Basics of Nuclear Power Plant Probabilistic Risk Assessment

Joint RES/EPRI Fire PRA Workshop
July and September, 2012
Bethesda, MD

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Course Objectives

- Introduce PRA modeling and analysis methods applied to nuclear power plants
  - Initiating event identification
  - Event tree and fault tree model development
  - Human reliability analysis
  - Data analysis
  - Accident sequence quantification
  - LERF analysis

Course Outline

1. Overview of PRA
2. Initiating Event Analysis
3. Event Tree Analysis
4. Fault tree Analysis
5. Human Reliability Analysis
6. Data Analysis
7. Accident Sequence Quantification
8. LERF Analysis

Overview of PRA

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

What is Risk?

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

Risk Definition

- Risk - the frequency with which a given consequence occurs

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

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

Risk Example: Death Due to Accidents

- Societal Risk = 93,000 accidental-deaths/year in 1991

  (based on Center for Disease Control actuarial data)

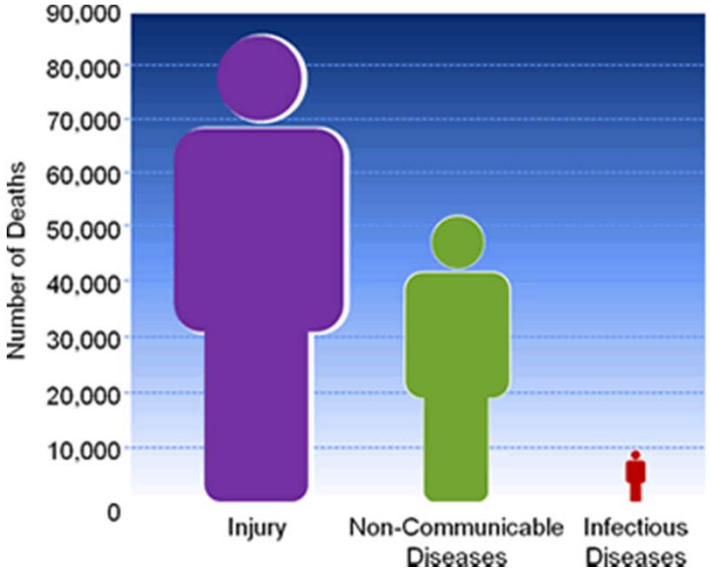
- Average Individual Risk

  = (93,000 Deaths/Year)/250,000,000 Total U.S. Pop.

  = 3.7E-04 Deaths/Person-Year

  ≈ 1/2700 Deaths/Person-Year

- In any given year, approximately 1 out of every 2,700 people in the entire U.S. population will suffer an accidental death



More people ages 1–44 die from injuries than from any other cause, including cancer, HIV, or the flu.

Note: www.cdc.gov latest data (2009) 38.4 unintentional deaths per 100,000, thus average individual risk ≈ 3.8E-04 Deaths/Person-Year

Risk Example: Death Due to Cancer

- Societal Risk = 538,000 cancer-deaths/year in 1991

  (based on Center for Disease Control actuarial data)

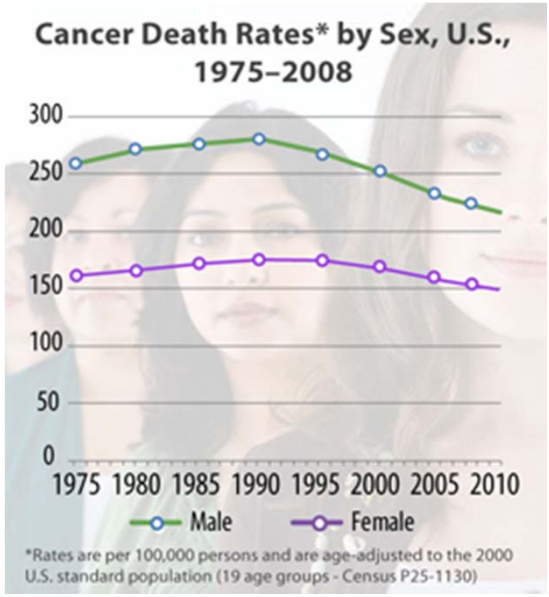
- Average Individual Risk

  = (538,000 Cancer-Deaths/Year)/250,000,000 Total U.S. Pop.

