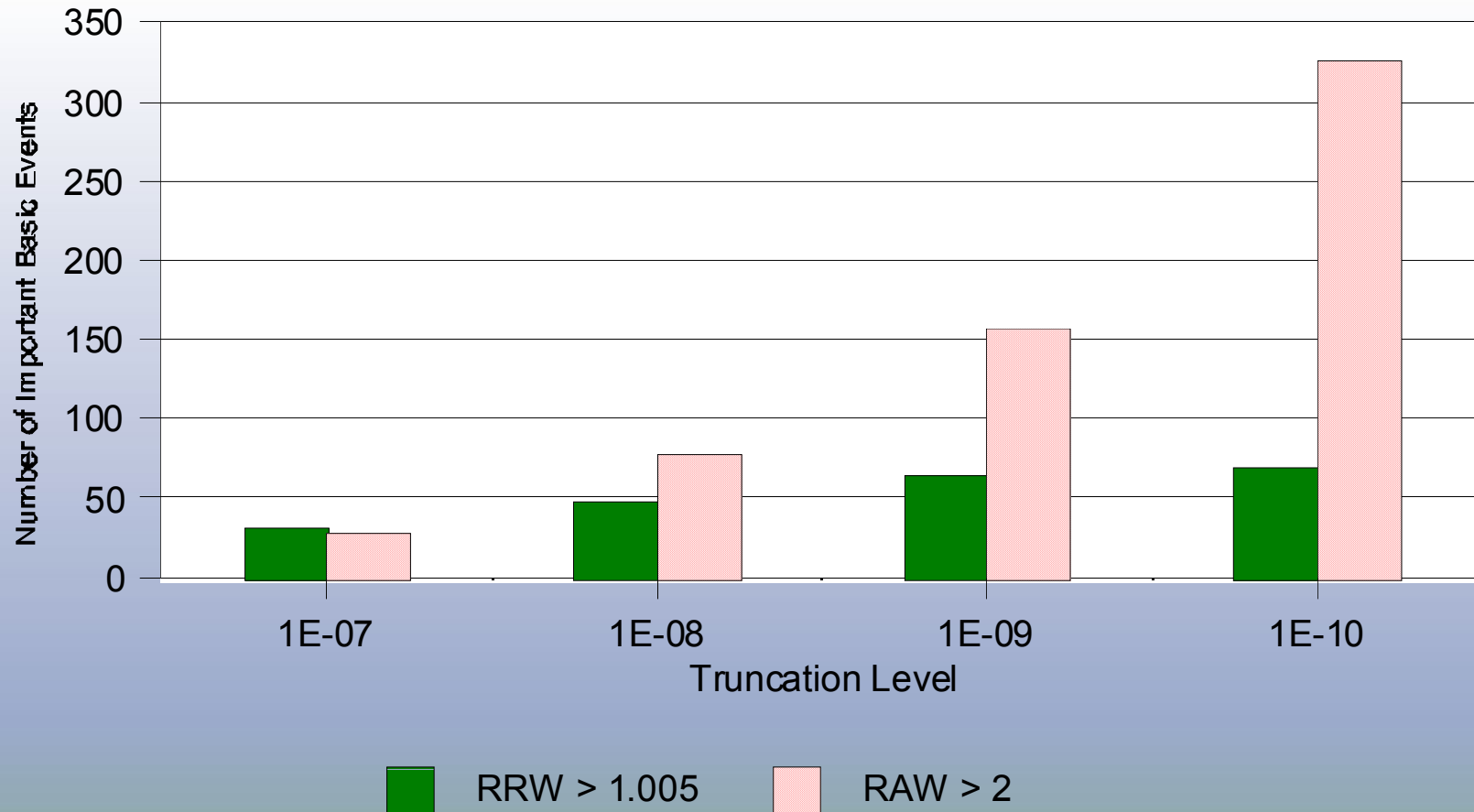
Limitations of Risk Importance Measures

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

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



Truncation Limits Affect Importance Rankings



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*
- *RAW provides indication of risk impact of taking equipment out of service but full impact may not be captured*
 - *That is, taking component out of service for test and maintenance may increase likelihood of initiating event due to human error*

Other Considerations When Using Importance Measures

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

Review Sequence Quantification Purpose and Objectives

- *Purpose: This topic will provide students with an understanding of the quantitative basis of PRA. Elements of accident sequence quantification and importance analysis will be presented.*
- *Objectives: At the conclusion, students will be able to:*
 - *Describe the major processes for accident sequence quantification*
 - *Explain the concepts of importance analysis*

Page Intentionally Left Blank

Idaho National Engineering and Environmental Laboratory

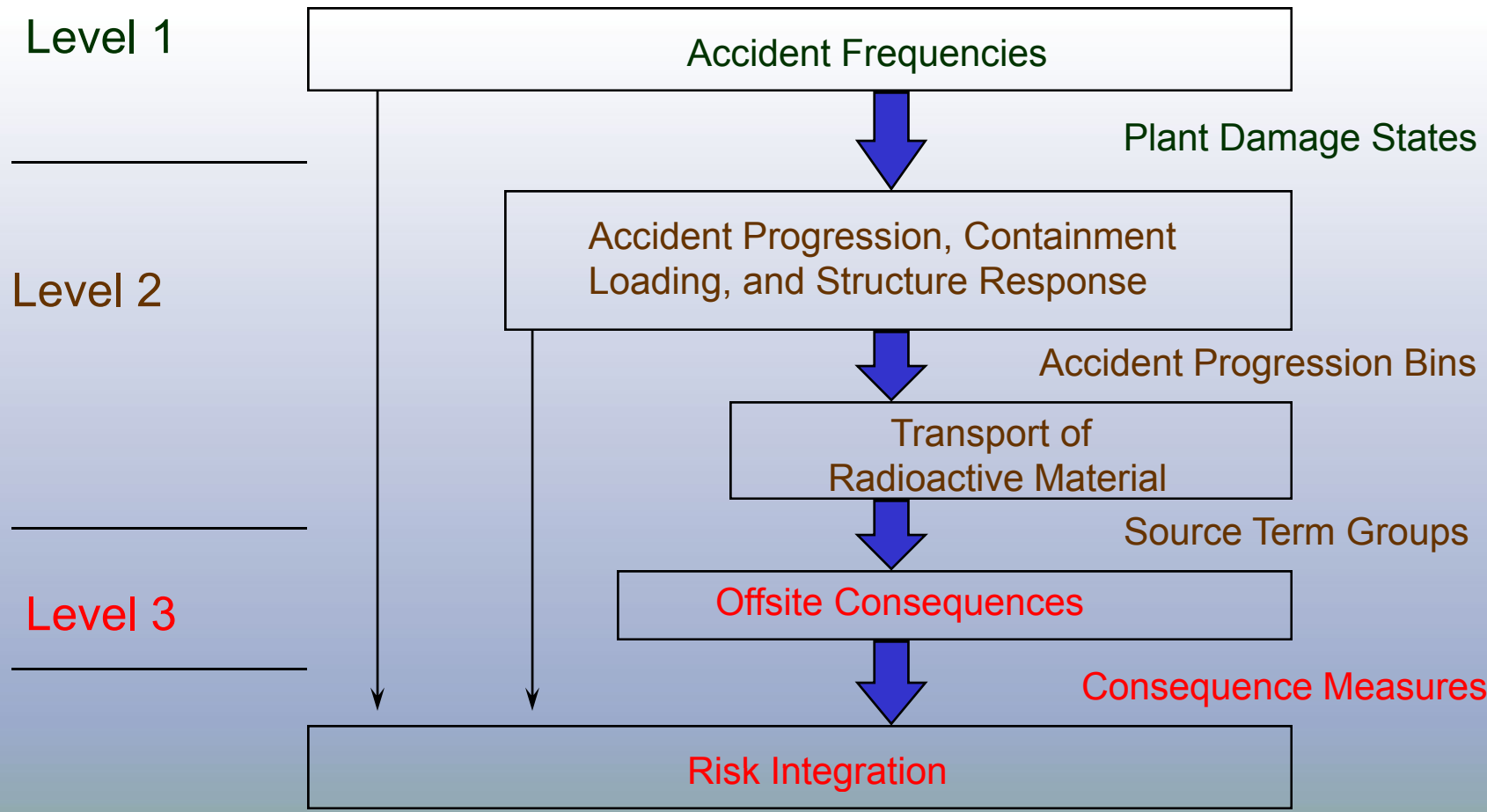
8. Accident Progression & Consequence Analysis



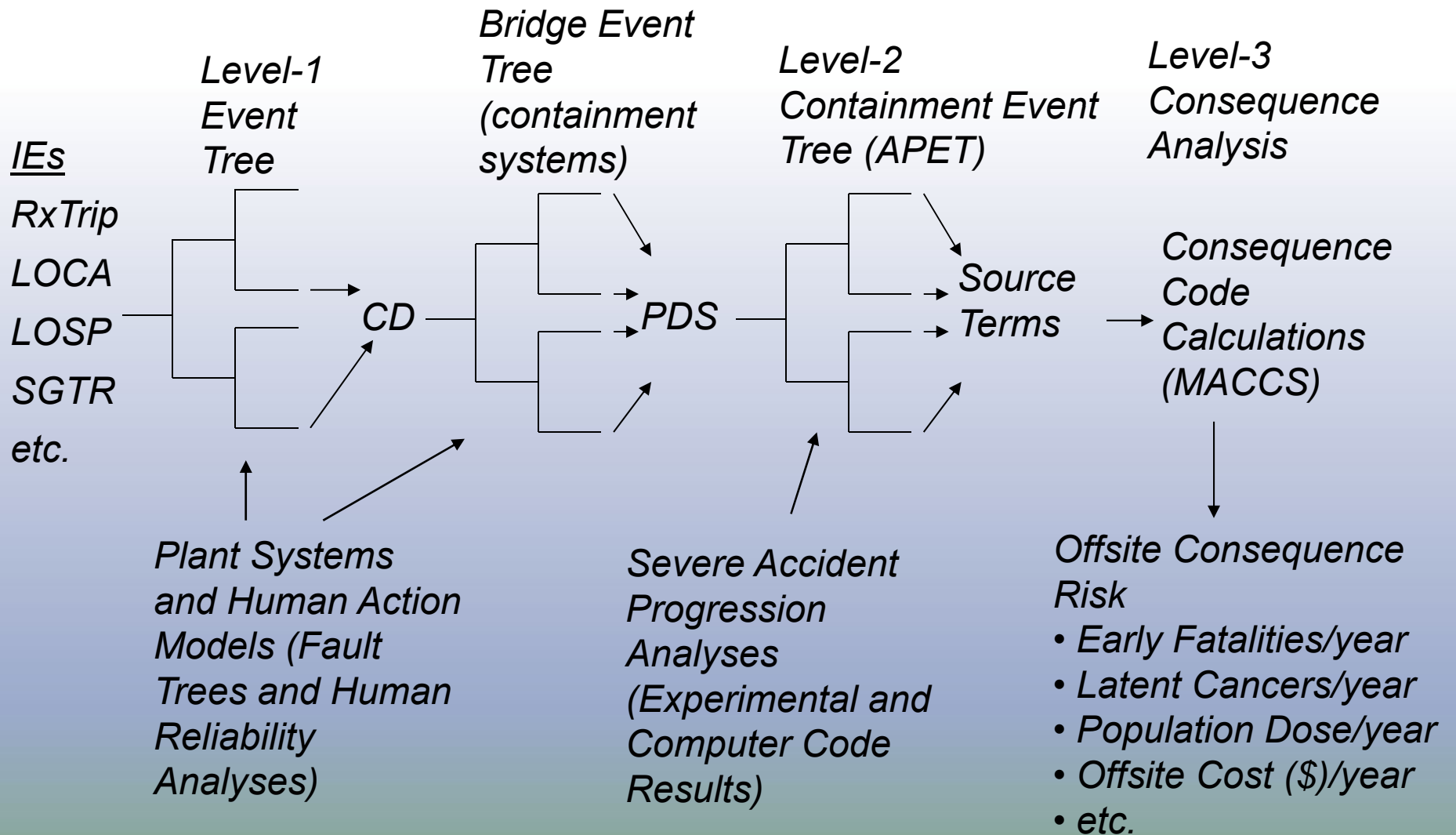
Accident Progression Analysis, Containment Response, Fission Product Transport, and Consequence Analysis

