System Modeling Techniques for PRA P-200

January 2016

United States
Nuclear Regulatory Commission

DISCLAIMER NOTICE

System Modeling Techniques for PRA P-200

Course Presented by

Michael B. Calley, INL
email: Michael.Calley@inl.gov
phone: (208) 526-9230

Jim Knudsen, INL
email: James.Knudsen@inl.gov
phone: (208) 526-6432

January 26 – January 29, 2015
NRC Professional Development Center
Rockville, MD

Idaho National Laboratory

Course Outline

Tuesday - AM
0. Introduction (9)
1. Basics (20)
2. Fault Trees (34)

Tuesday - PM
FT Practice examples
3. System Models (26)
Workshop (Appendix A)

Wednesday – AM
4. Uncertainties (22)
5. Event Trees (18)
   practice example
6. Sequence Models (17)
   practice example

Wednesday – PM
7. Common Cause Failure Models (36)
Workshops – ET & Sequence Logic (cutsets)

Thursday – AM
8. Quantifying Logic Models (29)
9. Data Analysis (14)
10. Human Error Modeling (21)
11. Results (16)

Thursday - PM
12. Special Topics (22)
Workshops – Cutsets, Quant., and CCF

Friday – AM
Questions/Review
Exam

Course Objectives

- Build PRA modeling and analysis skills
  - Event tree and fault tree model development
  - Dependent failures and common cause modeling
  - Component failure mechanisms
- Improve understanding of quantification process
- Improve ability to extract key results from a PRA
- Greater familiarity with PRA goals and process
- Aleatory (stochastic) versus Epistemic (state of knowledge) uncertainty

Required Background

- Elementary probability theory
- Probability distribution functions
- Fault Tree basics
- Cut sets
- Event trees
- Boolean Algebra

References

1. U.S. Nuclear Regulatory Commission, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), 1975.

2. S. Kaplan and B.J. Garrick, "On the Quantitative Definition of Risk," Risk Analysis, 1, 11-27(1981).

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

4. U.S. Nuclear Regulatory Commission, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, 1990.

5. American Nuclear Society and the Institute of Electrical and Electronics Engineers, PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, 1983.

6. U.S. Nuclear Regulatory Commission, Fault Tree Handbook, NUREG-0492, 1981.

References (cont.)

7. International Atomic Energy Agency, Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessment, IAEA-TECDOC-543, 1990.

8. G. Apostolakis and S. Kaplan, "Pitfalls in Risk Calculations," Reliability Engineering, 2, 135-145 (1981).

9. C. L. Atwood, et al., Handbook of Parameter Estimation for Probabilistic Risk Assessment, NUREG/CR-6823, 2003.

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

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

12. D. Sanzo, et al., Survey and Evaluation of Aging Risk Assessment Methods and Applications, NUREG/CR-6157, 1994.

References (cont.)

13. N. Siu, "Risk Assessment for Dynamic Systems: An Overview," Reliability Engineering and System Safety, 43, 43-73(1994).

14. A. Mosleh, D. Rasmuson, and F. Marshall, Guidelines on Modeling Common-Cause Failures in PRA, NUREG/CR-5485, 1998.

15. F. Marshall, D. Rasmuson, and A. Mosleh, Common Cause Failures Parameter Estimations, NUREG/CR-5497, 1998.

16. ASME/ANS RA-Sa-2009, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," Addendum A to RA-S-2008, ASME, New York, NY, American Nuclear Society, La Grange Park, Illinois, February 2009.

17. ANS, External-Events PRA Methodology, ANSI/ANS-58.21-2007, March 1, 2007.

Acronyms

A	Availability		IE	Initiating Event
AFW	Auxiliary Feedwater		λ	Failure rate
AOV	Air Operated Valve		LCO	Limiting Condition of Operation
APB	Accident Progression Bins		LOCA	Loss of Coolant Accident
APET	Accident Progression Event Tree		LOP	Loss of Power
AUTO	Automatic reactor trip		LOSP	Loss of Off-Site Power
BC	Boundary Conditions		LPI	Low Pressure Injection
CCF	Common Cause Failures		LPR	Low Pressure Recirculation
CCW	Component Cooling Water		LT	Long Term
CV	Check Valve		MACCS	MELCOR Accident Consequence Code System
DG	Diesel Generator		MAN	Manual reactor trip
ECCS	Emergency Core Cooling System		MDP	Motor Driven Pump
ECI	Emergency Coolant Injection		MOV	Motor Operated Valve
ECR	Emergency Coolant Recirculation		NPP	Nuclear Power Plant
EDG	Emergency Diesel Generator		P	Probability
ET	Event Tree		P&ID	Piping and Instrumentation Diagram
F	Unreliability		PCS	Power Conversion System
FT	Fault Tree		PDF	Probability Density Function
FTR	Fail To Run		PDS	Plant Damage State
FTS	Fail To Start		PL&G	Pickard, Lowe and Garrick
HE	Human Error		PORV	Power-Operated Relief Valve
HPSI	High Pressure Injection System		PRA	Probabilistic Risk Assessment
HRA	Human Reliability Analysis		PSA	Probabilistic Safety Analysis

Acronyms (cont.)

Q	Probability (of failure)
R	Reliability
Rx	Reactor
SIS	Safety Injection Signal
SLOCA	Small break LOCA
SPAR	Standardized Plant Analysis Risk Model
ST	Short Term
SWS	Service Water System
T&M	Testing and Maintenance
t	time
Tr	Train
Trans	Transient initiating event

System Modeling Techniques for PRA

Lecture 1 - PRA Basics

INL
Idaho National
Laboratory

Objective

- Review of basic concepts of PRA
- Review basic structure of a PRA

- Section Outline
  - Risk
  - System models for PRA
  - Probability vs. Frequency
  - Reliability vs. Availability
  - PRA structure for nuclear power plants
  - Elements of Level 1 PRA

Some Common Terms

- Conservative versus Non-Conservative
- Cutsets
  - Minimal and Non-Minimal
- Core Damage and Large Early Release
- PRA and PSA
- Accident Sequence versus Accident Scenario
- Complimented Events

Definition of Risk

- Formal (vector) definition used in NPP PRA (risk triplet):
  - Risk = {$scenario_i$, $probability_i$, $consequences_i$}
    - Multiple scenarios contribute to risk
    - Consequence can be a vector
      - e.g., different health effects (early fatalities, latent cancers, etc.)
- Commonly used scalar form:
  - Risk =   probability x consequences   (CDP)
    or
          =   frequency x consequences   (CDF)
- Note that the *consequence* can be just about anything, even just "core damage"
  - Therefore, *core damage frequency* is a risk metric

"Scenario" Defined in Terms of Cut Sets

- A *cut set* is a combination of events that cause the "top event" to occur
  - Top Event = Core Damage (consequence)
- Minimal cut set is the smallest combination of events that causes to top event to occur
- 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

Probability of Frequency Formalism

- Aleatory Uncertainty
  - Also known as stochastic and random uncertainty
  - Irreducible, given model of world
  - Characterized by (assumed) model parameters
- Epistemic Uncertainty
  - Also known as state-of-knowledge uncertainty
  - Reduces as data accumulates
  - Quantified by probability distributions
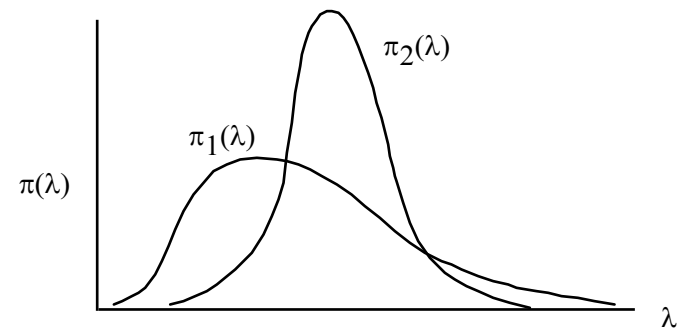
Common PRA Models

- Uncertainty in occurrence time of event - aleatory
  - Binomial
    - P{r failures in N trials |ϕ } = $\dfrac{N!}{r!(N-r)!}\phi^r(1-\phi)^{N-r}$

    - Probability of failure for a single demand
      - P{1 failure in 1 trial | ϕ } = ϕ
  - Poisson
    - P{r failures in (0,T) | λ } = $\dfrac{(\lambda\,T)^r}{r!}\,e^{-\lambda T}$

    - Probability of one or more failures => Exponential
      - P{T_f < t | λ } = $1 - e^{-\lambda t} \approx \lambda t$ (for small λt)
        - Note that P(1 or more failures) = 1 – P(zero failures)
- Uncertainty in rate of occurrence (i.e., on λ and ϕ) - epistemic
  - Lognormal
  - Other (e.g., Gamma, Beta, Maximum Entropy)

Probability and Frequency

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

Probability and Frequency Example

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

Reliability (R)

- Dictionary Definition:
  - Reliability ~ dependability, trustworthiness, repeatability
- Reliability Engineering/PRA Usage:
  - Reliability = Probability a component or system performs its intended function adequately over a given time interval, i.e., for a mission time t

    $R(t) = P\{T_f > t\}$

    where T_f is the time to failure
    - In other words, likelihood that component survives past mission time

Reliability (R)

- Note:
  - Reliability is a formal, quantitative measure
  - Concept does not address repair of component/system
  - Unreliability: $F(t) = 1 - R(t)$

Availability (A)

- Dictionary Definition
  - Availability ~ state of being capable for use in accomplishing a purpose

- Reliability Engineering/PRA Usage
  - Availability = Probability a component or system is able to perform its intended function at a given point in time, i.e.,
  - $A(t) = P\{X(t) = 1\}$
    - where:
      - $X(t) = 1$, component is "good"
      - $X(t) = 0$, component is "failed"

Availability (A)

- Note:
  - Concept allows for repair of component/system
  - Unavailability: $Q(t) = 1 - A(t)$
  - Average unavailability:

$$Q_{ave} = \frac{1}{T} \int_0^T Q(t)dt$$

Common Pitfall

- Confusion of frequency and probability

  - Example: SLOCA and subsequent LOSP

    $\lambda_{\text{SLOCA \& LOSP}} \neq \lambda_{\text{SLOCA}} \times \lambda_{\text{LOSP}}$

    If λ_{SLOCA} = 1E-3/year and λ_{LOSP} = 1E-2/year

    What is: frequency of SLOCA and subsequent LOSP?

Level-1 PRA (Internal Events Analysis)

IE

Plant Systems and Operator Actions (i.e., plant response to IE)

Typically quantified using fault trees or some other detailed system analysis technique

IEs
RxTrip
LOCA
LOSP
SGTR
etc.

P(success)

P(failure)

ok

CD_1

ok

CD_n

$Total\ CDF = \Sigma_{i=1,n}\ CDF_i$

Endstates

15

Principal Steps in PRA

Overview of Level-1/2/3 PRA

IEs

RxTrip

LOCA

LOSP

SGTR

etc.

Level-1
Event
Tree

Bridge Tree
(containment
systems)

Level-2

Containment Event
Tree (APET)

Level-3

Consequence
Analysis

CD

PDS

*APB
(Source
Terms)*

*Consequence
Code
Calculations
(MACCS)*

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

Severe Accident
Progression
Analyses
(Experimental and
Computer Code
Results)

Offsite Consequence
Risk
• Early Fatalities/year
• Latent Cancers/year
• Population Dose/year
• Offsite Cost ($)/year
• etc.

Risk Example - Death Due to Accidents

- Societal Risk = 130,557 Accidental-Deaths/year
- Average Individual Risk
    - = (139,557 Accidental-Deaths/Year)/316,128,180 Est. U.S. Pop.
    - = 4.1E-04 Accidental-Deaths/Person-Year
    - $\approx$ 1/2,421 Accidental-Deaths/Person-Year
- In any given year, approximately 1 out of every 2,421 people in the entire U.S. population will die from an accidental death
    - Note: Figures presented above are based on the National Vital Statistics Reports, Deaths: Preliminary Data for 2013, December 2014, Volume 64, Number 2, at www.cdc.gov which is the Centers for Disease Control and Prevention (CDC) National Center for Health Statistics (NCHS) for the United States.
    - Unintentional injuries is the preferred term to accidental deaths in the public health community.
    - The average individual risk for accidental deaths in the 1980s was approximately 5.0E-04 Deaths/Person-year.

Risk Example - Death Due to Cancer

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

- Average Individual Risk

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

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

    ≈ 1/540 Cancer-Deaths/Person-Year

- In any given year, approximately 1 out of every 540 people in the entire U.S. population will die from cancer

    – Note: Figures presented above are based on the National Vital Statistics Reports, Deaths: Preliminary Data for 2013, December 2014, Volume 64, Number 2, at www.cdc.gov which is the Centers for Disease Control and Prevention (CDC) National Center for Health Statistics (NCHS) for the United States.

    – Malignant neoplasms is the preferred term to cancer deaths in the public health community.

    – The average individual risk for cancer deaths in the 1980s was approximately 2.0E-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

- Metrics for new reactors (SRM on SECY-90-016, 6/26/90)
  - CDF < 1E-4/year
  - Large release frequency (LRF) < 1E-6/year
  - Conditional containment failure probability (CCFP) < 0.1

System Modeling Techniques for PRA

Lecture 2 - Fault Trees

INL
Idaho National Laboratory

Objectives

- Review of fault tree basics
- Develop understanding of:
    - When to use fault trees
    - Construction techniques
    - How to solve fault trees
    - How to quantify fault trees

Outline

- Boolean Algebra
- Basic Elements of a Fault Tree
- When to use a Fault Tree Model
- Cut sets
- Fault Tree construction
- Cut set generation

Basic Probability Concepts Used in PRAs

Venn Diagrams

$A \cup B$
A or B
A + B

$A \cap B$
A and B
A * B

$A \cup B$
A or B
A + B
when the events are mutually exclusive
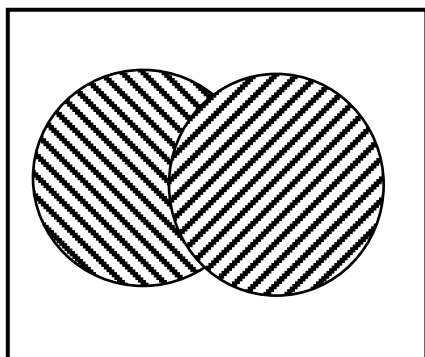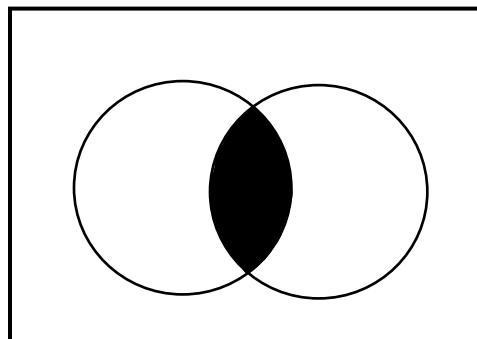
$A \cap /B$
A and /B
A * /B
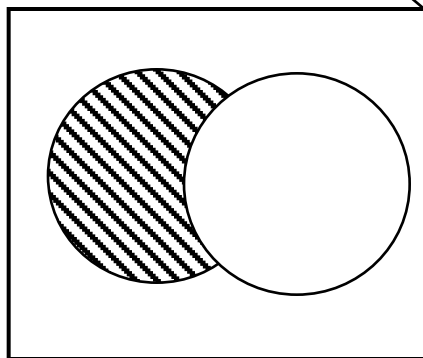
Complemented Event (B does not fail)

4
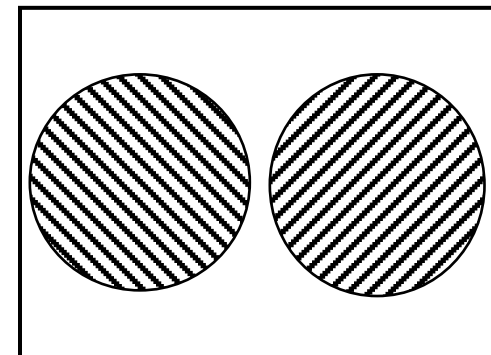
Manipulating Probabilities

- Rules for the OR Operation
    - In general, if A, B are not disjoint (*not mutually exclusive*)
        - Pr(A or B) = Pr(A) + Pr(B) - Pr(A AND B)
        - Can extend to three or more events
    - If A, B are disjoint (*mutually exclusive*)
        - Pr(A or B) = Pr(A) + Pr(B)
        - Example:
          with a die, Pr(1 or 2) = Pr(1) + Pr(2)
          because outcomes are disjoint
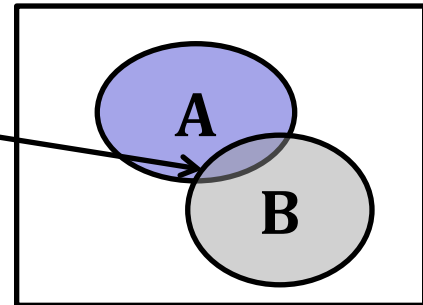
- Rules for the AND operation
    - If A, B are independent
        - Pr(A AND B) = Pr(A) • Pr(B) (definition)
    - If A, B are not independent (i.e., dependent)
        - Pr(A AND B) = Pr(A) • Pr(B|A)
                        = Pr(B) • Pr(A|B)
            - Pr(B|A) read as "probability of B occurring, given that A occurs,"
              or more simply, "probability of B, given A"
            - The "|" is statistical shorthand for "given that"
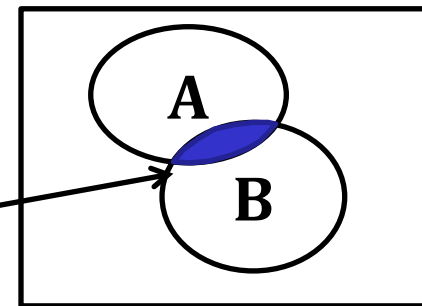
Basic Probability Concepts

- Independent:
  - Means that the occurrence (or non-occurrence) of an event (such as A) has no influence on the subsequent occurrence (or non-occurrence) of another event (such as B) and vice versa
  - If a fair coin is tossed randomly, the occurrence of Heads on the first toss should not influence the probability of Tails on the second toss.
  - This property allows us to write:
    - If A and B are two independent events, then Pr(A and B) = Pr(A) * Pr(B).
    - Example: Pr(H and T | two tosses) = Pr(H) * Pr(T)

- Mutually Exclusive:
  - Means that events (such as A and B) cannot both happen on a single trial of an experiment
  - With the toss of a fair coin, either a Head or a Tail is the expected outcome, cannot possibly get both a Head and a Tail as an outcome on a single toss
  - This property allows us to write:
    - If A and B are two mutually exclusive events, the Pr(A or B) = Pr(A) + Pr(B)
    - If Mutually Exclusive, Pr(A and B) = Pr(A)*Pr(B|A) = Pr(B)*Pr(A|B) = 0
    - Example: Pr(H or T | one toss) = Pr(H) + Pr(T) ∴ Pr(H and T | one toss) = 0

Basic Probability Concepts

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

- Complement (or "not")
  - Means the probability is "1 -" the probability of event
    - $\Pr(\text{not } A) = 1 - \Pr(A)$

- Conditional probability definition
  - In general $= \Pr(A \text{ AND } B) = \Pr(A) \bullet \Pr(B \mid A)$
  - The conditional probability is last term, $\Pr(B \mid A)$, so
    - $\Pr(B \mid A) = \Pr(A \text{ AND } B) / \Pr(A),\ \Pr(A) \neq 0$
    - $\Pr(A \mid B) = \Pr(A \text{ AND } B) / \Pr(B),\ \Pr(B) \neq 0$

7

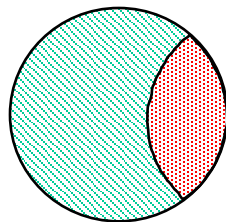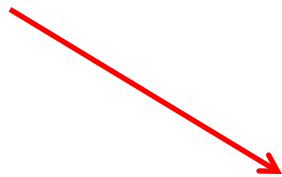# *Simple FT logic illustration*

- Two components in parallel (redundant)
  - Both need to fail to fail the system
  - P(system failure) = P(A) * P(B)

- Two components in series
  - Any one failure, fails the system
  - P(system failure) = P(A) + P(B)
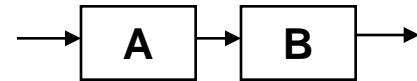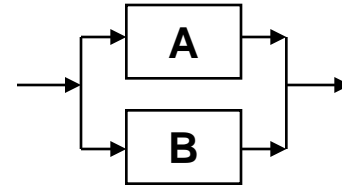
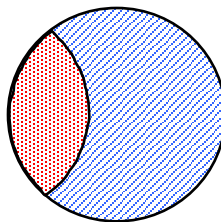# *Summing Probabilities*

- Need to account for the "double-counting of the overlap of the two events

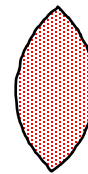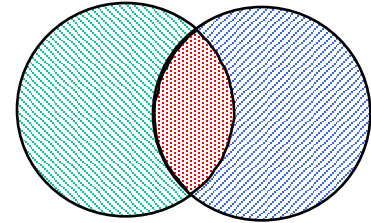- $P(A+B) = P(A) + P(B) - P(AB)$

A B

A + B - AB

- Extends to higher order number of events as well.

Rules of Boolean Algebra

Mathematical Symbolism	*Engineering Symbolism*	*Designation*

(1a) $X \cap Y = Y \cap X$ $X * Y = Y * X$ *Commutative Law*

(1b) $X \cup Y = Y \cup X$ $X + Y = Y + X$

(2a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ $X * (Y * Z) = (X * Y) * Z$ *Associative Law*

$X(YZ) = (XY)Z$

(2b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$ $X + (Y + Z) = (X + Y) + Z$

(3a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ $X * (Y + Z) = (X * Y) + (X * Z)$ *Distributive Law*

$X(Y+Z) = XY + XZ$

(3b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ $X + (Y * Z) = (X + Y) * (X + Z)$

Algebra

(4a) $X \cap X = X$ **Important!** $X * X = X$ *Idempotent Law*

(4b) $X \cup X = X$ $X + X = X$

(5a) $X \cap (X \cup Y) = X$ **Important!** $X * (X + Y) = X$ *Law of Absorption*

(5b) $X \cup (X \cap Y) = X$ $X + X * Y = X$

Important During Cut Set Generation

(6a) $X \cap X' = \Phi = 0$ $X * /X = \Phi = 0$ *Complementation*

(6b) $X \cup X' = \Omega = I$ $X + /X = \Omega = I$

(6c) $(X')' = X$ $/(/X) = X$

(7a) $(X \cap Y)' = X' \cup Y'$ $/(X * Y) = /X + /Y$ *DeMorgan's Theorem*

(7b) $(X \cup Y)' = X' \cap Y'$ $/(X + Y) = /X * /Y$

Boolean Algebra Exercises

Simplify:
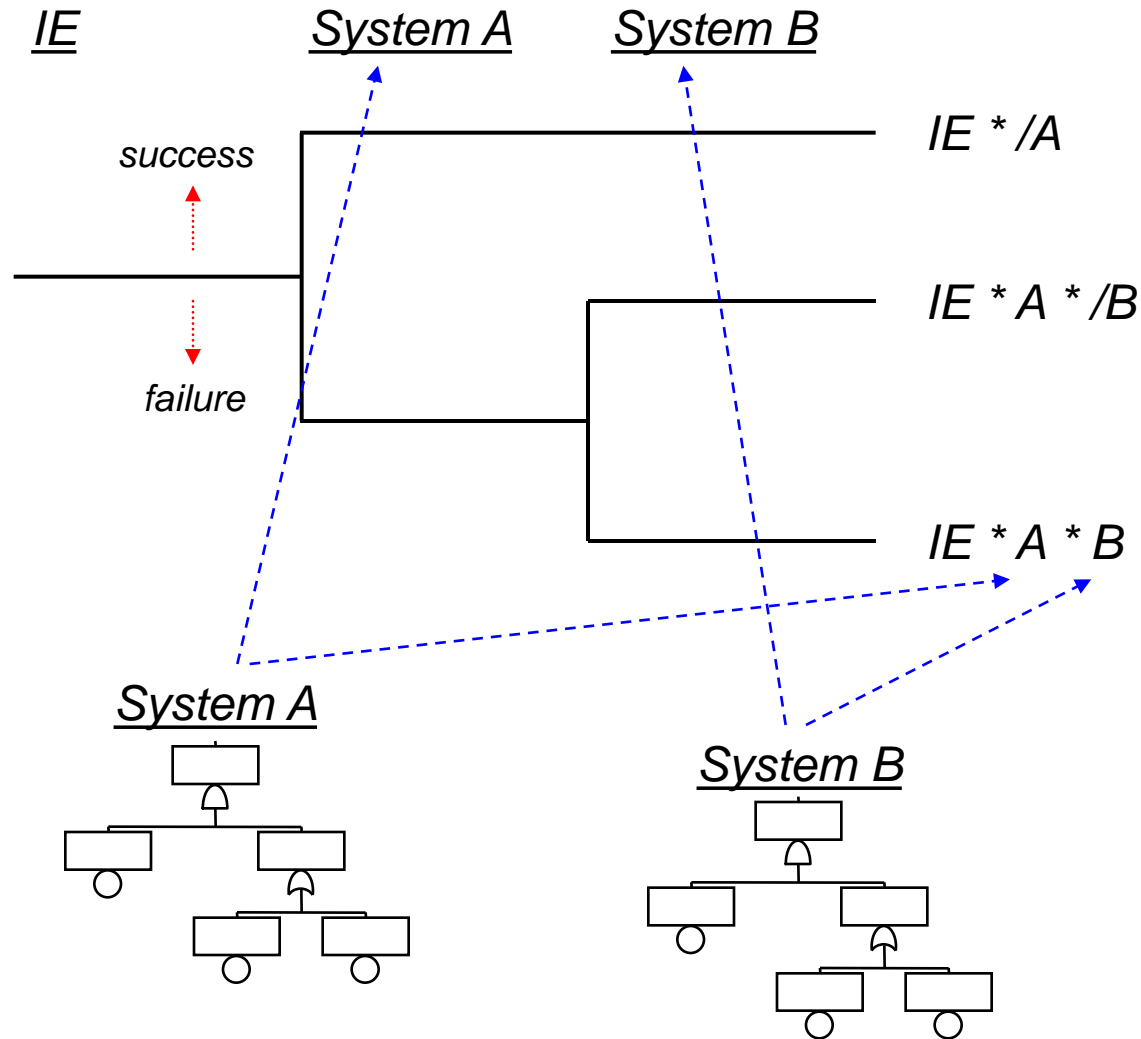
T1 = (A + B) * (B + C).
T2 = (D + E) * (/D + E).

Fault Trees and Event Trees

- Basic modeling tools in PRA
- Event Tree used for "high-level" sequence of events
    - Typically (but not necessarily) chronological
- Most high-level events on ET modeled in detail using fault trees
    - Fault trees often referred to as "system" models

12

FT & ET in PRA

Method Selection

- Consider *event trees* when:
  - Interested in *consequences* of an initiating event
    - Inductive reasoning
  - Multiple barriers, sequential challenges
  - Multiple outcomes of interest
  - Process-oriented users

- Consider *fault trees* when:
  - Interested in *causes* of an event
    - Deductive reasoning
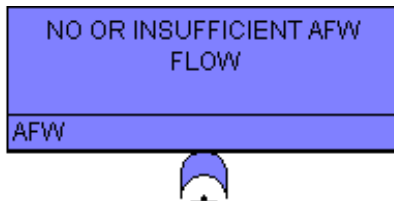 - Single top event of interest

Method Selection (cont.)

- Consider other methods (e.g., analytical methods, Markov models, dynamic event trees, direct simulation) when:
    - Time dependence is important
    - Process dynamics strongly affect sequence development and likelihood
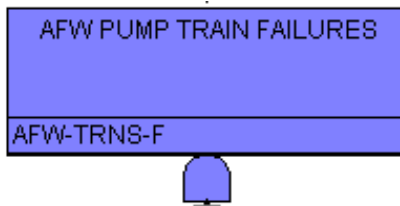
Basic Fault Tree Symbols

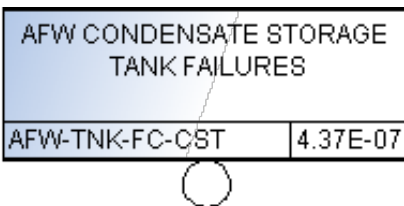| Symbol		Description
NO OR INSUFFICIENT AFW FLOW — AFW	"OR" Gate	Logic gate that implies any of the inputs is sufficient to produce an output (i.e., propagate up through the gate). The probability of an output from this gate is the sum of the probabilities of all the inputs to this gate.
AFW PUMP TRAIN FAILURES — AFW-TRNS-F	"AND" Gate	Logic gate that implies all of the inputs must occur for the output to occur. The probability of an output from this gate is the product of the probabilities of all of the inputs to this gate.
AFW CONDENSATE STORAGE TANK FAILURES — AFW-TNK-FC-CST 4.37E-07	Basic Event	Identifies the lowest (most basic) type of event in the fault tree. There is no further development (i.e., fault tree logic) below a basic event beyond assigning the basic event probability (by the analyst).

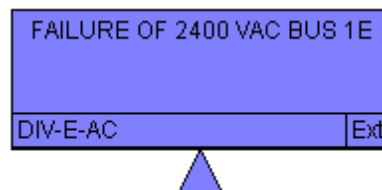16

Basic Fault Tree Symbols (cont.)
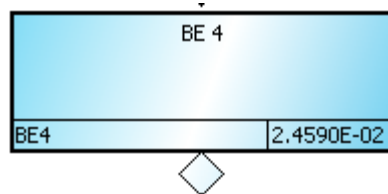
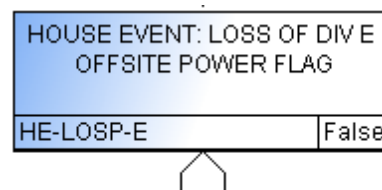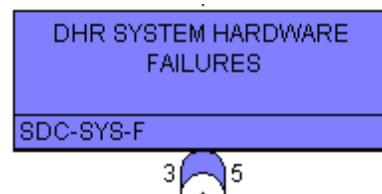| Symbol		Description
BE 4 BE4 — 2.4590E-02	Undeveloped Event	A fault event whose development is limited due to insufficient consequence or lack of additional detailed information. That is, in the PRA it is represented as just a probability, no logic.
FAILURE OF 2400 VAC BUS 1E DIV-E-AC — Ext	Transfer Gate	Symbol used to show there is additional logic under this event, but that logic is developed elsewhere in the PRA. Sometimes used to account for support system dependencies (i.e., the support system fault tree exists in the PRA, but is not explicitly reproduced every time it is needed).
HOUSE EVENT: LOSS OF DIV E OFFSITE POWER FLAG HE-LOSP-E — False	House Event	Logical True (or False) event in the fault tree logic. Note that this is different from just setting an event probability to 1 or zero. Used to model changes in plant system status.
DHR SYSTEM HARDWARE FAILURES SDC-SYS-F	N-of-M	Logic gate providing a representation of the Boolean union of input events. The output will occur if at least N of the M number of inputs occur.

Example Cut Sets - ECI
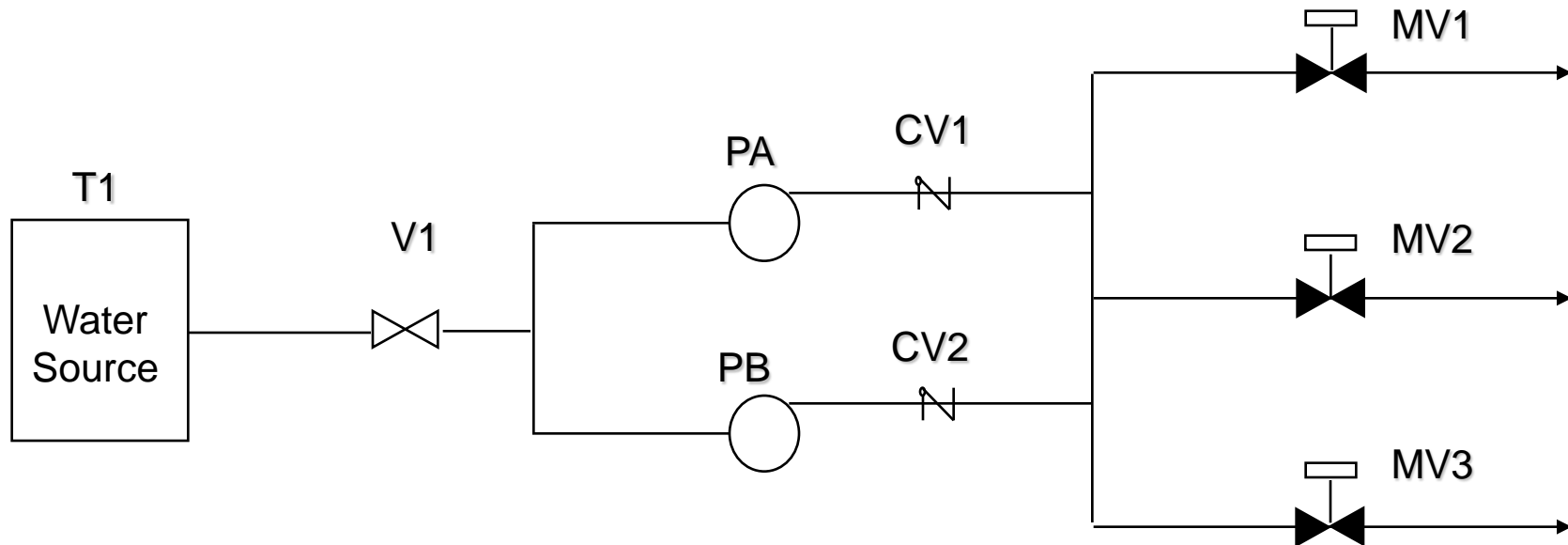
Success Criteria: *Flow from any one pump through any one MV*

T_ tank

*V_ manual valve, normally open*

PS-_ pipe segment

P_ pump

CV_ check valve

MV_ motor-operated valve, normally closed

Two Common Fault Tree Construction Approaches

- "Sink to source"
  - Start with system output (i.e., system sink)
  - Modularize system into a set of pipe segments (i.e., group of components in series)
  - Follow reverse flow-path of system developing fault tree model as the system is traced

- Block diagram-based
  - Modularize system into a set of subsystem blocks
  - Develop high-level fault tree logic based on subsystem block logic (i.e., blocks configured in series or parallel)
  - Expand logic for each block