  = 2.2E-03 Cancer-Deaths/Person-Year

  ≈ 1/460 Cancer-Deaths/Person-Year

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



Note: www.cdc.gov latest data (2007) 217.8 cancer deaths per 100,000, thus average individual risk ≈ 2.2E-03 Deaths/Person-Year

NRC Quantitative Health Objectives (QHOs)

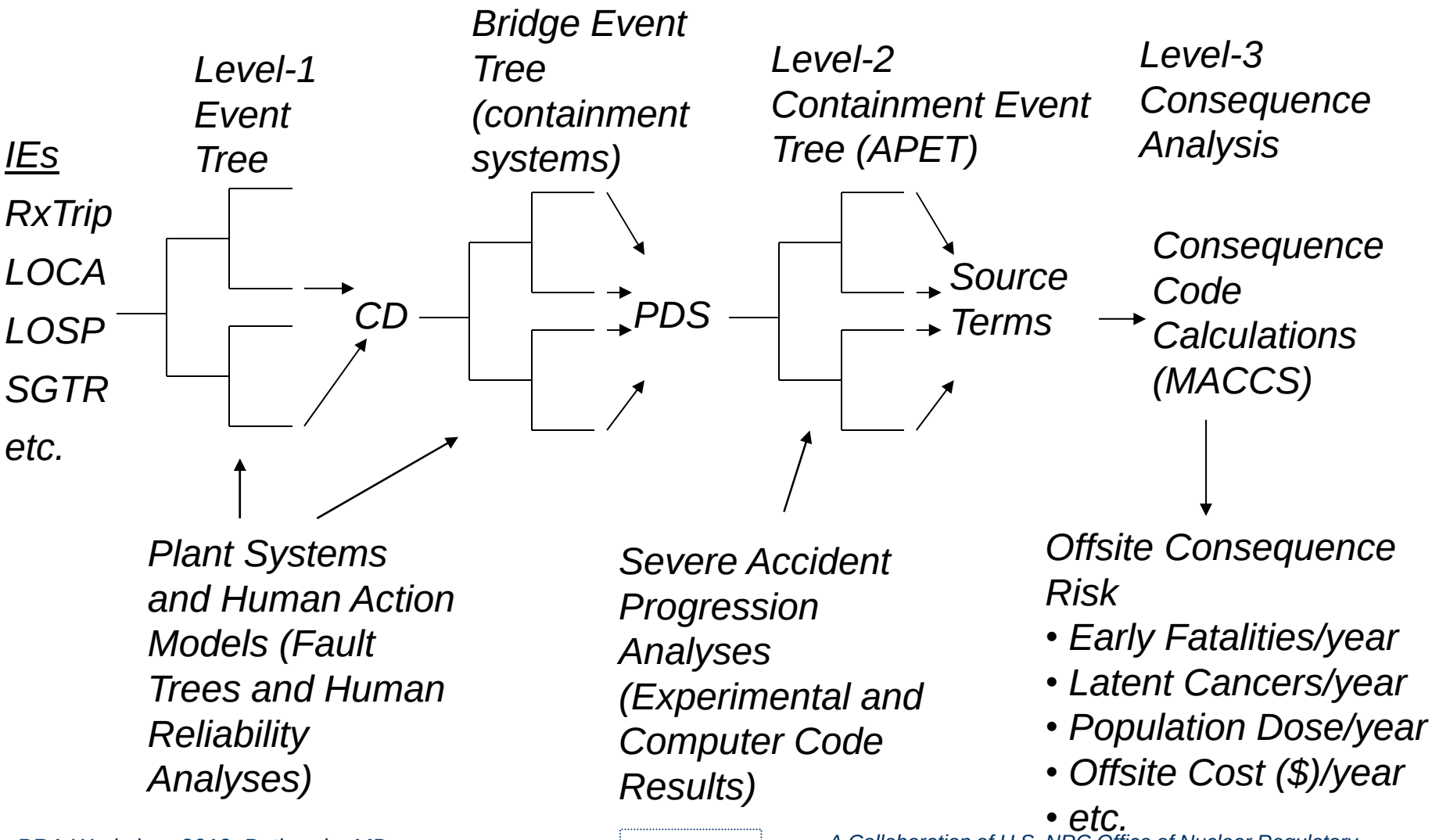
- Originally known as the Probabilistic Safety Goals
  - NRC adopted two probabilistic safety goals on August 21, 1986
- High-level goal: incremental risk from nuclear power plant operation < 0.1% of all risks
  - Average individual (within 1 mile of plant) early fatality (accident) risk
    < 5E-7/year
  - 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