- *Purpose: Students receive a brief introduction to accident progression (Level 2 PRA) and consequence analysis (Level 3 PRA).*
- *Objectives: At the conclusion of this topic, students will be able to:*
 - *List primary elements which comprise accident phenomenology*
 - *Explain how accident progression analysis is related to full PRA*
 - *Explain general factors involved in containment response*
 - *Explain general factors involved in fission product transport & consequences*
 - *Name the major computer codes used in accident process and consequence analysis*
- *Reference: NUREG/CR-2300, NUREG-1489 (App. C)*

Principal Steps in PRA Process



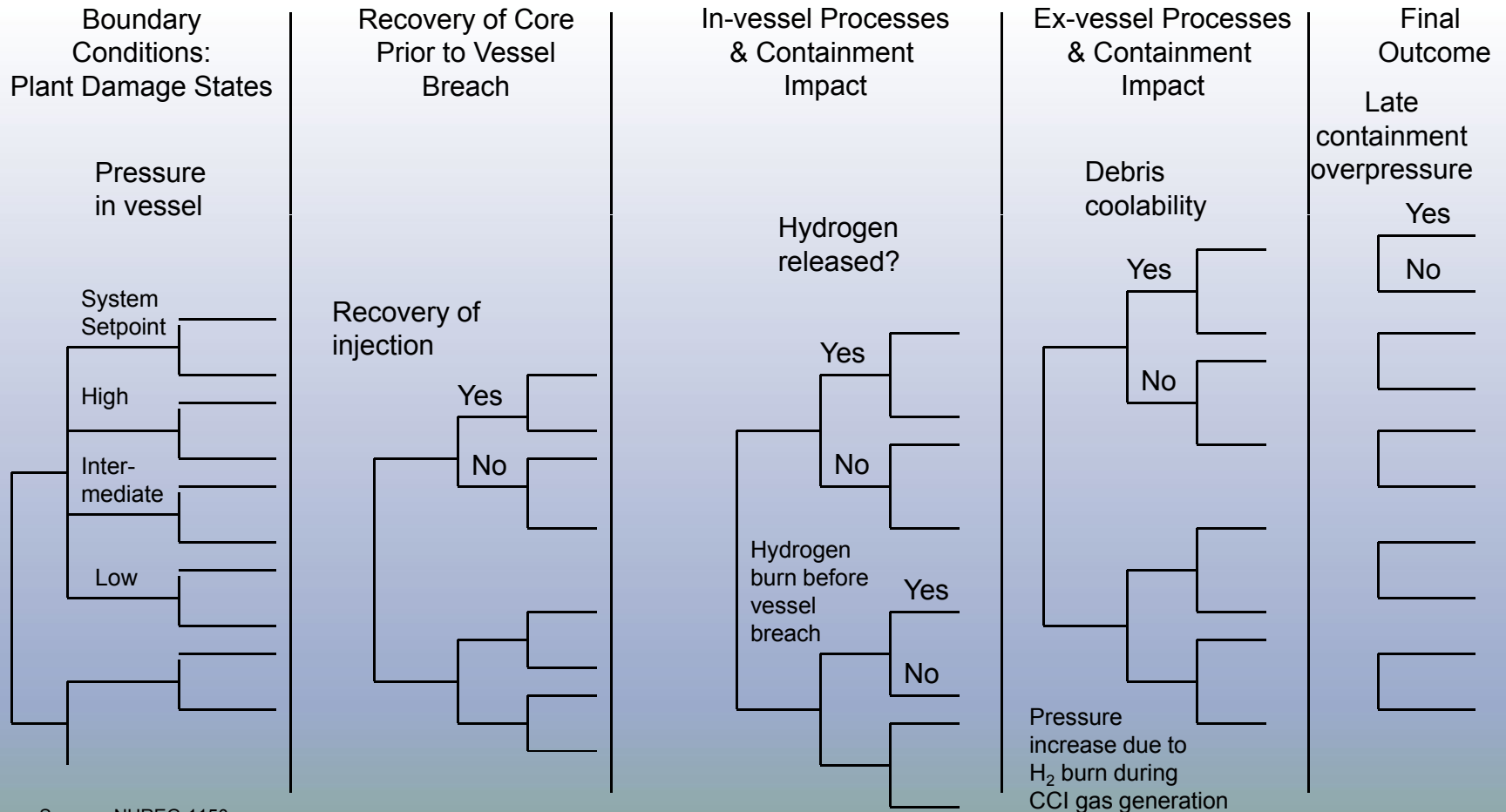
Overview of Level-1/2/3 PRA



Accident Progression Analysis

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

Schematic of Accident Progression Event Tree

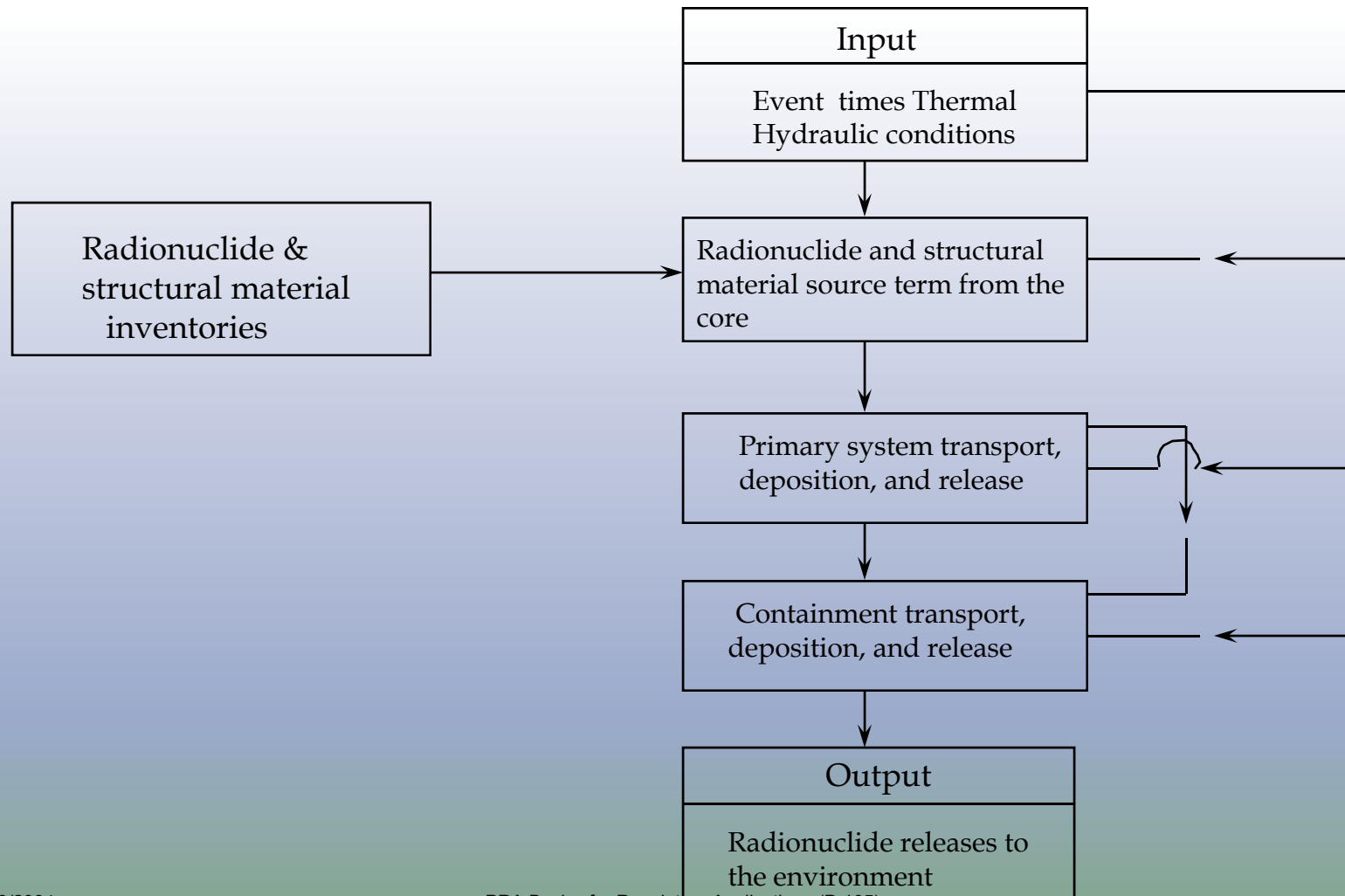


Source: NUREG-1150

Containment Response

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

Elements in the Analysis of Radionuclide Behavior in the Reactor



Computer codes used to model Accident Progression & Fission Product Behavior

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

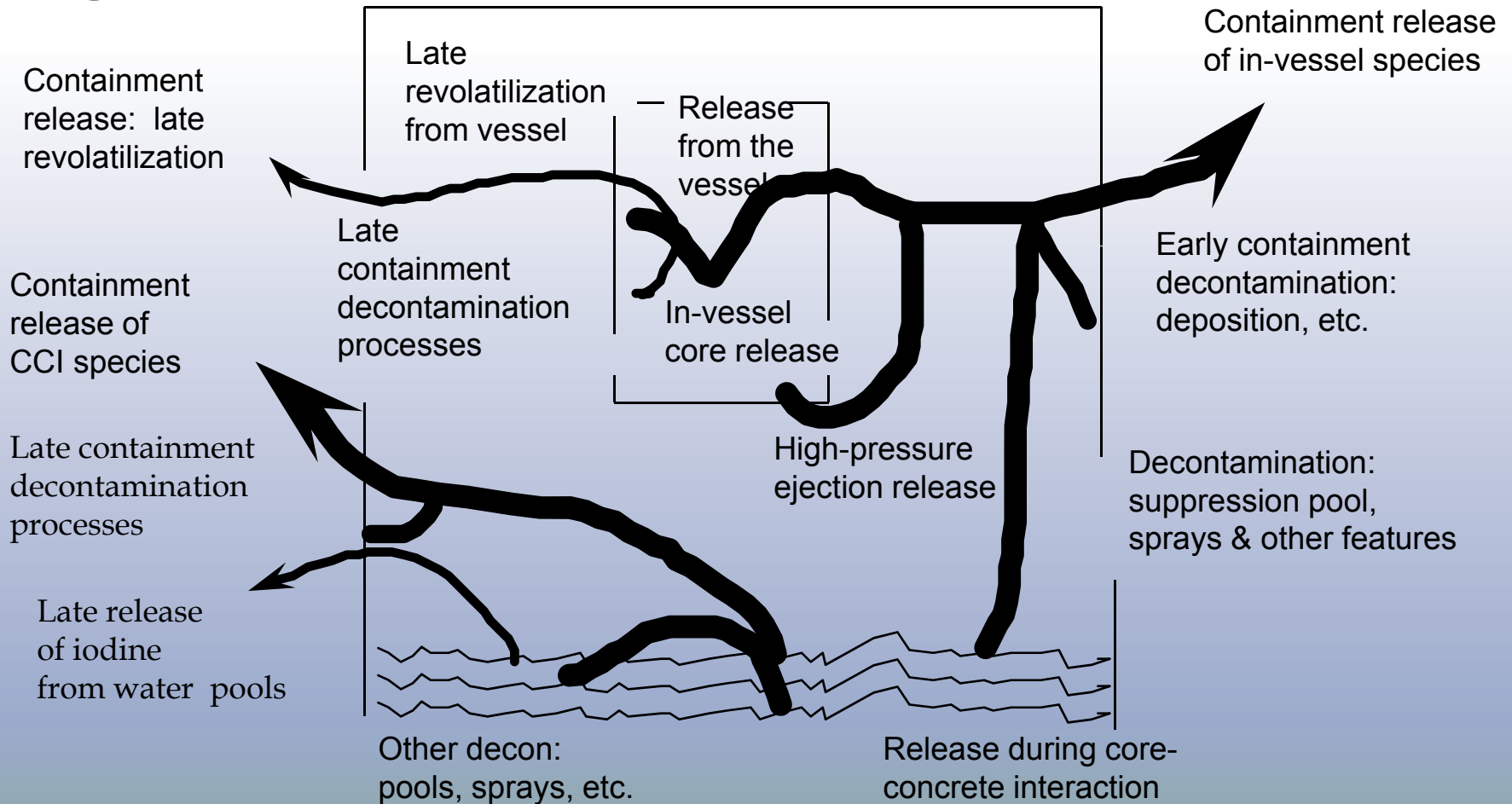
Fission Product Source Term Outcomes of Interest