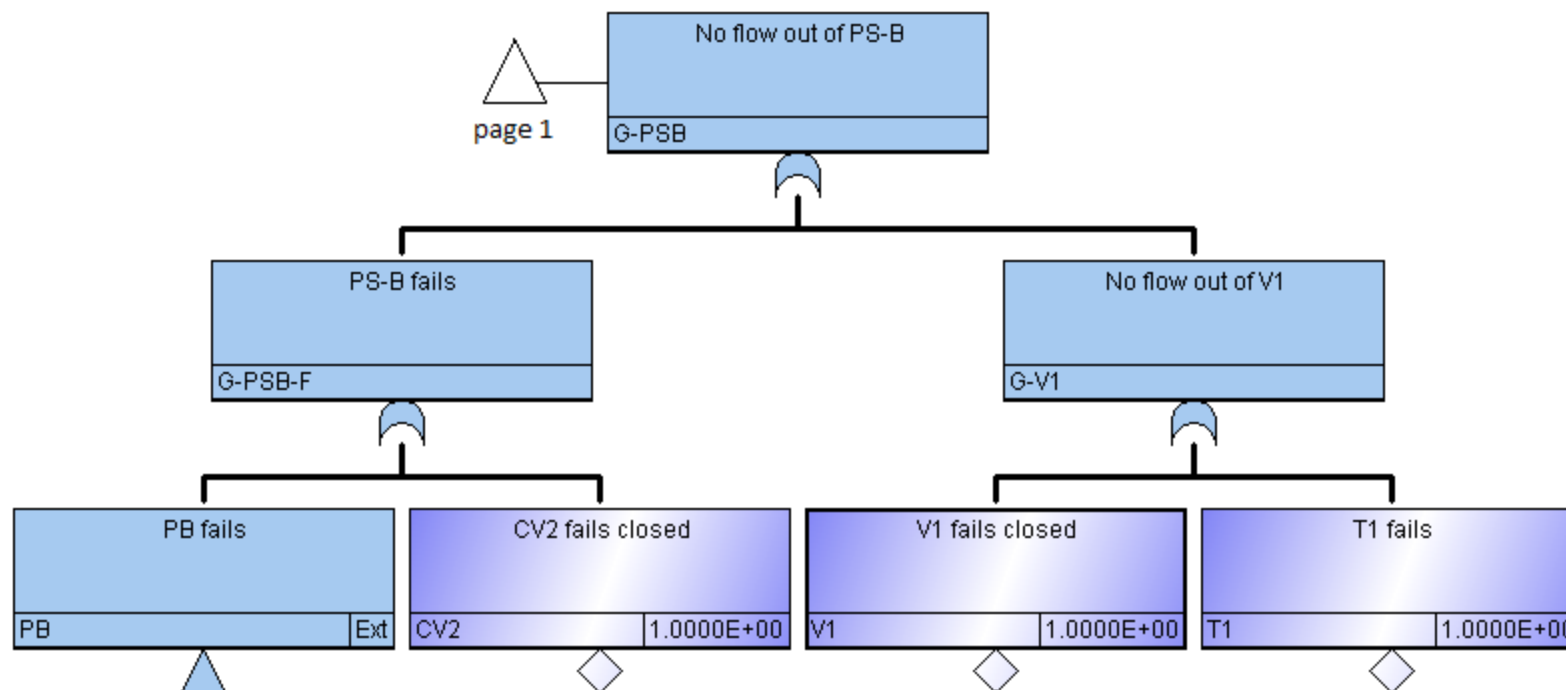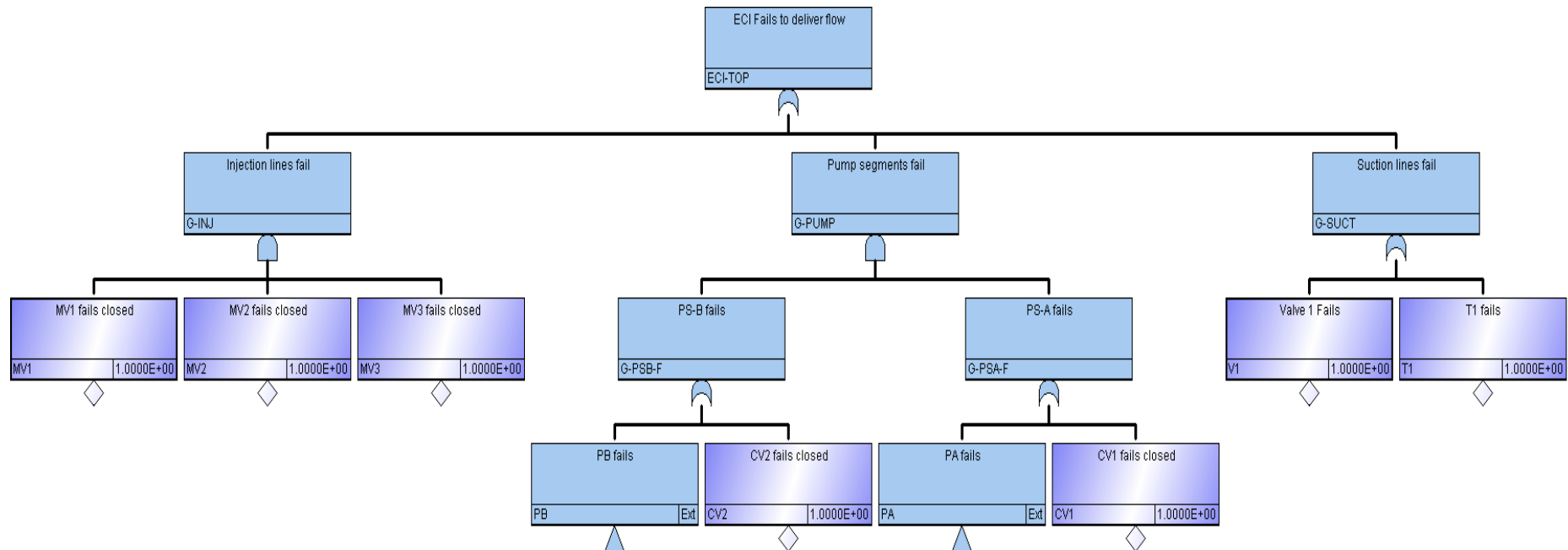# ECI System Fault Tree - Reverse Flow (page 1)
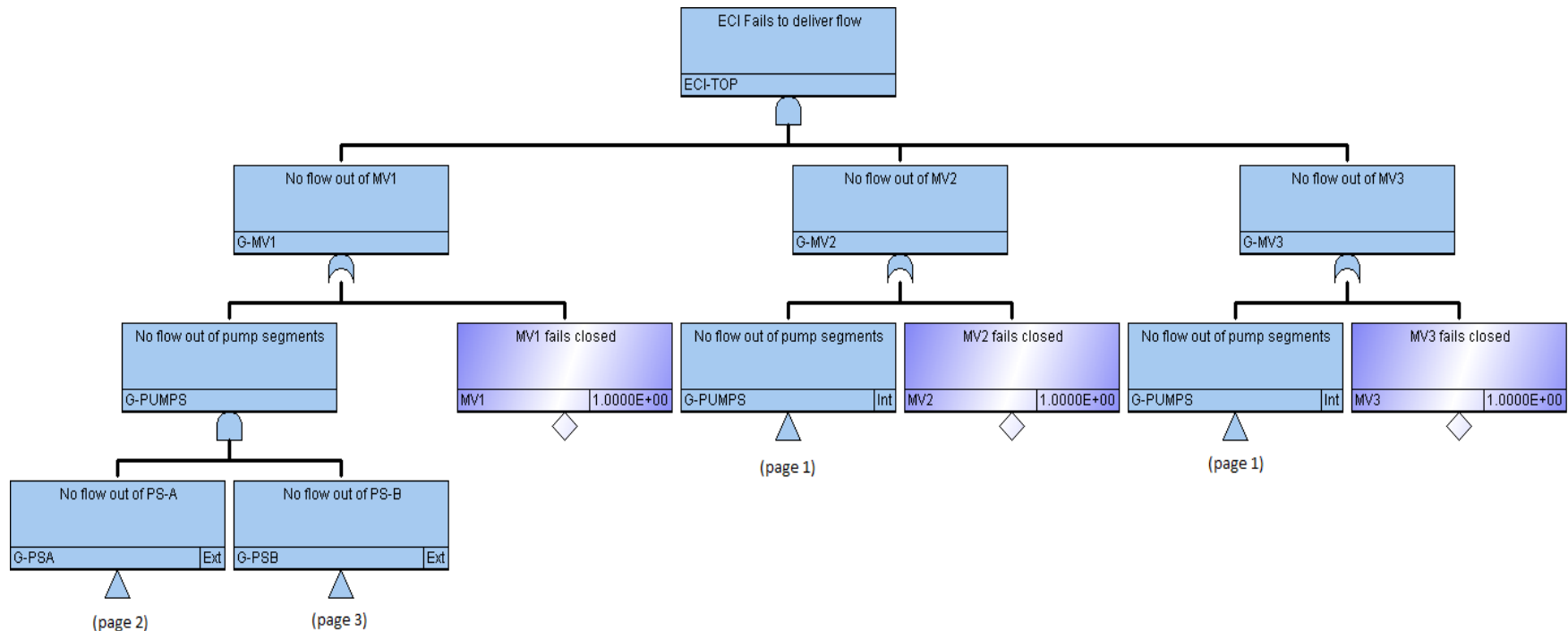
ECI System Fault Tree (page 2)
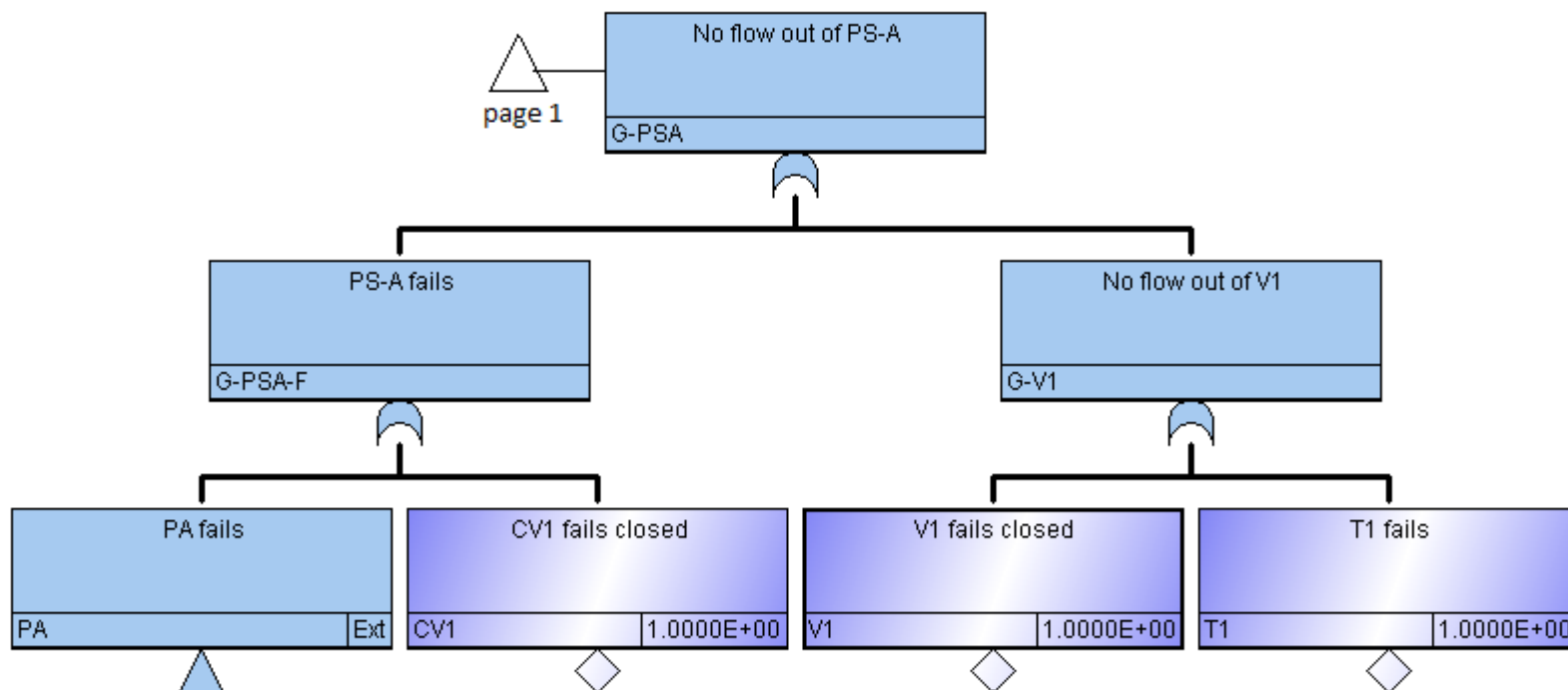
ECI System Fault Tree (page 3)

ECI System Fault Tree (block diagram method)

Cut Sets by Boolean Expansion of Fault Tree

ECI-TOP = G-MV1 * G-MV2 * G-MV3.   *Start substituting*

ECI-TOP = (MV1 + G-PUMPS) * (MV2 + G-PUMPS) * (MV3 + G-PUMPS)   *Keep substituting and performing Boolean algebra*
                                                                 (e.g., X*X = X)

ECI-TOP = (MV1 * MV2 * MV3) +
    (MV1 * MV2 * G-PUMPS) +
    (MV1 * G-PUMPS * MV3) +
    (MV1 * G-PUMPS * G-PUMPS) +
    (G-PUMPS * MV2 * MV3) +
    (G-PUMPS * MV2 * G-PUMPS) +
    (G-PUMPS * G-PUMPS * MV3) +
    (G-PUMPS * G-PUMPS * G-PUMPS).

ECI-TOP = (MV1 * MV2 * MV3) +
    (MV1 * MV2 * G-PUMPS) +
    (MV1 * G-PUMPS * MV3) +
    (MV1 * G-PUMPS) +
    (G-PUMPS * MV2 * MV3) +
    (G-PUMPS * MV2) +
    (G-PUMPS * MV3) +
    (G-PUMPS).

ECI-TOP = (MV1 * MV2 * MV3) +
    (G-PUMPS).

Cut Sets (cont.)

ECI-TOP = (MV1 * MV2 * MV3) +
(G-PSA * G-PSB).

ECI-TOP = (MV1 * MV2 * MV3) +
((G-PSA-F + G-V1) * (G-PSB-F + G-V1)).

ECI-TOP = (MV1 * MV2 * MV3) +
(G-PSA-F * G-PSB-F) +
(G-PSA-F * G-V1) +
(G-V1 * G-PSB-F) +
(G-V1).

ECI-TOP = (MV1 * MV2 * MV3) +
(G-PSA-F * G-PSB-F) +
(G-V1).

ECI-TOP = (MV1 * MV2 * MV3) +
(PA + CV1) * (PB + CV2) +
(V1 + T1).

ECI-TOP = MV1 * MV2 * MV3 +
PA * PB +
PA * CV2 +
CV1 * PB +
CV1 * CV2 +
V1 +
T1.

25

Specific Failure Modes Modeled for Each Component

- Each component associated with a specific set of failure modes/mechanisms determined by:
  - Type of component
    - E.g., Motor-driven pump, air-operated valve
  - Normal/Standby state
    - Normally not running (standby), normally open
  - Failed/Safe state
    - Failed if not running, or success requires valve to stay open

Typical Component Failure Modes

- Active Components
  - Fail to Start
  - Fail to Run
  - Unavailable because of Test or Maintenance
  - Fail to Open/Close/Operate
  - Definitions not always consistent among PRAs
    - e.g., transition from start phase to run phase can be defined differently (load/run)

Typical Component Failure Modes (cont.)

- Passive Components
  - Rupture
  - Plugging (e.g., strainers/orifice)
  - Fail to Remain Open/Closed (e.g., manual valve)
  - Short (cables)
  - Not always modeled in PRAs
    - Implicit assumption
      - P(passive failures) << P(active active)

Example FT for Pump
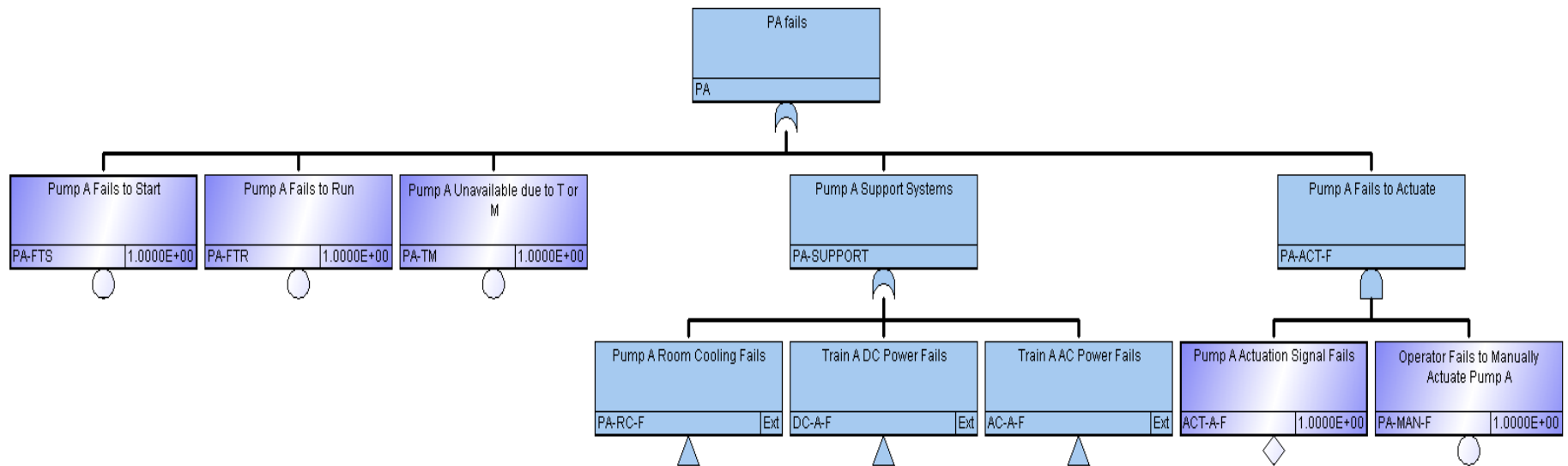
Component Boundaries

- Typically include all items unique to a specific component, e.g.,
    - Drivers for EDGs, MDPs, MOVs, AOVs, etc.
    - Circuit breakers for pump/valve motors
    - Need to be consistent with how data was collected
        - That is, should individual piece parts be modeled explicitly or implicitly
        - For example, actuation circuits (FTS) or room cooling (FTR)

Active Components Require "Support"

- Signal needed to "actuate" component
  - Safety Injection Signal starts pump or opens valve
- Support systems might be required for component to function
  - AC and/or DC power
  - Service water or component water cooling
  - Room cooling

Support System Dependencies

- Can be modeled at system level, train level or component level

- Dependency matrix is frequently used to document identified dependencies

Note: If support system serves more than one component or system, it is modeled separately (see next two slides)

Practice Example HPI Fault Tree

Support System Dependency:

AC power supports both pumps 1 and 2
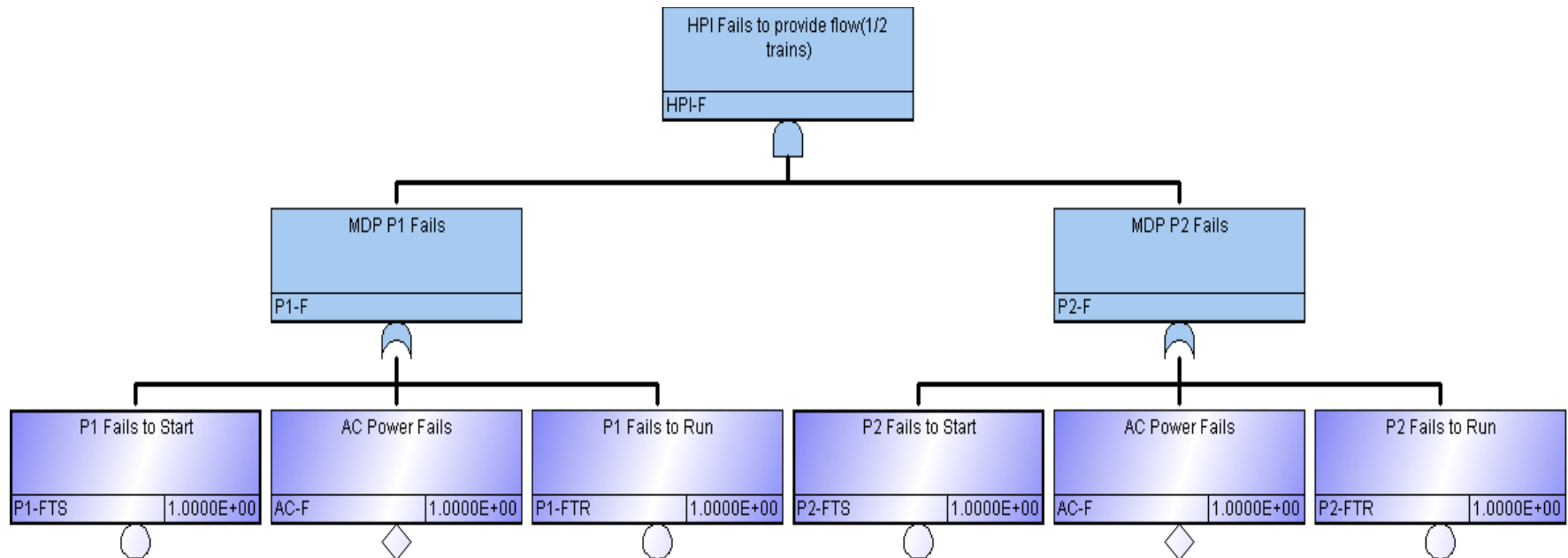
Practice Example
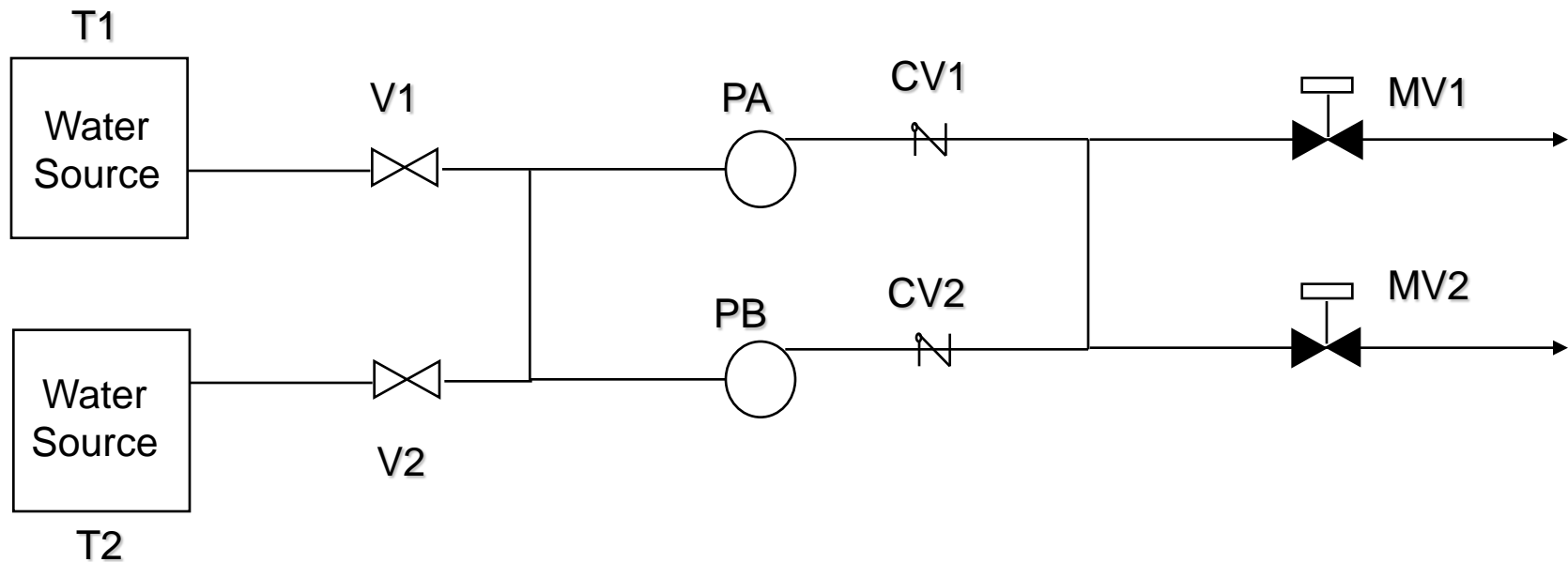
Success Criteria: One pump flow through both MV's

System Modeling Techniques for PRA

Lecture 3 - System Models

INL
Idaho National Laboratory

Objective

- Develop understanding of System Modeling, including:
  - Modeling goals
  - Modeling techniques and variations

Outline

- System Modeling Approach

- Missions

- Success Criteria

- Boundary Conditions

- Parallel/Series System Modeling

- System Level Fault Tree Modeling

- Results

System Modeling Approach

- Focus on individual plant systems

- Issues addressed by logic model
  - How can the system fail?
  - How likely is failure?
  - What are the dominant contributors?

- Key questions for understanding the system
  - What does the system do?
  - What is "failure"?
  - What is the "system"?
  - What are the analysis boundaries?

System Mission Affects Model

- Demand based missions (binomial)
  - Normally in standby
  - Required to perform one (or more) times
  - e.g., actuation systems, relief valves

- Time based missions (Poisson)
  - Either in standby or normally operating
  - Required to operate for some length of time, which affects unreliability
  - e.g., ECCS, SWS

Success Criteria

- Needed to employ binary logic modeling
  - Note that same system may be modeled under different conditions for different initiators
- Developed from physical analyses
- Can be sequence-dependent
- Must consider details of expected mission (e.g., mission time, actuation signals, status of support systems)

Analysis Scope and Boundaries

- Plant Operating Mode

- Hardware
  - power supply/powered system
  - common actuation/actuated system
  - cooling system/cooled system
  - cross-ties

- Failure Modes
  - internal vs. "external"
  - errors of commission

- Mission Time

- Organization

Definition of Problem Must be Specific and Precise

- Sample Success Criteria
  - Improper:
    - HPIS is successful
  - Proper:
    - Uninterrupted flow from 2/3 HPIS pumps for 24 hours
    - Generally defined from thermal-hydraulics calculations

Series System

Schematic — 1 — 2 — ... — N — **(P&ID)**
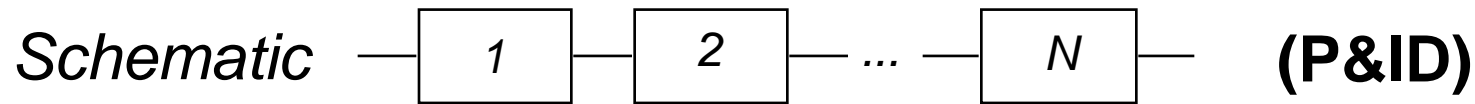
Fault Tree

(OR Gate)
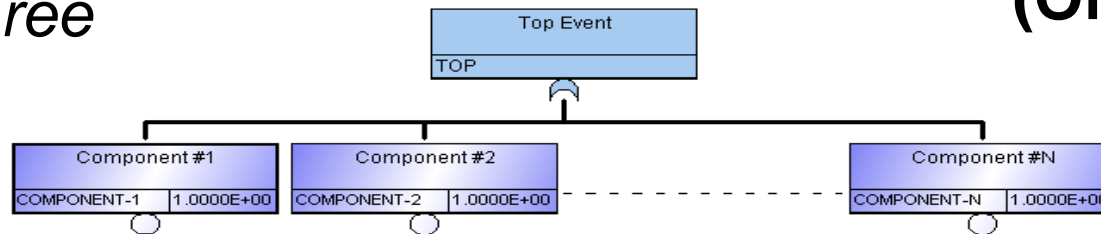
Boolean and Quantification

$$Top = \sum_{i=1}^{N} X_i$$

(Cut Sets)

$$P\{Top\} = 1 - \prod_{i=1}^{N}(1-Q_i) \quad \textit{(if independent)}$$

$$\approx \sum_{i=1}^{N} Q_i \quad \textit{(rare event approximation)}$$

Series System Example
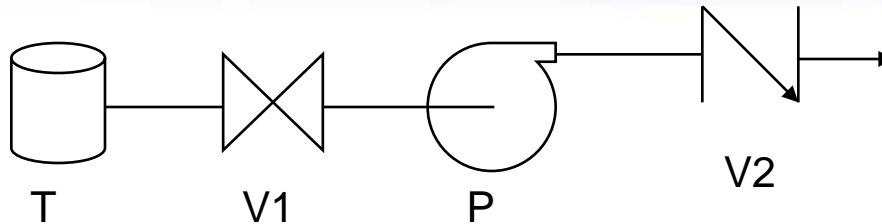
- Any component failure fails the system
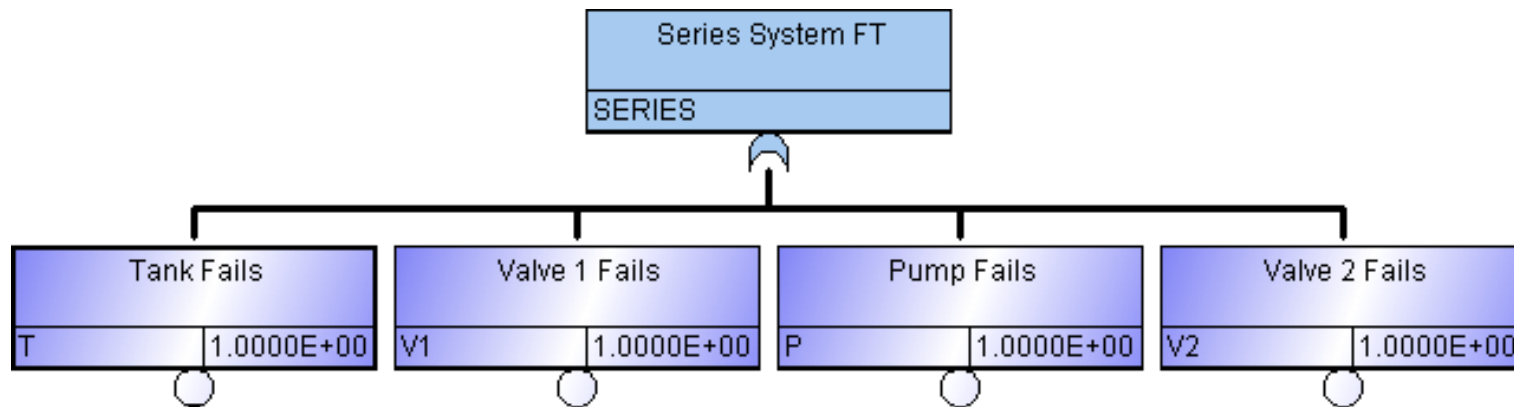
Parallel System

Schematic
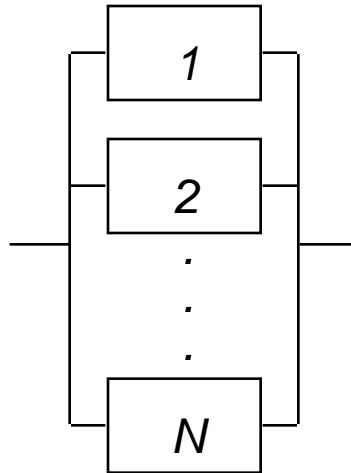
Fault Tree

(AND Gate)

(P&ID)
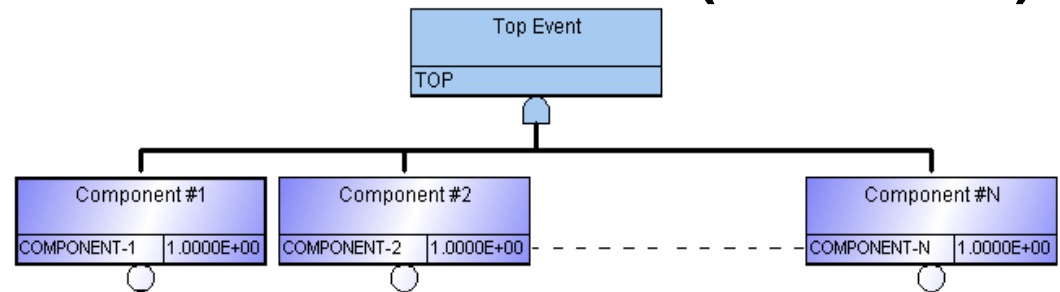
Boolean and Quantification

$$Top = \prod_{i=1}^{N} X_i$$

$$P\{Top\} = \prod_{i=1}^{N} Q_i \quad \text{(if independent)}$$

(Cut Sets)

Parallel System Example
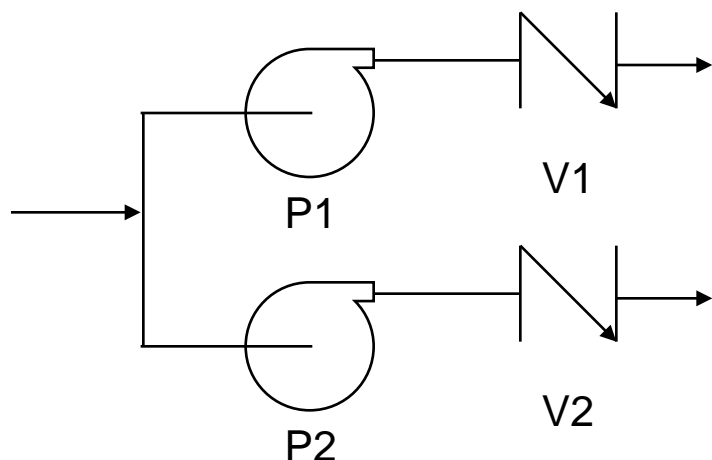
System redundancy requires multiple component failures to fail system

Parallel System Example
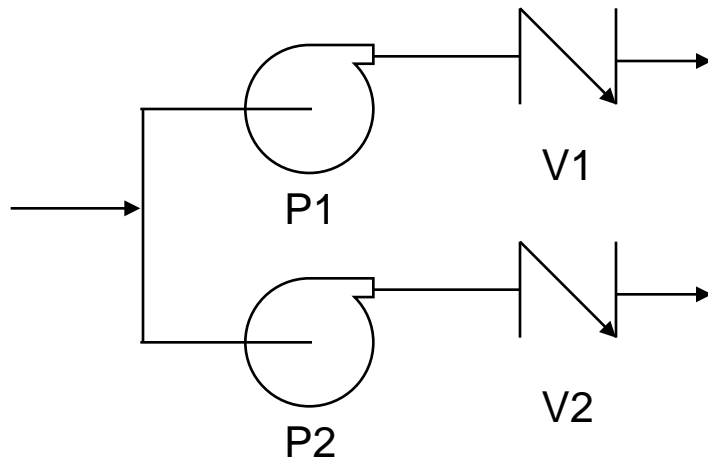
System redundancy requires multiple component failures to fail system

V1

P1

V2

P2

Set basic event P1 to TRUE

Parallel System FT
PARALLEL

Train 1
TR-1

Train 2
TR-2

Pump 1 Fails	
P1	1.0000E+00

Valve 1 Fails	
V1	1.0000E+00

Pump 2 Fails	
P2	1.0000E+00

Valve 2 Fails	
V2	1.0000E+00
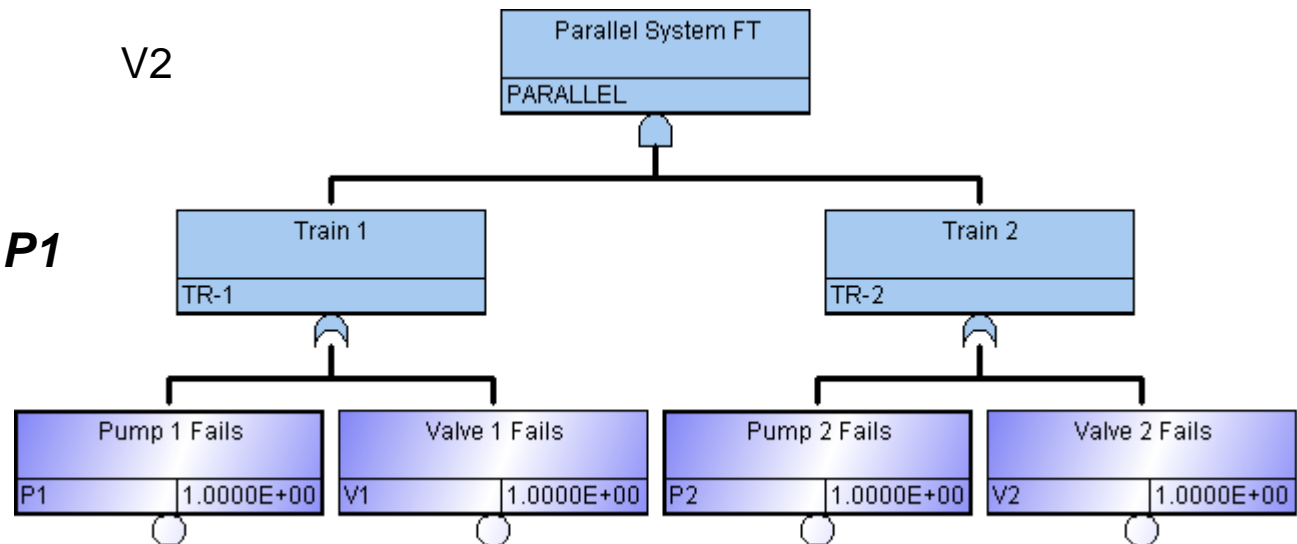
Fault Tree Construction

- Items to consider
  - Dependent Failures
  - Functional Dependencies
    - Support Systems
  - Shared Equipment Dependencies
    - LPR requires same pumps as LPI
  - Test/Maintenance (T&M) Dependencies
    - Single T&M procedure can make multiple components unavailable
  - Common Cause Failures

Fault Tree Construction (cont.)