Overview of PRA Process

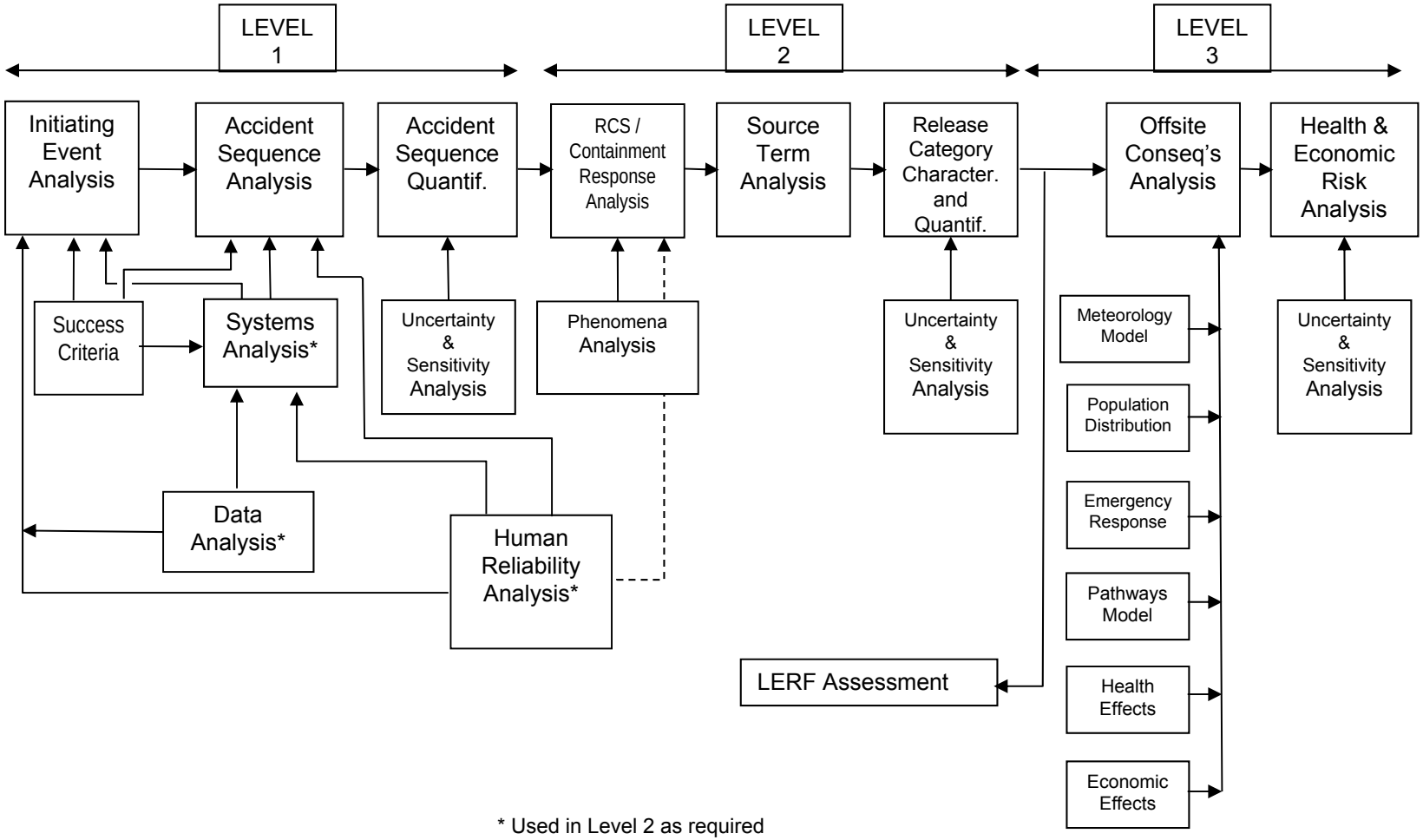
- PRAs are performed to find severe accident weaknesses and provide quantitative results to support decision-making. Three levels of PRA have evolved:

Level	An Assessment of:	Result
1	Plant accident initiators and systems'/operators' response	Core damage frequency & contributors
2	Frequency and modes of containment failure	Categorization & frequencies of containment releases
3	Public health consequences	Estimation of public & economic risks

Overview of Level-1/2/3 PRA



Principal Steps in PRA



* Used in Level 2 as required

PRA Classification

- Internal Hazards – risk from accidents initiated internal to the plant
  - Includes internal events, internal flooding and internal fire events
- External Hazards – risk from external events
  - Includes seismic, external flooding, high winds and tornadoes, airplane crashes, lightning, hurricanes, etc.
- At-Power – accidents initiated while plant is critical and producing power (operating at >X%* power)
- Low Power and Shutdown (LP/SD) – accidents initiated while plant is <X%* power or shutdown
  - Shutdown includes hot and cold shutdown, mid-loop operations, refueling

**X is usually plant-specific. The separation between full and low power is determined by evolutions during increases and decreases in power*

Focus of Course is on At-Power PRA

- In early risk studies, risk from at-power operation was assumed to be dominant because during shutdown:
  - Reactor is subcritical
  - Longer time is available to respond to accidents (lower decay heat)
- However, limited risk studies of low-power and shutdown operations have suggested that shutdown risk may be significant because
  - Systems may not be available as Tech. Specs. allow more equipment to be inoperable than at power
  - Initiating events can impact operable trains of systems providing critical plant safety functions (e.g., loss of RHR)
  - Human errors are more prevalent because operators may find themselves in unfamiliar conditions not covered by training and procedures
  - Plant instruments and indications may not be available or accurate

Specific Strengths of PRA

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

Principal Limitations of PRA

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

Evolution of PRA Use

- First PRA study (WASH-1400, 1975)
  - provided a better understanding of how nuclear plant accidents might occur and what the potential consequences might be
- Three Mile Island accident in 1979
  - validated the importance of PRA
  - led to efforts to improve state-of-the-art of PRA, in research into severe accident phenomena, and performance of PRAs on more reactors
- NRC Safety Goals (1986)
  - Risk to the public from nuclear power plant operation should be less than 0.1% of the total risk from other man-made causes