- *Fractions Released Outside Containment*
 - *Noble Gases*
 - *Iodine*
 - *Cesium - Rubidium*
 - *Tellurium - Antimony*
 - *Barium - Strontium*
 - *Ruthenium -
Molybdenum - Rhenium -
Technetium - Cobalt*
 - *Lanthanum and other
rare earth metals*
- *Parameters for Consequence Model*
 - *Time of release*
 - *Duration of release*
 - *Warning time for
evacuation*
 - *Elevation of release*
 - *Energy of release*

Source Term Calculation Models

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

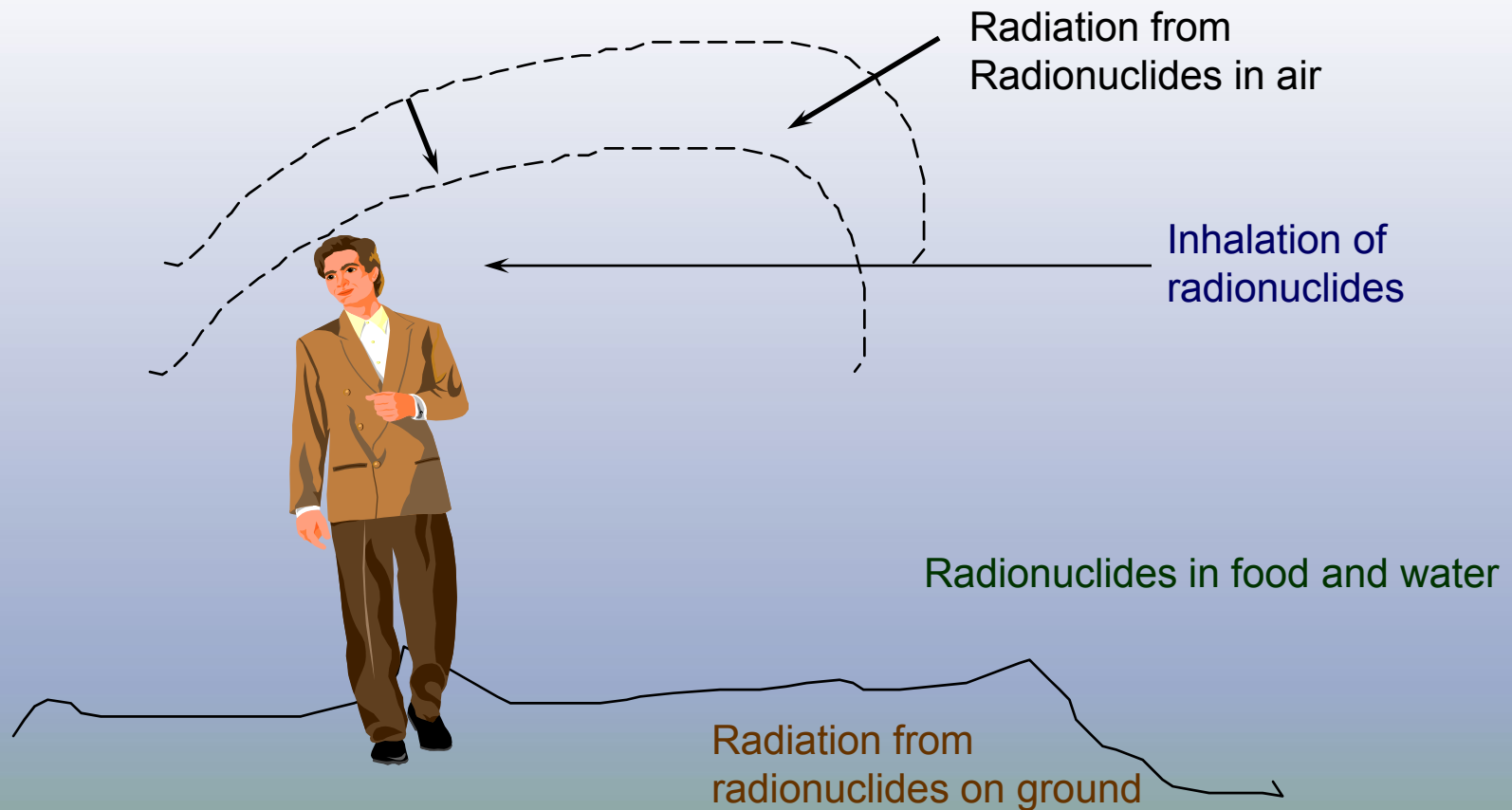
Schematic of Parametric Source Term Algorithm



Components of a Consequence Model

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

Pathways to People



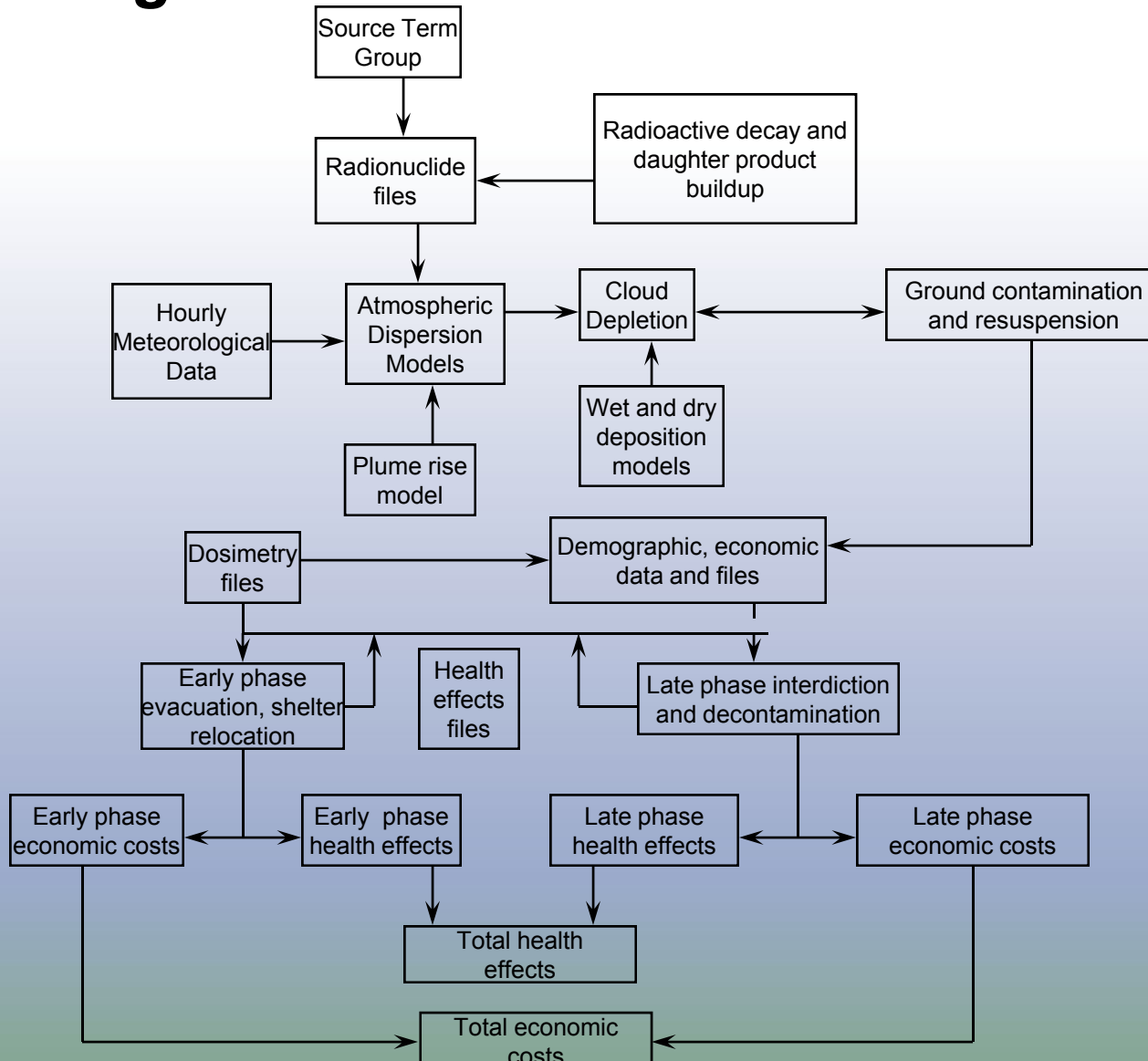
Consequences

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

Consequence Evaluation Models

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

Block Diagram of MACCS Models



Dominant Risk Contributors Sometimes Not Dominant With Respect to CDF

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

Review Accident Progression & Consequence Analysis Purpose and Objectives

- *Purpose: Students receive a brief introduction to accident progression (Level 2 PRA) and consequence analysis (Level 3 PRA).*
- *Objectives: At the conclusion of this topic, students will be able to:*
 - *List primary elements which comprise accident phenomenology*
 - *Explain how accident progression analysis is related to full PRA*
 - *Explain general factors involved in containment response*
 - *Explain general factors involved in fission product transport & consequences*
 - *Name the major computer codes used in accident process and consequence analysis*

Page Intentionally Left Blank

9. *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 the objectives of the IPEEE and the acceptable approaches for seismic events and fires*
 - *Explain the ways in which external events may be evaluated and how this evaluation is related to the overall PRA task flow.*
- *Reference: NUREG/CR-2300, PRA procedures Guide; Generic Letter 88-20 Supplements 4 and 5, NUREG-1407*

Overview of External Events Analysis

- *External Events (EE) refers to those events that are external to system being analyzed*
 - *e.g., fires, floods, earthquakes*
 - *Includes on-site events such as flooding of various rooms within plant*
- *Concern is with dependent nature of EE*
 - *i.e., EE both initiates potential core damage accident AND results in failure of safety systems*
- *General approach*
 - *Identify hazard and its intensity*
 - *Conditional probability of plant SSCs failure*
 - *Assess overall plant response to event*

NPP External Events Risk First Analyzed 1979

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

Initial List of Potential External Event Hazards Very Extensive (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 Very Extensive (2 of 2)

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

Most Hazards Excluded for Various Reasons

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

External Events Analyses Performed at Various Levels of Detail

- *Seismic*
 - *Seismic PRA*
 - *Seismic Margins Assessment (includes HCLPF - high confidence of low probability of failure assessment)*
- *Fire*
 - *Fire PRA*
 - *Fire-Induced Vulnerability Evaluation (FIVE)*
- *Other*
 - *External Event PRA*
 - *Screening analysis*