- Human errors in fault trees
  - HEs lead to additional basic-events/failure-modes
  - Examples: Fail to restore, failure to initiate, improper termination (rarely modeled)
  - HEs in fault trees are local in scope
- Modeling T&M unavailability can result in illogical cut sets
  - Multiple redundant trains are generally not out at same time
  - Using complemented events (e.g., A_{tm} * /B_{tm}) complicates the quantification
- Putting recovery in FT might give overly optimistic results

Fault Tree Pitfalls

- Inconsistent or unclear basic event names
  - $X*X = X$, so if X is called X1 in one place and X2 in another place, incorrect results are obtained

- Missing dependencies or failure mechanisms
  - An issue of completeness

- Unrealistic assumptions
  - Availability of redundant equipment
  - Credit for multiple independent operator actions
  - Violation of plant LCO

- Logic loops
  - Will talk about what they are and how to fix them…

Logic Loops Result From Circular Support Function Dependencies

– ECI pump requires AC power

– AC power supplied from either Offsite Power or Diesel Generators (DGs)

– DGs require Component Cooling Water (CCW) for cooling

– CCW pumps require AC power
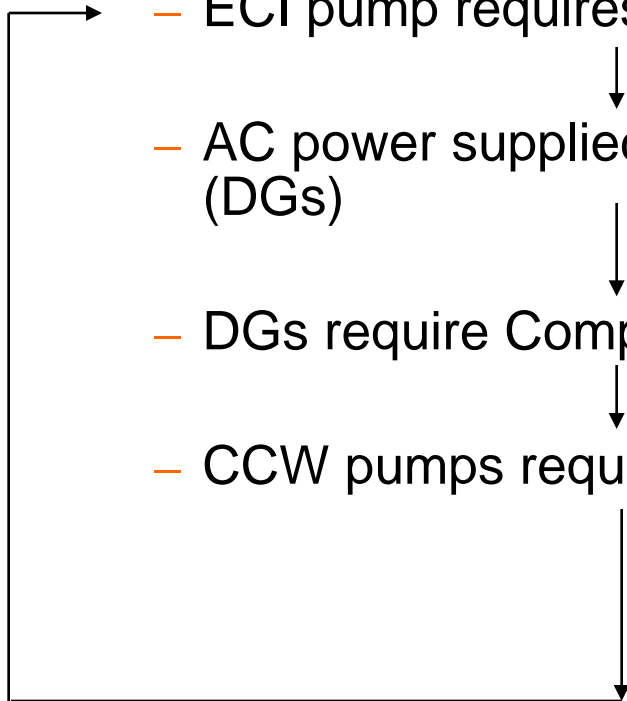
Logic Loops 1
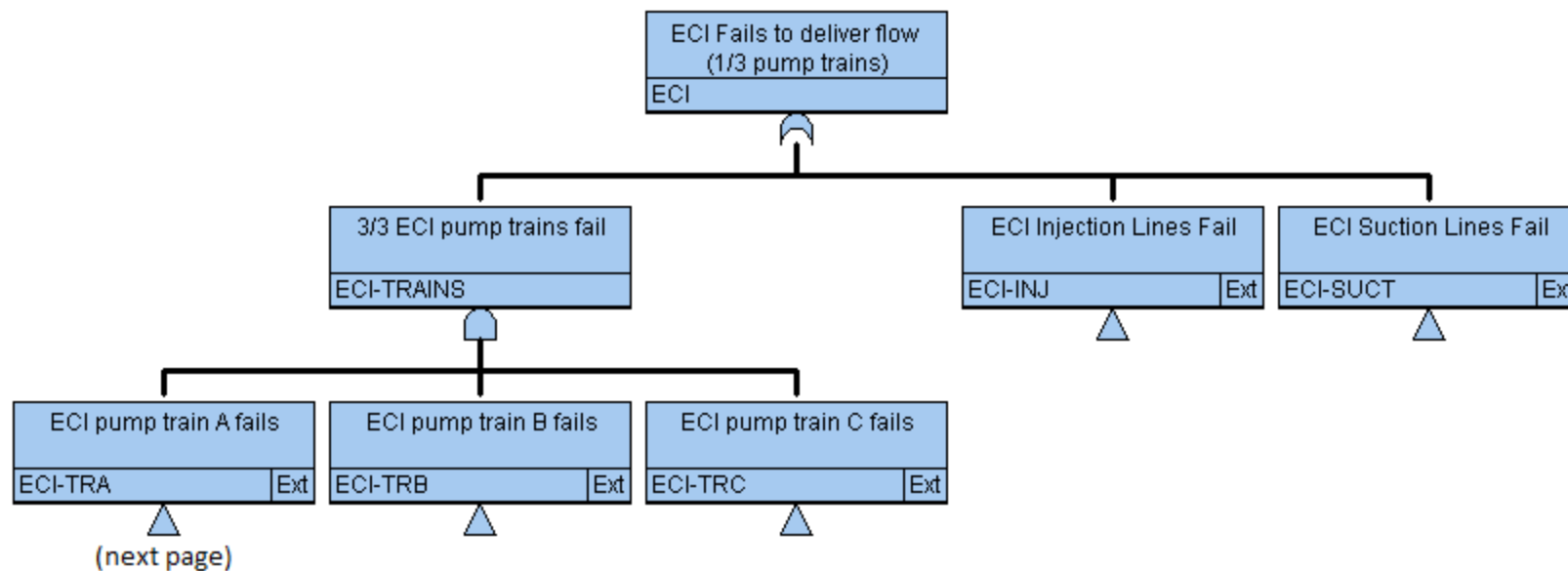
Logic Loops 2
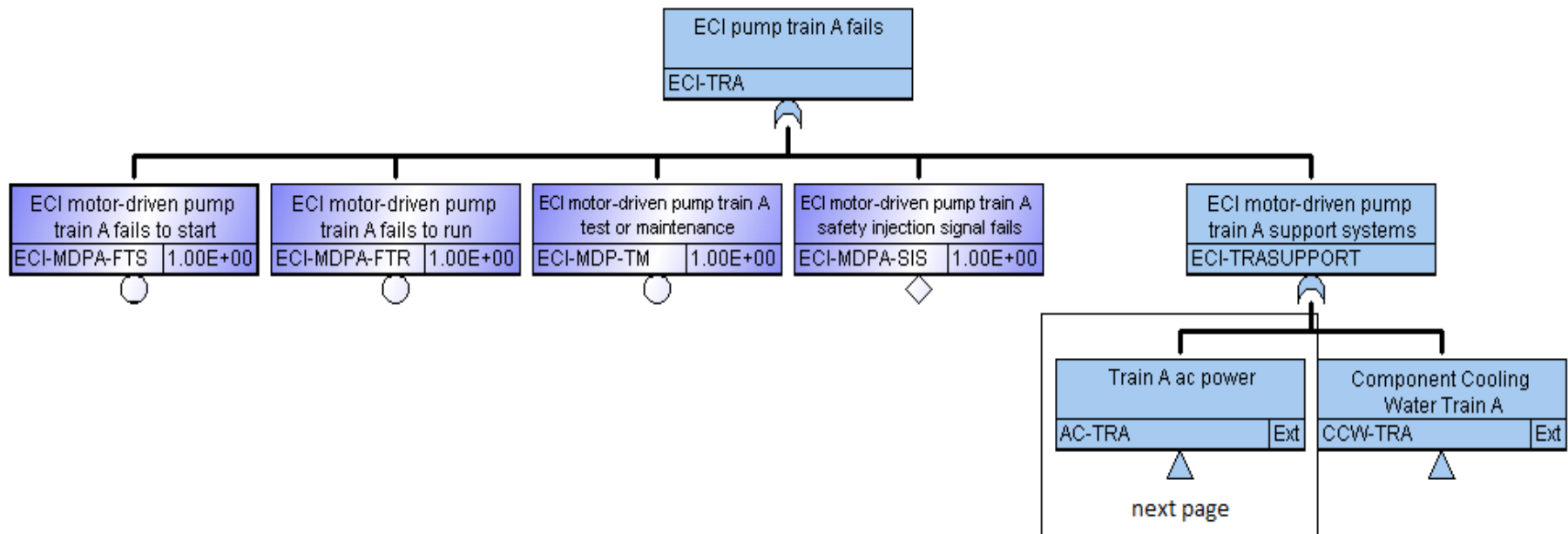
Logic Loops 3
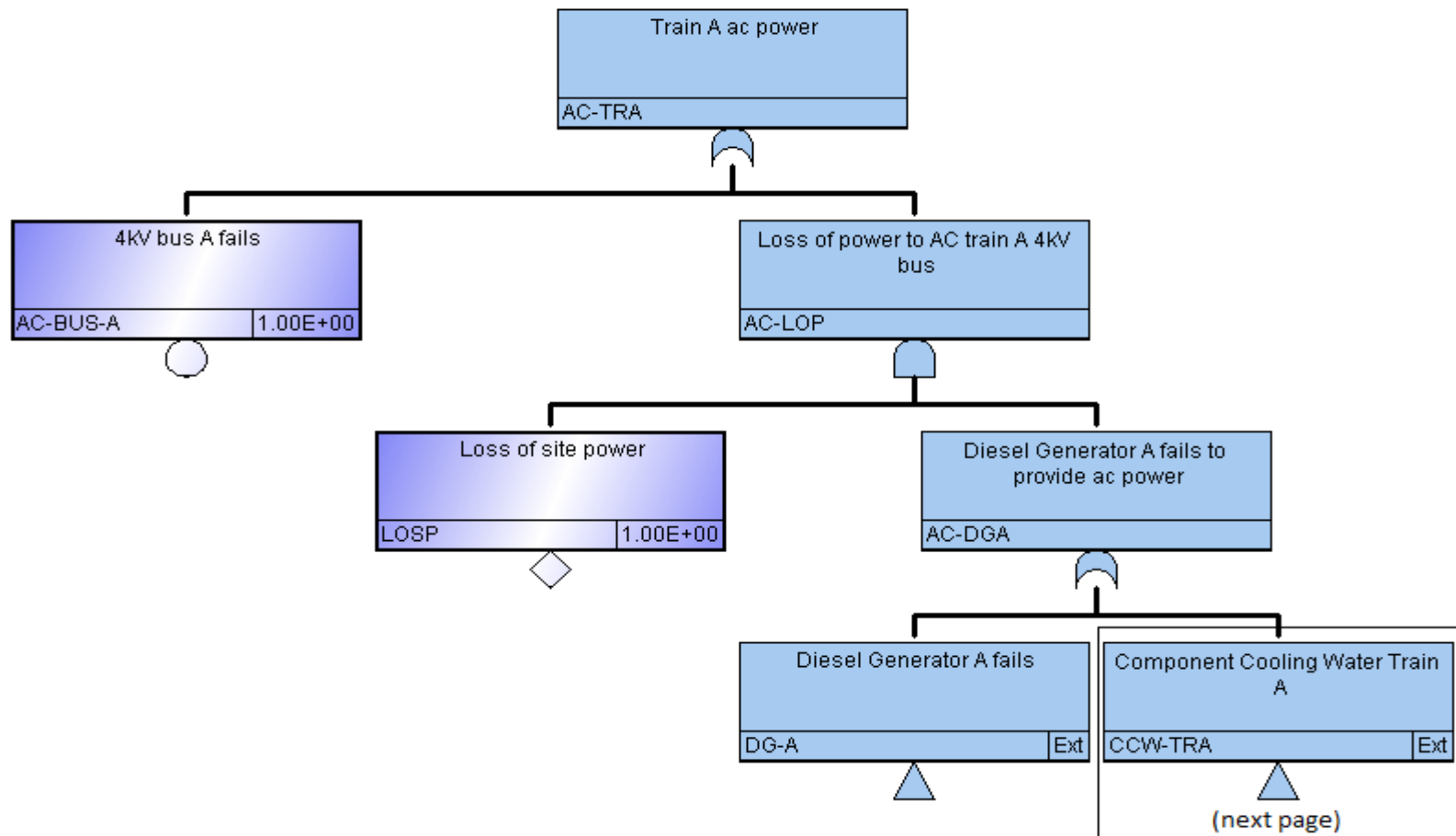
Logic Loops 4
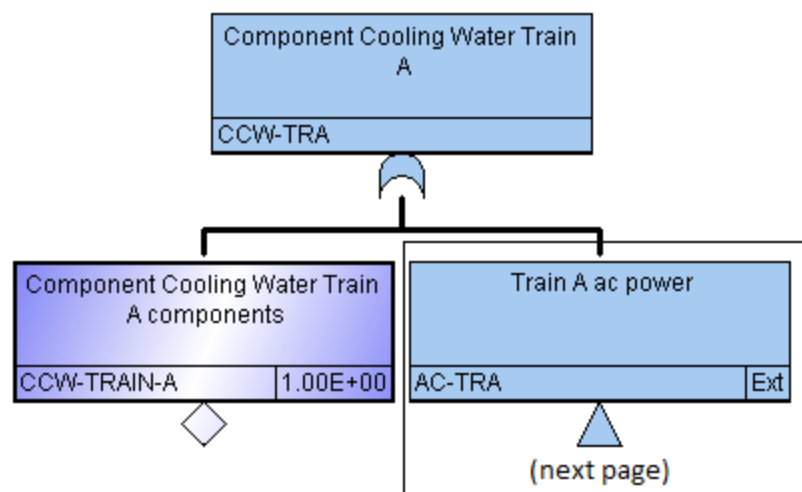
Logic Loops 5

This AC subtree is a new version of *AC Train A fails* (from Logic Loops 3, specific for the CCW tree.
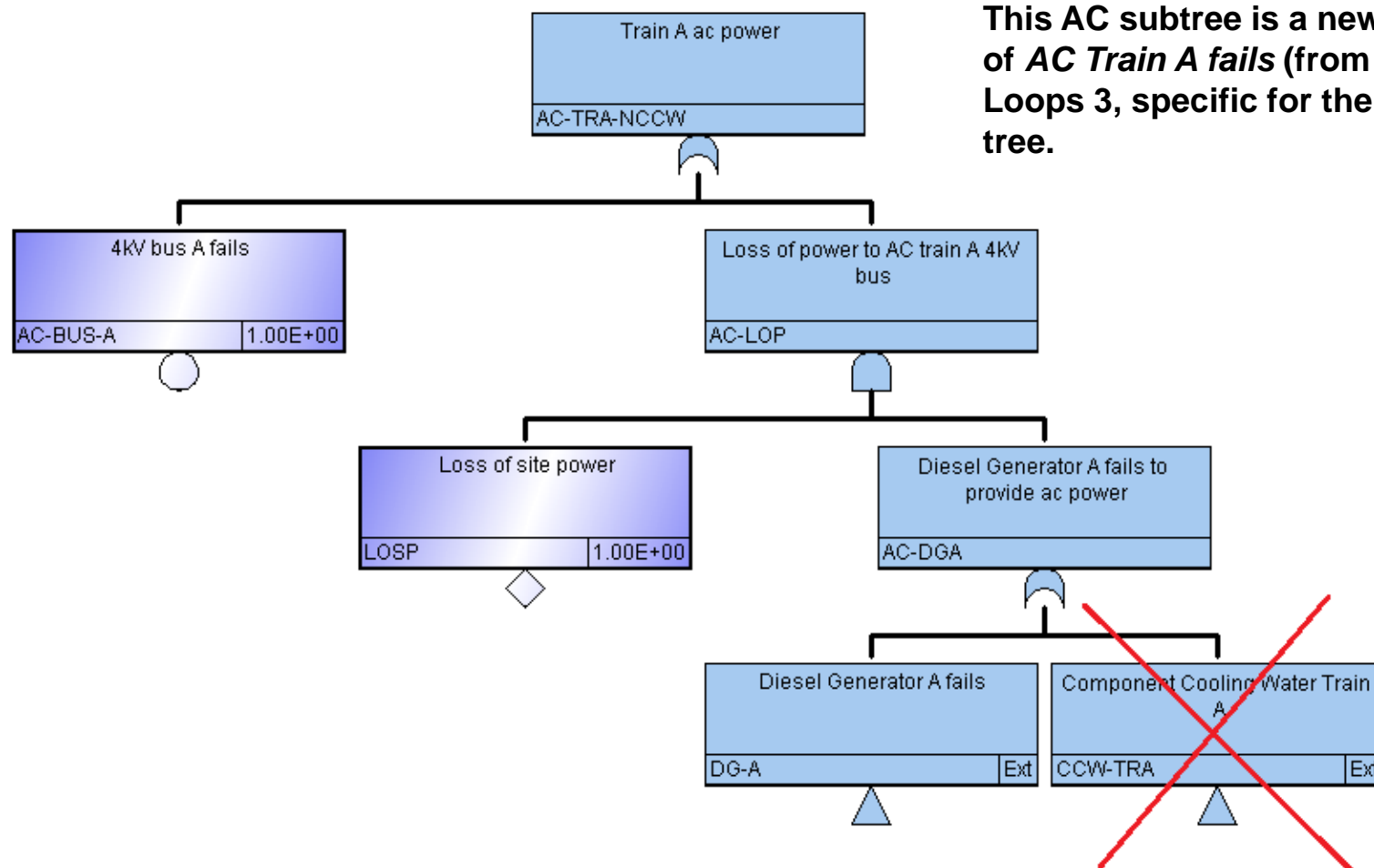
Generate Cut Sets
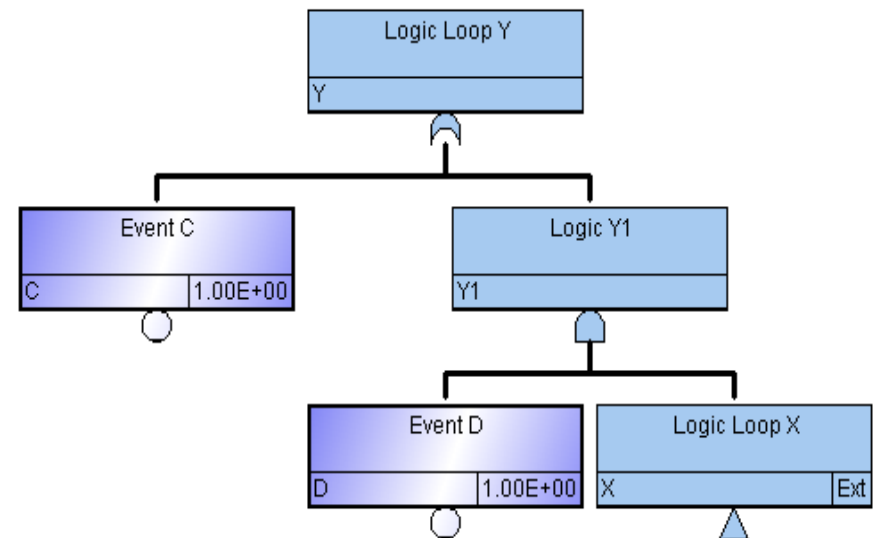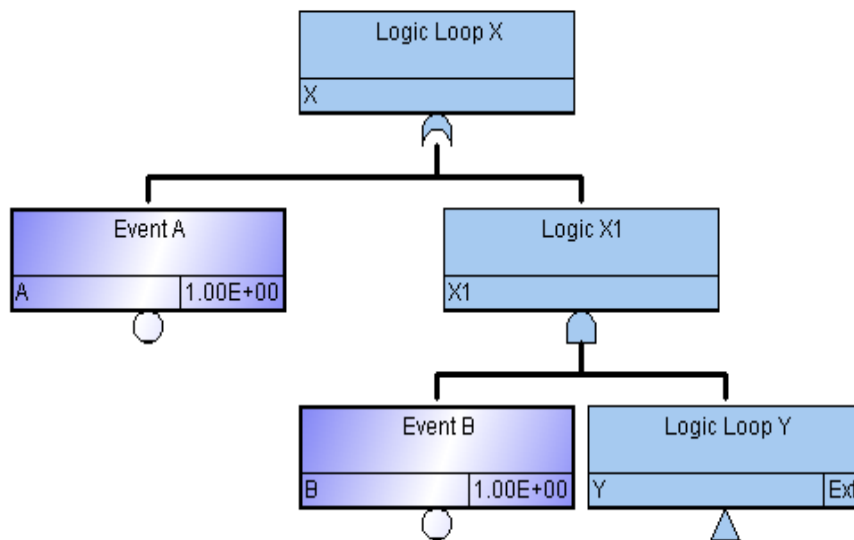
Results

- Sanity checks on cut sets
  - Symmetry
    - If Train-A failures appear, do Train-B failures also appear?
  - Completeness
    - Are all redundant trains/systems really failed?
    - Are failure modes accounted for at component level?
  - Realism
    - Do cut sets make sense (i.e., Train-A out for T&M ANDed with Train-B out for T&M)?
  - Predictive Capability
    - If system model predicts total system failure once in 100 system demands, is plant operating experience consistent with this?

What is Wrong?

System XYZ Pumps Fail =

PumpA-FTS * PumpB-FTS +

PumpA-FTS * PumpB-FTR +

PumpA-FTS * PumpB-TM +

PumpA-FTR * PumpB-FTR +

PumpA-FTR * PumpB-TM +

PumpA-TM * PumpB-FTS +

PumpA-TM * PumpB-FTR +

PumpA-TM * PumpB-TM.

PRA Modeling Mindset

- *All systems can fail*
  - Under what conditions is failure more likely? How likely are these?
  - Are all potentially significant mechanisms identified and treated?

- Catastrophic system failures are rare events
  - May need creative search for failure mechanisms
  - Maximize use of available information, which implies that Bayesian methods to be used

- System failure is a "systems" issue
  - Need to identify and address systems interactions
  - Avoid drawing analysis boundaries too tightly

System Modeling Techniques for PRA

Lecture 4 – Uncertainty

www.inl.gov

INL
Idaho National Laboratory

Objective

- Understand implications of uncertainty associated with PRAs
- Understand different types and sources of uncertainty
- Understand mechanics of how uncertainty is calculated
- Understand why we calculate uncertainty

- Outline
  - Types of uncertainties
  - Uncertainty Measures
  - Propagation of Uncertainties

Stochastic Uncertainties

- Measure of randomness or variability in process
  - e.g., coin flip - sometimes heads, sometimes tails
- Also called random or *aleatory* uncertainty
- Distribution is result of assumptions about a process
  - Failure occur randomly in time (Poisson)
  - Failure occur randomly given a demand (binomial)
- Distribution is a function of parameter values (e.g., failure rate λ), which are uncertain

State-of-Knowledge Uncertainties

- Lack of accuracy in model parameters (i.e., uncertainty in λ's)

- Also called subjective or *epistemic* uncertainty

- Distribution reflects data, relevant model predictions, engineering judgment

- Typically generated using Bayesian methods (covered in Statistics course)

Uncertainties

- Summary Measures
  - Mean:

$$E[\lambda] = \int_0^\infty \lambda \; \pi(\lambda) \; d\lambda \qquad \text{Note: } \int_0^\infty \pi(\lambda) d\lambda = 1$$

  - Variance:

$$E[(\lambda - E[\lambda])^2] = \int_0^\infty (\lambda - E[\lambda])^2 \pi(\lambda) \; d\lambda$$

$$= E[\lambda^2] - (E[\lambda])^2$$

  - αth percentile:

$$\alpha = P\{\lambda \leq \lambda\alpha\} = \int_0^{\lambda_\alpha} \pi(\lambda) \; d\lambda$$

  - 95th percentile:

$$0.95 = \int_0^{\lambda_{0.95}} \pi(\lambda) \; d\lambda$$

Uncertainties

- Probability of Parameter Value
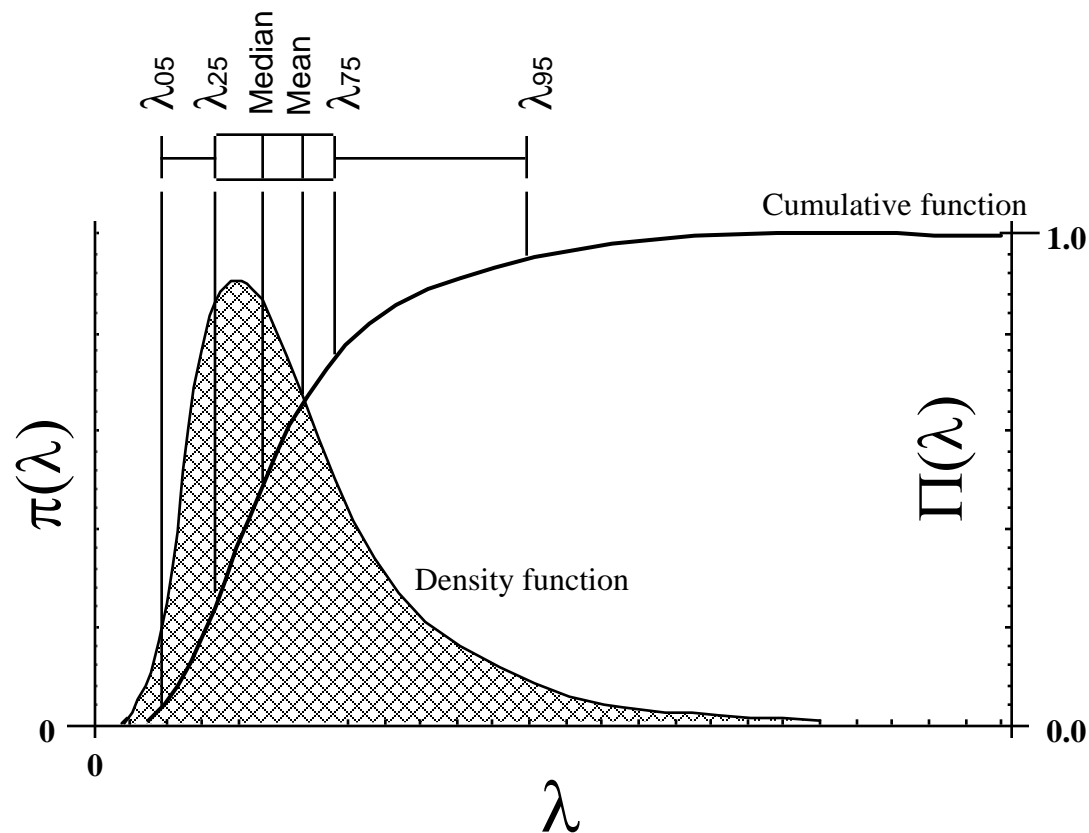
Error Factors (EF)

- Lognormal distribution

- $f(x) = \frac{1}{x\sqrt{2\pi\sigma^2}} e^{-(\ln(x)-\mu)^2/2\sigma^2}$

- for x > 0

- SAPHIRE software (software used for SPAR models development)
  - requires the EF and mean

  - where: $\mu_{ln} = e^{\mu+\frac{\sigma^2}{2}}$ and $EF = e^{1.645\sigma}$

- PRAs use lognormal distributions and 90% coverage for components.

- Depending upon information error factors can be calculated as:
  - $EF = \sqrt{\lambda_{95}/\lambda_{05}}$
  - $EF = median/\lambda_{05}$
  - $EF = \lambda_{95}/median$

Other Distributions (commonly used for data analysis)

- Beta distribution

- $f(x) = \left[\frac{1}{B(a,b)}\right] x^{a-1}(1-x)^{b-1}$

- for $0 \leq x \leq 1$, where B(a,b) is the beta function

- SAPHIRE software (software used for SPAR models development)
  - requires the b parameter and mean
  - a is calculated: a = (μ*b)/(1-μ)
  - where: μ = a/(a+b)

- PRA typically assume beta distribution for demand related components (e.g., fails to start)

Other Distributions (commonly used for data analysis)

- Gamma distribution

- $f(x) = \left[\dfrac{\lambda^r}{\Gamma(r)}\right] x^{r-1} e^{-\lambda x}$

- for x > 0, where Γ(r) is the gamma function

- SAPHIRE software (software used for SPAR models development)
  - requires the r parameter and mean
  - λ is calculated: λ = r/μ
  - where: μ = r/λ

- PRAs typically assume gamma distribution for operating related components (e.g., fails to run)

Propagation of Uncertainties
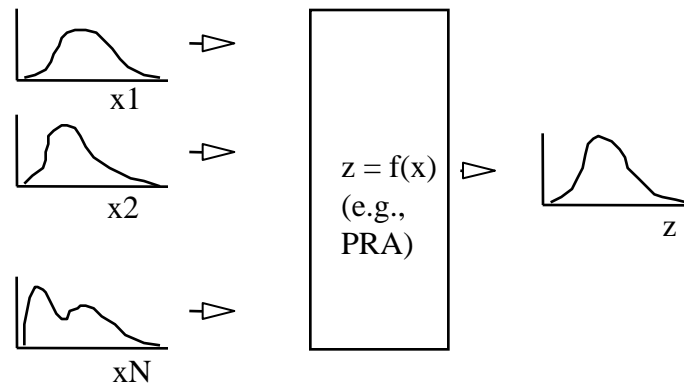
- Problem

Remember, a PRA is basically a very large boolean algebra equation (or function)

Propagation of Uncertainties

- Problem
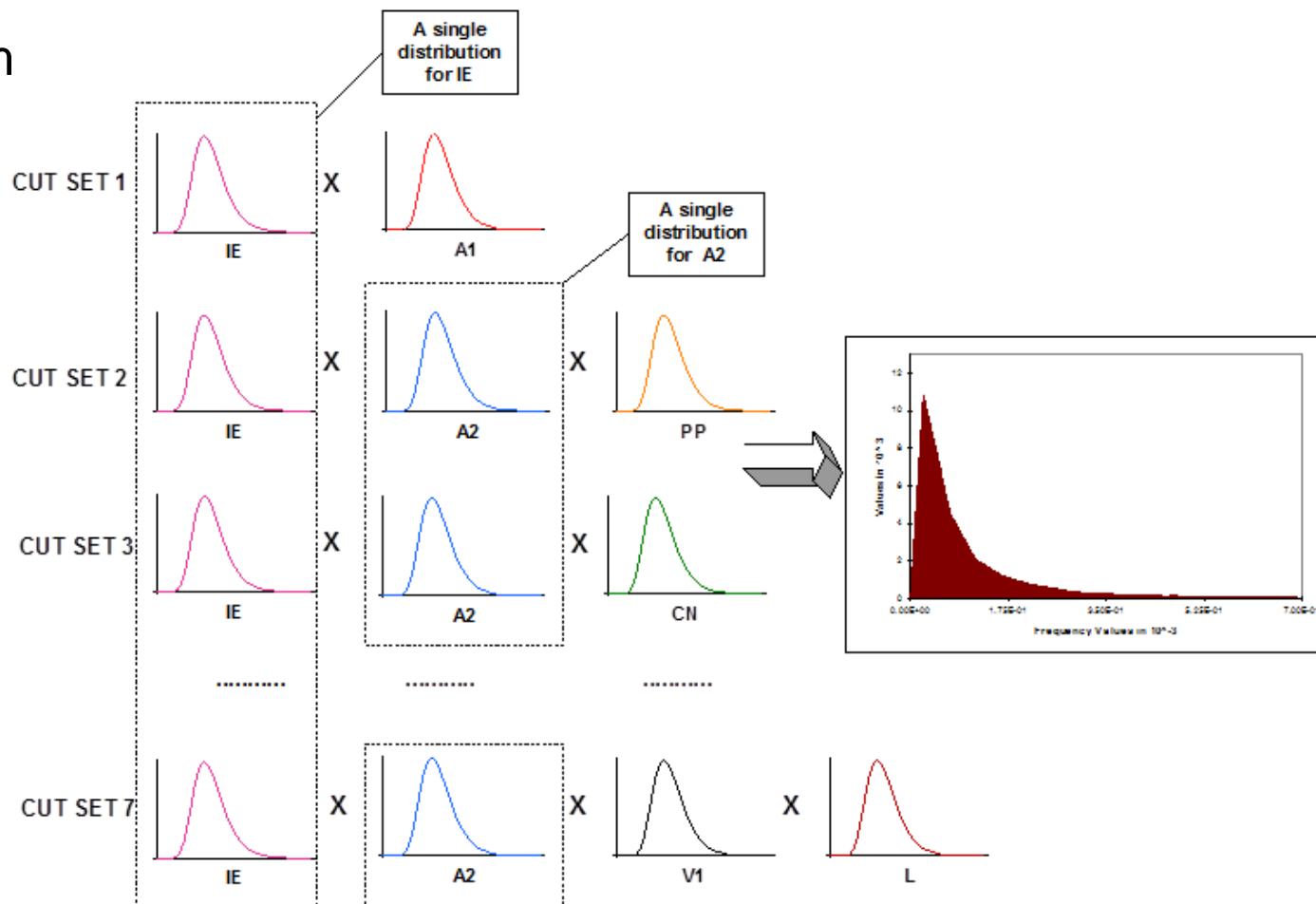
Remember, a PRA is basically a very large boolean algebra equation (or function)

Propagation of Uncertainties

- Method of Moments
    - Let X and Y be independent variables, and let
        Z = X + Y
    - The mean and variance of Z can then be found:
        E[Z] = E[X] + E[Y]
        Var[Z] = Var[X] + Var[Y]   (if X and Y independent)

Propagation of Uncertainties

- Method of Moments

  More generally, if X and Y are dependent,

  $Var[Z] = Var[X+Y]$

  $\qquad = E[\,(X+Y- E[X+Y])^2\,]$

  $\qquad = E[\,(X+Y)^2\,] - E\,[X+Y]^2$

  $\qquad = E[X^2] + 2E[XY] + E[Y^2] - E[X]^2 - 2E[X]E[Y] - E[Y]^2$

  $\qquad = Var[X] + Var[Y] + 2Cov[X,Y]$

Propagation of Uncertainties

- Method of Moments
  - Let X and Y be independent variables, and let
    Z = X•Y
  - Then
    E[Z] = E[X]•E[Y]
    Var[Z] = Var[X]•Var[Y] +Var[X]E[Y]^2 +Var[Y]E[X]^2

Analytical Methods Impractical

- Typical PRA comprises
    - Hundreds (if not thousands) of basic events
    - Many tens of significant core damage sequences
    - Often hundreds of thousands (if not millions) of core damage sequence cut sets
- Analytical methods - not just difficult, but infeasible

The Problem: Level-1/2 PRA Uncertainty Integration
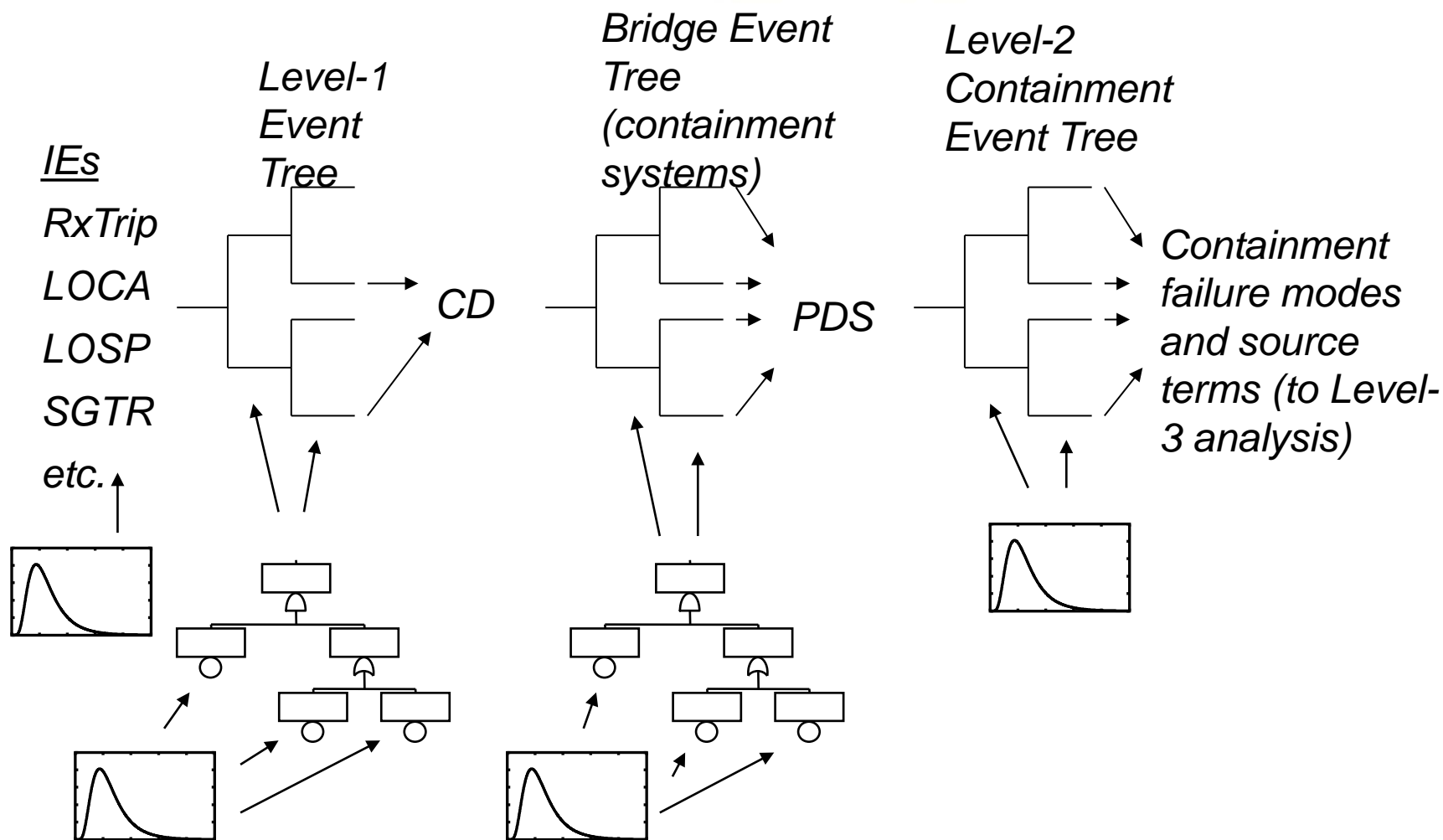
Propagating Uncertainties