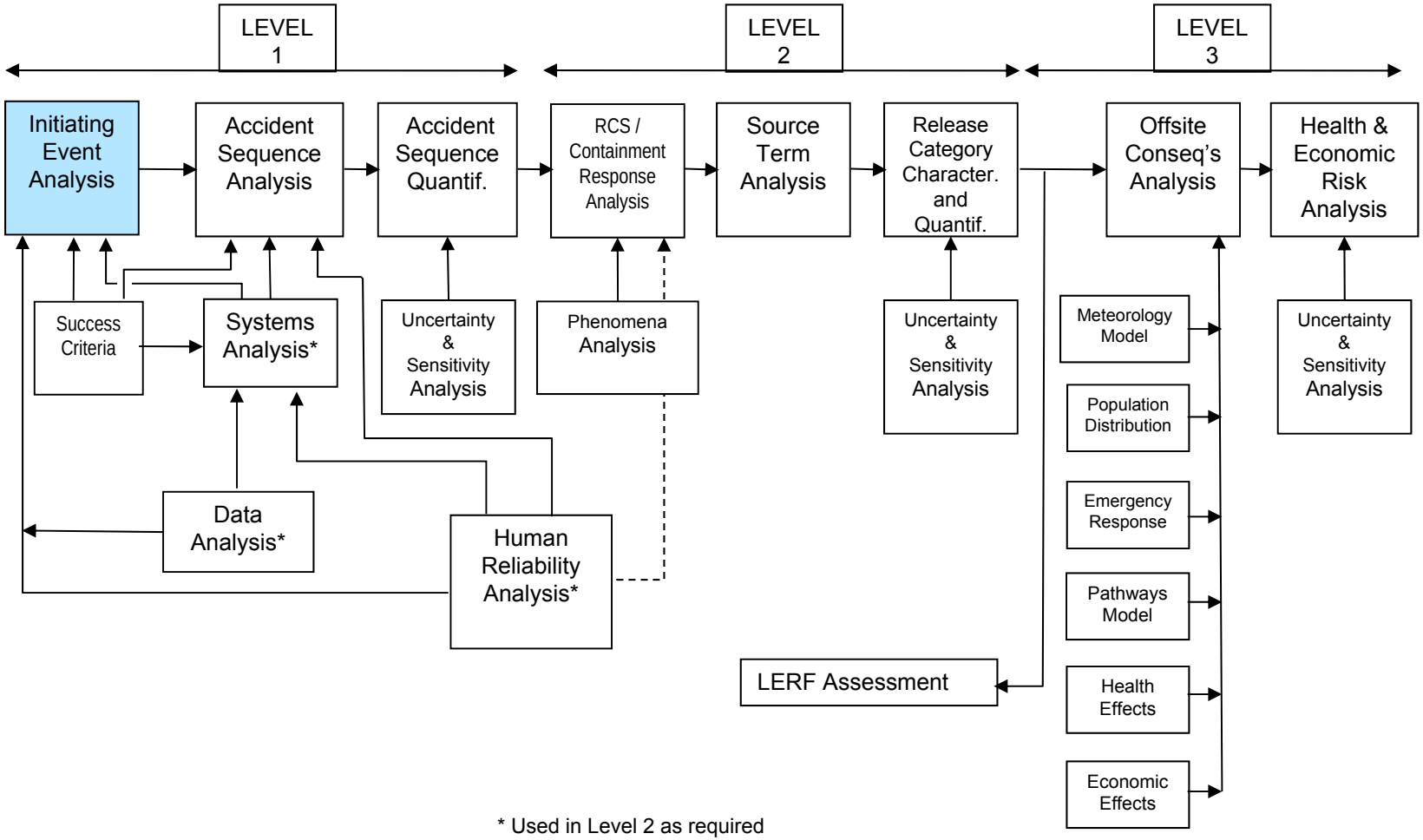
Evolution of PRA Use (cont.)

- Generic Letter 88-20 (1988)
  - requested all nuclear power plant licensees to conduct an Individual Plant Examination (IPE) to investigate plant-specific risk and identify any vulnerabilities. All plants performed a PRA. Plants later identified risk from external events in IPEEE (Individual Plant Examination of External Events)
- NRC Policy Statement on the use of PRA in regulatory matters (1995)
  - " the use of PRA technology should be increased to the extent supported by the state of the art in PRA methods and data and in a matter that complements the NRC's deterministic approach"
  - Risk-Informed Regulation Implementation Plan generated to define and organize PRA-related activities

Initiating Event Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

Initiating Event Analysis

- Purpose: Students will learn what is an initiating event (IE), how to identify them, and group them into categories for further analysis.

Objectives:

  - Understand the relationship between initiating event identification and other PRA elements
  - Identify the types of initiating events typically considered in a PRA
  - Become familiar with various ways to identify initiating events
  - Become familiar with criteria for eliminating initiating events
  - Understand how initiating events are grouped

- References:
  - NUREG/CR-2300, NUREG/CR-5750, NUREG/CR-3862, NUREG/CR-4550, Volume 1, NUREG/CR-6928

Initiating Events

- Definition – Any potential occurrence that could disrupt plant operations to a degree that a reactor trip or plant shutdown is required. Initiating events are quantified in terms of their frequency of occurrence (i.e., number of events per calendar year of operation)
- Can occur while reactor is at full power, low power, or shutdown
  - Focus of this session is on IEs during full power operation
- Can be internal to the plant or caused by external events
  - Focus of this session is on internal IEs
- Basic categories of internal IEs:
  - transients (initiated by failures in the balance of plant or nuclear steam supply)
  - loss-of-coolant accidents (LOCAs) in reactor coolant system
  - interfacing system LOCAs
  - LOCA outside of containment
  - special transients (generally support system initiators)