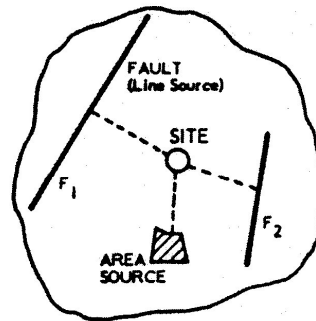
Seismic Hazard PRA - 3 Basic Steps

- *Hazards analysis (frequency-magnitude relationship for earthquakes)*
 - *Location-specific hazard curves produced by NRC (LLNL) and EPRI*
- *Fragility analysis (“strength” of component)*
 - *Conditional probability of failure given a specific earthquake severity*
- *Accident sequence analysis*

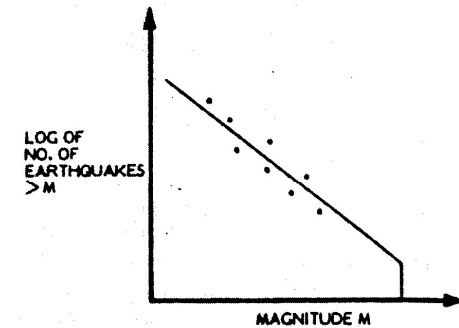
Analysis process briefly looked at in following slides

Four Steps in Seismic Hazard Curve Development

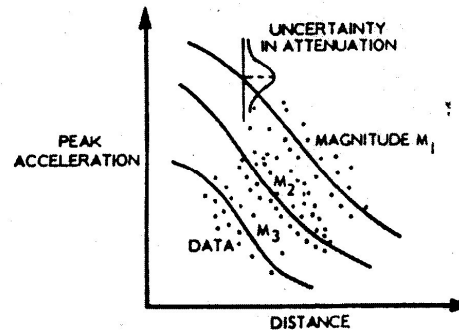
1. Identify seismic sources
2. Develop frequency-magnitude model for each source
3. Develop ground motion model for each source
4. Integrate over sources



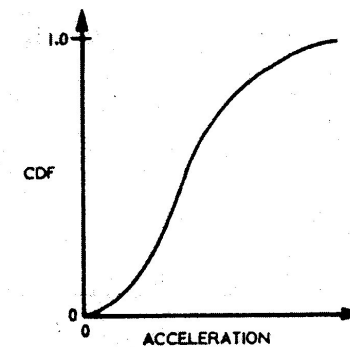
STEP 1
SOURCES



STEP 2
RECURRENCE



STEP 3
ATTENUATION



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

Frequencies Estimated for Various Ground Acceleration Levels

- *Frequency of 0.1g, 0.2g, 0.3g, etc. earthquake estimated*
- *Each g-level earthquake analyzed separately (i.e., as a separate and unique event)*
- *Failure probabilities of plant SSCs calculated based on g-level and fragility of SSC*
- *Internal events PRA re-evaluated using “new” seismic failure probabilities*

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*

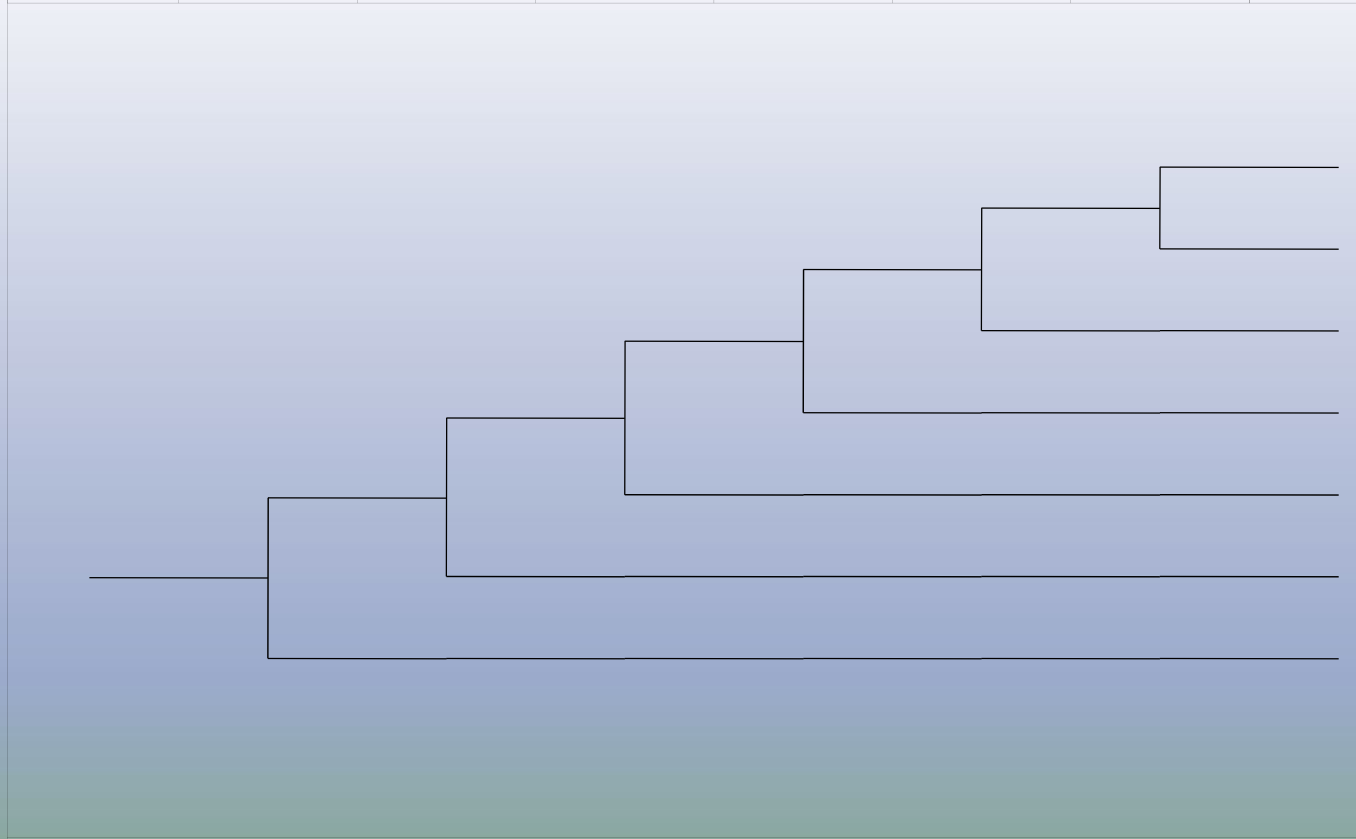
Range of Seismic Fragilities for Selected Components*

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

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

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

Seismic Event Occurs	Reactor Vessel Rupture	Large LOCA	Medium LOCA	Small LOCA	Loss of Off-Site Power	Rx-Trip with FW nominally available	
EQ	RVR	LLOCA	MLOCA	SLOCA	LOSP	T	



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*

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, and fire suppression*
 - *Modeled with specialized computer codes (COMPBRN IIIe)*
- *Component fragilities and failure mode evaluation*
- *Fire detection and suppression modeling*
- *Detailed fire scenarios analyzed using transient ET*

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*

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 OP 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)*

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*

Review External Events Purpose and Objectives

- *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 the objectives of the IPEEE and the acceptable approaches for seismic events and fires*
 - *Explain the ways in which external events may be evaluated and how this evaluation is related to the overall PRA task flow.*

Page Intentionally Left Blank

10. Shutdown Risk



Low-Power and Shutdown Risk

- *Purpose: Discusses why low-power and shutdown modes of operation are thought to be of concern from a risk perspective.*
- *Objective: Understand the reasons for quantifying LP/SD risk and the issues of concern.*
- *References:*
 - *NUREG-1449 - Review of shutdown events*
 - *NUREG/CR-6143 and -6144 - Analysis of low-power shutdown risks at Grand Gulf and Surry*
 - *NUREG/CR-6616 - Risk comparison of scheduling preventive maintenance at shutdown versus at power operation for PWRs*

Risk From LP/SD Operations Was Not Considered in Early PRAs

- *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*
- *In early risk studies, risk from full power operation was assumed to be dominant because during shutdown:*
 - *Reactor is subcritical*
 - *Decay heat decreases with time*
 - *Longer time is available to respond to accidents*

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

- *Precursor events implied that potential generic vulnerabilities existed:*
 - *April 87 Diablo Canyon event resulting in loss of RHR while in mid-loop operation (and numerous similar events at other plants)*
 - *March 90 Vogtle plant loss of all AC power while shutdown*
 - *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*

Operating Experience Insights Reinforced by Early LP/SD Risk Studies

- *Limited risk studies of low-power and shutdown operations have suggested that shutdown risk may be significant because*
 - *Systems may not be available as Tech. Specs. allow more equipment to be inoperable than at power*
 - *Initiating events can impact operable trains of systems providing critical plant safety functions*
 - *Human errors are more prevalent because operators may find themselves in unfamiliar conditions not covered by training and procedures*
 - *Plant instruments and indications may not be available or accurate*

Subsequent LP/SD Risk Studies Examined a Range of Issues

- *Studies included:*
 - *Further review of operating experience for domestic and foreign reactors (discussed on next slide)*
 - *Analysis of selected significant events to estimate conditional probability of core damage using SPAR models (ASP program)*
 - *Review of PRAs that included LP/SD operations*
 - *NRC sponsored Level 1 PRAs for LP/SD operations for Surry and Grand Gulf*

Operating Experience Analysis

- *AEOD* investigation of approximately 90 significant shutdown events out of 348 that occurred between January 1988, and July 1990 yielded the following major categories:*
 - *Loss of S/D cooling due to loss of system flow or loss of heat sink (27 events: 16 PWR and 11 BWR), e.g., errors during emergency power switching logic circuit testing caused a loss of AC power, resulting in loss of RHR for 15 minutes*
 - *Loss of reactor coolant inventory (22 events: 10 PWR and 12 BWR), e.g., opening RHR pump suction relief valve or PORV, or valve lineup errors*
 - *Loss of electrical power (19 events: 13 PWR and 6 BWR), e.g., loss of an AC, DC or instrument bus due to maintenance errors*
 - *Flooding and spills (3 PWR events)*
 - *Inadvertent reactivity addition (10 events: 4 PWR and 6 BWR), e.g., boron dilution without operator's knowledge*
 - *Breach of containment integrity (8 events, all human error)*

** AEOD Special Report - Review of Operating Events Occurring During Hot and Cold Shutdown and Refueling, December 4, 1990*

NRC Continued Monitoring Operating LP/SD Experience

- *AEOD performed follow-up investigation of shutdown events that occurred between January 1993 and May 1995, after licensees had time to implement NUMARC 91-06, “Guidelines for Industry Actions to Assess Shutdown Management” (December 1991), and found:*
 - *Significant number of events during shutdown still occurring (486 during the 29-month investigation period), with 64 events having some measure of risk significance*
 - *Events similar to those of earlier investigation and still dominated by human errors during test and maintenance*

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 S/D*
 - *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*

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 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*

Subsequent PRA Studies (Cont.)