- Simulation methods are only practical approach
  - Simply sample from possible input values many times and plot results

- Two simulation methods commonly used
  - Monte Carlo
  - Latin Hypercube

Propagation of Uncertainties

- Monte Carlo
  - Empirically generates distribution for Z = f(X, Y) by sampling from distributions for X and Y
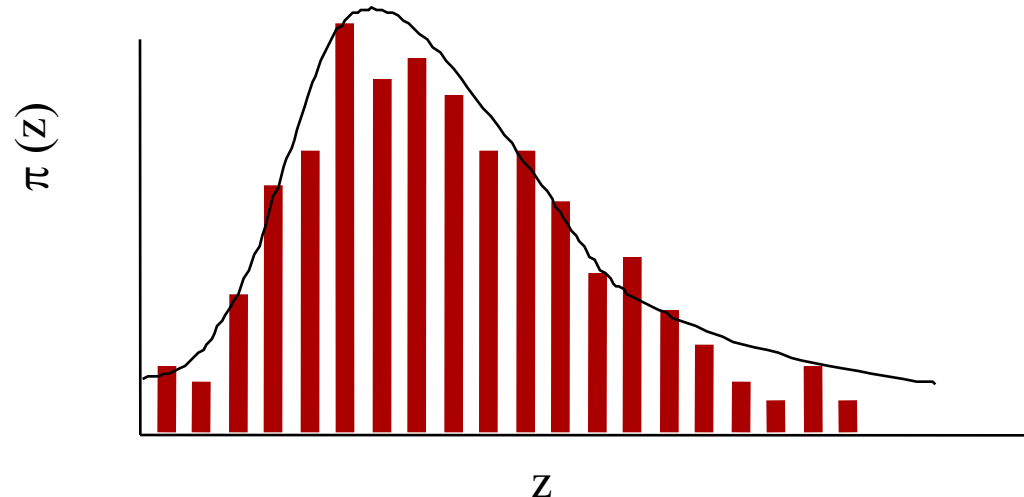
Propagation of Uncertainties

- Monte Carlo
  - Sampling approach (one variable)
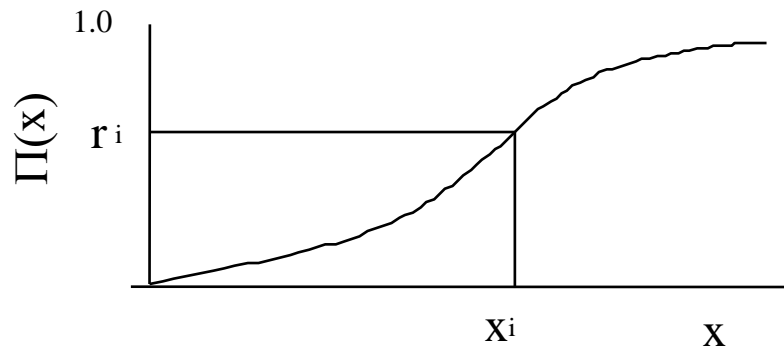
  - Cautions
    - Sampling extreme values
    - Accuracy (proportional to $1/\sqrt{N}$ (N=# samples)
    - Sampling algorithm and random # generator

Monte Carlo Sampling (5 Samples) on input parameter λ

Selected λ's

λ

CumPr($\lambda < \lambda$')

Random Numbers (normalized to between zero and one)
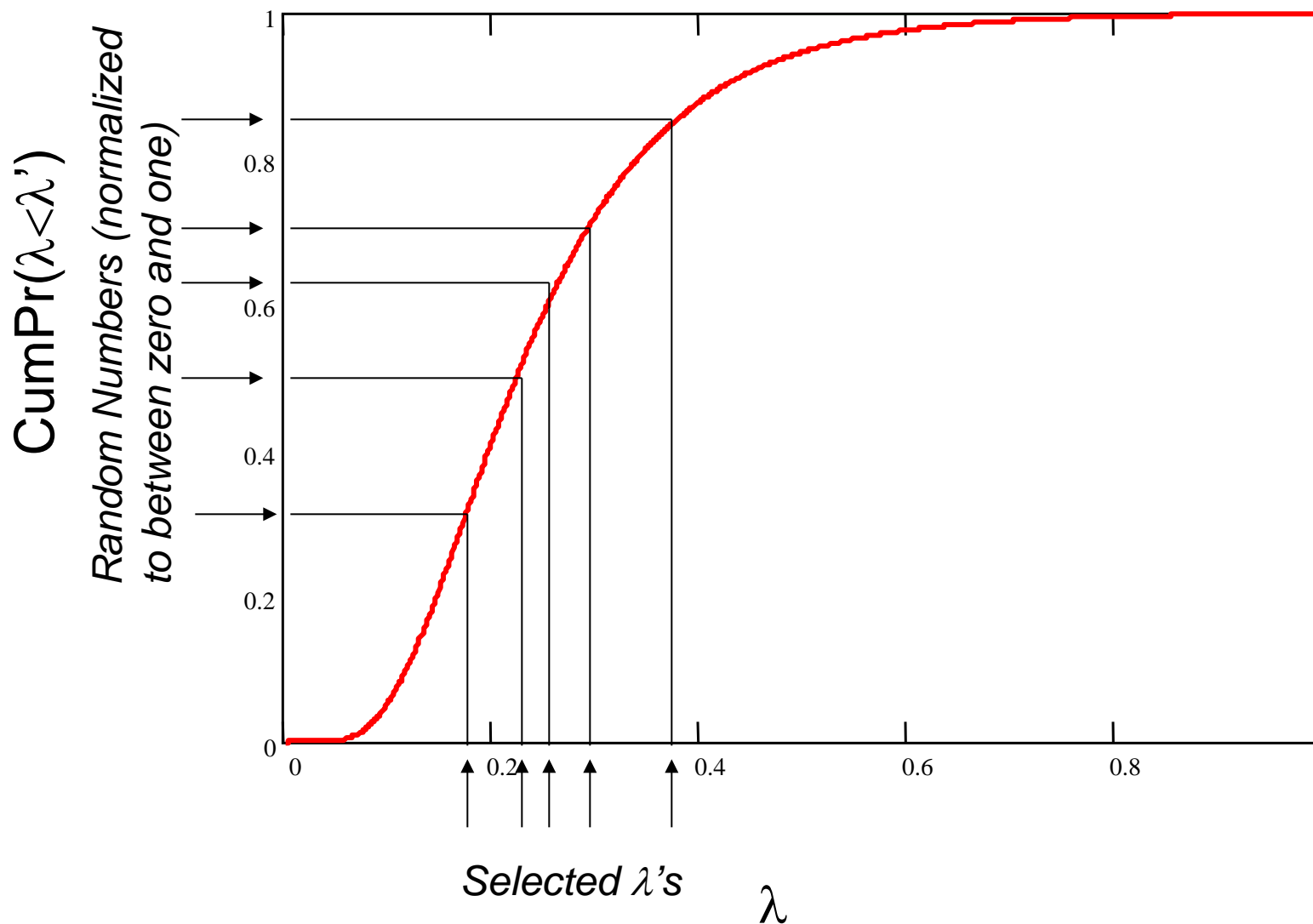
Propagation of Uncertainties

- Latin Hypercube
  - Empirically generates distribution for Z = f(X) by stratified sampling from distribution for X
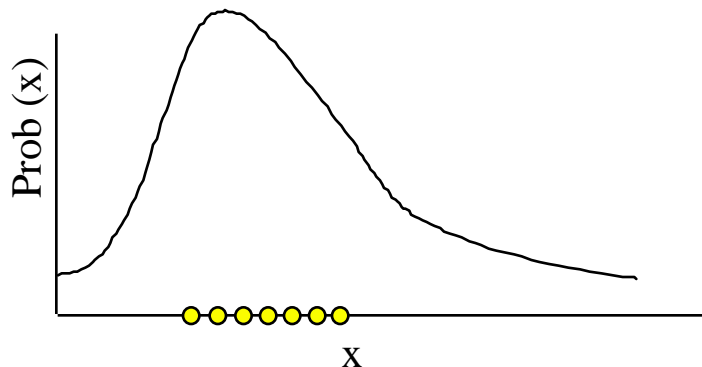
Crude Monte Carlo
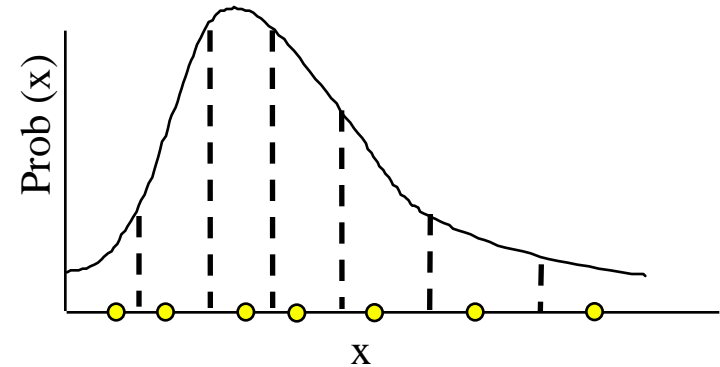
Latin Hypercube

  - Better coverage of extreme values than Monte Carlo

Latin Hypercube Sampling (one λ selected from each equal-probability area)

Equal probability regions (0.2)
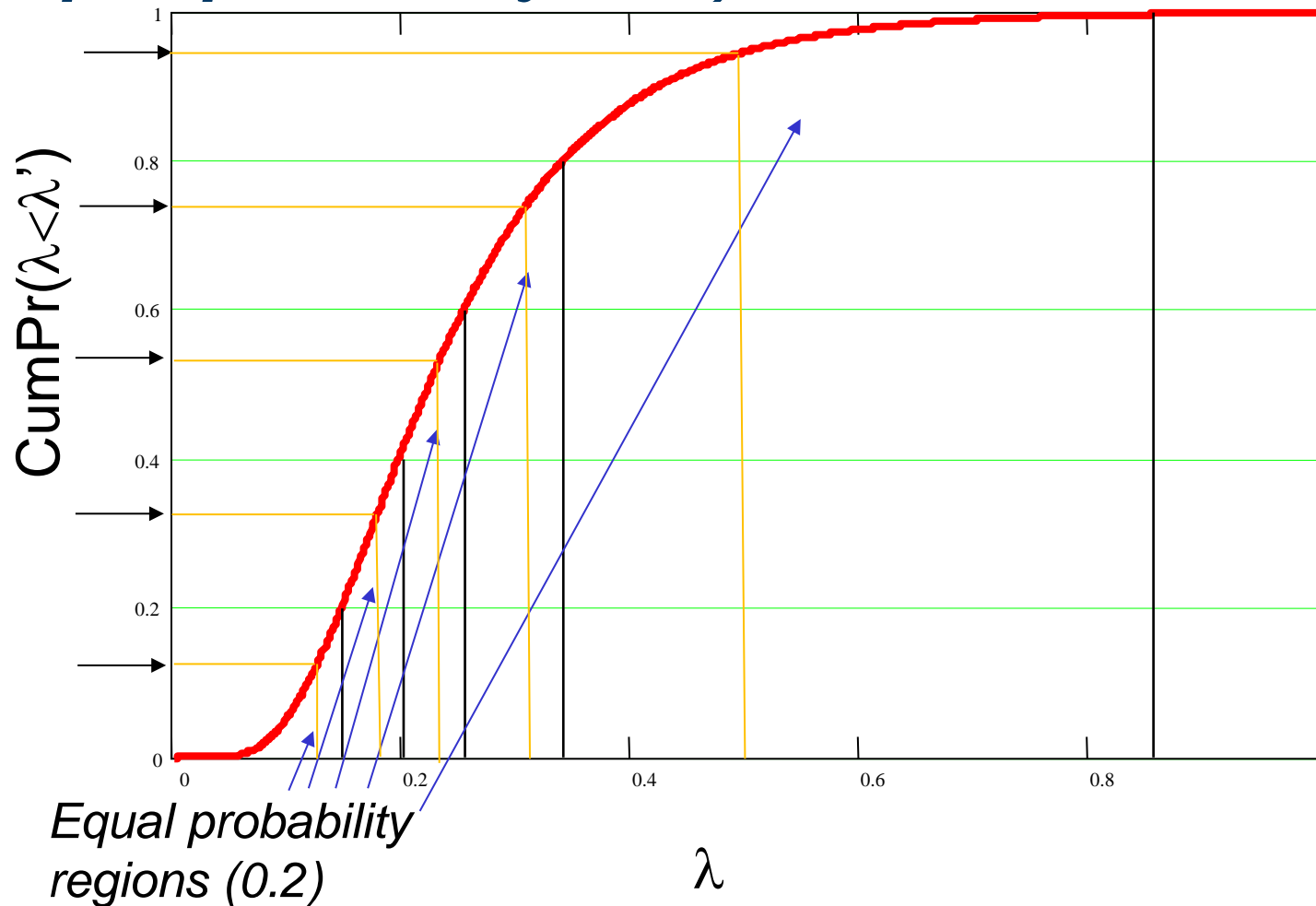
System Modeling Techniques for PRA

Lecture 5 - Event Trees

Idaho National Laboratory

Objectives

- Understand underlying process implied by event tree models
- Understand common event tree conventions
- Understand model applications and limitations

- Outline
  - Appropriate applications for event trees
  - Event tree conventions and construction
  - Modeling of dependencies

Event Trees

- Model what happens after initiating event
  - Typically (but not necessarily), a chronological ordering of major events
- Reflect system interactions
- Provide vehicle for sequence quantification
  - A sequence is an initiating event combined with a set of top events, usually system successes and failures
- Provide simple display of results

Event Tree Underlying Model

- After initiating event, safety barriers are challenged
- Barrier (system) failure is an aleatory event
  - IE * barrier success/failure → assumed to be Poisson distributed
- Overall sequence frequency is $\lambda \, \phi$
  (frequency of IE) x (Probability of system failure)
- λ and ϕ have uncertainty (epistemic)

Event Tree Models Sequence of Events
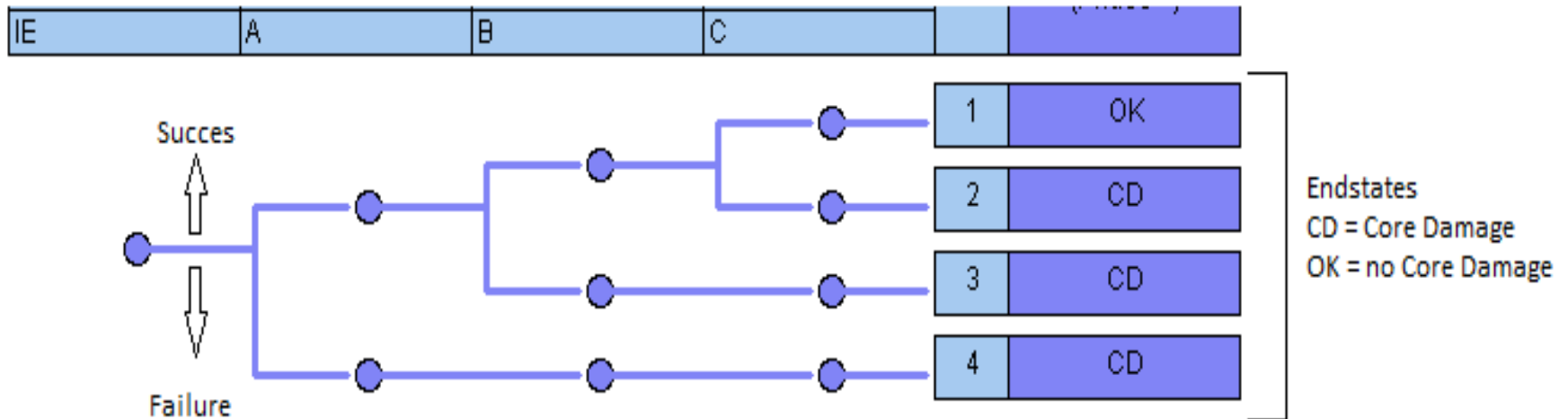
That is, IE occurs, then a combination of plant systems A, B and C are challenged.

Two Basic Approaches for Event Tree Models

- Analysis process includes two methods
- Linked fault trees (event trees are the mechanism for linking the fault trees)
  - Employs Boolean logic and fault tree models to pick up intersystem dependencies
  - Sometimes called Small-ET/Large-FT approach, used by most of the PRA community
- Event trees with boundary conditions (BC) (many event trees constructed, each with a unique set of support system BC)
  - Involves analyst quantification and identification of intersystem dependencies
  - Sometimes called Large-ET/Small-FT or PL&G approach

Event Tree Construction

- Modeling Approach
  - Linked fault trees
    - Automatic treatment of shared event dependencies
    - One-step quantification
    - Often use large, general-purpose fault trees
    - Used by SPAR models and majority of utility PRAs

Event Tree with Boundary Conditions

- Modeling Approach
    - Objective: Explicitly separate-out dependencies to facilitate quantification of sequences
    - Focuses attention on context (i.e., the boundary conditions) for performance
    - Requires intermediate numerical results (conditional split fractions)
    - Often implemented using multiple, linked event trees
    - Sometimes referred to as Large-ET approach

Both Event Tree Approaches Link Models*

Fault trees to event trees:
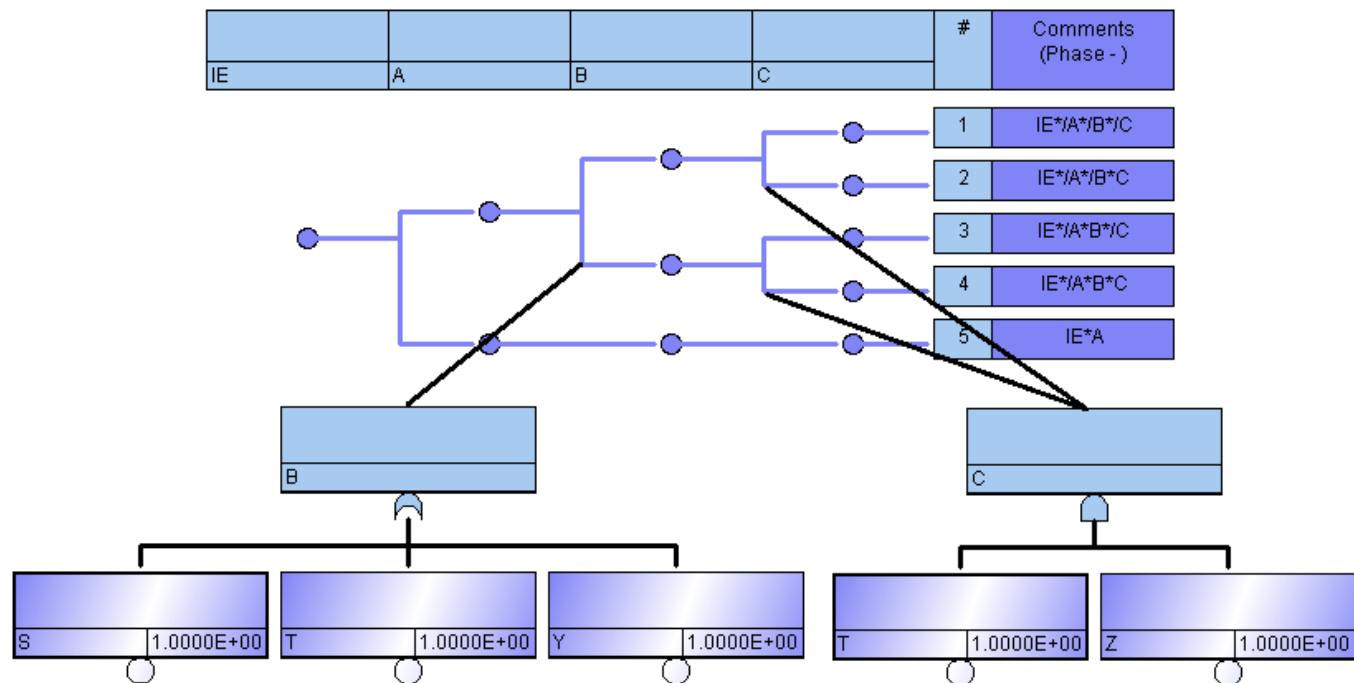
* *Necessary in order to accurately reflect dependencies*

Both Event Tree Approaches Link Models*

Event trees to event trees:
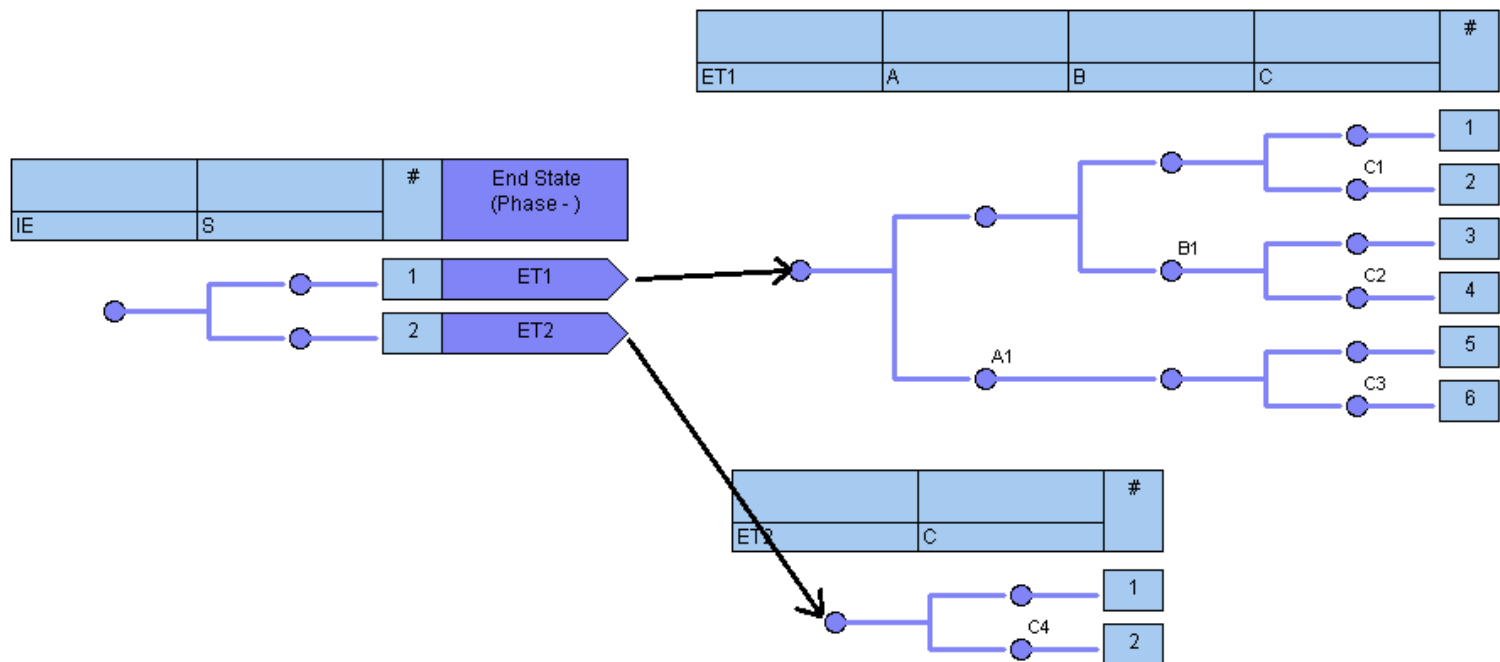
* *Necessary in order to accurately reflect dependencies*

Dependent Failures Overview

- Importance of Modeling
  - For systems with defense in depth, an accident requires failure of multiple safety barriers
  - Multiple independent failures are highly unlikely (unless safety barriers are unreliable)
  - Scenarios involving coupled failures of barriers will dominate risk
    - If A and B are dependent, then
      - $P(AB) \neq P(A) * P(B)$, and instead…
      - $P(AB) = P(A) * P(B|A) = P(B) * P(A|B)$

Modeling Dependent Failures

- Analysis Approaches
    - Explicit modeling
    - Implicit modeling
        - Parametric common cause failure analysis, discussed later

Dependencies Modeled in Fault Trees

- Example of shared equipment dependency:
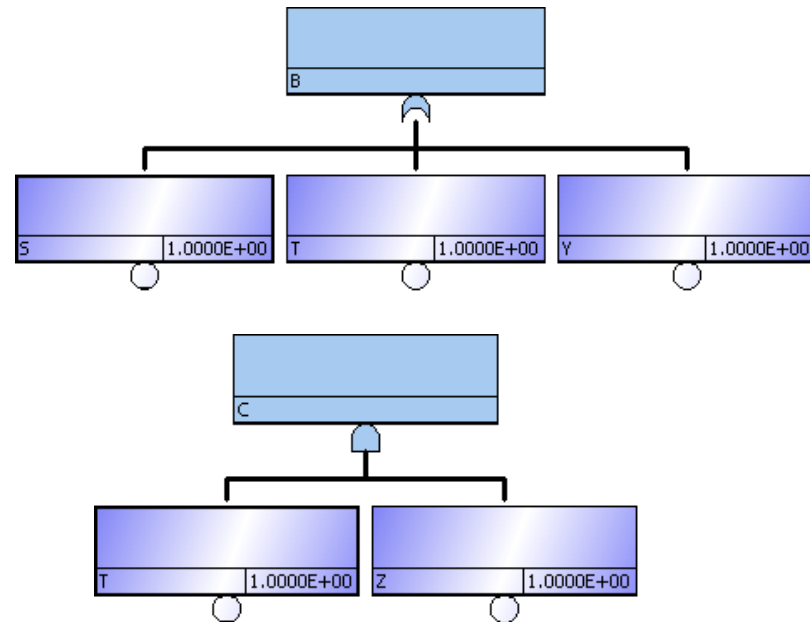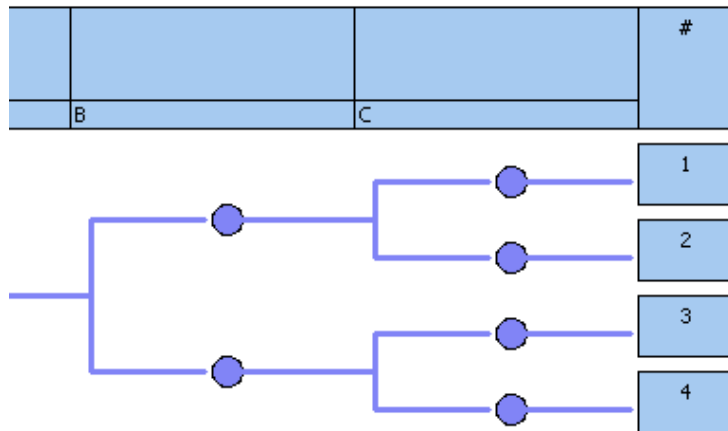
- Sequence 4 = B * C (i.e., both B and C occur/fail)

Shared Equipment Dependencies

- Fault Tree Linking for Sequence 4 (B and C)
  - Sequence 4 = (S + T + Y)*(T*Z)

                      = (S*T*Z + T*T*Z + Y*T*Z)

                      = T*Z
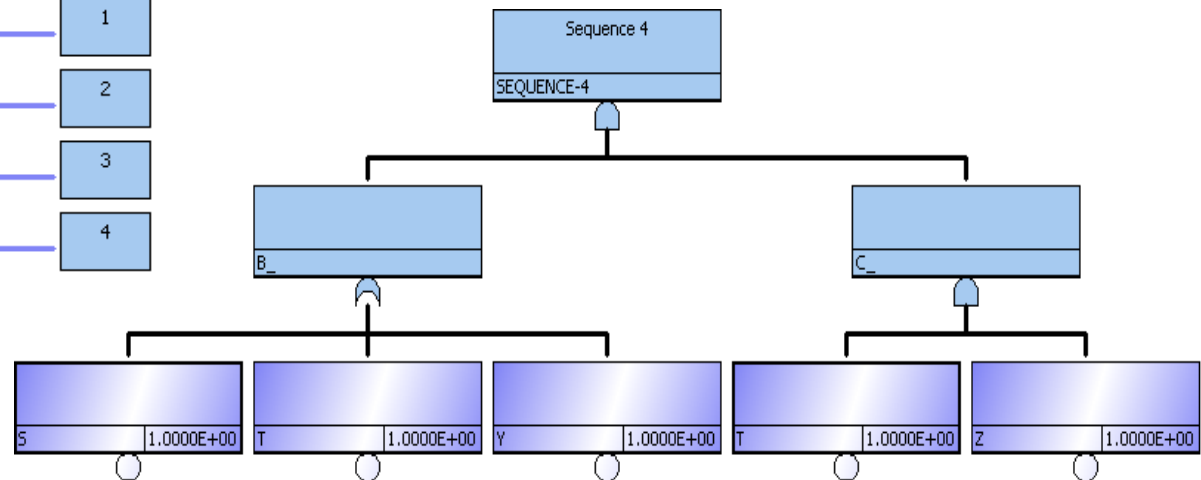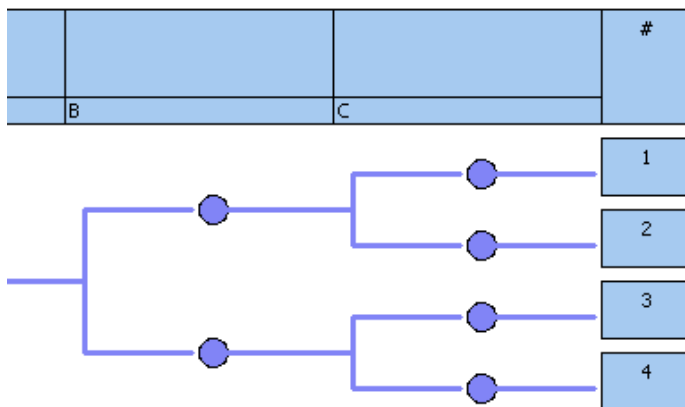
Practice Example

- Re-Solve Sequence 4 with System-B as an AND gate, and System-C as an OR gate.

Dependencies Modeled in Event Trees

- Event Trees with Boundary Conditions
  - Dependency can be represented with a separate top event (usually used for support systems)
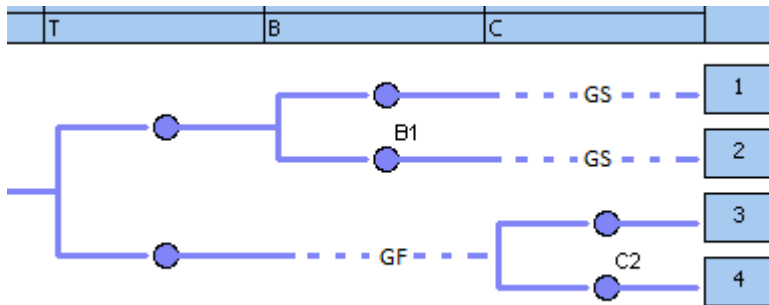
$$\phi_{B_1} = \Pr\{B \mid / T\} \approx \phi_S + \phi_Y$$

$$\phi_{C_2} = \Pr\{C \mid T, B\} = \phi_Z$$

GS - Guaranteed Success

GF - Guaranteed Failure
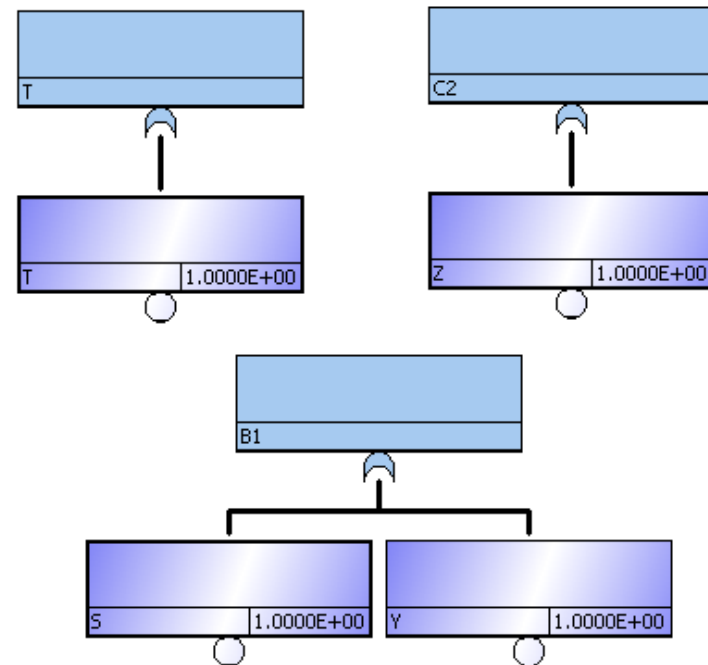
Shared Equipment Dependencies Without Separating as a Support System

- Event Trees with Boundary Conditions
  - Shared equipment dependencies can also be modeled using just conditional split fractions
  - Example:

    Sequence 3 = B*C = (S + T + Y)*(T*Z) = T*Z
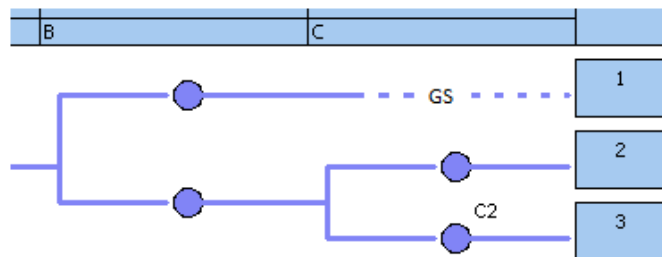
$$\phi_{C_2} = Pr\{C \mid B\} = \frac{Pr\{B\ AND\ C\}}{Pr\{B\}} = \frac{Pr\{T * Z\}}{Pr\{S + T + Y\}}$$

$$\approx \frac{\phi_T \cdot \phi_Z}{\phi_S + \phi_T + \phi_Y}$$

Practice Example

- Shared equipment dependency in linked fault trees
- Solve for Sequence 2 (via fault tree linking, need to use Boolean Algebra rules from Lecture-3 on Fault Trees)
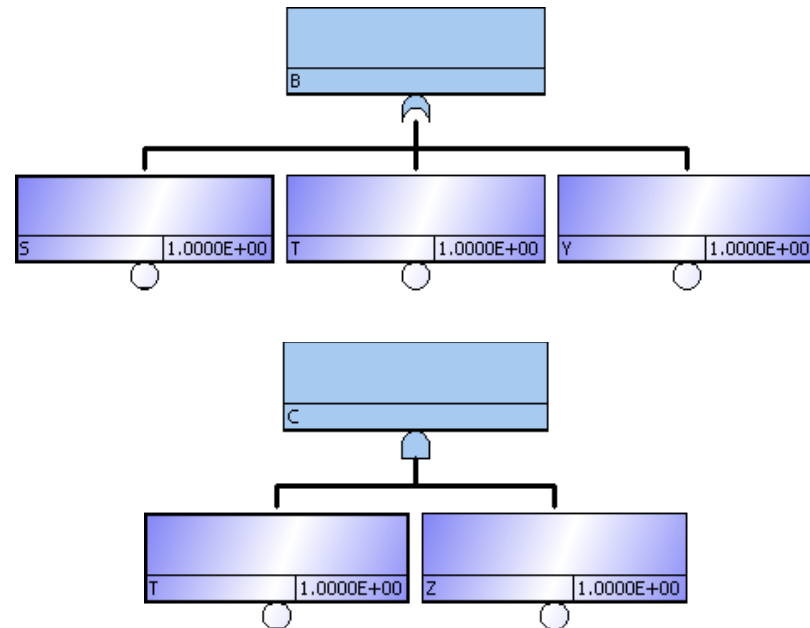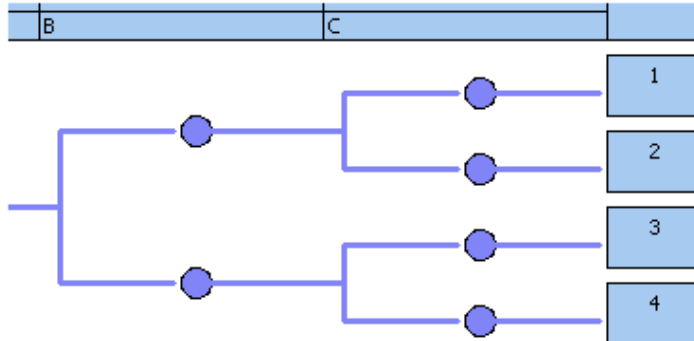
System Modeling Techniques for PRA

Lecture 6 - Sequence Models

www.inl.gov

INL
Idaho National
Laboratory

Objectives

- Understand general process of modeling "systems"

- Greater understanding of event tree modeling techniques

- Outline
  - PRA Modeling Process
  - Initiating Events
  - Event Tree Modeling Techniques
    - Functional Event Trees
    - Systemic Event Trees
    - Sequence Logic and Cut Sets

PRA Modeling Process

- Identify initiating events
- Identify mitigating functions
- Develop event trees for sequence logic
- Develop success criteria for top events
- Develop fault trees for top events
- Develop detailed sequence logic
  - Sequence cut sets (linked fault tree approach)
  - Conditional split fractions (Event Trees w/BC)

Initiating Events

- Methods for Identification
  - Deductive methods
    - Master logic diagram (what causes a reactor trip?)
  - Failure modes and effects analysis (FMEA)
  - Analysis of historical events
    - Licensee event reports
  - Comparison with other studies
  - Feedback from modeling
    - Support system dependencies identified

Initiating Events

- Potential Problem Areas
  - Quantification given little or no statistical evidence
    - Large LOCA frequency (none have occurred)
  - Violations of Poisson assumptions
    - Time dependent failure rate (aging)
  - Too many initiating events
  - Lack of completeness
  - Ambiguity in definition
    - Does loss of feedwater imply the condensate system is unavailable?