Role of Initiating Events in PRA

- Identifying initiating events is the first step in the development of accident sequences
- Accident sequences can be conceptually thought of as a combination of:
  - an initiating event, which triggers a series of plant and/or operator responses, and
  - A combination of success and/or failure of the plant system and/or operator response that result in a core damage state
- Initiating event identification is an iterative process that requires feedback from other PRA elements
  - system analysis
  - review of plant experience and data

Initiating Event Analysis

- Collect information on actual plant trips
- Identify other abnormal occurrences that could cause a plant trip or require a shutdown
- Identify the plant response to these initiators including the functions and associated systems that can be used to mitigate these events
- Grouping IEs into categories based on their impact on mitigating systems
- Quantify the frequency of each IE category (Included later in Data Analysis session)

Methods for Identification and Grouping IEs

- Comprehensive Engineering Evaluation (commonly used)
  - Analysis of historical events
  - Comparison with other studies
  - Plant-specific design data
- Deductive methods (master logic diagram)
  - Good process when there is no history of accident initiators (e.g., an advanced reactor)
- Failure Modes and Effects Analysis (FMEA)
  - Formalized tabular process used to identify potential failures, determine the effect on the plant operation, and identify mitigating actions
  - Primarily used to examine support system failures

Comprehensive Engineering Evaluation

- Review historical events (reactor trips, shutdowns, system failures)
- Discrete spectrum of LOCA sizes considered based on location of breaks (e.g., in vs. out of containment, steam vs. liquid), components (e.g., pipe vs. SORV), and available mitigation systems
- Review comprehensive list of possible transient initiators based on existing lists (see for example NUREG/CR-3862) and from Safety Analysis Report
- Review list of initiating event groups modeled in other PRAs and adapt based on plant-specific information – typical approach for existing LWRs
- Feedback provided from other PRA taks

Sources of Data for Identifying IEs

- Plant-specific sources:
  - Licensee Event Reports
  - Scram reports
  - Abnormal, System Operation, and Emergency Procedures
  - Plant Logs
  - Safety Analysis Report (SAR)
  - System descriptions
- Generic sources:
  - NUREG/CR-3862
  - NUREG/CR-4550, Volume 1
  - NUREG/CR-5750
  - Other PRAs

Criteria for Eliminating IEs

- Some IEs may not have to modeled because:
  - Frequency is very low (e.g., <1E-7/ry)
    - ASME PRA Standard exclude ISLOCAs , containment bypass, vessel rupture from this criteria
  - Frequency is low (<1E-6/ry) and at least two trains of mitigating systems are not affected by the IE
  - Effect is slow, easily identified, and recoverable before plant operation is adversely affected (e.g., loss of control room HVAC)
  - Effect does not cause an automatic scram or an administrative demand for shutdown (e.g., waste treatment failure)

Initiating Event Grouping

- For each identified initiating event:
  - Identify the safety functions required to prevent core damage and containment failure
  - Identify the plant systems that can provide the required safety functions
- Group initiating events into categories that require the same or similar plant response
- This is an iterative process, closely associated with event tree construction. It ensures the following:
  - All functionally distinct accident sequences will be included
  - Overlapping of similar accident sequences will be prevented
  - A single event tree can be used for all IEs in a category

Example Initiating Events (PWR) from NUREG/CR-6928

Category	Initiating Event	Mean Frequency (per critical year)
B	Loss of offsite power	4.0E-2
L	Loss of condenser	0.2
P	Loss of feedwater	0.1
Q	General transient	0.8
F	Steam generator tube rupture	4.0E-3
	ATWS	8.4E-6*
G7	Large LOCA (BWR, PWR)	7.0E-6, 1.2E-6
G6	Medium LOCA (BWR, PWR)	1.0E-4, 5.0E-4
G3	Small LOCA (BWR, PWR)	5.0E-4, 6.0E-4

*From NUREG/CR-5750

Example Initiating Events (PWR) from NUREG/CR-6928 (cont.)