- *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*

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 and NUREG/CR-6144*
- *Most utilities have opted to manage LP/SD risk using simple 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 software to implement this approach (ORAM*)*

* Outage Risk Assessment and Management

SPAR Program Developing Limited Number of LP/SD Models

- *Scheduled to produce 8 LP/SD models (Mar-02 to Mar-04)*
- *Models organized using 15 Plant Operating States (POSs) based on plant configuration evolutions and 4 Time Windows (time after reactor shutdown, i.e., different decay heat levels)*
- *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*

Review Shutdown Risk Purpose and Objectives

- *Purpose: Discusses why low-power and shutdown modes of operation are thought to be of concern from a risk perspective.*
- *Objective: Understand the reasons for quantifying LP/SD risk and the issues of concern.*

Page Intentionally Left Blank

Idaho National Engineering and Environmental Laboratory

11. Uncertainties in PRA



Uncertainties in PRA

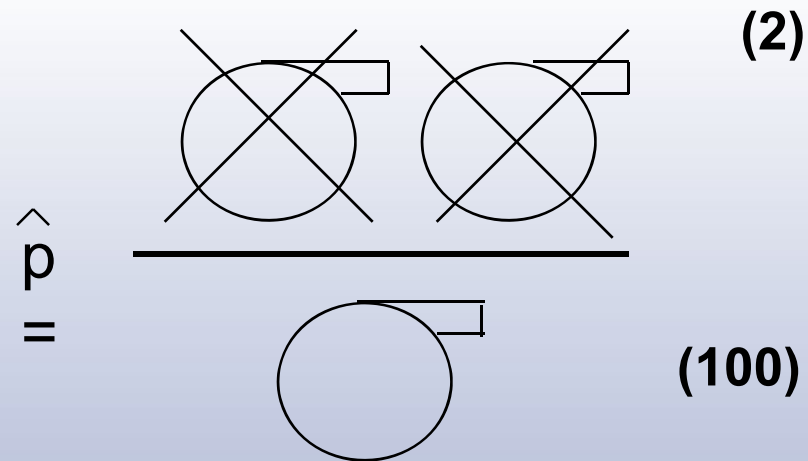
- *Purpose: To acquaint students with how PRA treats uncertainty, including the identification of two types of uncertainty, aleatory and epistemic, and the characterization of one type of epistemic uncertainty with probability distributions.*
- *Objectives: Students will be able to identify the two types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

Uncertainty Arises From Many Sources

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

Key Terminology: Frequentist Interpretation of Probability

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



$$= 1/50$$

$$= 0.02$$

$$= 2E-2$$

Key Terminology: Subjectivist (Bayesian) Interpretation of Probability



↑ *$Pr(N_1)$ is the degree of belief
the analyst holds about the
likelihood of event N_1
occurring*

***PRA*s Identify Two Types of Uncertainty**

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

Aleatory Uncertainty

- *Variability in or lack of precise knowledge about underlying conditions makes events unpredictable. Such events are modeled as being probabilistic in nature. In PRAs, these include initiating events, component failures, and human errors.*
- *For example, PRAs model initiating events as a Poisson process, similar to the decay of radioactive atoms*
- *Poisson process characterized by frequency of initiating event, usually denoted by parameter λ*

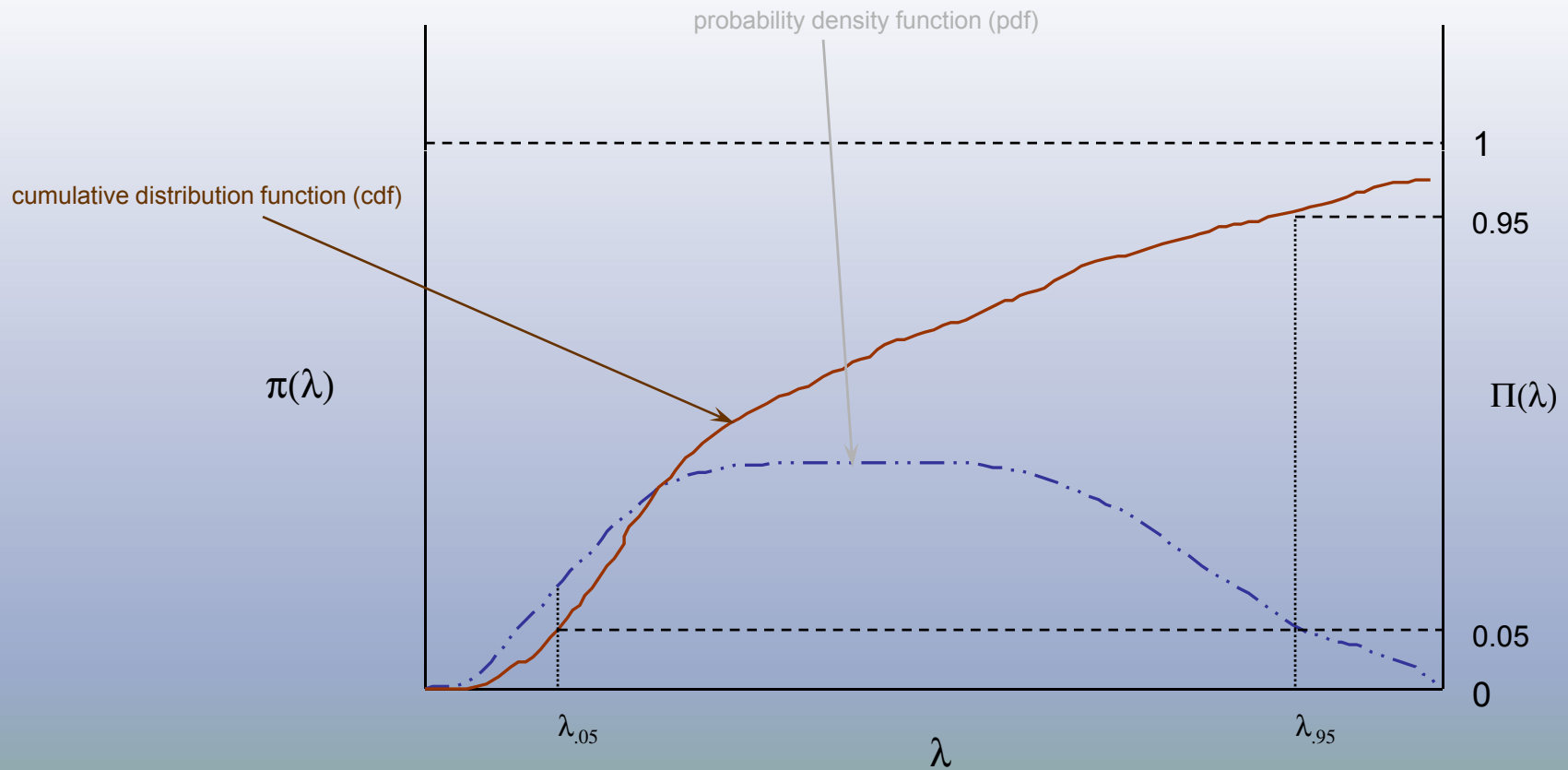
Epistemic Uncertainty

- *Value of λ is not known precisely*
- *Could model uncertainty in estimate of λ using statistical confidence interval*
 - *Can't propagate confidence intervals through PRA models*
 - *Can't interpret confidence intervals as probability statements about value of λ*
- *PRA model lack of knowledge about value of λ by assigning (usually subjectively) a probability distribution to λ*
 - *Probability distribution for λ can be generated using Bayesian methods.*

Epistemic Uncertainty (cont.)

- *Advantages to Bayesian Approach*
 - *Allows uncertainties to be propagated easily through PRA models*
 - *Allows probability statements to be made concerning λ and outputs that depend upon λ*
 - *Provides unified, consistent framework for parameter estimation*

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*

Other Epistemic Uncertainties in PRA

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

Other Epistemic Uncertainties in PRA (cont.)

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

Addressing Other Epistemic Uncertainties

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

Review Uncertainties in PRA

Purpose and Objectives

- *Purpose: To acquaint students with how PRA treats uncertainty, including the identification of two types of uncertainty, aleatory and epistemic, and the characterization of one type of epistemic uncertainty with probability distributions.*
- *Objectives: Students will be able to identify the two types of uncertainty, along with their sources, and interpret probability distributions as an expression of epistemic uncertainty.*

Uncertainty in PRA

- *For additional information:*
 - *Probability & Statistics for PRA (P-102) course covers modeling and propagation of uncertainty in great detail. It covers both the frequentist and Bayesian approaches and compares and contrasts the two.*

Idaho National Engineering and Environmental Laboratory

12. 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 Regulation 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 Regulation 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	[Shaded bar spanning 1995-2005]										
PRA Implementation Plan	[Shaded bar spanning 1995-1999]										
NRC Strategic plan, FY 2000 - 2005						[Shaded bar spanning 2000-2005]					
Risk-Informed Regulation Implementation Plan; SECY-00-0062, SECY-00-0213, SECY-01-0218, SECY-02-0131, SECY-03-0044, SECY-03-0181, SECY-04-0068 (March 23, 2004)						[Shaded bar spanning 2000-2005 with text: 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*
 - *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*

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.*
- *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

- *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 (cont.)

- *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*
- *Events analysis and significance (Accident Sequence Precursors)*
- *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*

Review Introduction to Risk-Informed Regulation Purpose and Objectives

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

Page Intentionally Left Blank

Idaho National Engineering and Environmental Laboratory

13. 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)*
 - *Describe differences between IPE and IPEEE*
 - *Identify intended uses of IPE and IPEEE*
- *References*
 - *GL 88-20*
 - *NUREG-1335, IPE Submittal Guidance*
 - *NUREG-1407, IPEEE Submittal Guidance*
 - *NUREG-1560, Perspectives Gained From IPE Program*
 - *NUREG-1742, Perspectives Gained From IPEEE Program*

Brief History of GL 88-20

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

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 (& IPEEEES) was for Utilities to:

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

IPEs (& IPEEEs) did not Require PRA

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

Intended NRC Staff Uses of IPE Results

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

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

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

IPE Results – NUREG-1560

- *Few licensees explicitly identified vulnerabilities*
 - *4 BWRs and 15 PWRs*
- *Almost all identified plant improvements*
 - *over 500 improvements proposed*
 - ~45% *procedural/operational*
 - ~40% *design/hardware*
 - some both*

BWR Vulnerabilities Identified

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

PWR Vulnerabilities Identified

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

Range of CDFs Reported in IPEs

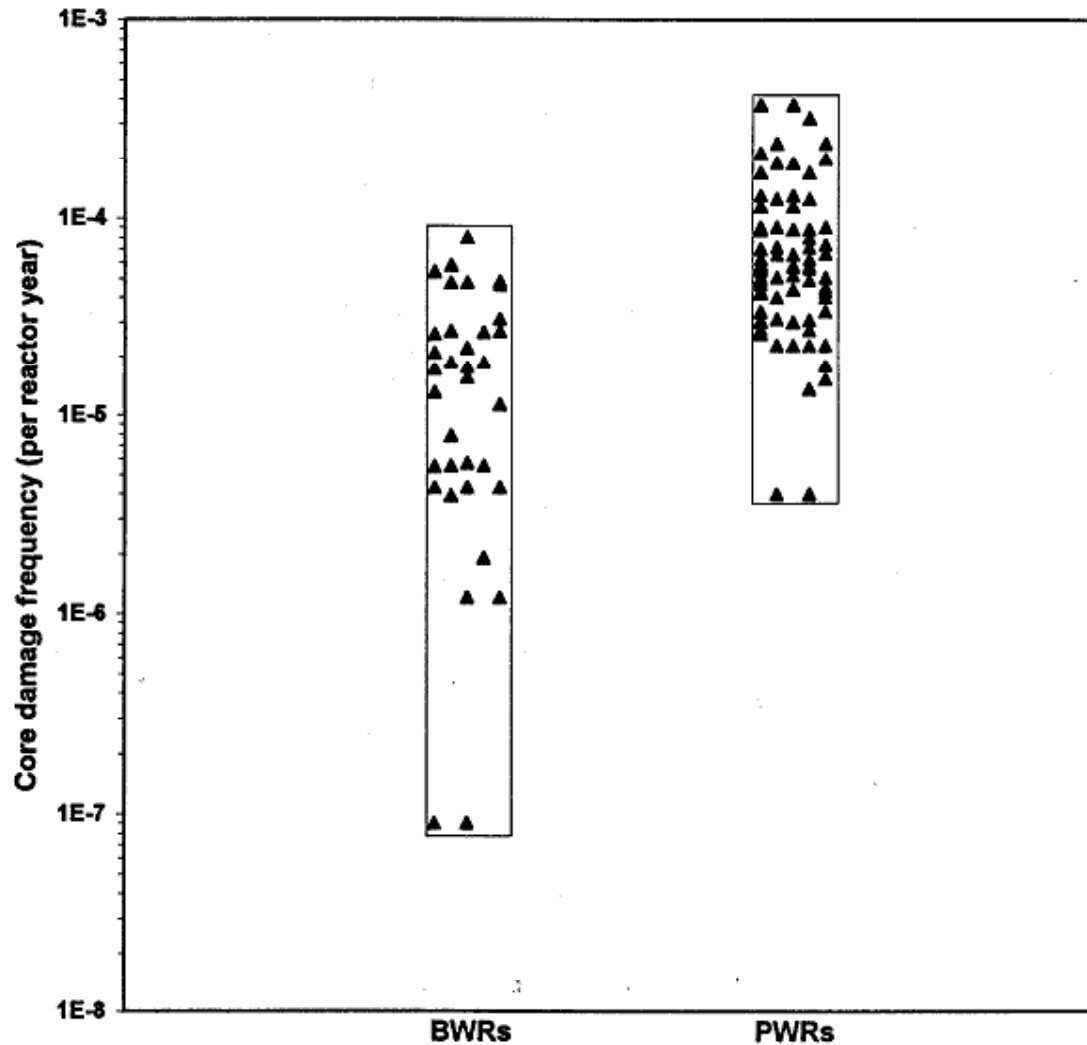


Figure E.1 Summary of BWR and PWR CDFs as reported in the IPEs.