Development of Event Trees

- Unique event tree developed for each initiating event
  - Can group like initiators if they have similar impacts to the plant
- Based on safety functions necessary to achieve safe shutdown (functional event tree)
- Top events list systems capable of performing necessary safety functions (success criteria)

Functional Event Tree

High-level representation of vital safety functions required to mitigate abnormal event

- Generic response of the plant to achieve safe and stable condition

- What safety functions must be fulfilled?
    - For example:

        Reactor subcritical

        Early core cooling (injection)

        Late core cooling (recirculation)

- Provides a starting point for more detailed system-level event tree model

Functional Event Tree
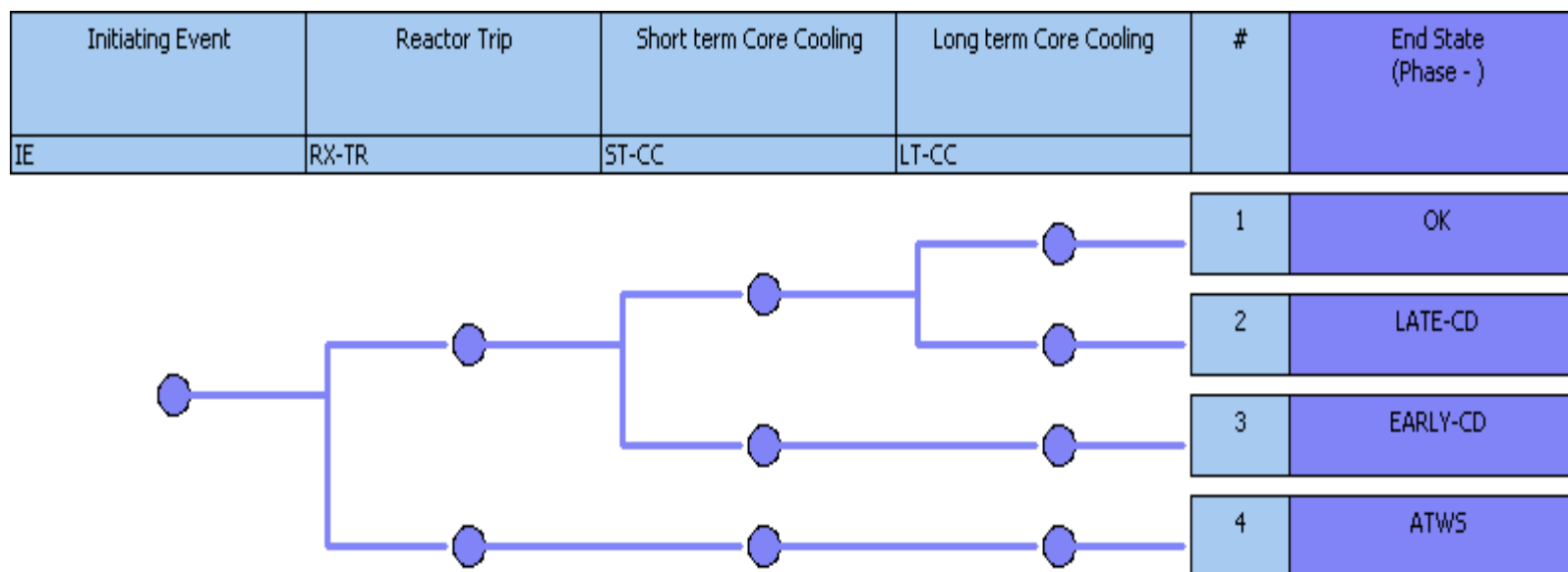
Identify Systems Capable of Fulfilling Functions

- For each initiating event identified
  - Which systems are capable of providing:
    - Reactor subcritical
    - Early core cooling (injection)
    - Late core cooling (recirculation)
- Specific success criteria need to be defined for each system

Success Criteria

IE	Reactor Trip	Short Term Core Cooling	Long Term Core Cooling
Trans	Auto Rx Trip or Man. Rx Trip	PCS or 1 of 3 AFW or 1 of 2 PORVs & 1 of 2 ECI	PCS or 1 of 3 AFW or 1 of 2 PORVs & 1 of 2 ECR
LOCA	Auto Rx Trip or Man. Rx Trip	1 of 2 ECI	1 of 2 ECR

System-Level Event Tree

- Typical ET seen in PRAs

- ET re-drawn after inserting systems as ET top-events

- More top-events consequently more complicated logic

- Unique event tree developed for each initiating event
  - Implies unique plant response to each IE
  - If plant response is not unique, simply combine IE frequencies into a single IE

Accident Sequences From ET

Initiating Event	Rx Trip	Rx Trip	Short term Core Cooling	Long term Core Cooling	#	End State (Phase -)	Comments (Phase -)
LOCA	AUTO	MAN	ECI	ECR			
					1	OK	
					2	LATE-CD	IE*/AUTO*/ECI*ECR
					3	EARLY-CD	IE*/AUTO*ECI
					4	OK	
					5	LATE-CD	IE*AUTO*/MAN*/ECI*ECR
					6	EARLY-CD	IE*AUTO*/MAN*ECI
					7	ATWS	IE*AUTO*MAN
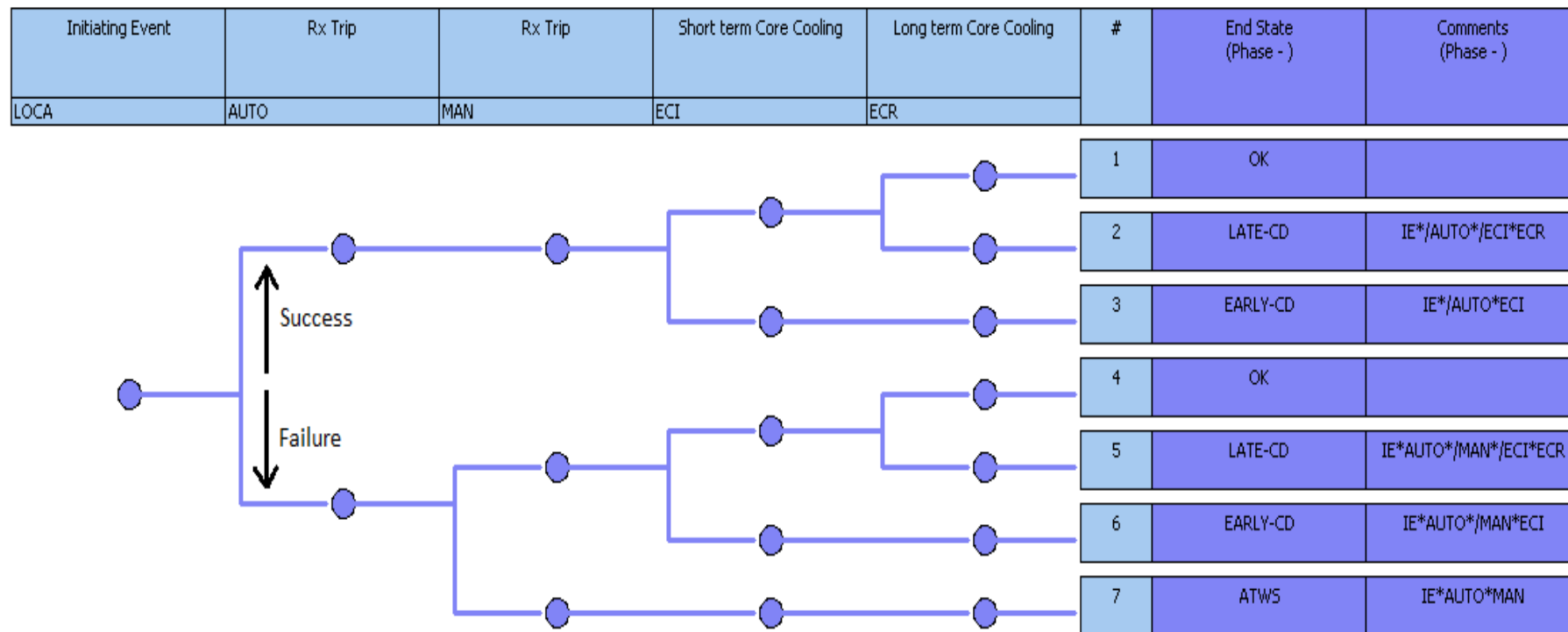
Sequence Logic Used to Combine System Fault Trees into Accident Sequence Models

- System fault trees (or cut sets) are combined, using Boolean algebra, to generate core damage accident sequence models.
  - CD seq. #5 = LOCA * AUTO * /MAN * /ECI * ECR
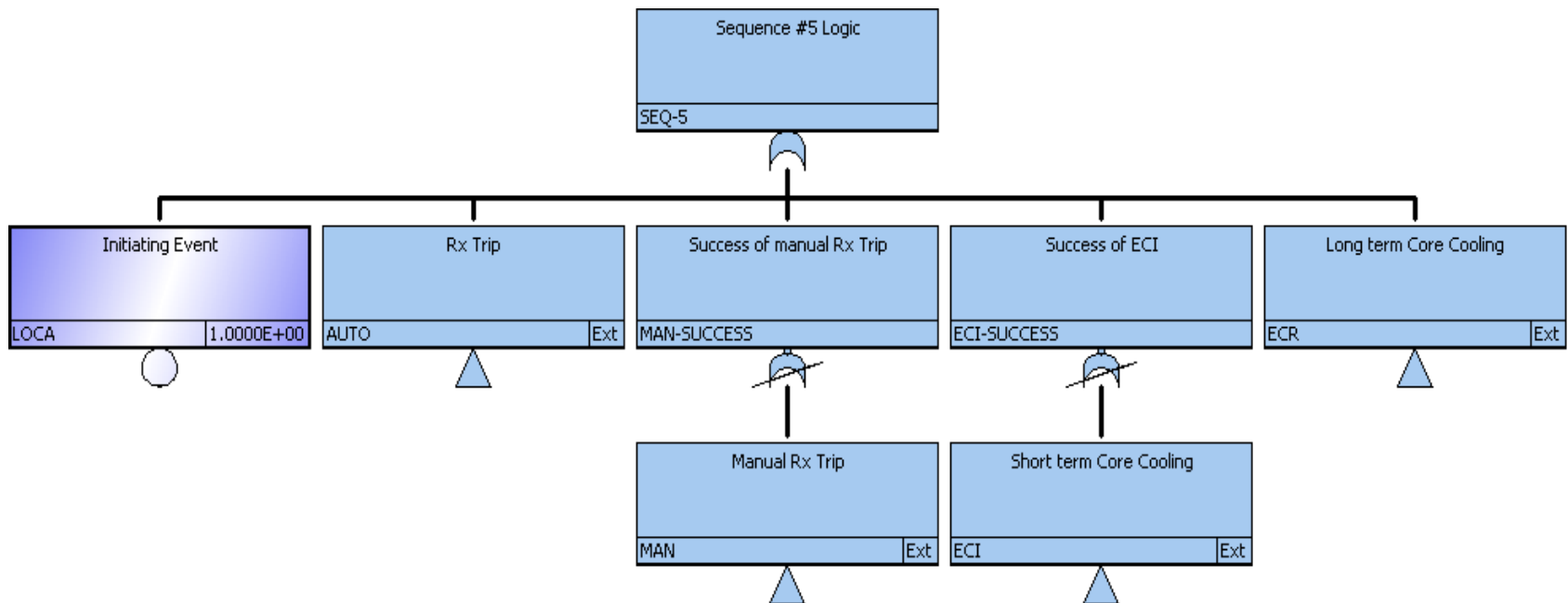
Sequence Cut Sets Generated From Sequence Logic

- Sequence cut sets generated by combining system fault trees (or cut sets) comprised by sequence logic

- Cut sets can be generated from sequence #5 "Fault Tree"
  - Sequence #5 cut sets = (LOCA) * (AUTO cut sets) * (/MAN cut sets) * (/ECI cut sets) * (ECR cut sets)
  - Or, to simplify (avoid complemented terms) the calculation (via "delete term")
    - Sequence #5 cut sets $\approx$ (LOCA) * (AUTO cut sets) * (ECR cut sets) minus any cut sets that contain (MAN + ECI cut sets)
      - Develop cut set list for: LOCA * AUTO * ECR
      - Develop cut set list for: MAN + ECI
      - Look for item 2 cut sets in item 1 cut sets, and delete them since logically they cannot occur

Delete Term Example

- Sequence logic = IE * /Inj * Rec
    Inj = P + V1 => /Inj = /P * /V1
    Rec = P + V2

- Cut sets = IE * (/P * /V1) * (P + V2)
    = IE * /P * /V1 * P +
        IE * /P * /V1 * V2.
    = IE * /P * /V1 * V2.

- Cut sets via delete term:
    Seq. CS = IE * (P + V2) minus cut sets that contain Inj (failure) cut
        sets.
    = IE * P + IE * V2 (minus cut sets that contain either P + V1).
    = IE * V2.

Practice Example:

Generate Cut Sets for Sequence #5
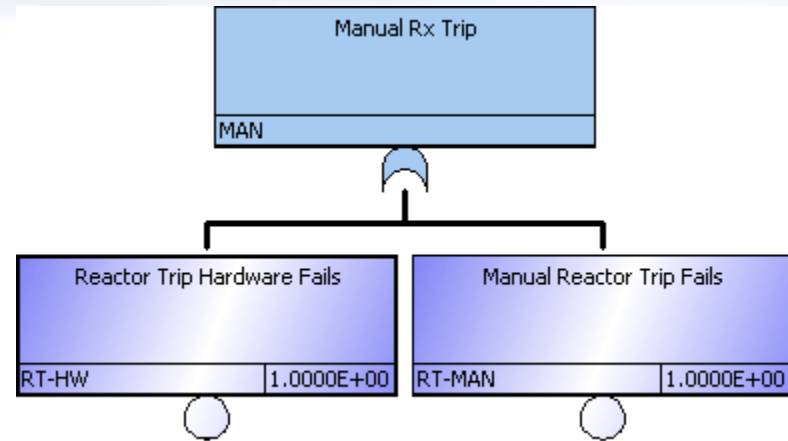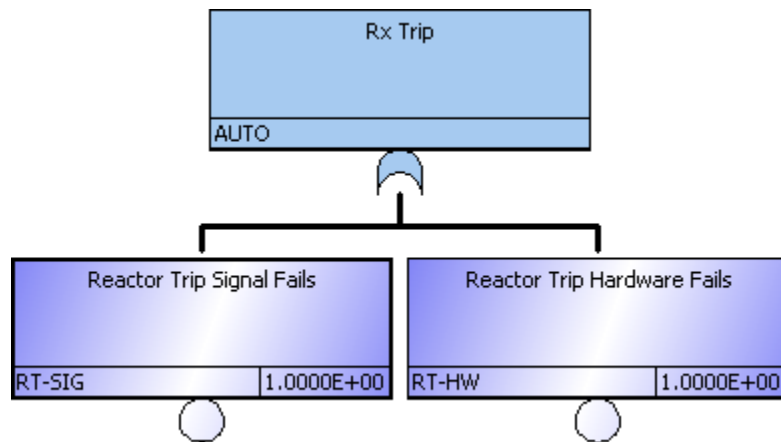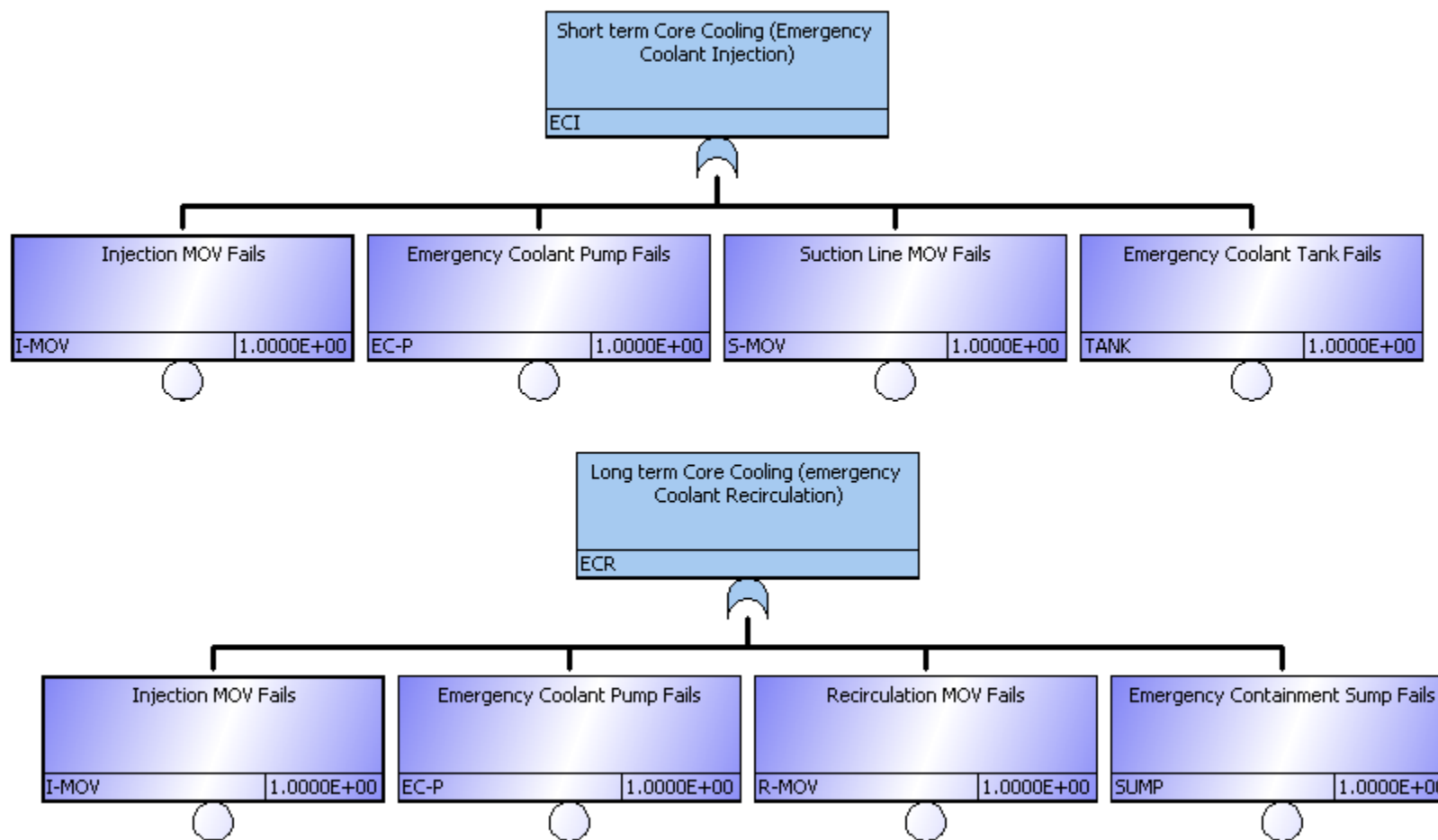
System Modeling Techniques for PRA

Lecture 7 - Common Cause Failure Models

www.inl.gov

Objectives

- Understand fundamental theory of CCF modeling

- Become familiar with different CCF models

- Outline
  - Motivation for CCF Models
  - Basic Parameter Model
  - Motivation for Parametric Models
  - Beta-Factor Model
  - Multiple Greek Letter Model
  - Alpha-Factor Model
  - Notes on Analysis Process

Why is CCF Modeling Important?

- Commercial nuclear power plants are designed with safety a priority
    - Redundancy
    - Diversity
    - Defense in depth
- NPP are effectively single failure "proof"
- Only combinations of failures can seriously challenge reactor integrity

Focus on Dependent Failures

- Combinations of independent failures extremely rare events
- Dependent failures pose major challenge to safety
  - Shared equipment and support system dependencies
    - Explicitly modeled in PRA logic
  - Failures of multiple components from a common (or shared) cause
    - Cause not explicitly modeled
    - Treated parametrically – CCF models

4

Definition of Dependency

- Events A and B are said to be dependent events if
  $$P(A*B) = P(A|B) * P(B)$$
  $$= P(B|A) * P(A)$$
  $$\neq P(A) * P(B)$$

- Typically (not always) if events are dependent
  $$P(A*B) > P(A) * P(B)$$
  - This is why they are a safety concern

Examples of CCF

- Human interaction
  - Maintenance technician incorrectly sets setpoints on multiple components
  - Incorrect or incorrectly applied lubricant

- Physical or environmental
  - Bio-fouling (e.g., clams, muscles, fish)
  - Design or manufacturing defect
  - Contamination in lubricant or fuel

- Again, not represented explicitly, only parametrically

Basic Parameter Model

- Background
  - Consider a group of 3 identical components: A, B, and C.
  - Notation:
    $A\overline{B}\overline{C} \equiv$ Failure of A, success of B and C
  - $AB\overline{C} \equiv$ Failure of A and B, success of C

    $ABC \equiv$ Failure of A, B and C

    $Q_{XYZ} \equiv$ Probability of event XYZ
  - Modeling assumption: Failure probabilities are symmetrical

    $Q_{A\overline{BC}} = Q_{\overline{A}B\overline{C}} = Q_{\overline{AB}C} \equiv Q1$ (only one component fails)

    $Q_{AB\overline{C}} = Q_{A\overline{B}C} = Q_{\overline{A}BC} \equiv Q2$ (only two components fail)

    $Q_{ABC} \equiv Q3$

$\overline{X}$ Means component X
Is not failed

Basic Parameter Model

- Model Parameters
  - The $Q_{k's}$ are system parameters
    - They quantify probabilities of system events (CCFs for specific groups of k components)
  - Relating $Q_{k's}$ to the total component failure rate:
    $$Q_{t(A)} = Q_A = Q_{A\overline{BC}} + Q_{A\overline{B}C} + Q_{AB\overline{C}} + Q_{ABC}$$
    $$= Q_1 + 2Q_2 + Q_3$$
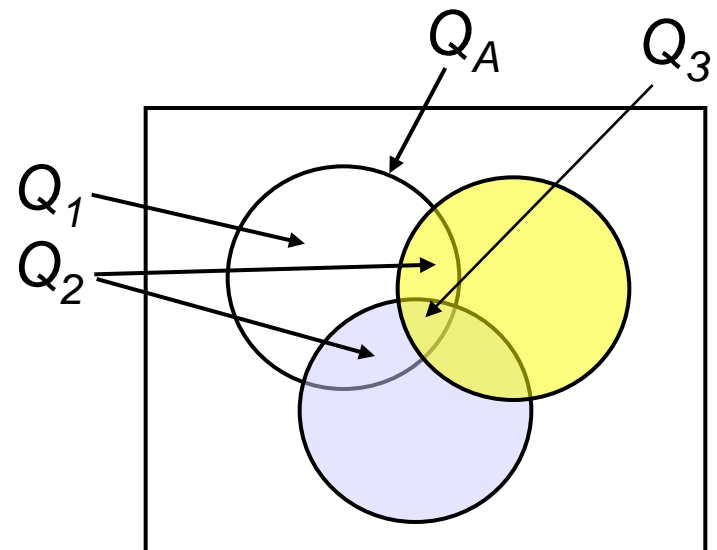
Basic Parameter Model

- Model Parameters
  - General expression: $Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k$

    where:

    - $m \equiv$ number of identical components (size of "common cause component group")
    - $Q_t \equiv$ total failure probability for a given component

    Binomial Coefficient:

    $$\binom{m-1}{k-1} \equiv \frac{(m-1)!}{(k-1)!(m-k)!} \quad , \quad (\; x! \equiv x * (x - 1) * (x - 2) * \ldots * 2 * 1)$$

Basic Parameter Model - example

- Find Q_t when m = 3

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k \qquad\qquad Q_t = \sum_{k=1}^{3} \binom{3-1}{k-1} Q_k$$

Motivation for Parametric Models

- Data needed to estimate Q_k in basic parameter model are not generally available

- Available data include:
  - Generic failure probabilities/rates for components (i.e., Q_t)
  - Compilations of dependent failures (without demand data)

- Alternative models use latter information to develop relative fractions of dependent failure events

β -Factor Model

- Originally developed for 2-component systems; later extended to handle larger systems

- Based on notion that component failures can be divided into two groups
  - Those that are independent
  - Those that involve dependent failure of all components

β -Factor Model

Allocation model:

$$Q_t = Q_1 + Q_m = (1 - \beta)Q_t + \beta Q_t$$

Independent   dependent

contribution   contribution

Therefore:

$$\beta \equiv Q_m/(Q_1 + Q_m)$$

β -Factor Estimation

- In general,

$$Q_k = \begin{cases} (1-\beta)Q_t & k = 1 \\ 0 & 2 \le k < m \\ \beta Q_t & k = m \end{cases} \qquad \hat{\beta} = \dfrac{\displaystyle\sum_{k=2}^{m} kN_k}{\displaystyle\sum_{k=1}^{m} kN_k}$$

where:
  N_k is the number of <u>events</u> involving failure of exactly k components so that the product kN_k represents number of failed <u>components</u>.

β -Factor Estimation

- Example:
    - Consider a system with two components: A and B.
    - Component A has failed 3 times in 50,000 hours of service; out of those 3 failure events, 1 event was a common cause failure (involving component B).
    - Component B also has 50,000 hours of service, and it has failed 2 times (including the joint failure event with A).

β-Factor Estimation

- Point estimates for λ_t and β are then,

    λ_t = 5 failures / 100,000 hr = 5.0×10^{-5}/hr

    $\beta = 2/(3+2) = 0.4$

- And,

    $\lambda_{CCF} = \lambda_t * \beta = 5.0 \times 10^{-5}$/hr $* 0.4$

    $\lambda_{CCF} = 2.0 \times 10^{-5}$/hr

- In the absence of plant-specific data, base component failure rate (λ_t) is obtained from generic failure rates

Multiple Greek Letter (MGL) Model

- β - factor extended to treat multiple levels of CCF
- Definitions:
  - β ≡ conditional probability that cause of a specific component failure will be shared by one or more additional components
  - γ ≡ conditional probability that common cause failure of a specific component that has failed two components will be shared by one or more additional components
  - δ ≡ conditional probability that common cause failure of a specific component that has failed three components will be shared by one or more additional components

Multiple Greek Letter (MGL) Model

- Parameters
  - A: Failures involving component X
  - B: Failures involving CCF of X and at least 1 other component
  - C: Failures involving CCF of X and at least 2 other components
  - D: Failures involving CCF of X and at least 3 other components
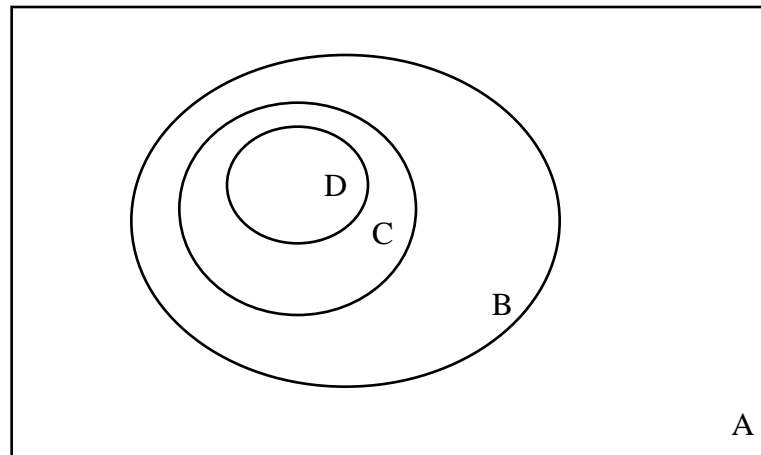
$\beta = P(B|A)$

$\gamma = P(C|B)$

$\delta = P(D|C)$

Multiple Greek Letter (MGL) Model

– Estimators

$$\hat{\beta} = \frac{\sum\limits_{k=2}^{m} kN_k}{\sum\limits_{k=1}^{m} kN_k}, \quad \hat{\gamma} = \frac{\sum\limits_{k=3}^{m} kN_k}{\sum\limits_{k=2}^{m} kN_k}, \quad \hat{\delta} = \frac{\sum\limits_{k=4}^{m} kN_k}{\sum\limits_{k=3}^{m} kN_k}$$

N_k is the number of <u>events</u> involving the failure of exactly k components. Therefore, kN_k is the number of failed <u>components</u>.

Multiple Greek Letter (MGL) Model

- Relations to Q_k's
  - m = 3
  - m = 4

$$\hat{\beta} = \frac{2N_2 + 3N_3}{N_1 + 2N_2 + 3N_3}$$

$$\hat{\gamma} = \frac{3N_3}{2N_2 + 3N_3}$$

$$Q_1 = (1 - \beta)Q_t$$

$$Q_2 = \frac{1}{2}\beta(1 - \gamma)Q_t$$

$$Q_3 = \beta\gamma\, Q_t$$

$$\hat{\beta} = \frac{2N_2 + 3N_3 + 4N_4}{N_1 + 2N_2 + 3N_3 + 4N_4}$$

$$\hat{\gamma} = \frac{3N_3 + 4N_4}{2N_2 + 3N_3 + 4N_4}$$

$$\hat{\delta} = \frac{4N_4}{3N_3 + 4N_4}$$

$$Q_1 = (1 - \beta)Q_t$$

$$Q_2 = \frac{1}{3}\beta(1 - \gamma)Q_t$$

$$Q_3 = \frac{1}{3}\beta\gamma(1 - \delta)Q_t$$

$$Q_4 = \beta\gamma\delta\, Q_t$$

$\alpha-$*Factor Model*

- Background
  - Simple expressions for exact distributions of MGL parameters (accounting for uncertainties) are not always obtainable
  - Approximate methods leading to point estimators provided earlier underestimate uncertainty
  - α-factor model developed to address this issue

$\alpha-$*Factor Model*

- Definition

  - $\alpha_k \equiv$ conditional probability that a failure event involves k components failing due to a shared cause, given a failure event

$$\alpha_k = \frac{\binom{m}{k} Q_k}{\sum\limits_{k=1}^{m} \binom{m}{k} Q_k} \qquad where \qquad \binom{m}{k} = m!/k!(m-k)!$$

Note: This definition emphasizes shocks to the <u>system</u> (i.e., failure events) rather than to the <u>components</u> (i.e., failures)

α-Factor Model

- Example (m = 3)
  - Failure events involving only 1 component are:

  $$\mathrm{A\overline{BC}, \ \overline{A}B\overline{C}, \ \overline{AB}C}$$

  - Since

  $$Q_1 = Q_{\mathrm{A\overline{BC}}} = Q_{\mathrm{\overline{A}B\overline{C}}} = Q_{\mathrm{\overline{AB}C}}, \text{ then } \ \alpha_1 = \frac{3Q_1}{3Q_1 + 3Q_2 + Q_3}$$

  - Similarly,

  $$\alpha_2 = \frac{3Q_2}{3Q_1 + 3Q_2 + Q_3}$$

  $$\alpha_3 = \frac{Q_3}{3Q_1 + 3Q_2 + Q_3}$$

  - Note that $\alpha_1 + \alpha_2 + \alpha_3 = 1$ as expected.

α-Factor Model

- Key Expressions
    - Point Estimators

$$\hat{\alpha}_k = \frac{N_k}{\sum_{i=1}^{m} N_i}$$

- Expression for Q_k's

$$Q_k = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\sum_{i=1}^{m} i\,\alpha_i} Q_t$$

  (from NUREG/CR-5485, page 41, for non-staggered testing)

α-Factor Model

- Example (m = 3)
  - Expression for Q_k's

$$Q_1 = \frac{\alpha_1}{\alpha_1 + 2\alpha_2 + 3\alpha_3} Q_t$$

$$Q_2 = \frac{\alpha_2}{\alpha_1 + 2\alpha_2 + 3\alpha_3} Q_t$$

$$Q_3 = \frac{3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3} Q_t$$

α-*Factor Model*

Example (m = 3) (cont.)

Relationships with MGL parameters

$$\beta = \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3}$$

$$\gamma = \frac{3\alpha_3}{2\alpha_2 + 3\alpha_3}$$

$$\alpha_1 = \frac{3(1-\beta)}{3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma}$$

$$\alpha_2 = \frac{\frac{3}{2}(\beta - \beta\gamma)}{3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma}$$

$$\alpha_3 = \frac{\beta\gamma}{3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma}$$

Analysis Process

- General Steps
  1. Starting with system logic model, identify common cause component groups
  2. Develop CCF model
  3. Gather and analyze data
  4. Quantify CCF model parameters
  5. Quantify CCF basic events

Modeling Process

- "Common Cause Component Groups"
  - Definition: A group of components that has a significant likelihood of experiencing a common cause failure event
  - Consider similarity of:
    - Component type
    - Manufacturer
    - Mode of operation/mode of failure
    - Environment
    - Location
    - Mission
    - Test and Maintenance Procedures

Modeling Process

- "Common Cause Component Groups"
  - Diversity (e.g., in operation, missions) is a possible reason for screening out
    - Note: diverse components can have common piece parts (e.g., common pumps, different drivers)

Modeling Process

Development of CCF Model
Explicit representation example
Specific combinations of components are explicitly shown on fault tree
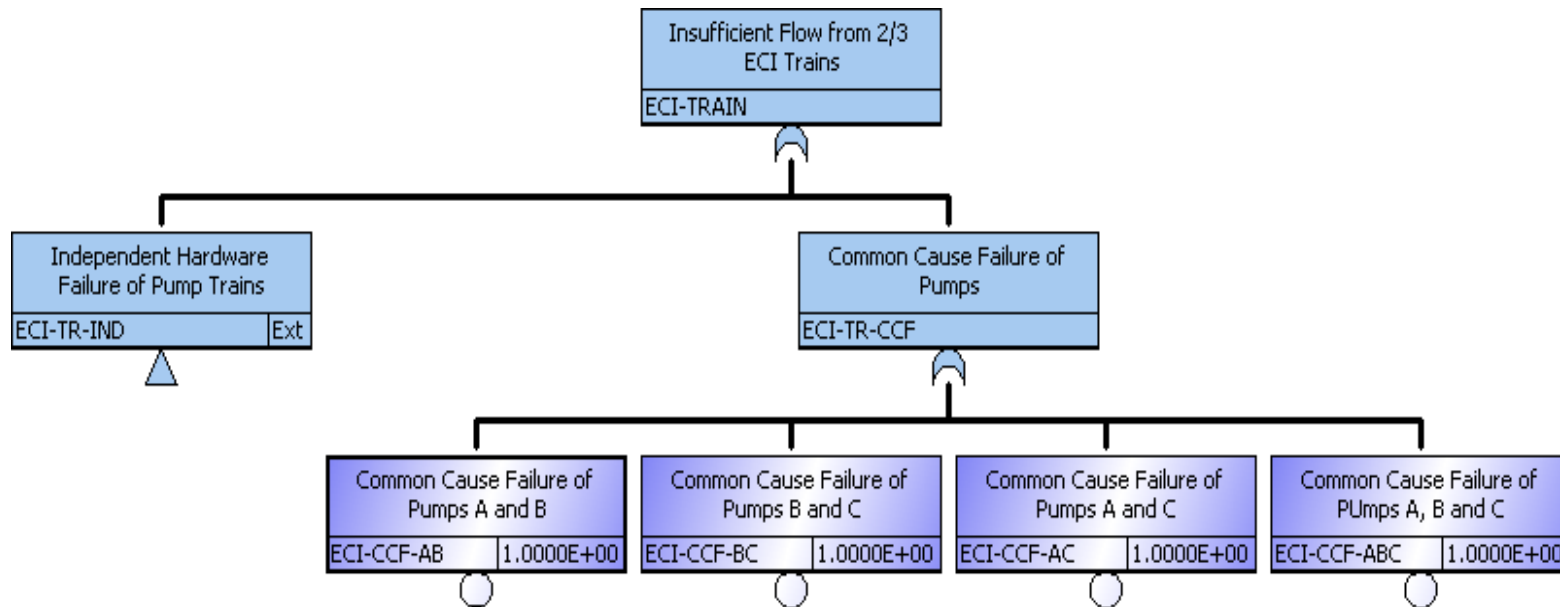
Modeling Process

- Implicit modeling example (3 trains)
  - P(top event due to CCF) = $3Q_2 + Q_3$
  - Probabilities of different combinations are "rolled-up" into the CCF term.
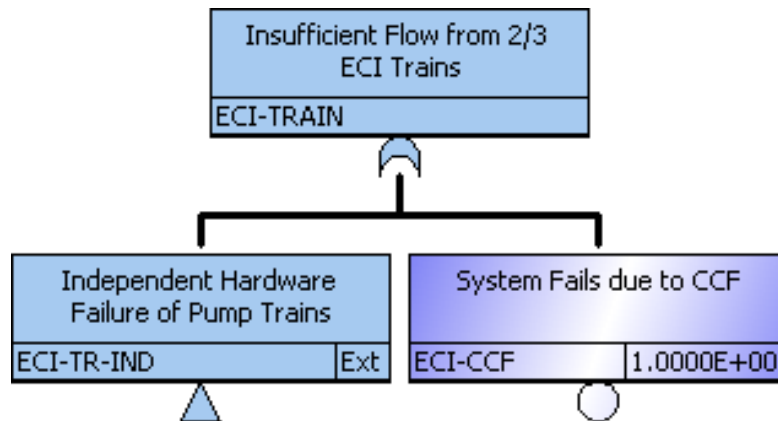
Data Analysis Process

- Data Sources
    - Generic raw data compilations (e.g., LERs, LER summaries, NPE)
    - Plant-specific raw data records (e.g., test and maintenance records, work orders, operator logs)
    - Generic event data and parameter estimates (e.g., NUREG/CR-2770, EPRI NP-3967)
    - NRC/INL CCF database (NUREG/CR-6268)
    - Parameter information stored on the web at: nrcoe.inel.gov/resultsdb/ParamEstSpar/

Data Analysis Process

- Examines *failure events* (not all demands or success events)
- Relatively few failures are clear-cut CCFs
  - Demands on redundant components do not always occur simultaneously
  - "Failures" are sometimes not demonstrated failures
    - Second component inspected and revealed similar degradation/conditions
- Interpretation and judgment used to "fill-in" the gaps in the data
  - *Degradation Value* technique
    - Assigns probabilities for likelihood an event was an actual CCF event

Data Analysis Process

– Classification example

Plant Type (Date)	Event Description	Component Group Size	Degradation Values		
			P_0	P_1	P_2
PWR (12/73)	Two motor-driven AFW pumps were inoperable due to air in common suction line	2	0	0	1

– Data typically collected include
  - Component group size
  - Number of components affected
  - Shock type (lethal vs. non-lethal)
  - Failure mode

Adjusting for System Size

- "Mapping up" and "mapping down" performed for individual p-values
- Algorithms provided in NUREG/CR-4780
- Example: Mapping from m = 3 to m = 2

$$p_0^{(2)} = p_0^{(3)} + \frac{1}{3} p_1^{(3)}$$

$$p_1^{(2)} = \frac{2}{3} p_1^{(3)} + \frac{2}{3} p_2^{(3)}$$

$$p_2^{(2)} = \frac{1}{3} p_2^{(3)} + p_3^{(3)}$$

Adjusting for System Size

– Example: Mapping from m = 3 to m = 4

- Lethal shock: $p_3^{(3)} = p_4^{(4)}$

- Non-lethal shock:

$$p_1^{(4)} = \tfrac{4}{3}(1-\rho)\,p_1^{(3)}$$

$$p_2^{(4)} = \rho\,p_1^{(3)} + (1-\rho)\,p_2^{(3)}$$

$$p_3^{(4)} = \rho\,p_2^{(3)} + (1-\rho)\,p_3^{(3)}$$

$$p_4^{(4)} = \rho\,p_3^{(3)}$$

where $\rho \equiv$ conditional probability of a component's failure, given a non-lethal shock.

System Modeling Techniques for PRA

Lecture 8 – Quantification

Idaho National Laboratory

Objectives

- Understand the process of quantifying cut sets
- Understand value and limitations of different approximations
- Understand impact of correlation of data on quantification results

- Outline
  - Cut set definition
  - Approximations
  - Correlating failure rates

Cut Sets

- A *cut set* is a combination of events that cause the "top event" to occur

- Minimal cut set is the smallest combination of events that causes the top event to occur

- 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

Quantification of Cut Sets

- Three different quantification methods to quantify the probability of cut sets:
    - Exact Solution
    - Rare Event Approximation
    - Minimal Cut Set Upper Bound Approximation
        [also know as Min-Cut Approximation]

Quantification – Exact Solution

- Exact Solution for Cut Sets = A **OR** B:
  - $P(\text{Cut Sets}) = P(A + B) = P(A) + P(B) - P(AB)$
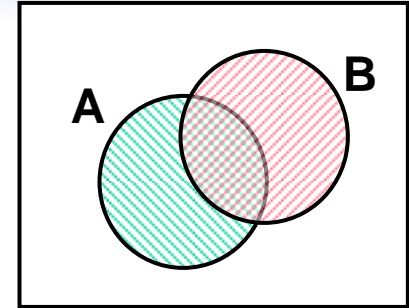
- Cross terms become unwieldy for large lists of cut sets
  For example; if Cut Sets = A **OR** B **OR** C, then:
  P(Cut Sets) =
  $P(A)+P(B)+P(C) - [P(AB)+P(AC)+P(BC)] + P(ABC)$

  Add the Singles   Subtract the Doubles   Add the Triples
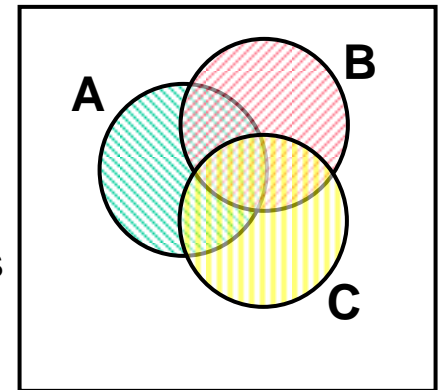
Quantification - Rare Event Approximation

- P(Cut Sets) ≈ sum of probabilities of each individual cut set
- P(Cut Sets) ≈ $\displaystyle\sum_{k=1}^{K} P(Cutset_k)$

  - Assumes cross term values are sufficiently small (rare) and thus are ignored (i.e., the cross-term values are simply left out)
  - P(Cut sets) quantified as if the cut sets are mutually exclusive
  - For Example; if Cut Sets = A OR B, then
    P(Cut Sets Rare Event) = P(A) + P(B)

- P(A AND B) judged sufficiently small (rare) and are ignored

- In general,
  P(Exact Solution) ≤ P(Rare Event)
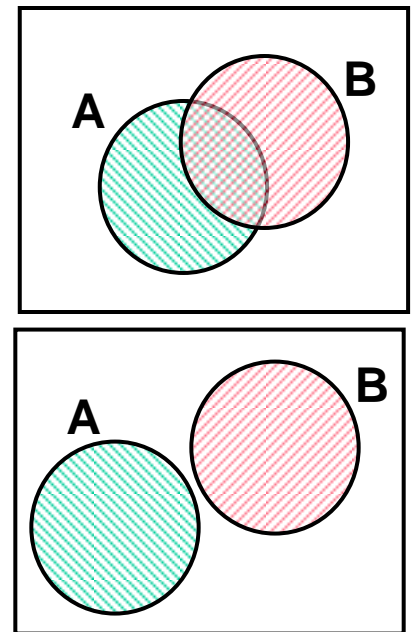
Quantification - Min-Cut Approximation

- P(Cut Sets) ≈ 1 – P(Complemented Cut Sets)

  - P(Minimal Cut Set Upper Bound for Cut Sets) = 1.0 minus the product of each individual cut set NOT occurring

  - P(MCSUB for Cut Sets) = $1 - \prod_{k=1}^{K}[1 - P(Cutset_k)]$

  - For Example; if Cut Sets = A OR B, then
    P(Cut Sets Min-Cut) = 1 - [(1 - P(A)) * (1 - P(B))]

- Assumption is that each cut set contains elements that are not shared in any other cut sets (i.e., each cut set is independent of all other cut sets)

- In general,
  P(Exact Solution) ≤ P(Min-Cut) ≤ P(Rare Event)

B=be3*be4

A=be1*be2
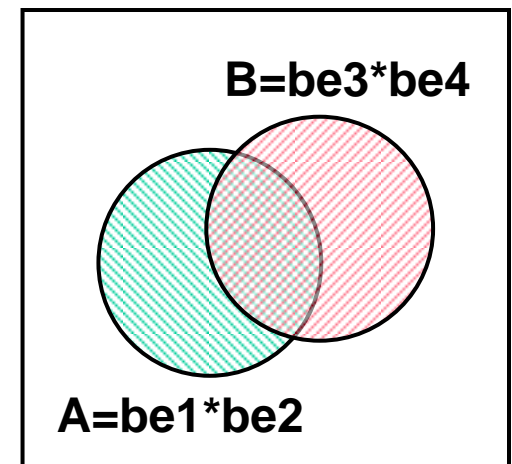
Examples of P(A+B) Quantification Methods for Cut Sets A OR B

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

Example Cut Sets - ECI
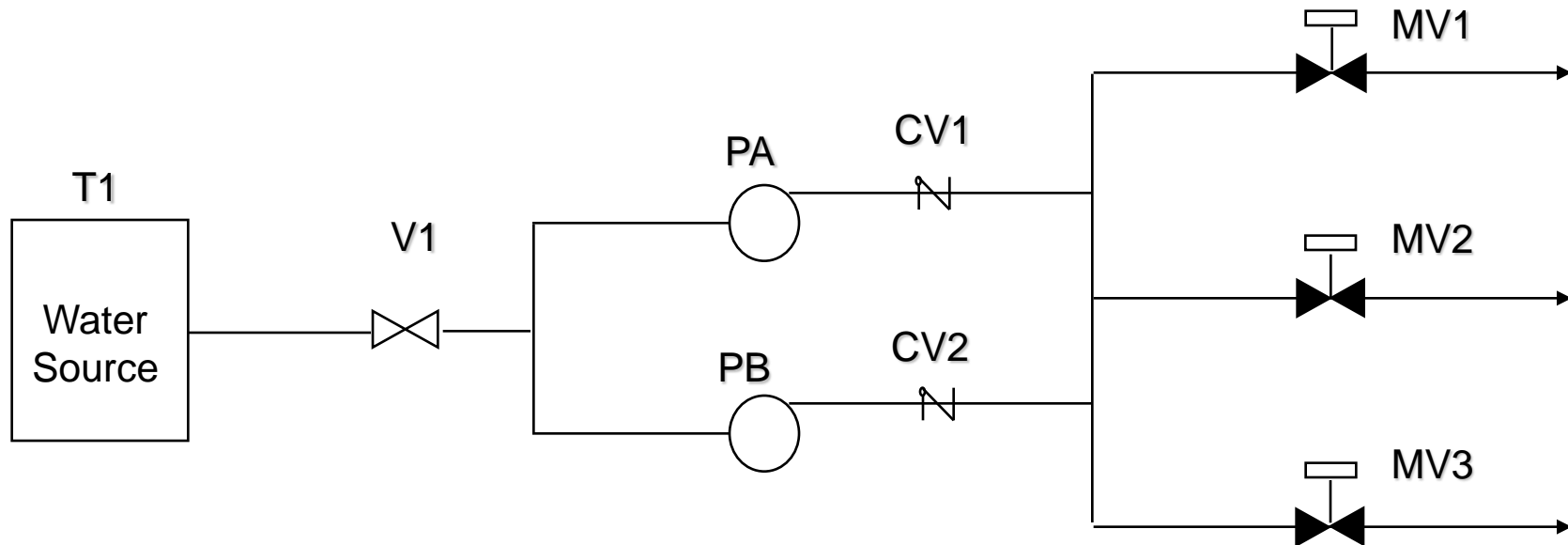
Success Criteria: *Flow from any one pump through any one MV*

T_   tank

V_   manual valve, normally open

PS-_   pipe segment

P_   pump

CV_   check valve

MV_   motor-operated valve, normally closed

9

ECI Component Failure Rates

T1 = 1E-6

V1 = 5E-5

PA = PB = 1E-2

CV1 = CV2 = 1E-4

MV1 = MV2 = MV3 = 3E-3

Cut Sets – Quantify

ECI-TOP =

  MV1 * MV2 * MV3 +

  PA * PB +

  PA * CV2 +

  CV1 * PB +

  CV1 * CV2 +

  V1 +

  T1

Point Estimates

- Point estimate calculation usually refers to mean values.
    - Result will be approximate mean value
    - For Lognormal distribution [mean > median]
        - mean/median = $\exp\{1/2[\ln(EF)/z]^2\}$
          (for example: EF = 10, 90% coverage:
          z = 1.645 and mean/median = 2.66)
    - e.g., for median = 1E-3 and EF = 10
      then
      mean = 1E-3 x 2.66 $\cong$ 3E-3 (factor of 3 greater than median)

Truncation Issues

- Becoming less of a concern as computer/software increase in capabilities

- Cut set order
  - Truncating on number of basic events in a cut set generally limited to vital area analyses

- Low probability events can accumulate
  - 1,000 cut sets at 1E-9 each = 1E-6
  - 10,000 cut sets at 1E-9 each = 1E-5

Truncation Issues

- Can affect importance analyses…number of basic events in results increases as truncation decreases
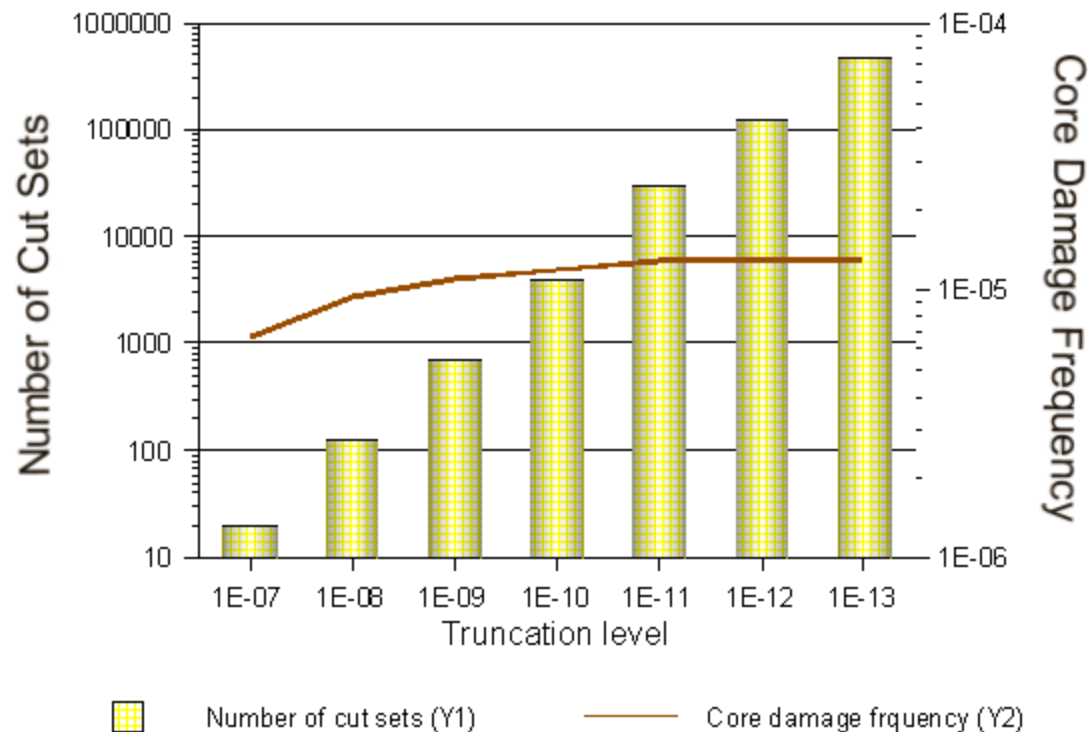
CDF and Number of Cut Sets Sensitive to Truncation Limits (PWR SPAR Model)
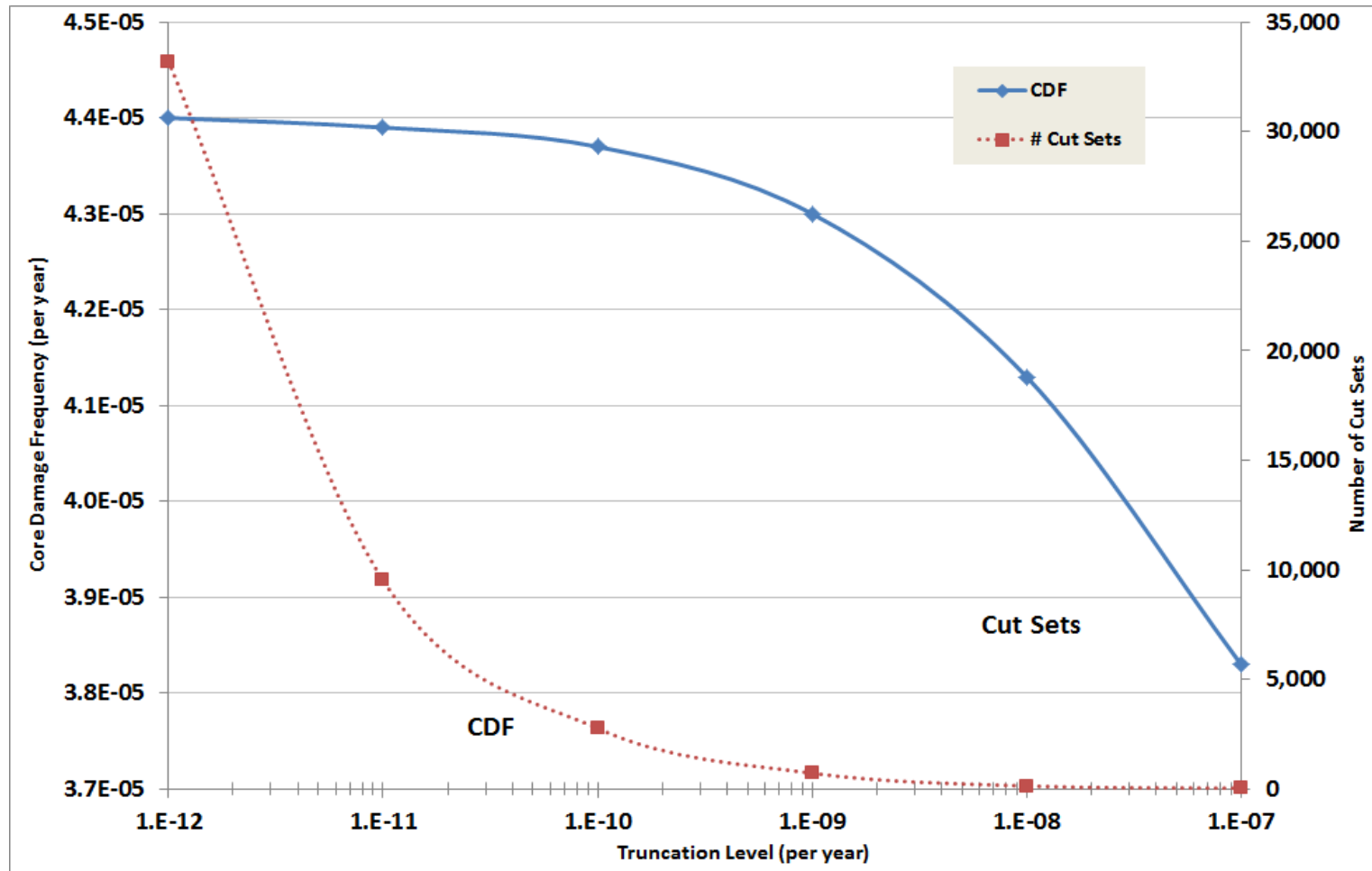
Correlating Data - Outline

- What are correlated data?
  - Implications on uncertainty results

- Combined (either explicitly or implicitly) data can be interpreted in different ways (depending on our assumed model)
  - Pooling data to estimate an average or mean occurrence rate
  - Models variability among similar individual components/events
  - Models variability among different component/event groups

What are Correlated Data?

- Only an issue when performing uncertainty analysis

- When quantifying a model, does the analyst assume
  - All similar (correlated) events occur at the same rate, or
  - Can occurrence rates vary among similar events?

- Specifically, when performing a simulation quantification (Monte Carlo or Latin Hypercube)
  - Should each simulation run pick a single value, which is applied to all similar events, or
  - Pick a different value for each event?

State of Knowledge Dependencies

- Some sources of dependence
  - Common design/manufacturer
  - Organizational factors (including testing and maintenance quality)
- Treatment (e.g., simple two component system)
  - Identical distributions, completely correlated sampling
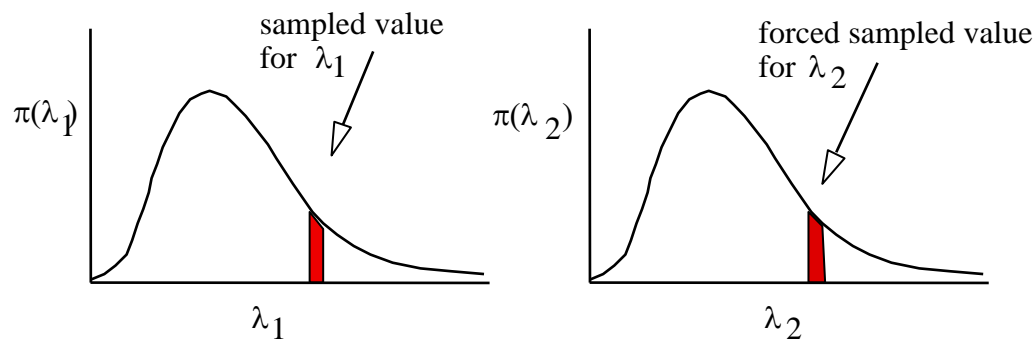
Effect on Results

- Correlating data produces wider uncertainty in results
  - Without correlating a randomly selected high value will usually be combined with randomly selected lower values (and vice versa), producing an averaging effect
    - Reducing calculated uncertainty in the result
  - Mean value of probability distributions that are skewed right (e.g. lognormal, commonly used in PRA) is increased when uncertainty is increased

Reference: Pitfalls of Risk Calculations, Reliability Engineering 2, 1981, pg. 135 – 145, Apostolakis and Kaplan

Correlating Failure Rates

- Important when uncertainties are included in analysis

- Mathematically…
    - $E(\lambda^2) \neq E(\lambda)^2$
    - $E(\lambda^2) = E(\lambda)^2 + Var(\lambda)$

- Simple example:
    - 2 valves, failure of both fails system
    - If $E(\lambda) = 1E-3$ (mean), EF = 10, and λ is lognormally distributed, then
    - $E(\lambda)^2 = (10^{-3})^2 = 1E-6$ (uncorrelated)
    - $E(\lambda^2) = (10^{-3})^2 + Var(\lambda) \cong 6E-6$ (correlated)

20

When Should Events Be Correlated?

- Issue illustrated with following example with four nominally identical components

Component	C_1	C_2	C_3	C_4
Failures	10	1	5	10
Demands	100	10	20	30

Probability Density Functions (PDFs)

22
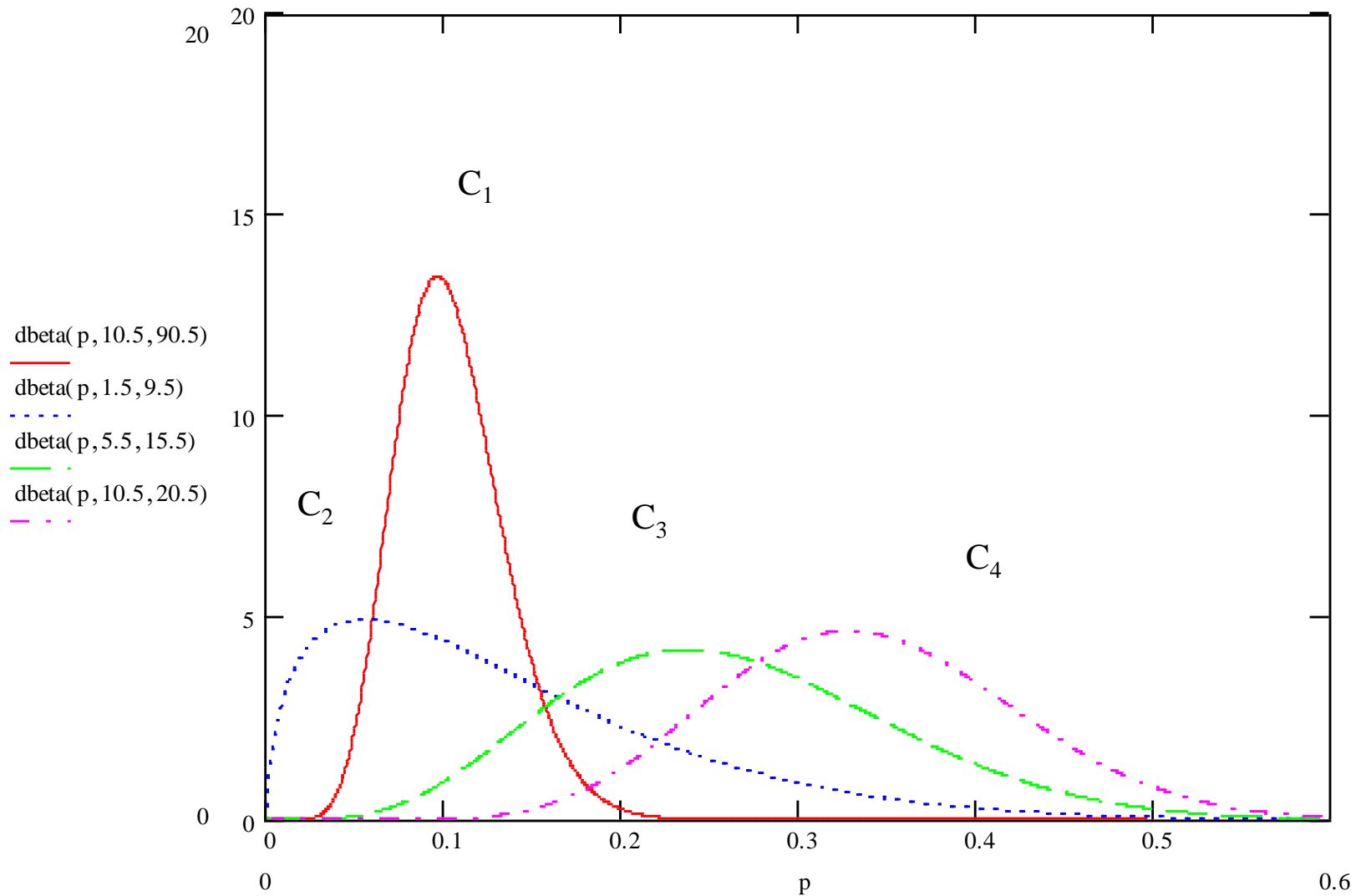
However - Common Situation is to "pool" data for like components

Component	C_1	C_2	C_3	C_4	Aggregate
Total Failures					26
Total Demands					160
Average Failure Probability					0.16

Pooled Data Only Provides an Estimate of the Average Probability

- $f_t / d_t = p_{ave}$

- Effectively, a weighted average of the failure probabilities for C_1, C_2, C_3 and C_4

- Uncertainty associated with p_{ave} represents our knowledge in estimate of p_{ave} (not variability in p_i's)

- More data reduces uncertainty in p_{ave}

Pooling Data Gives Reduced Uncertainty. But, Uncertainty Only Reflects Confidence in Our Estimate of Average Failure Rate.
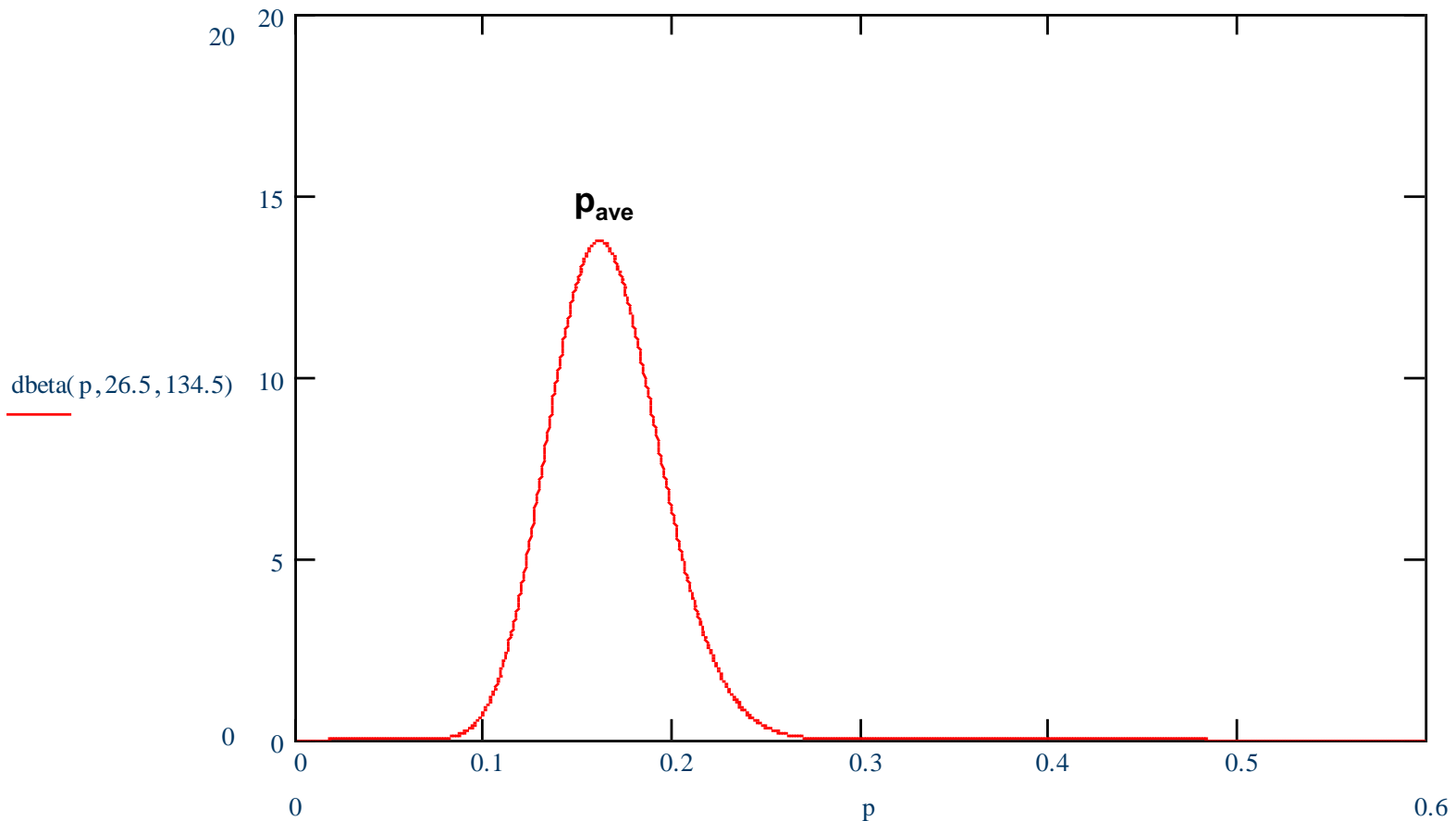
Pooled Data Implies Correlated Failure Rates

- Used to estimate a single parameter: p_{ave}

- Implies $p_1 = p_2 = p_3 = p_4 = p_{ave}$

- Assumed model based on existence of a single "true" value for p that describes performance of all similar components (i.e., the C_i's)

- Uncertainty a measure of knowledge in p_{ave} estimate
  - Therefore, failure rate estimates are correlated

Summing Distributions (Not Data) Captures Variability Among Possible Values of p
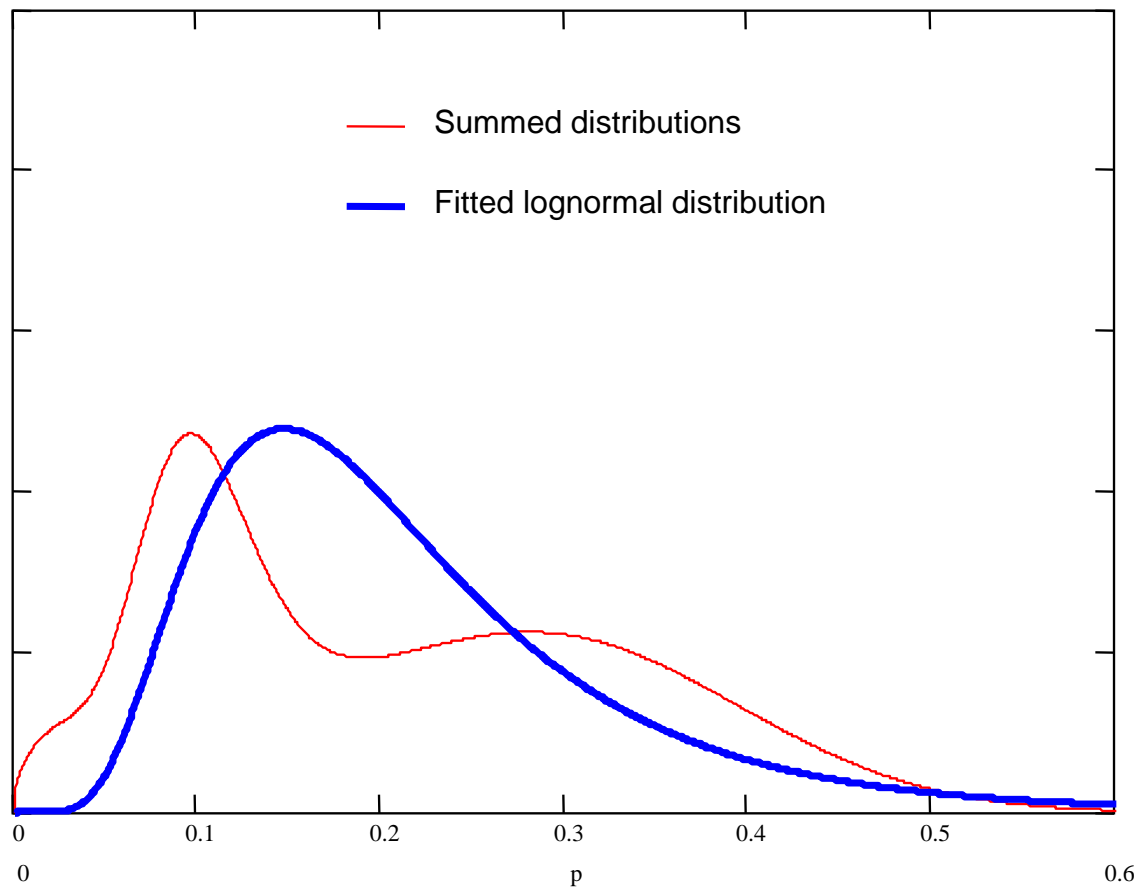
Should Not Correlate Samples From PDF That Models Variability

- Basic Premise: $p_1 \neq p_2 \neq p_3 \neq p_4 \neq p_{ave}$

- Uncertainty in distribution reflects variability in components operating conditions and environment

- Conditions at one component are NOT related to conditions at another component

- Failure rates are NOT correlated

Conclusion

- If PDF on input data reflects knowledge on an average value using pooled data, then should correlate

- If PDF on input data reflects variability or range of possible values, then should not correlate

- If PDF on input data reflects variability or range of groups of values (e.g., plant-to-plant variability), then should correlate (i.e., once a plant is selected the data should be consistent)

- Correlating failure events will generally produce higher system failure probabilities (and higher core damage frequencies)

System Modeling Techniques for PRA

Lecture 9 - Data Analysis

www.inl.gov

INL
Idaho National Laboratory

Objectives

- Understand the data requirements of a PRA, including:
  - Implications of modeling assumptions
    - Including Bayesian techniques
  - Potential pitfalls

- Outline
  - PRA Parameters
  - Bayesian Methods
  - Component Failure Rates
  - Component Failure Probability Models
  - Data/Quantification Issues

PRA Parameters

- Initiating Event Frequencies
- Basic Event Probabilities
  - Hardware
    - component unreliability (fail to start/run/operate/etc.)
    - component unavailability (test or maintenance)
  - Human Errors (discussed later)
  - Common Cause Failures (already discussed)

Initiating Events (for NPP PRAs)

- Typically, only parameter in PRA that is quantified as a frequency
  - General Transients
    - with and without main feedwater
  - LOCAs
    - pipe breaks and stuck open PORVs and SRVs
  - Containment Bypass Event
    - SGTRs and ISLOCAs
  - Support System Failures
    - ac & dc power, SWS, CCW, instrument air

Initiating Event Data

- Typically combination of:
  - Generic data for rare events (e.g., LOCAs)
  - Plant-specific data for more common events (most transients)
- NUREG/CR-5750
  - Contains both plant-specific and industry-wide estimates
  - Three versions available
    - Original: Feb. 1999 (1987-1995)
    - Draft update issued: Mar. 2000 (1987-1998)
    - Electronic data and results updated through 2010
      - http://nrcoe.inel.gov/results/
- NUREG/CR-6928 (January 2007) contains industry-average rates for initiating events and components (used in SPAR models).