Range of CCFPs Reported in IPEs

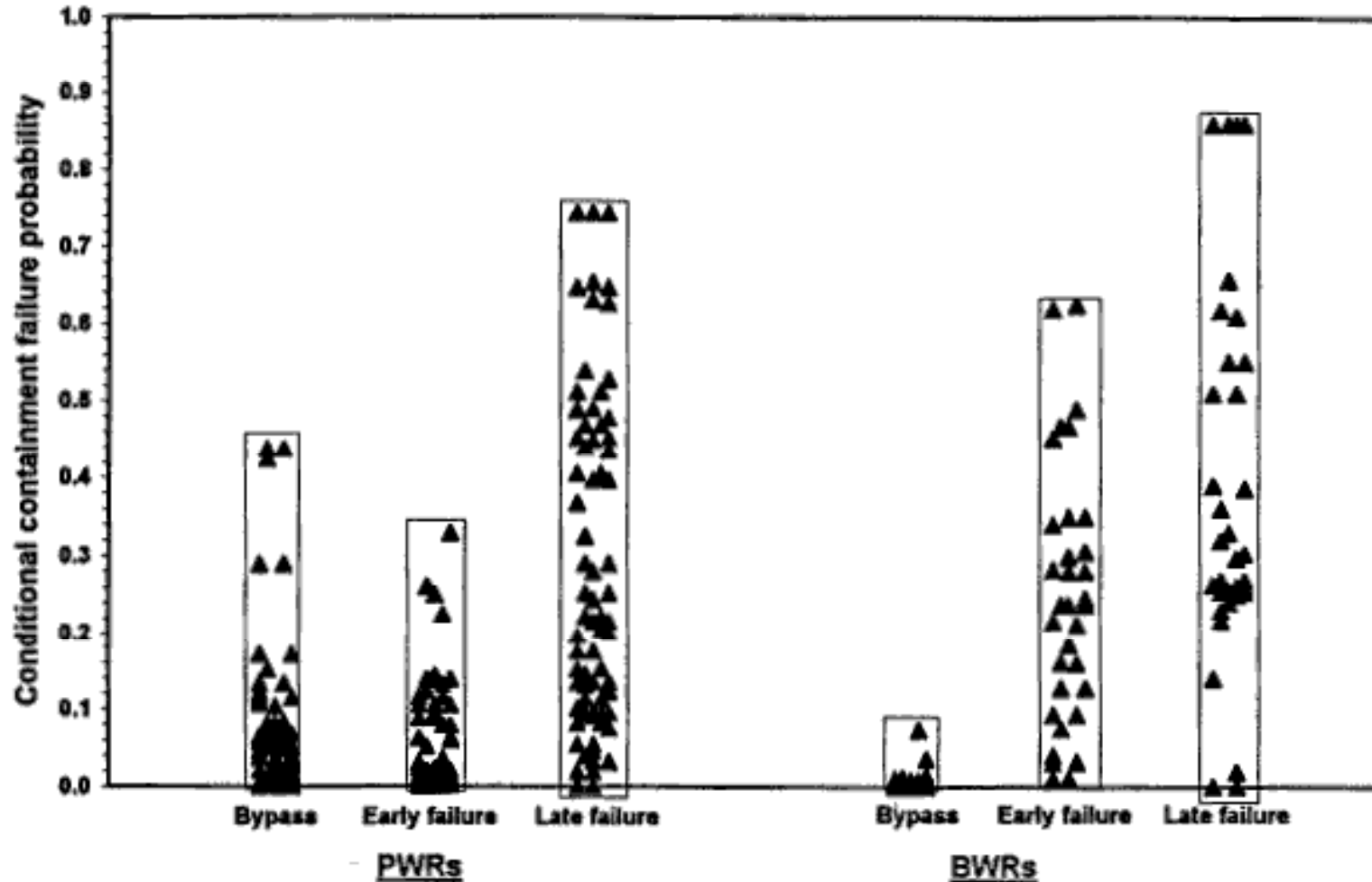


Figure E.2 Summary of conditional containment failure probabilities for BWRs and PWRs as reported in the IPEs.

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

- *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)*
 - *Describe differences between IPE and IPEEEE*
 - *Identify intended uses of IPE and IPEEEE*

Idaho National Engineering and Environmental Laboratory

14. Configuration Risk Management



Configuration Risk Management

- *Purpose: To acquaint students with the basic concepts of using PRA models to control configuration risk by planning maintenance.*
- *Objectives: Students will be able to explain;*
 - *Why base case PRA results cannot be used for maintenance planning*
 - *What is meant by “configuration risk management”*
 - *How configuration risk management is related to risk-informed regulation*
- *Reference: NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications*

Configuration Risk Management

- *Plant configuration: state of the plant as defined by status of plant components*
- *Involves taking measures to avoid risk-significant configurations, limit duration and frequency of such configurations that cannot be avoided*

Configuration Risk Management

Why an Issue?

- *Economics - Plants are moving towards increased maintenance while at power, to reduce outage durations*
- *Safety*
 - *Increased maintenance while at power not covered in IPEs/PRA*
 - *Increased on-line maintenance can produce high-risk plant configurations*

Configuration Risk Management

Why an Issue?

“In general, the industry appears to be adopting the practice of on-line maintenance faster than it is developing and implementing effective controls to manage the safety (risk) implications of this practice.”

[Temporary Instruction (TI) 2525/126, “Evaluation of On-line Maintenance, February 1995,” page 5]

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*

Configuration Risk Management Traditional Approaches

- *Weaknesses of Traditional Approaches*
 - *Generally based on engineering judgment and limited to Technical Specification equipment*
 - *No limit on frequency of equipment outages - only on duration of each outage*
- *Is the traditional approach good enough, given the increased emphasis on on-line maintenance?*
- *How can PRA help?*