Non-IE Basic Events are Probabilities

- Probability of failure depends on the failure rate (i.e., the λ or p) and the mission time
  - Typically modeled as either Poisson or Binomial
  - Unavailability (e.g., T&M) calculated directly as a probability
    - However, T&M unavailability can be estimated as an unreliability (like binomial) as well
- Key feature (of data) is that the set of failure events and set of demands (or time) must be consistent with each other

Component Failure Rate Estimates

- Point Estimate
  - Demand Failures, Q_d(1 demand) $= \hat{\phi} = f/d$
    - f = total number of demand failures
    - d = total number of demands
  - Time related failures
    - Running failure rate, $\hat{\lambda}_r = f_r/t_r$
      - f_r = total number run failures
      - t_r = total number run hours
    - Standby failure rate, $\hat{\lambda}_s = f_s/t_s$
      - f_s = total number standby failures
      - t_s = total number hours in standby
  - Unavailability due to T or M (both scheduled and unscheduled), $Q_{TM} = t_d/t_t$ = down-time/total-time = time out of service/total-time
  - Probability distribution (density functions) on λ's generated using Bayesian methods

Failure Probability Models

- Demand Failures
  - Binomial: prob(r failures in n demands)
    $$= \binom{n}{r} p^r (1-p)^{n-r}$$
    prob(1 failure|1 demand) = p = Q_d

- Failures in Time
  - Poisson: prob(r failures in time t) = $\dfrac{(\lambda t)^r e^{-\lambda t}}{r!}$

    prob(r >0, in time t) = $1-e^{-\lambda t} \approx \lambda t$ (for $\lambda t < 0.1$)

$\binom{n}{r}$ = n!/(r!(n-r)!) = number of ways n items can be grouped r at a time

Bayesian Methods Employed to Generate Uncertainty Distributions

- Two motivations for using Bayesian techniques
  - Generate probability distributions (classical methods generally only produce uncertainty intervals, not pdf's)
  - Compensate for sparse data (e.g., no failures)
- In effect, Bayesian techniques combine an initial estimate (prior) with plant-specific data (likelihood function) to produce a final estimate (posterior)
- However, Bayesian techniques rely on (and incorporate) subjective judgement
  - different options for choice of prior distribution (i.e., the starting point in a Bayesian calculation)

Bayesian Technique Starts With Subjective Judgment

- Prior represents one's belief about a parameter before any data have been "observed"

- Prior can be either informative or non-informative
  - Three common priors
    - Non-informative (Jeffreys) prior
    - Informative prior (e.g., generic data)
    - Constrained non-informative prior

Non-Informative Prior

- Imparts little prior belief or information
- Minimal influence on posterior distribution
  - Except when updating with very sparse data
- Basically assumes 1/2 of a failure in one demand (for binomial, or in zero time for a Poisson process)
  - If update data is very sparse, mean of posterior will be pulled to 0.5

E.g.: for plant-specific data of 0/10 (failures/demands)

Update=> 0.5/1 (prior) + 0/10 (likelihood) => 0.5/11 (posterior)

Informative Prior

- Maximum utilization of <u>all</u> available data

- Prior usually based on generic or industry-wide data

- Avoids potential conservatism that can result from use of non-informative prior

- However, good plant-specific data can be overwhelmed by a large generic data set

  e.g., prior = 100/10000 (failures/demands) = 1E-2

          plant-specific = 50/100 (failures/demands) = 0.5

          posterior = 150/10100 = 1.5E-2 (basically the prior)

Constrained Non-informative Prior

- Combines certain aspects of informative and non-informative priors
  - Weights the prior as a non-informative (i.e., 1/2 of a failure)
  - However, constrains the mean value of the prior to some generic-data based value

- For example - generic estimate of previous example would be "converted" to a non-informative prior

  100/10000 => 0.5/50 (this then used as the prior)

  Update=> 0.5/50 + 50/100 => 50.5/150 = 0.34

Other Update Methods and Priors Exist

- For Example:
    Empirical Bayes Method
    Hierarchical Bayes Method
    "Two-Stage" Bayesian Method
    Maximum entropy priors
    Non-Conjugate priors

System Modeling Techniques for PRA

Lecture 10 - Overview of Human Reliability Analysis for PRA

www.inl.gov

iNL
Idaho National
Laboratory

Objectives

- Understand Human Reliability Analysis (HRA) as an input to PRA
- Understand basic philosophies and techniques in HRA modeling

- Outline
  - HRA Process
  - Performance Shaping Factors
  - Human Error Categorization and Quantification
  - HRA modeling concerns

Human Reliability Analysis

- Objective
  - Provide input to PRA regarding likelihood of human failure events
- PRA-Based Classification of Human Error (HE)
  - Pre-initiator (latent)
  - Initiating event
  - Post-initiator (dynamic)
  - Recovery
- Contribution from some HE's already accounted for in hardware failure data
  - Typically PRA only includes:
    - Post-initiator actions (i.e., operator responses guided by emergency operating procedures)
    - Recovery actions

HRA Process

- Identify relevant human actions/errors
  - Necessary actions
  - Responses to situation
- Identify influences that affect human performance (both positively and negatively)
  - Stress, time available, training, etc.
- Quantify human error probability
  - Various techniques available

Human Error Identification

- Two basic roles modeled in PRA
  - Human as an integral part of plant response
  - Human as the "fixer" of failures
- Sometimes include human as the *source* of failures
  - Very problematic – how to identify all the mistakes the human operator might make?
- Two general types of human errors
  - Errors of Omission (EOO)
    - Operator fails to accomplish a needed action
  - Errors of Commission (EOC)
    - Operator successfully accomplishes an incorrect action
    - Sometimes segregated into cognitive and non-cognitive EOCs
      - Was it the operators intention to perform the (incorrect) action?

Typical Roles Modeled in PRA

- Human as integral part of system
  - Basically, procedure follower
    - "Operator fails to perform required action"
    - Errors of omission

- Human as performer of recovery action
  - "Operator fails to manually initiate injection given failure of automatic actuation"
  - Errors of omission

- Errors of commission seldom modeled
  - Lack of basis for postulating a specific EOC
  - Potential number of EOCs virtually unlimited
    - How do you identify all the inappropriate actions a person might do?

Influences on Human Performance

- Circumstances that might enhance or reduce the likelihood of a human error

- What specific aspect of event context mostly affect the likelihood of the human error
  – General environment
    • Safety culture, training, job aids, etc.
  – Individual/team
    • Education, aptitude, cooperation, etc.
  – Specific situation
    • Procedures, instrumentation, task aids, etc.

- Referred to as: Performance Shaping Factors (PSFs)

- Every Human Reliability Analysis technique has it's own unique list

Common HRA Methods

- Technique for Human Error Rate Prediction (THERP)

- Accident Sequence Evaluation Program (ASEP) HRA Procedure

- Human Cognitive Reliability (HCR)/Operator Reliability Experiments (ORE) Method

- Cause-Based Decision Tree (CBDT) Method

- Electric Power Research Institute (EPRI) HRA Calculator®

- Standard Plant Analysis Risk HRA (SPAR-H) Method

- A Technique for Human Event Analysis (ATHEANA)

- Success Likelihood Index Methodology (SLIM) Multi-Attribute Utility Decomposition (MAUD)

- Failure Likelihood Index Methodology (FLIM)

- A Revised Systematic Human Action Reliability Procedure (SHARP1)

Timeline of HRA Methods

CD's First Released — Return of Halley's Comet — Hubble Telescope Launched — Existence of Black Holes Proven — Olympic Games Atlanta — First Balloon Trip Around the World — Today

| 1983 | 1986 | 1990 | 1994 | 1996 | 1999 | 2013 |

ASEP (1987) Simplified THERP

ASP/SPAR (1994)

ATHEANA (1996)

ATHEANA (Rev.1 2000)

SPAR-H (2005)

HEART (1986)

CREAM (1998)

NARA (2004)

SHARP (1984) HRA Framework

SHARP1 (1991) Revised Framework

CAHR (1999)

HCR (1984) First HCR

ORE (1989) Operator Reliability Experiments

CBDTM (1992) Cause-Based Decision Trees

MERMOS (1998)

EPRI (2000) HRA Users Group

SLIM-MAUD (1984)

PSFs Used in ATHEANA

1. Applicability and Suitability of Training/Experience
2. Suitability of Relevant Procedures and Administrative Controls
3. Operator Action Tendencies and Informal Rules
4. Availability and Clarity of Instrumentation (Cues to Take Actions and Confirm Expected Plant Response)
5. Time Available and Time Required to Complete the Act, Including the Impact of Concurrent and Competing Activities
6. Complexity of the Required Diagnosis and Response, the Need for Special Sequencing, and the Familiarity of the Situation
7. Workload, Time Pressure, and Stress
8. Team/Crew Dynamics and Crew Characteristics [Degree of Independence Among Individuals, Operator Attitudes/Biases/Rules, Use of Status Checks, Approach for Implementing Procedures (e.g., Aggressive Crew vs. Slow/Methodical Crew)]
9. Available Staffing/Resources
10. Ergonomic Quality of the Human-System Interface (HSI)
11. Environment in Which the Action Needs To Be Performed
12. Accessibility and Operability of the Equipment To Be Manipulated
13. Need for Special Tools (Keys, Ladders, Hoses, Clothing Such as To Enter a Radiation Area)
14. Communications Strategy and Coordination, and Whether One Can Be Easily Heard
15. Special Fitness Needs
16. Realistic Accident Sequence Diversions and Deviations (e.g., Extraneous Alarms, Outside Discussions, or Sequence Evolution Not Exactly Like That on Which Operators Are Trained)

Quantification -Two Levels

- Conservative (screening) level useful for determining which human errors are most significant contributors to overall system error

- Those found to be potentially significant contributors can be analyzed in greater detail (which often lowers the HEP)
  - These revised HEP are then put back into the PRA

Different Techniques View Human Errors Differently

- Classification Approaches
    - Omission/Commission
    - Skill/Rule/Knowledge
    - Slip/Lapse/Mistake/Circumvention

- Decomposition Approaches
    - None (e.g., Time-Based Methods)
    - Functional (e.g., detection/diagnosis/decision and action)
    - Task-based

Estimating Human Error Probability (HEP)

- Classification of Human Error provides starting point for quantification
  - Typically, HRA method provides a library of Base Human Error Probabilities (BHEPs)
- BHEP is then modified to include effects of PSFs
  - Each PSF evaluated to determine effects on estimated HEP
  - HRA method will provide guidance on how to scale BHEPs to produce final HEP

Example Classification Scheme

		Action Type		
		Skill	Knowledge	Rule
Error Type	Omission			
	Commission (Cognitive)			
	Commission (Non-Cognitive)			

Directory of THERP Tables for Quantification of Human Errors (NUREG/CR-1278)

Figure 20-2

Screening
- Diagnosis [1]
- Rule-Based Actions [2]

Diagnosis
- Nominal Diagnosis [3]
- Postevent CR Staffing [4]

Errors of Omission
- Written Materials Mandated
  - Preparation [5]
  - Administrative Control [6]
  - Procedural Items [7]
- No Written Materials
  - Administrative Control [6]
  - Oral Instruction Items [8]

Errors of Commission
- Displays
  - Display Selection [9]
  - Read/Record Quantitative [10]
  - Check-Read Quantitative [11]
- Control & MOV Selection & Use [12]
- Locally Operated Valves
  - Valve Selection [13]
  - Stuck Valve Detection [14]

PSFs
- Tagging Levels [15]
- Stress/Experience [16]
- Dependence [17] [18] [19]
- Other PSFs (see text)

Uncertainty Bounds
- Estimate UCBs [20]
- Conditional HEPs and UCBs [21]

Recovery Factors
- Errors by Checker [22]
- Annunciated Cues [23] [24]
- Control Room Scanning [25] [26]
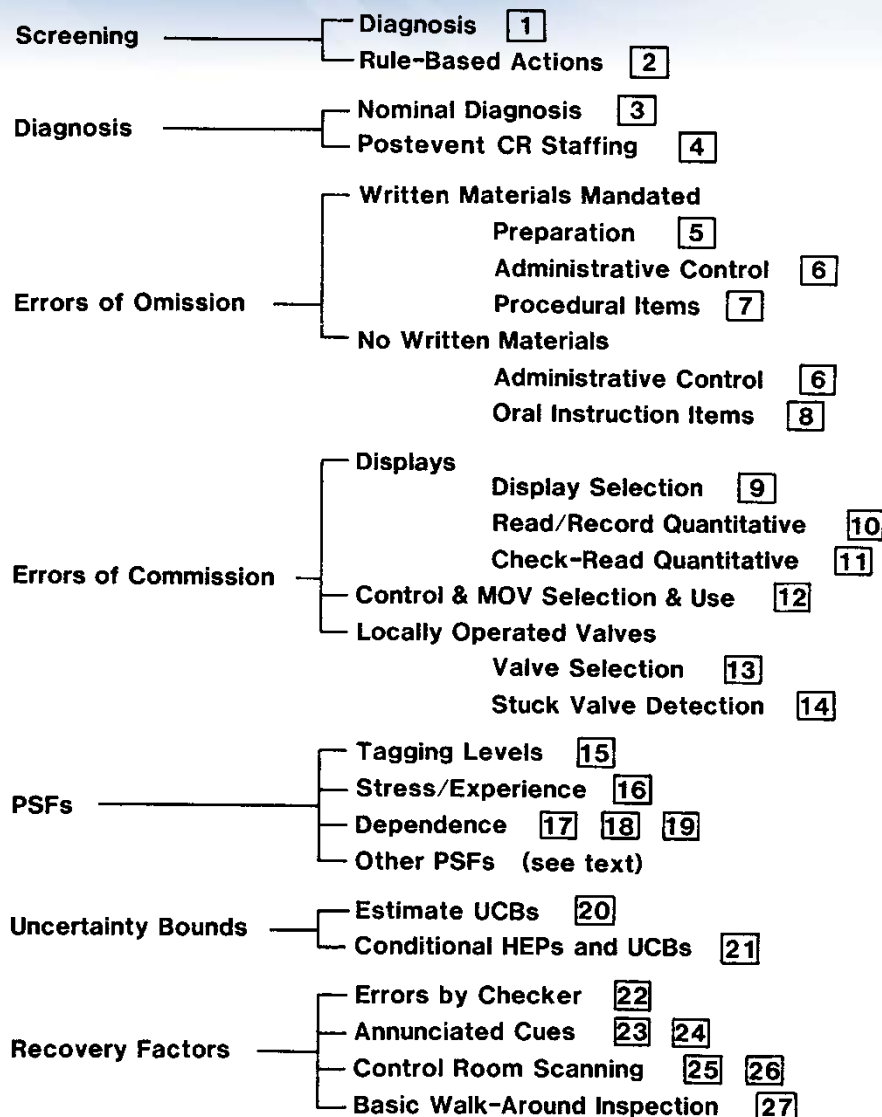- Basic Walk-Around Inspection [27]

Figure 20-2 Quick reference guide to Chapter 20 tables.

15

Example THERP Table

(Procedural Items - 7)

Table 20-7 Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified* (from Table 15-3)

Item**	Omission of item:	HEP	EF
	When procedures with checkoff provisions are correctly used[†]:		
(1)	Short list, ≤10 items	.001	3
(2)	Long list, >10 items	.003	3
	When procedures without checkoff provisions are used, or when checkoff provisions are incorrectly used[††]:		
(3)	Short list, ≤10 items	.003	3
(4)	Long list, >10 items	.01	3
(5)	When written procedures are available and should be used but are not used[††]	.05[‡]	5

*The estimates for each item (or perceptual unit) presume zero dependence among the items (or units) and must be modified by using the dependence model when a nonzero level of dependence is assumed.

**The term "item" for this column is the usual designator for tabled entries and does <u>not</u> refer to an item of instruction in a procedure.

[†]Correct use of checkoff provisions is assumed for items in which written entries such as numerical values are required of the user.

[††]Table 20-6 lists the estimated probabilities of incorrect use of checkoff provisions and of nonuse of available written procedures.

[‡]If the task is judged to be "second nature," use the lower uncertainty bound for .05, i.e., use .01 (EF = 5).

HCR Model Categorizes Actions as Knowledge, Rule or Skill Based

![INL Idaho National Laboratory]
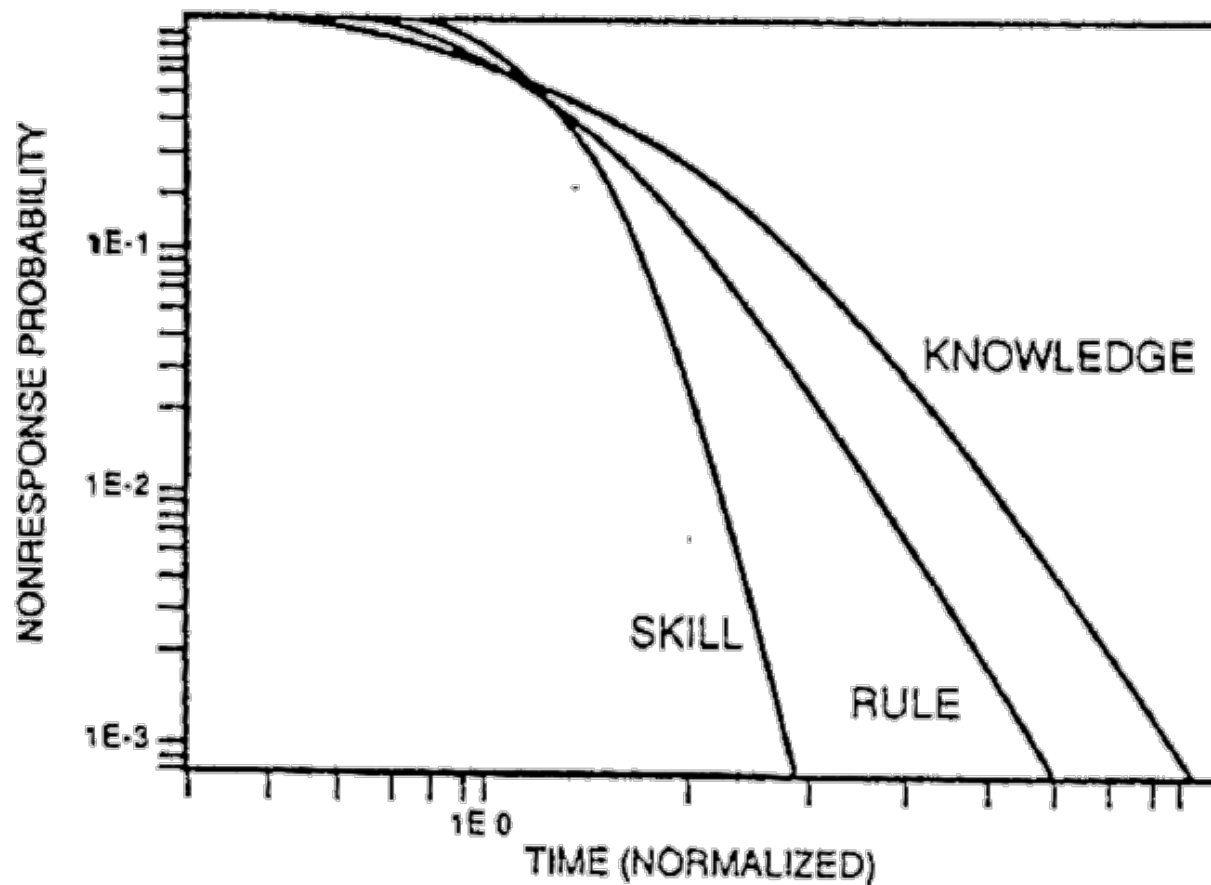
SPAR-H (NUREG/CR-6883)

- The SPAR HRA, or SPAR-H, method was developed at the INL to support the NRC

- SPAR-H is a simplified approach based on THERP
  - HEPs in SPAR-H derived from THERP
  - Approach uses performance shaping factors (PSFs) instead of sample scenarios, making it easier to generalize

- Base HEP for SPAR-H is:
  - Diagnosis = nominal value of 1.0E-2
  - Action = nominal value of 1.0E-3

SPAR-H Quantification

- SPAR-H Worksheets are used to quantify HEPs by considering factors (PSFs) that may increase/decrease likelihood of error

  - Available time
  - Complexity
  - Procedures
  - Fitness for duty
  - Stress/stressors
  - Experience/training
  - Ergonomics/HMI
  - Work Processes

Example: Available Time

- *inadequate time → p(failure)* = 1.0

- *barely adequate time → p(failure)* = HEP x 10

- *nominal time → p(failure)* = HEP x 1

- *extra time → p(failure)* = HEP x 0.1

- *expansive time → p(failure)* = HEP x 0.01

HRA Modeling Concerns

- HRA is intended to be a prospective analysis aimed at predicting the occurrence and likelihood of human errors during some possible future event
    - Unlike hardware failures, which are statistically quantified, human errors are modeled "contextually"
        - Context is characterized, then the probability is estimated (typically using engineering judgment)
    - How well can the context for some future potential accident be characterized?
    - What are all the influences (PSFs) that might (will?) affect the performance of the operator?

HRA Modeling Concerns (cont.)

- HRA data is very limited
  - Little experience data available
  - THERP is based on 1960's data from assembling nuclear weapons
  - HCR based on simulator experiments
    - Operators are expecting something to happen
    - Would operators really perform the same in an actual emergency situation?

System Modeling Techniques for PRA

Lecture 11 - Risk Assessment Results

INL
Idaho National
Laboratory

Objectives

- Be able to understand typical PRA results

- Understand value and limitations of importance factors

- Outline
  - Dominant Contributors
  - Importance Measures

Sample Summary Level 1 Results

Plant	Study Sponsor	Method	No. of Dominant Sequences	%CDF
Beaver Valley 2	Utility	ET/BC	12	42
Brunswick 1	Utility	Linked FT	10	95
Brunswick 2	Utility	Linked FT	10	95
Dresden	Utility	ET/BC	10	95
Farley	Utility	ET/BC	19	35
FitzPatrick	Utility	ET/BC	9	87
Grand Gulf	USNRC	Linked FT	3	96
La Salle	USNRC	Linked FT	5	95
Oyster Creek	Utility	ET/BC	10	51
Peach Bottom	USNRC	Linked FT	11	95
Sequoyah	USNRC	Linked FT	15	95
Surry	USNRC	Linked FT	20	95
Zion	USNRC	ET/BC	13	95

Sample Summary Level 1 Results

Surry (NUREG-1150)
Westinghouse PWR

Seq	Description	% CDF	Cum
1	Station Blackout (SBO) - Batt Depl.	26.0	26.0
2	SBO - RCP Seal LOCA	13.1	39.1
3	SBO - AFW Failure	11.6	50.7
4	SBO - RCP Seal LOCA	8.2	58.9
5	SBO - Stuck Open PORV	5.4	64.3
6	Medium LOCA - Recirc Failure	4.2	68.5
7	Interfacing LOCA	4.0	72.5
8	SGTR - No Depress - SG Integ'ty Fails	3.5	76.0
9	Loss of MFW/AFW - Feed & Bleed Fail	2.4	78.4
10	Medium LOCA - Injection Failure	2.1	80.5
11	ATWS - Unfavorable Mod. Temp Coeff.	2.0	82.5
12	Large LOCA - Recirculation Failure	1.8	84.3
13	Medium LOCA - Injection Failure	1.7	86.0
14	SBO - AFW Failure	1.6	87.6
15	Large LOCA - Accumulator Failure	1.6	89.2
16	ATWS - Emergency Boration Failure	1.6	90.8
17	Very Small LOCA - Injection Failure	1.5	92.3
18	Small LOCA - Injection Failure	1.1	93.4
19	SBO - Battery Depletion	1.1	94.5
20	SBO - Stuck Open PORV	0.8	95.3

Grand Gulf (NUREG-1150)
BWR

Seq	Description	% CDF	Cum
1	Station Blackout (SBO) With HPCS And RCIC Failure	89.0	89.0
2	SBO With One SORV, HPCS And RCIC Failure	4.0	93.0
3	ATWS - RPS Mechanical Failure With MSIVs Closed, Operator Fails To Initiate SLC, HPCS Fails And Operator Fails To Depressurize	3.0	96.0

Dominant Contributors

- Implications
  - Typically small number of scenarios
  - Can concentrate on a small number of issues
  - As outliers are addressed, more scenarios become the "important" contributors
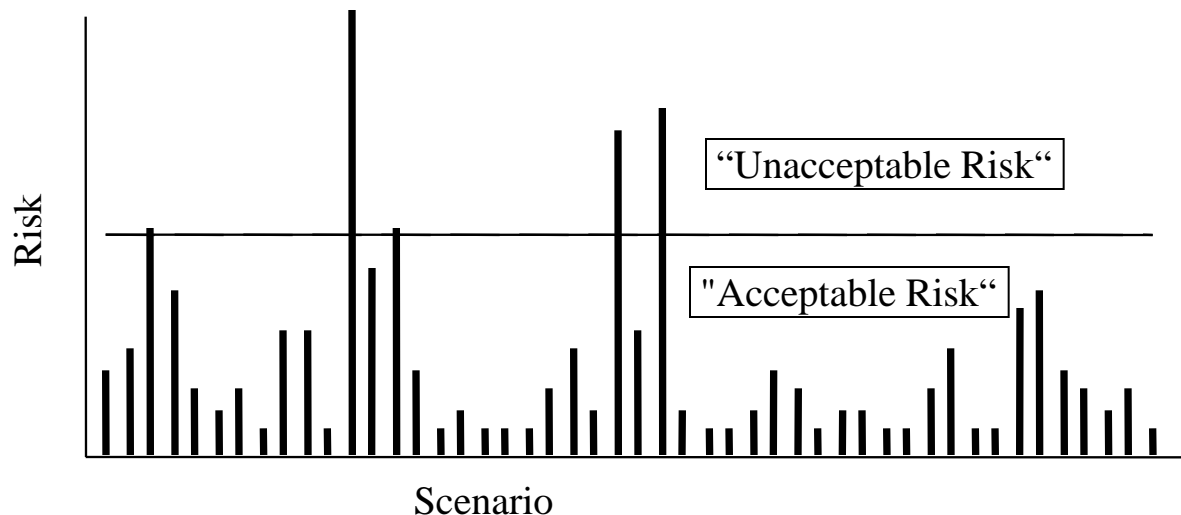
Dominant Contributors

- Contributors to risk can be identified at many levels
  - Initiating events (e.g., LOCA)
    - Sum of all CD sequences with particular IE
  - Accident sequences (e.g., S5 = LOCA * AUTO * /MAN * /ECI * ECR)
  - Minimal cut sets (e.g., ECI = PS-A * PS-B)
  - Failure causes (e.g., CCF of PS-A and PS-B)

What are Importance Measures

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

Importance Measures

- Provide quantitative perspective on dominant contributors to risk and sensitivity of risk to changes in input values

- Usually calculated at core damage frequency level

- Common importance measures include:
  - Fussell-Vesely
  - Risk Reduction or Risk Reduction Worth
  - Risk Increase or Risk Achievement Worth (RAW)
  - Birnbaum

Fussell-Vesely (FV)

- Measures the overall percent contribution of cut sets containing a basic event of interest to the total risk

- Calculated by finding the value of cut sets that contain the basic event of interest (x_i) and dividing by the value of all cut sets representing the total risk

    $FVx_i = F(i) / F(x)$

    or alternate equations

    $FVx_i = [F(x) - F(0)] / F(x) = 1 - F(0) / F(x) = 1 - 1/RRRx_i$

    where,

    - $F(x)$ is the total risk from all cut sets with all basic events at their nominal input value

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

    - $F(0)$ is the total risk from all cut sets with basic event of interest (x_i) set to 0

- The FV range is from 0 to 1 (0% to 100%)
    - Example: If a basic event such as check valve A (CVA) appears in minimal cut sets contributing 2×10^{-6} to CDF and the total CDF from all minimal cut sets is 1×10^{-5}, then the $FV_{CVA} = (2 \times 10^{-6})/(1 \times 10^{-5}) = 0.2$ (20%)

Risk Reduction Importance (Risk Reduction Worth)

- Measures the amount that the total risk would decrease if a basic event's input value were 0 (i.e., never fails)

- Calculated as either ratio or difference between the value of all cut sets representing the total risk with all basic events at their nominal input value and the value of the total risk with the basic event of interest (x_i) set to 0
    - Ratio: $RRRx_i = F(x) / F(0)$
    - Difference (or Interval): $RRIx_i = F(x) - F(0)$
        where,
    - $F(x)$ is the total risk from all cut sets with all basic events at their nominal input value
    - $F(0)$ is the total risk from all cut set with basic event of interest (xi) set to 0

- The Risk Reduction Ratio range is from 1 to ∞

- Risk Reduction gives the same ranking as Fussell-Vesely

- For Maintenance Rule (10 CFR 50.65), NUMARC Guide 93-01 (endorsed by NRC) uses a RRR significance criterion of 1.005 (which is equivalent to Fussell-Vesely importance of 0.005)
    - Example: If a basic event such as check valve A (CVA) results in a CDF of $3{\times}10^{-6}$ when not failed and total CDF from all minimal cut sets is $1{\times}10^{-5}$, then the $RRRCVA= (1{\times}10^{-5})/(3{\times}10^{-6}) = 3.33$

Risk Increase Importance (Risk Achievement Worth)

- Measures the amount that the total risk would increase if a basic event's input value were 1 (e.g., component is failed or taken out of service)

- Calculated as either ratio or difference between the value of the total risk with the basic event of interest (xi) set to 1 and the total risk with all basic events at their nominal input value
  - Ratio: $RAWx_i$ or $RIRx_i = F(1) / F(x)$
  - Difference (or Interval): $RIIx_i = F(1) - F(x)$
    where,
  - $F(x)$ is the total risk from all cut sets with all basic events at their nominal input value
  - $F(1)$ is the total risk with basic event of interest (x_i) set to 1

- Ratio measure referred to as Risk Achievement Worth (RAW)

- The 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
  - Example: If a basic event such as check valve A (CVA) results in a CDF of 2×10^{-5} when failed and the total CDF from all minimal cut sets is 1×10^{-5}, then the $RAW_{CVA} = (2\times10^{-5})/(1\times10^{-5}) = 2$

Birnbaum (B)

- Measures the rate of change in total risk as a result of changes to the input value of an individual basic event

- Ranks events according to the effect they produce on the risk level when they are modified from their nominal values
    - $B_x = \partial F(x) / \partial x$

        where,
    - $F(x)$ is the total risk from all cut sets with all basic events at their nominal input value
    - $\partial/\partial x$ is the first derivative of the risk expression with respect to the basic event of interest (x_i)

- When the risk expression has a linear form
    - $B_{xi} = F(1) - F(0)$

        where,
    - $F(1)$ is the total risk with basic event of interest (x_i) set to 1
    - $F(0)$ is the total risk from all cut set with basic event of interest (x_i) set to 0

- The B range is between 0 and the cumulative initiating event frequency (i.e., B = 0 indicates little risk sensitivity and B = cumulative initiating event frequency indicates large risk sensitivity)
    - Example: If a basic event such as check valve A (CVA) results in a CDF of 3×10^{-6} when not failed and results in a CDF of 2×10^{-5} when failed, then the $B_{CVA} = (2\times10^{-5}) - (3\times10^{-6}) = 1.7\times10^{-5}$

Application Notes

- Relations between measures
  - $FV = 1 - 1/RRR_i$
  - $Br_i \cong F_i(1) = F(x) + RII_i$
    [if $F_i(0) << F_i(1)$]

- Measures can be computed for systems and components as well as basic events
  - Concerns about how to computationally generate these (i.e., importance measures generally do not "add" due to overlap between cut sets)

Application Notes (cont.)

- Cautions
  - Improper/misleading labeling of basic events
  - Exclusion of components not in model (e.g., passive components)
  - Parameter values used for other events in model
    - Inconsistent levels of conservatism among BE probabilities can skew ranking
  - Present configuration of plant (equipment that is already out for test/maintenance)
  - Model truncation during quantification and the affect on Birnbaum and RAW

Core Damage Frequency and Number of Cut Sets Sensitive to Truncation Limits
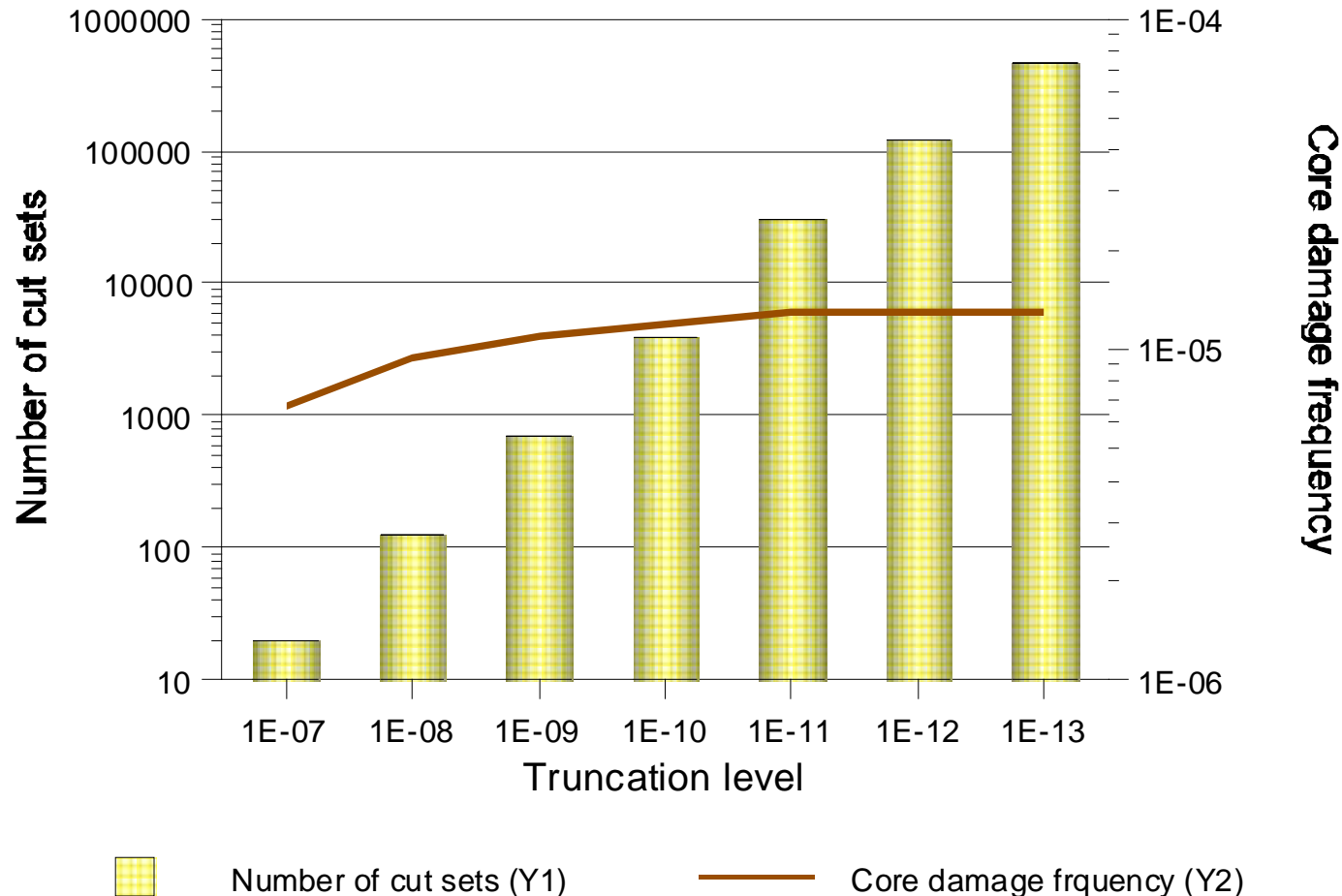
Truncation Limits Affect Importance Rankings
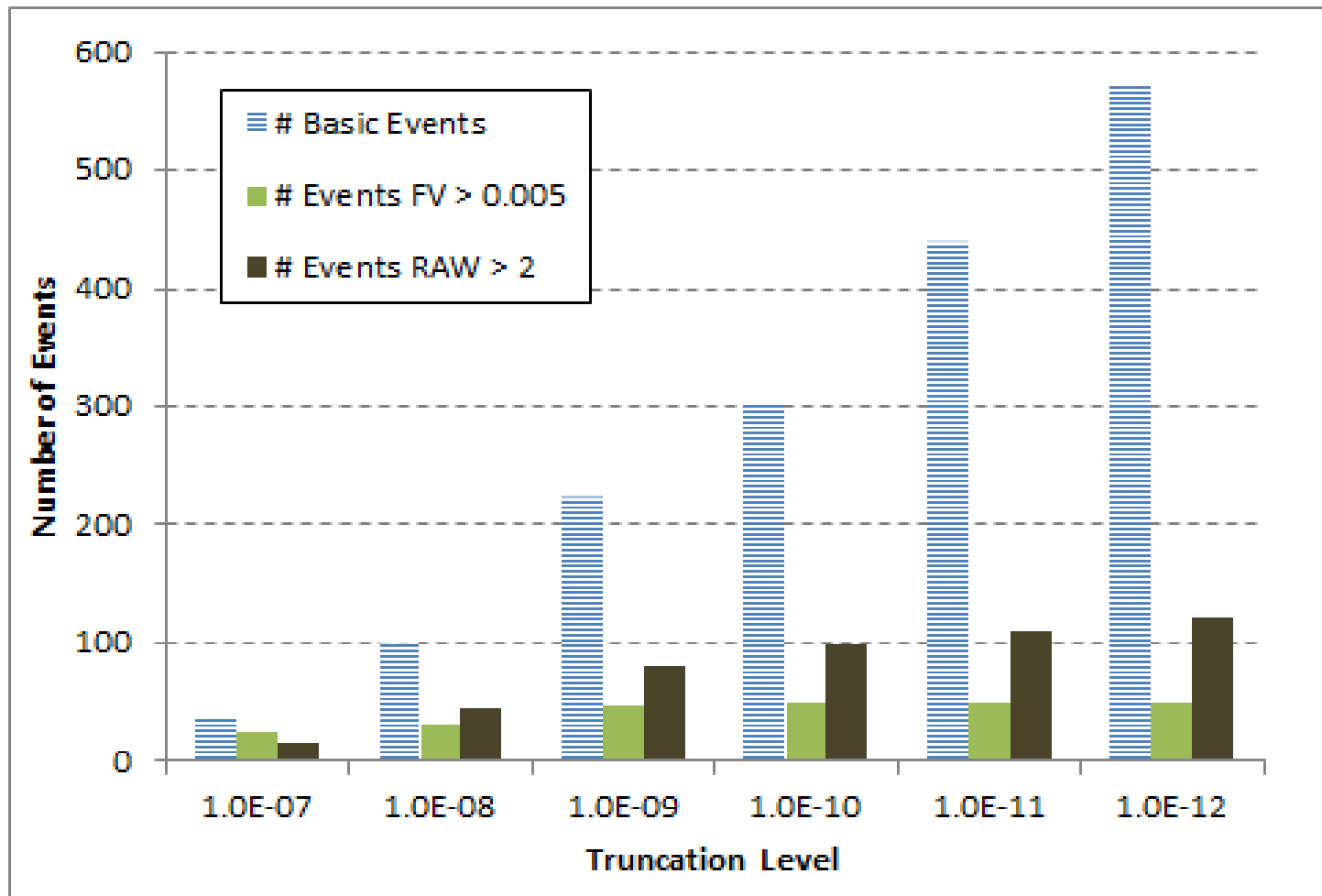
System Modeling Techniques for PRA

Lecture 12 - Special Topics

www.inl.gov

INL
Idaho National
Laboratory

Objectives

- General understanding of special topics and issues associated with PRA

- Outline
  - Recovery Analysis
  - Level 2 and Level 3
  - Aging
  - External Events

Recovery Analysis Required for Realistic Estimate of Risk

- Options are typically available to control room operators for recovering from component/system failures
  - Manually actuating equipment
  - Re-aligning flow around failed equipment
  - Cross-tie systems from "other" unit
  - Utilizing non-safety grade equipment
- Typically quantified using detailed HRA

Recovery Analysis (cont.)

- Ideally treated at cut set specific level

- Specific set of basic events (in cut set) examined to identify potential recover actions
  - Incorporating into system models usually not a good idea (can create situations of multiple recovery actions in same scenario; can result in impossible recovery actions)

- Recovery possibilities can depend on specific failure modes and mechanisms
  - e.g., HPI MDP fails to start due to actuation failure, can be recovered via manual start (mechanical FTS might not be recoverable)

Level 2/3 Analysis

- Level-1 accident sequences analysis typically quantifies core damage frequency (CDF)

- Containment analysis (Level 2) and consequence analysis (Level 3) usually performed "separate" from CDF analysis

- Method needed to link accident sequence analysis to containment analysis

Expanded Systems Analysis Needed to Support Level-2 Model

IE   Level-1 Event Tree

*Bridge Event Tree
Appends Containment
Systems to Level-1 ET*

IEs

RxTrip

LOCA

LOSP

SGTR

etc.

ok

CD_1

ok

CD_n

PDS_1

PDS_2

PDS_3

.
.

PDS_n
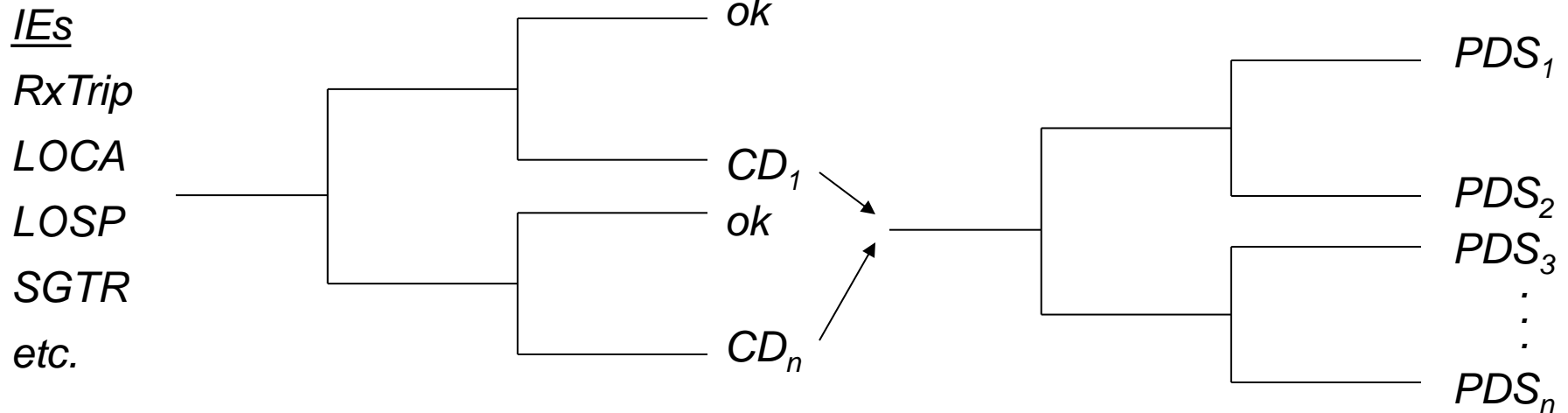
Bridge Event Trees

- Additional system models and analyses needed before containment analysis can be performed
    - "Core Damage" result, not adequate for starting containment analysis
    - Containment system models need to be integrated with Level 1 system analysis (i.e., need to capture dependencies)
    - Bridge Event Tree (BET) used to model additional systems/phenomena, linked to Level 1 event trees
        - Typically generates Plant Damage State (PDS) vectors

Plant Damage States

- Output (end states) of BET defined in terms of specific details on CD accident sequence

- Method utilizes a vector framework
    - e.g., ACCBABDC
    - Each character identifies the status of a particular system or event
    - Vector is "read" by the Level 2 analysis

Example Plant Damage State Vector Framework

Character	PWR	BWR
1	Status of RCS at onset of core damage	Status of RPS
2	Status of ECCS	Status of electric power
3	Status of containment heat removal	RPV integrity
4	Status of electric power	RPV pressure
5	Status of contents of RWST	Status of HPI
6	Status of heat removal from S/Gs	Status of LPI
7	Status of cooling for RCP seals	Status of containment heat removal
8	Status of containment fan coolers	Status of containment venting
9		Level of pre-existing leakage from containment
10		Time to core damage

Palisades IPE PDS Characteristics

# Characteristic	Description
1 Initiator	Affects potential for containment bypass, fission product retention by the RCS, pressure of the RCS at vessel failure, etc.
2 CD Time	Time of fission product release and amount of warning time for offsite protective actions.
3 Secondary Cooling	Can affect late revaporization of fission products retained in the RCS
4 Pressurizer PORV	Affects RCS pressure during the core relocation/vessel failure phase of a CD sequence
5 Containment Systems	Affect long term integrity of containment. Can affect debris coolability, flammable gas behavior, fission product releases

Palisades IPE PDS Character #1 (Initiator)

ID	Description
A1	Large LOCA (d > 18 in.)
A2	Medium LOCA (2 in. < d < 18 in.)
B	Small LOCA (1/2 in. < d < 2 in.)
C	Interfacing System LOCA
D	SGTR
T	Transient

Palisades IPE PDS Char. #'s 2, 3 & 4

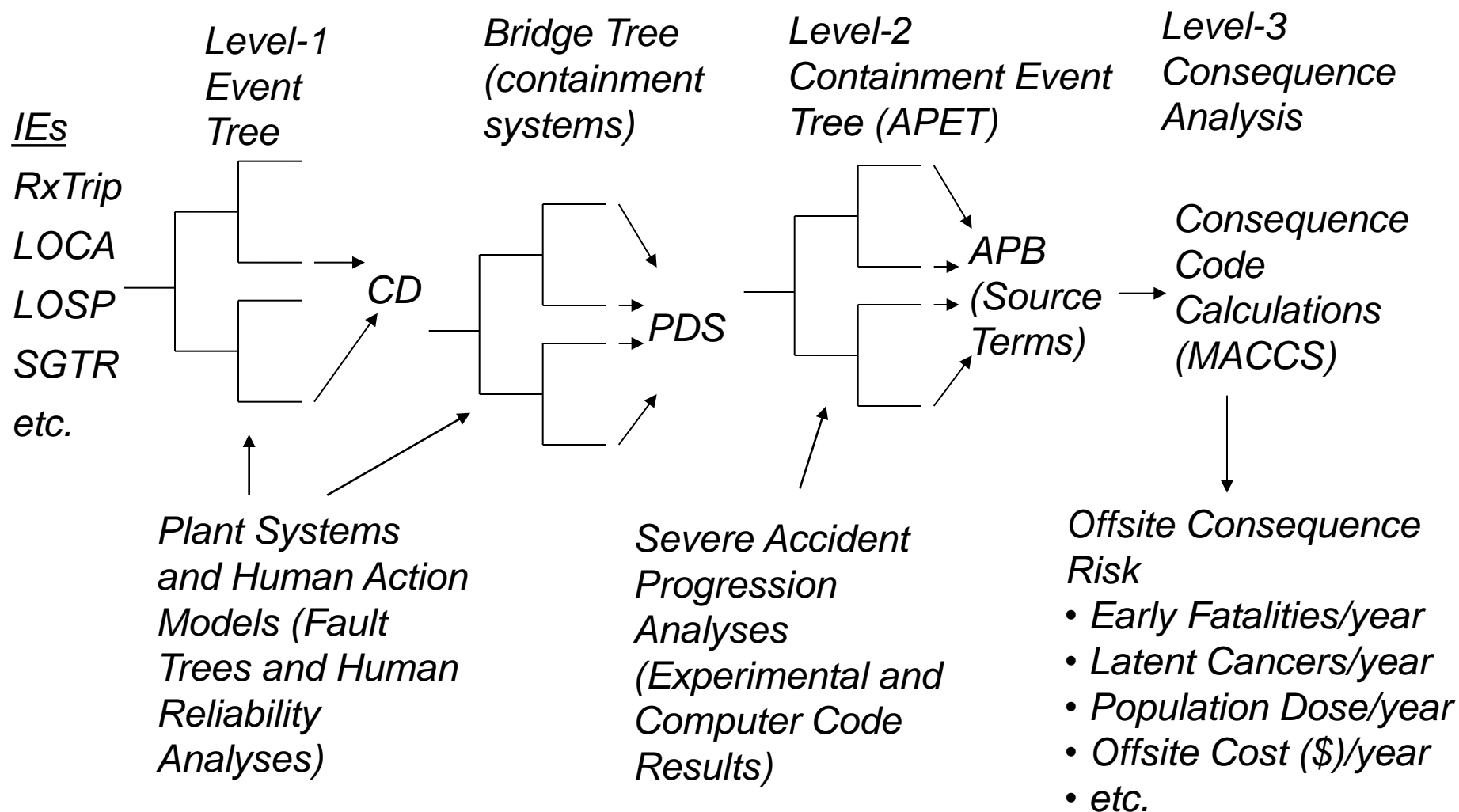| 2	Core Damage Timing
E	Early CD
L	Late CD
3	Secondary Cooling
G	Secondary Cooling Available
J	No Secondary Cooling
4	Pressurizer PORV
M	PORV Available
N	PORV Unavailable

Palisades IPE PDS Char. #5 (Containment Systems)

ID	Description
P	Containment sprays and air coolers available
Q	Cont. sprays avail. and cont. air coolers NOT avail.
R	Only cont. air coolers avail., RWST contents in cont.
S	Only cont. air coolers avail., RWST contents NOT in cont.
V	No cont. systems avail., RWST contents in cont.
W	No cont. systems avail., RWST contents NOT in cont.
X	Late (post VB) operation of only HPSI/LPSI

Overview of Level-1/2/3 PRA

IEs

RxTrip

LOCA

LOSP

SGTR

etc.

Level-1 Event Tree

Bridge Tree (containment systems)

Level-2 Containment Event Tree (APET)

Level-3 Consequence Analysis

CD

PDS

APB (Source Terms)

Consequence Code Calculations (MACCS)

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

Severe Accident Progression Analyses (Experimental and Computer Code Results)

Offsite Consequence Risk
- *Early Fatalities/year*
- *Latent Cancers/year*
- *Population Dose/year*
- *Offsite Cost ($)/year*
- *etc.*

14

Aging

- – Not accounted for in vast majority of PRAs/IPEs
- – System is no longer memoryless
  - • Violation of Poisson assumption; failure rate is not constant (termed "hazard function")
    - – Failure rate is time dependent

*Burn-in
Failures*

*Steady-State
performance*

$\lambda(t)$

Typical Bathtub Curve

*Wear-out
Failures
(Aging)*
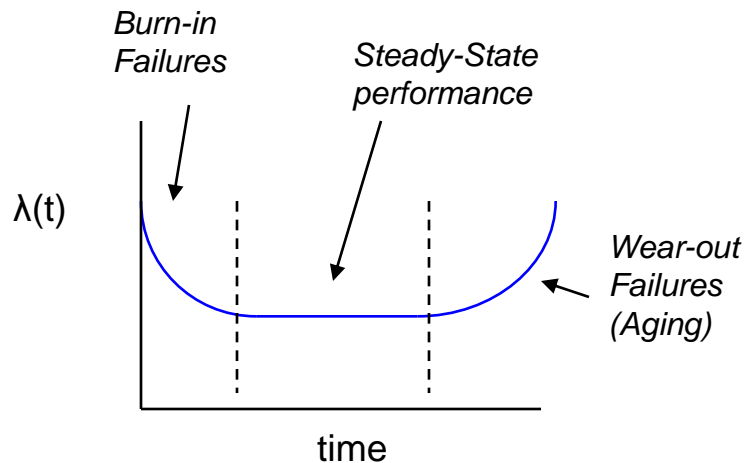
time

Aging (cont.)

- Given $\lambda(t)$ quantification is straightforward
  - Failure rate changes only affect numerical values in fault tree, not structure
  - Failure rate usually changes slowly enough that time-dependent effects are not important during accident
- Aging is particularly of interest for passive components
  - Active components are maintained and sometimes replaced
  - Passive components are often left out of the analysis because of their initially low failure rates

Aging (cont.)

- Estimation of $\lambda(t)$: some work suggests that a linear aging model is reasonable
$$\lambda(t) = a + b \cdot t$$

- Alternatively, physical models for component behavior can be used
  - i.e., explicitly accounting for physical aging mechanisms
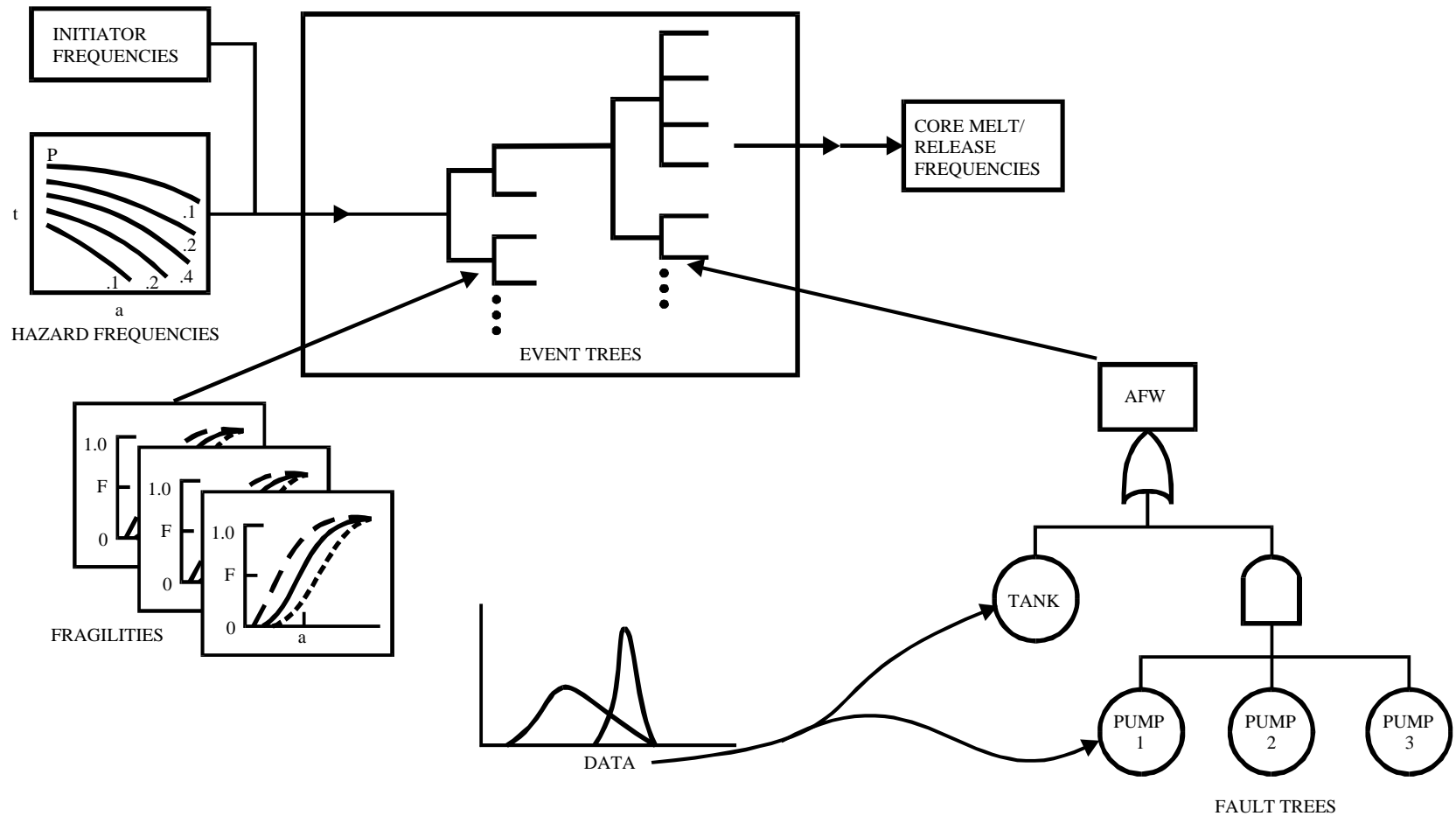
External Events Analysis

Objective

- Estimate risk contribution due to "external events"
- Events modeled typically include:
  - Seismic events
  - Area events
    - Fires
    - Floods (internal and external)
- Require detailed plant layout information

External Events Analysis (Seismic)

- Seismic events analysis requires 3 basic steps
  - Hazards analysis (frequency-magnitude relationship for earthquakes)
    - Location-specific hazard curves produced by NRC (LLNL) and EPRI
    - New Curves related by USGS in 2014
  - Fragility analysis ("strength" of components)
    - Conditional probability of failure given a specific earthquake severity
  - Accident sequence analysis

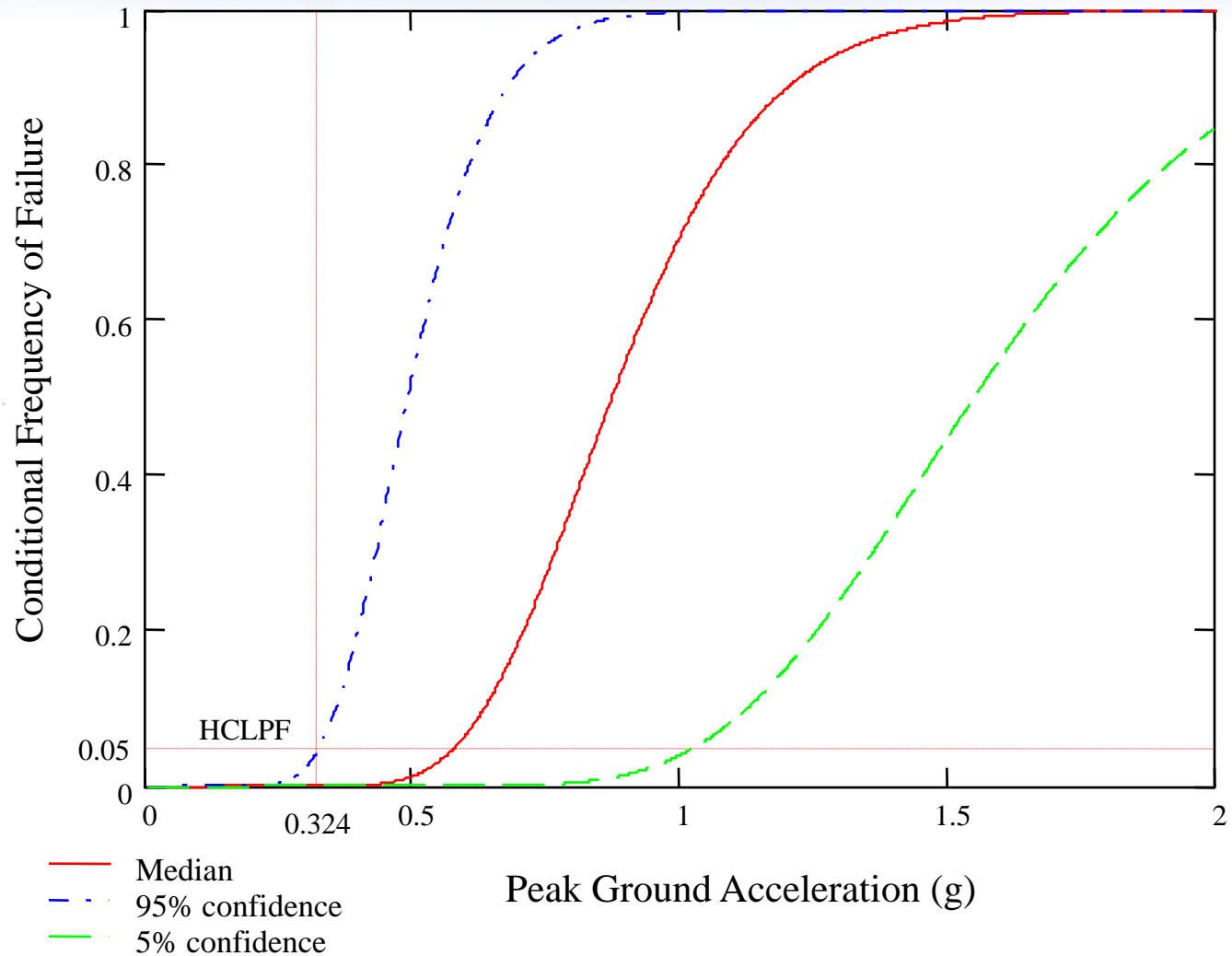# *External Events Analysis (Seismic)*

Component Fragility Curves

$A_m = 0.87$ g

$\beta_r = 0.25$

$\beta_u = 0.35$

Conditional Frequency of Failure

Peak Ground Acceleration (g)

HCLPF

0.324

— Median
-·- 95% confidence
-- 5% confidence

External Events Analysis (Area)

- Spatially coupled events analysis requires 4 basic steps
  - Spatial interactions analysis
  - Frequency analysis
  - Damage analysis
  - Accident sequence analysis

System Modeling Techniques for PRA

Appendix A – Workshops

www.inl.gov

Idaho National Laboratory

Probability and Frequency

1. An event occurs with a frequency of 0.02 per year.
    1.1. What is the probability that an event will occur within a given year?
    1.2. What is the probability that an event will occur during the next 50 years?
2. Event A occurs with a frequency of 0.1 per year. Event B occurs with a frequency of 0.3 per year.
    2.1. What is the probability that an event (either A or B) will occur during the next year?
    2.2. What is the probability that an event (either A or B) will occur during the next 5 years?
3. An experiment has a probability of 0.2 of producing outcome C.
    3.1. If the experiment is repeated 4 times, what is the probability of observing at least one C?
    3.2. This same experiment has a probability of 0.4 of producing outcome D; however, if C occurs, then the probability of outcome D on the next trial is 0.6 (probability of C remain unchanged at 0.2). If the experiment is repeated (i.e., performed twice), what is the probability of at least one D?

Useful Values for Workshops
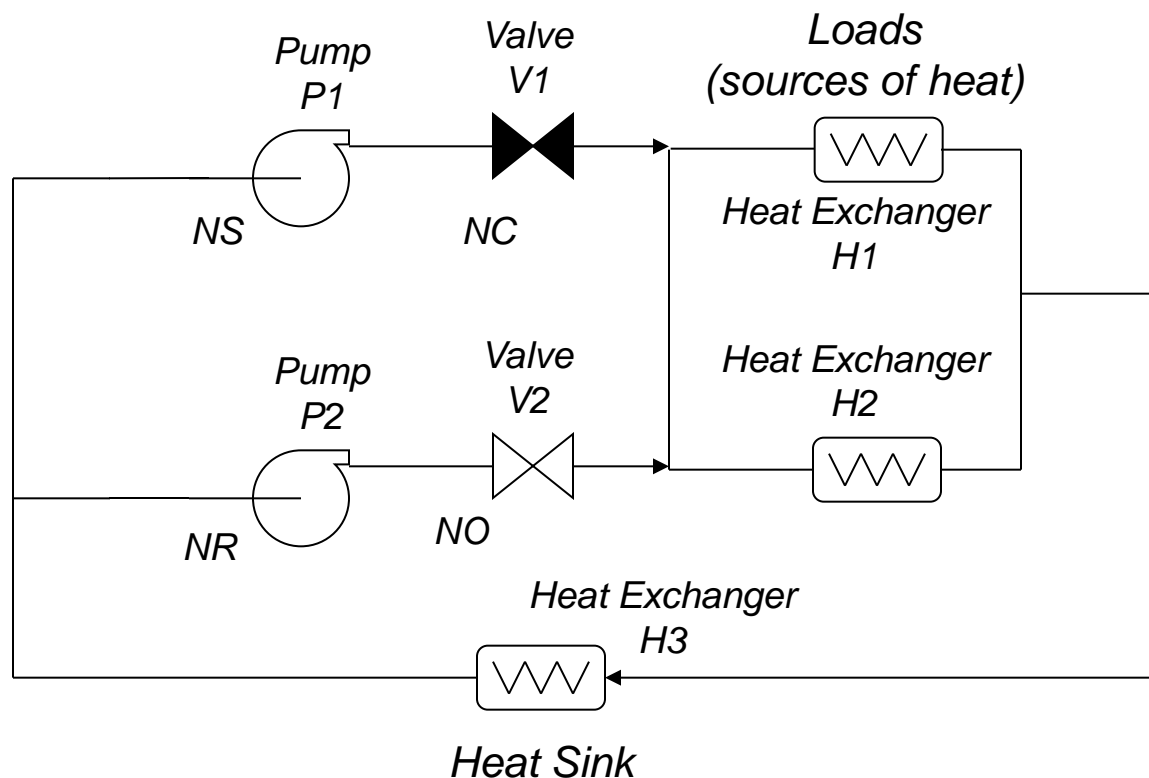
$e^{-0.02} = 0.9802$

$e^{-0.10} = 0.9048$

$e^{-0.30} = 0.7408$

$e^{-0.50} = 0.6065$

$e^{-1.00} = 0.3679$

$e^{-1.50} = 0.2231$

Fault Tree - #1

Closed loop cooling system cools loads via heat exchangers H1 and H2.
Heat is then remove from system through heat exchanger H3.
System successfully performs its function when heat is absorbed through both H1
and H2 , and expelled through H3, with flow maintained by either pump P1 or P2.

Motor Operated Valve – Normally Closed (requires ac power to operate).

Motor Operated Valve – Normally Open (requires ac power to operate).

Motor Operated Pump

Air Operated Valve – Normally Open (requires dc power and compressed air to operate, however typically will move to the "safe" position on loss of either).
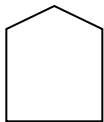
Air Operated Valve – Normally Closed (requires dc power and compressed air to operate, however typically will move to the "safe" position on loss of either).

Manually Operated Valve – Normally Open (operates using a hand-wheel or chain-wheel located on the valve itself).
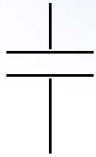
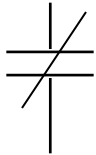*Check Valve – Operates passively, allows flow in only one direction.*

Water Tank – Typically source of water for system

Heat Exchanger – Used to transfer heat from one fluid system to another (i.e., connects two fluid systems in order for one system to cool the other

Electrical contacts or switch - Normally open (i.e., in "off" position)

Electrical contacts or switch - Normally closed (i.e., in "on" position)

Electrical coil or solinoid - Used to operate piece of equipment (e.g., a set of electrical contacts)

NS   Normally Stopped

NR   Normally Running

*NC   Normally Closed*

NO   Normally Open

Fault Tree - #2

- Cooling water pumps have the following support system dependencies:
  - AC power
  - Room cooling
  - Start signal

- Pump P1 is normally in standby and must be either automatically or manually started. When the pump is needed to start and run, an automatic actuation signal is sent to the pump. However, if the auto signal fails, the operators can manually start the pump. Also, room cooling is only required during the hot summer months of July and August. The rest of the year, room cooling is not needed. Lastly, the pump is made unavailable for eight hours, twice a year for maintenance.

- Successful operation requires the pump to start and run for 24 hours.

- Construct a fault tree for P1.

Data

Component	*Failure Mode*	*Failure Rate*
V - manual valve	fails to open (FTO)	5E-5/demand
P - motor driven pump	fails to run (FTR) fails to start (FTS)	3E-5/hr 3E-3/demand
ac – ac power	loss of power (LOP)	1E-7/hr
rm – room cooling	loss of room cooling (LOC)	1E-6/hr
H – heat exchanger	plug (PG)	1E-8/hr
ACT – Actuation	Manual fails (HE) Automatic fails (AU)	0.1/demand 0.01/demand

Simple Emergency Coolant Injection/Recirculation
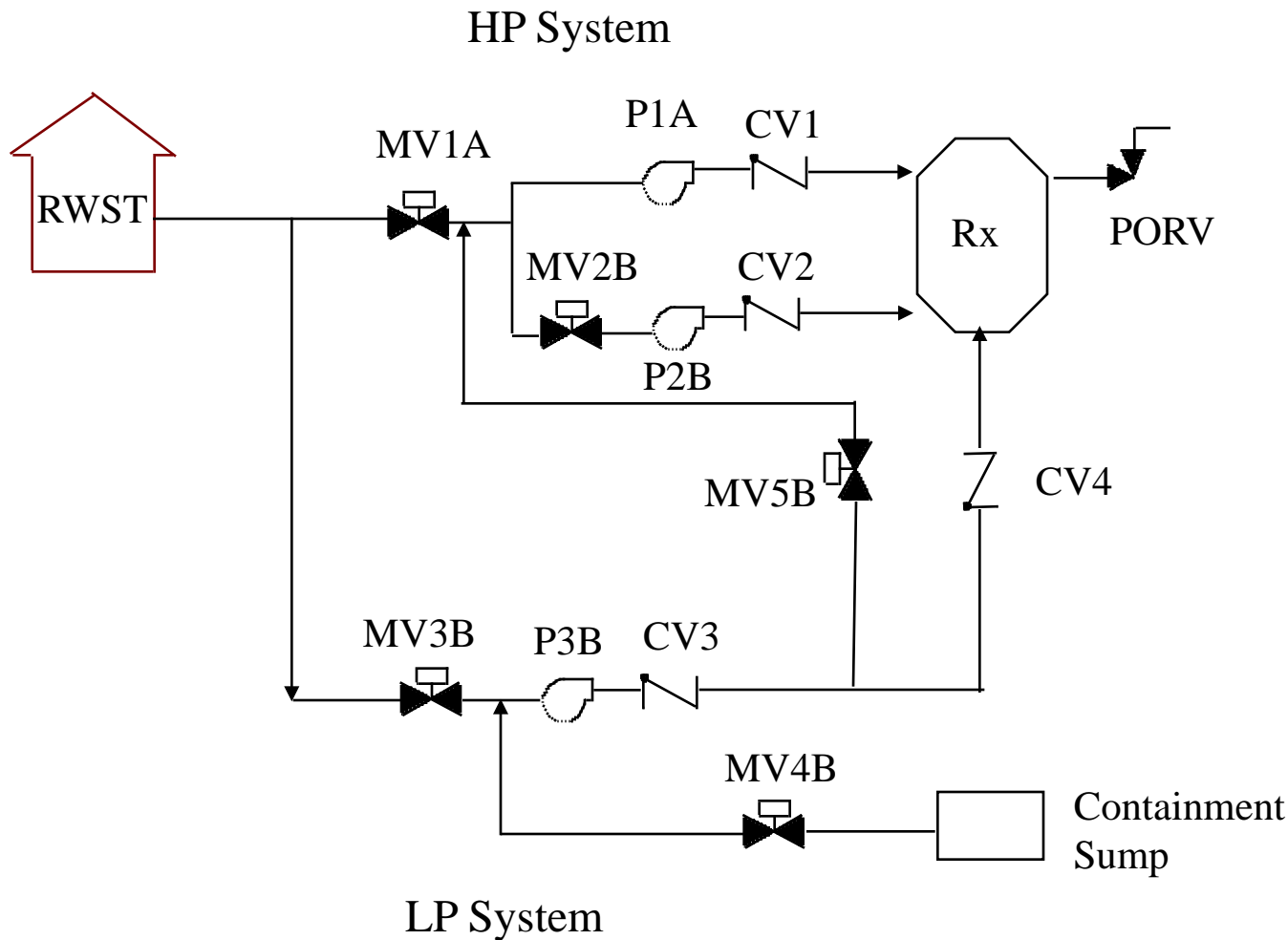
Boundary Conditions

1. No equipment cooling requirements (room, lube oil, or seal)
2. No maintenance of equipment during plant operations, no partial actuation system failures
3. "A" components powered from ac bus A
4. "B" components powered from ac bus B
5. Control power transformed from motive power for all valves (i.e., ignore control power dependencies for valves)
6. Control power for pumps provided by respective dc buses, which in turn can be powered from either the same train ac bus or dedicated a battery
7. Power operated relief valve (PORV) can be manually opened from control room to depressurize the reactor vessel (Rx) and is powered from dc bus B
8. "A" train components actuated automatically by safety injection (SI) signal (powered by dc bus A)
9. "B" train components must be manually actuated (from control room)
10. If high pressure (HP) system fails, operators can depressurize using PORV and cool reactor using the low pressure (LP) system
11. Success criteria for high pressure injection (HPI) is 1 of 2 pumps delivering flow to the reactor vessel (Rx).
12. System can operate in a total of four operating modes: HPI, low pressure injection (LPI), high pressure recirculation (HPR), and low pressure recirculation (LPR).
13. Ignore heat removal from LPR/HPR water.

Event Tree & Fault Tree Workshop

1. Only function required: Provide cooling to reactor vessel (Rx)
2. Develop system-level event tree for small loss of coolant accident (SLOCA)
3. Generate core damage accident sequence logic
4. Develop fault trees for HPI, HPR, LPI and LPR.
5. Generate cut sets for HPI, HPR, LPI and LPR.
6. Generate core damage sequence cut sets