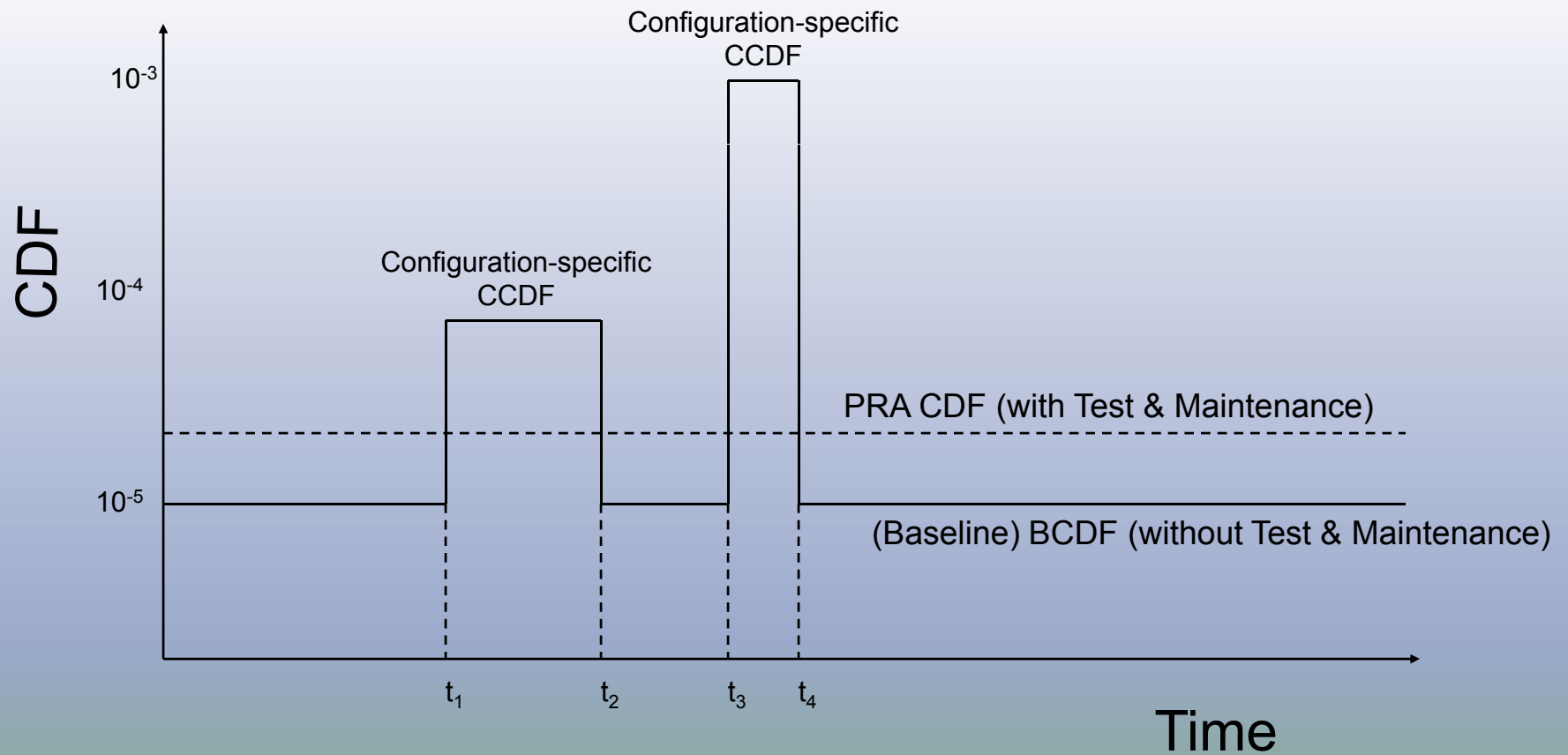
Configuration Risk Management

- *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)*

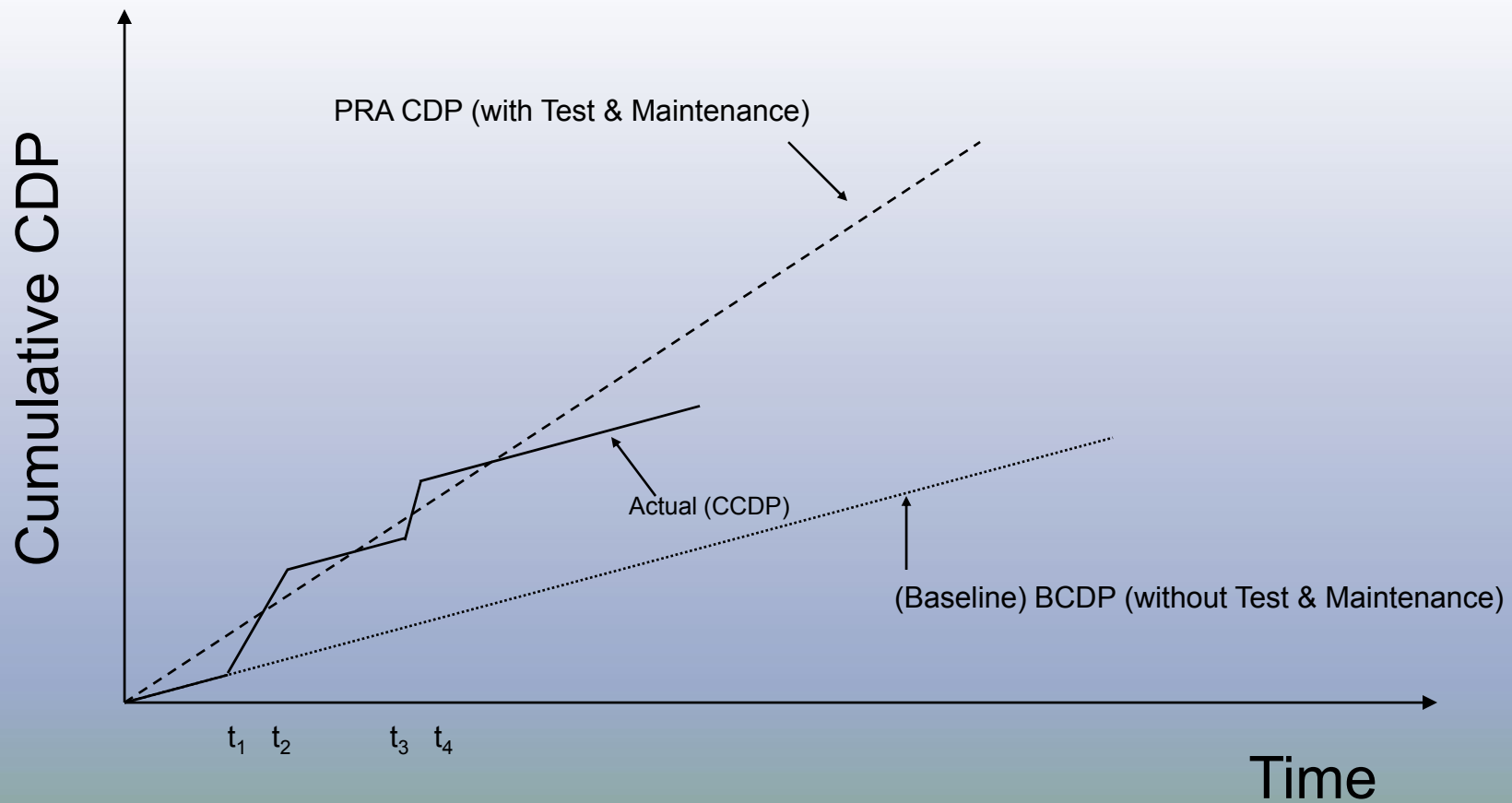
Configuration Risk Management

- Configuration risk has various measures
 - Core damage frequency profile (instantaneous)
 - Baseline CDF (BCDF, i.e., the zero maintenance CDF)
 - Configuration-specific (conditional) CDF (CCDF)
 - Incremental CDF (ICDF)
 - = $CCDF - BCDF$
 - Core damage probability (CDP)
 - = $CDF * duration$
 - Incremental core damage probability (ICDP)
 - = $ICDF * duration$
 - = $CCDP - BCDP$
 - Incremental large early release probability (ICLERP)
 - = $ILERF * duration$
 - = $CLERP - BLERP$

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 CCDP over time*
- (each of these discussed on the following slides)

Managing OOS Components

- *Involves scheduling maintenance and tests to avoid having critical combinations of components or systems out of service concurrently*
- *For Maintenance Rule, 10 CFR 50.65*
 - *A value of 1E-3/year is suggested in NUMARC 93-01 for a ceiling for configuration-specific CCDF*
 - *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

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

Managing Backup Components

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

Controlling Frequency

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

Why Configuration Risk Management is Needed...

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

Preventive Maintenance Risk Calculations

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

Risk Monitors

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

Current Risk Monitor Software Packages

- *Erin Engineering Sentinel*
- *Sciencetech/NUS Safety Monitor*
 - *The NRC acquired this package from Sciencetech, and has an agency-wide license covering its use*
- *EPRI R&R Workstation*
- *Commonwealth Edison OSPRE*

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 (cont.)

- *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*

Risk Monitor Strengths and Weaknesses

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

Risk Monitor Strengths and Weaknesses (cont.)

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

Additional Sources of Information

- *Further details on configuration risk management can be found in NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications*
- *Risk Assessment for Event Evaluation (P-302) course in the PRA Technology Transfer Program curriculum explores the use of PRA techniques for evaluating the risk significance of operational events, as well as plant configuration risk management, discusses the other risk measures mentioned in this module (e.g., CCDP and event importance), and illustrates use of the GEM code to perform the necessary PRA calculations.*

Review Configuration Risk Management Purpose and Objectives

- *Purpose: To acquaint students with the basic concepts of using PRA models to control configuration risk by planning maintenance.*
- *Objectives: Students will be able to explain;*
 - *Why base case PRA results cannot be used for maintenance planning*
 - *What is meant by “configuration risk management”*
 - *How configuration risk management is related to risk-informed regulation*

Idaho National Engineering and Environmental Laboratory

15. Introduction to Risk-Informed Decision-Making



Introduction to Risk-Informed Decision-Making

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

Risk-Informed Regulatory Guides and SRPs

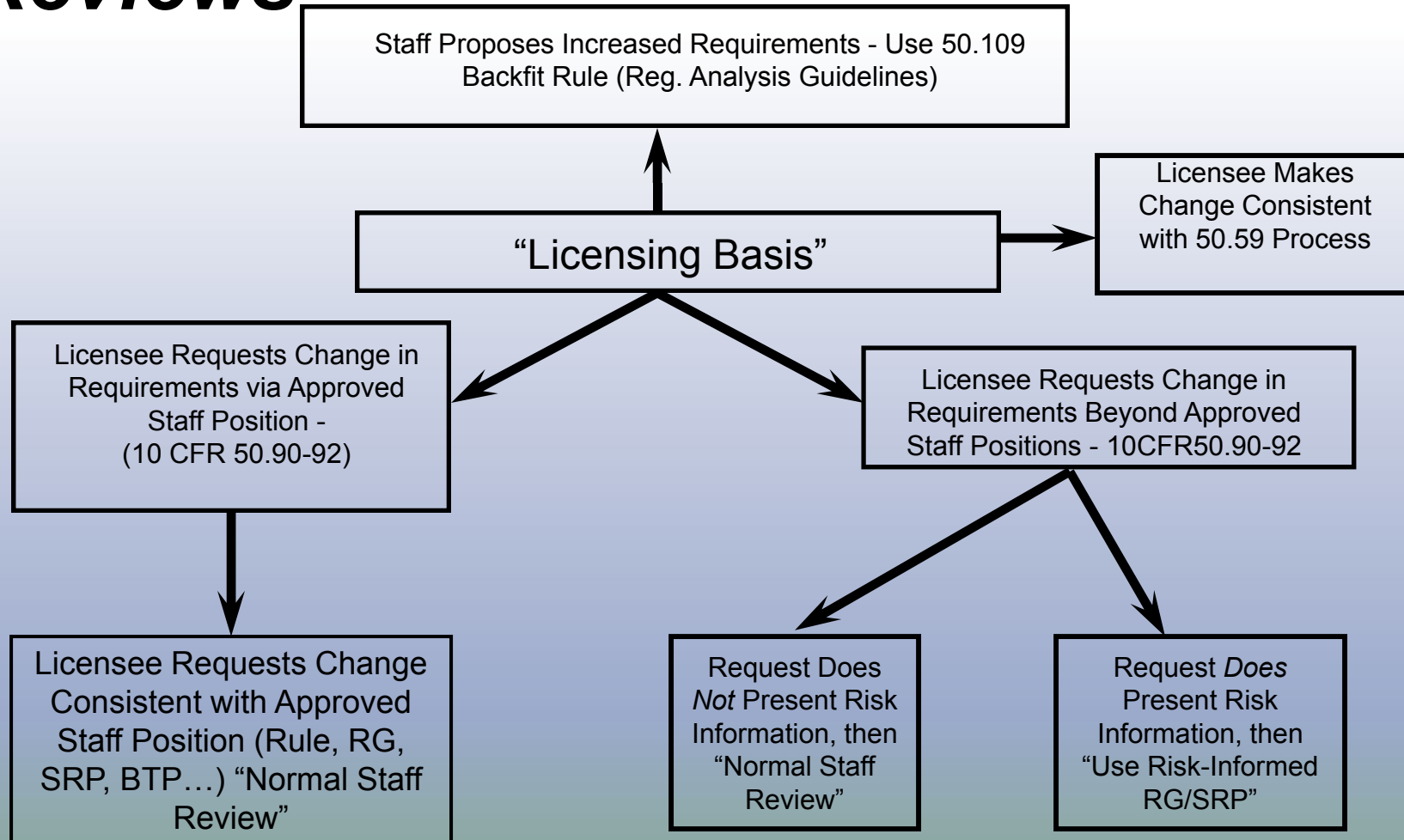
Regulatory Guide

- *R. G. 1.174 - General guidance to licensees*
- *R.G.-1.175 - Application-specific guidance on in-service testing*
- *R.G. – 1.176 - Application-specific guidance on graded quality assurance*
- *R.G. – 1.177 - Application-specific guidance on technical specifications*
- *R.G. – 1.178 - Application-specific guidance on in-service inspection*

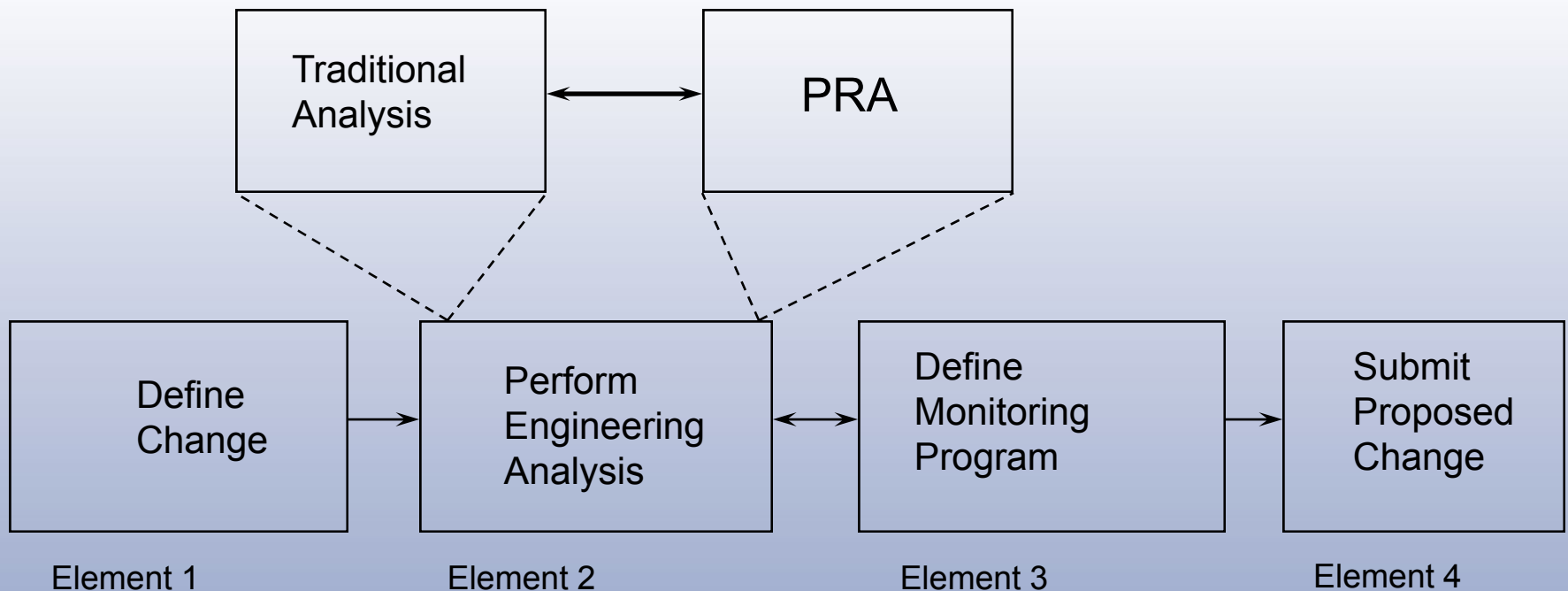
Standard Review Plan

- *SRP Chapter 19 - General guidance to staff*
- *SRP Section 3.9.7 - Application-specific guidance on IST*
- *Inspection guidance - under development*
- *SRP Section 16.1 - Application-specific guidance on technical specifications*
- *SRP Section 3.9.8 - Application-specific guidance on ISI*

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 (cont.)

- *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 (cont.)

- *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 (cont.)

- *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*

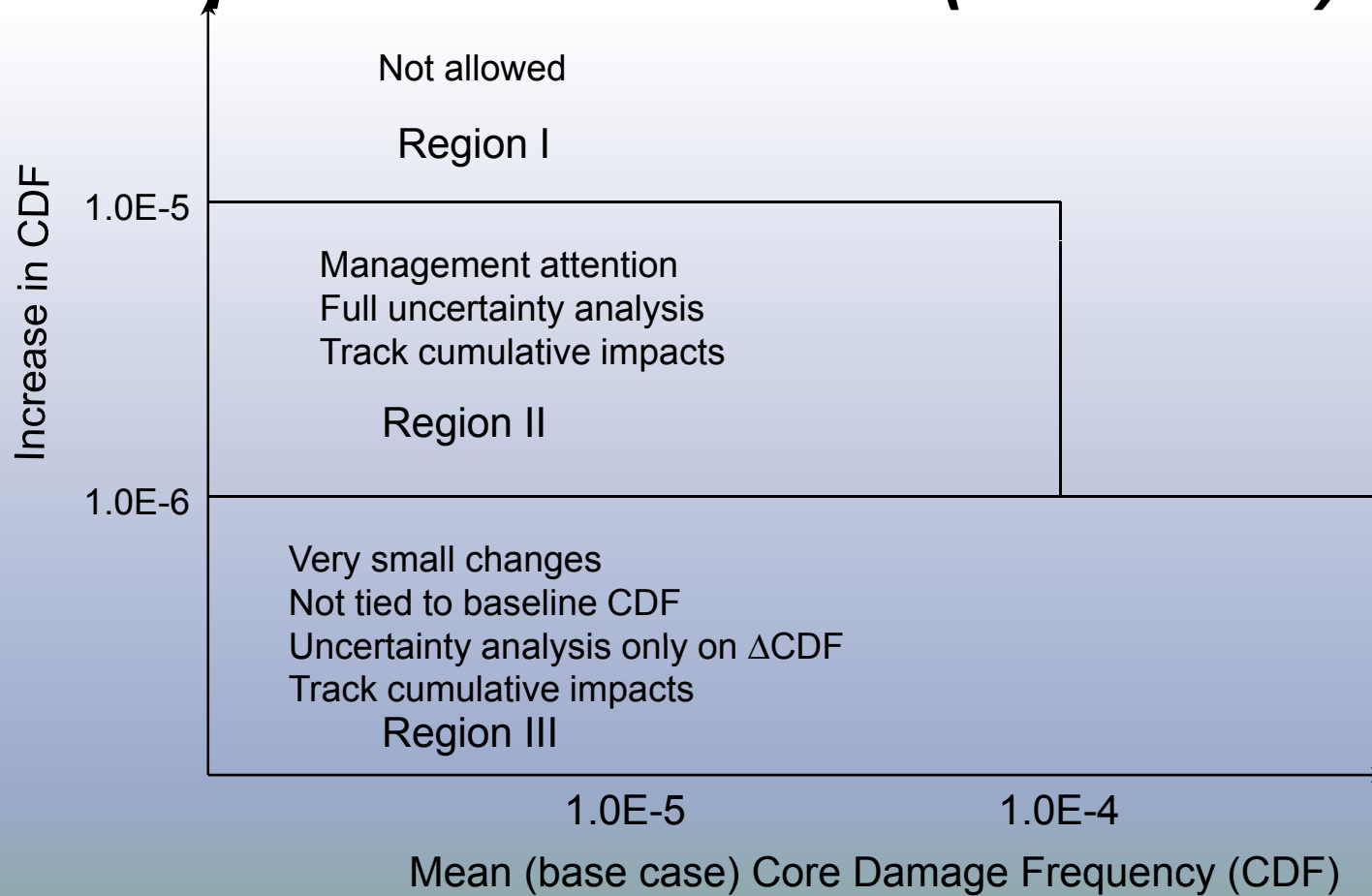
Acceptance Guidelines (cont.)

- *Defense-in-depth is maintained (cont.)*
 - *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*

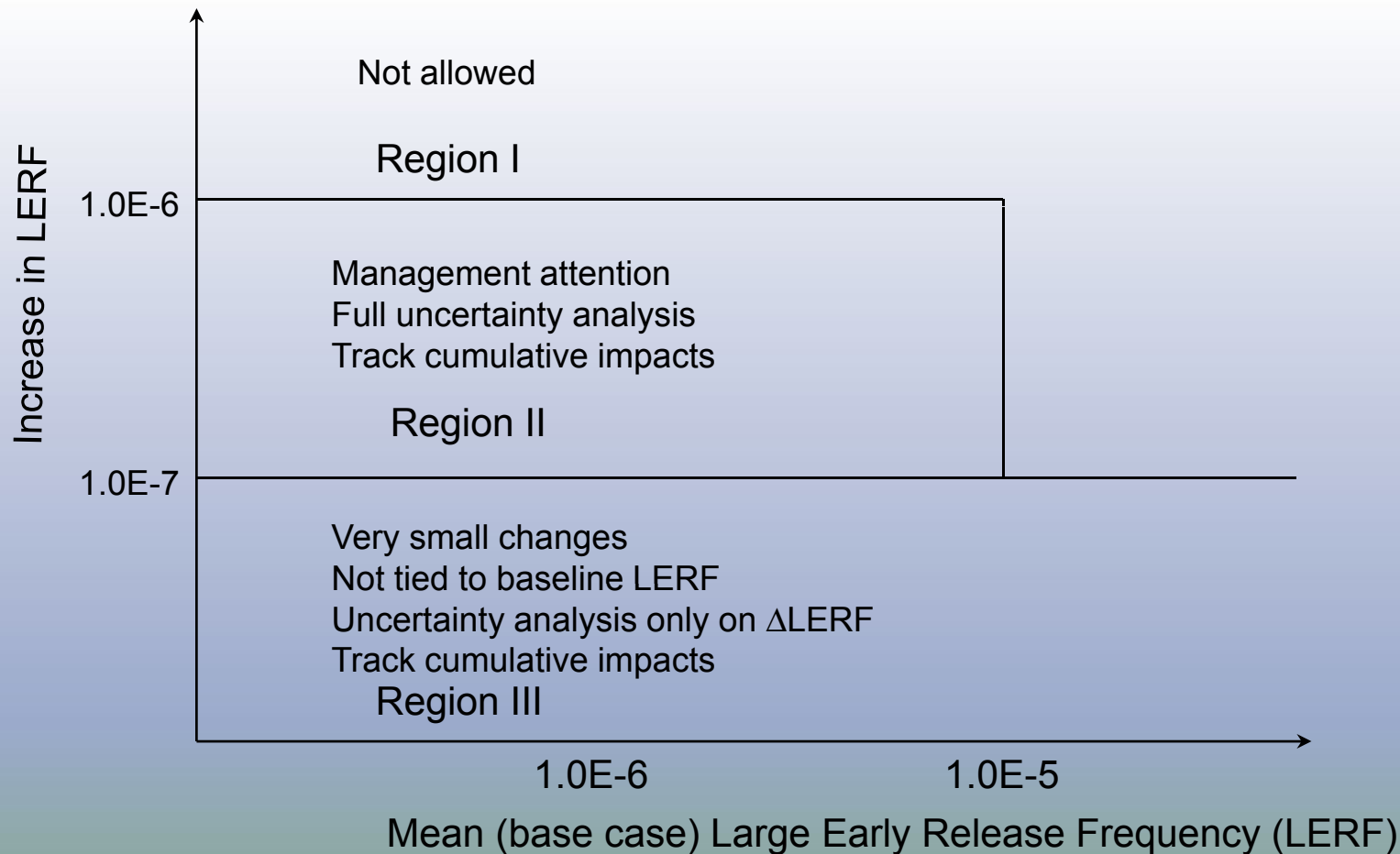
Acceptance Guidelines (cont.)

- *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)



Mean Large Early Release Frequency Acceptance Guidelines (RG 1.174)



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*
 - *Certification*
 - *Standards (e.g., new ASME and ANS standards)*

NRC Staff and Management Responsibilities

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

Review Introduction to Risk-Informed Decision-Making Purpose and Objectives

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

Page Intentionally Left Blank

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?
 - $P\{\text{event} < 1 \text{ year}\} = 1 - e^{-(2E-2)(1)} = 1 - 0.9802 = 0.0198 = 1.98E-2$
 - Or $P\{\text{event} < 1 \text{ year}\} \approx \lambda t \approx (2E-2)(1) \approx 2E-2$
 - 1.2. What is the probability that an event will occur at least once during the next 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 an event (either A or B) will occur during the next 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 an event (either A or B) will occur during the next 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 $P(A + B) = P(A) + P(B) - P(AB) = 1 - e^{-(\lambda A + \lambda B)t} = 1 - e^{-(0.1 + 0.3)5} = 1 - 0.1353 = 8.647E-1$
- 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?
 - $P\{\text{at least 1 failure in 4 trials} \mid 0.2\} = 1 - P\{0 \text{ failures in 4 trials} \mid 0.2\}$

$$= 1 - \frac{4!}{0!(4-0)!} 0.2^0 (1-0.2)^4 = 1 - 0.4096 = 0.5904$$

Probability and Frequency Questions

- $P\{\text{exactly 0 failures in 4 trials} \mid 0.2\} =$
- $= \frac{4!}{0!(4-0)!} 0.2^0(1-0.2)^4 = (1)(1)(0.4096) = 0.4096$

- $P\{\text{exactly 1 failure in 4 trials} \mid 0.2\} =$
- $= \frac{4!}{1!(4-1)!} 0.2^1(1-0.2)^3 = (4)(0.2)(0.512) = 0.4096$

- $P\{\text{exactly 2 failures in 4 trials} \mid 0.2\} =$
- $= \frac{4!}{2!(4-2)!} 0.2^2(1-0.2)^2 = (6)(0.04)(0.64) = 0.1536$

- $P\{\text{exactly 3 failure in 4 trials} \mid 0.2\} =$
- $= \frac{4!}{3!(4-3)!} 0.2^3(1-0.2)^1 = (4)(0.008)(0.8) = 0.0256$

- $P\{\text{exactly 4 failures in 4 trials} \mid 0.2\} =$
- $= \frac{4!}{4!(4-4)!} 0.2^4(1-0.2)^0 = (1)(0.0016)(1) = 0.0016$