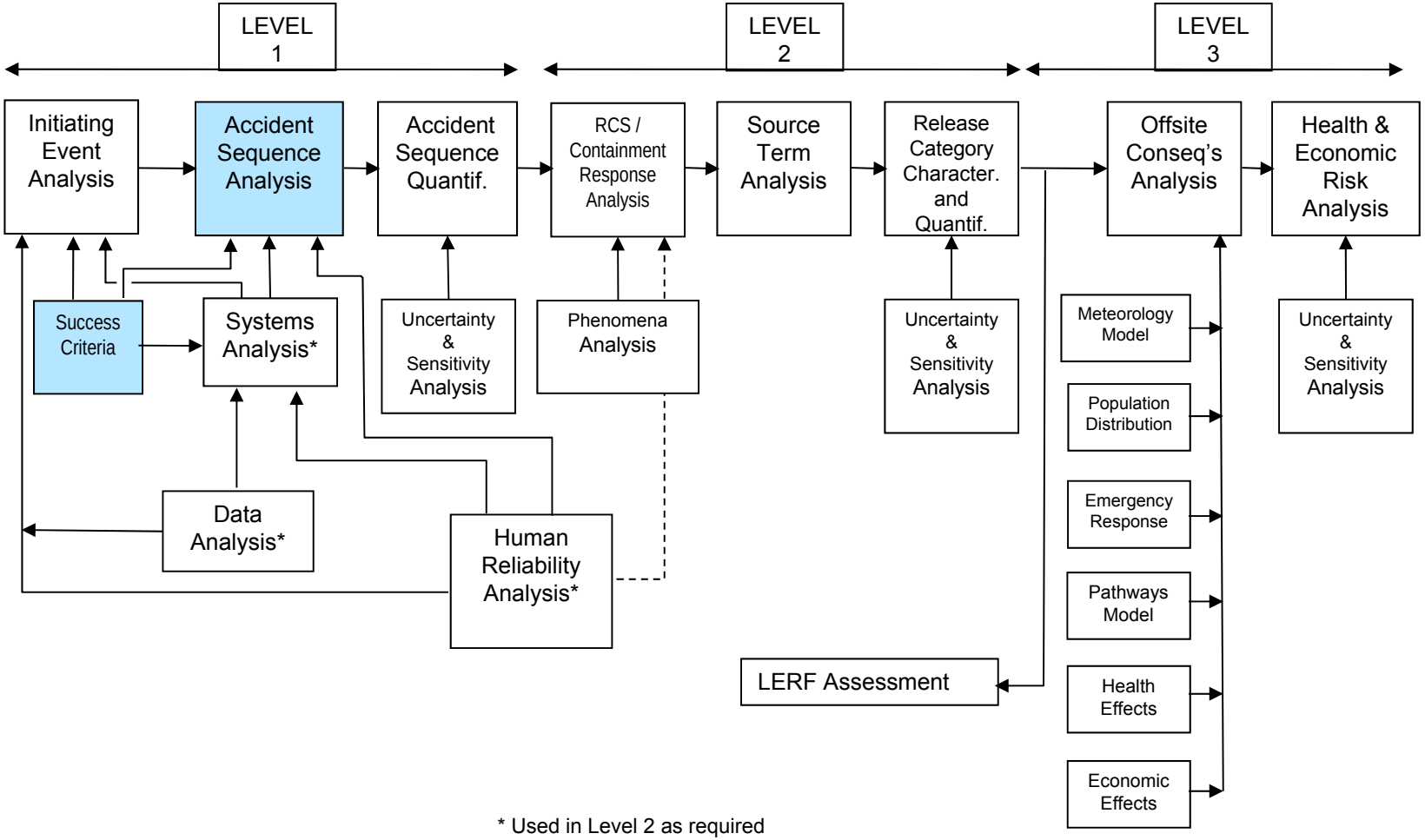
Category	Initiating Event	Mean Frequency (per critical year)
G2	Stuck-open relief valve (BWR, PWR)	2.0E-2, 3.0E-3
K1	High energy line break outside containment	1.0E-2*
C1+C2	Loss of vital medium or low voltage ac bus	9.0E-3
C3	Loss of vital dc bus	1.2E-3
D	Loss of instrument or control air	1.0E-2
E1	Total loss of service water, total loss of component cooling water	4.0E-4

*From NUREG/CR-5750

Accident Sequence Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

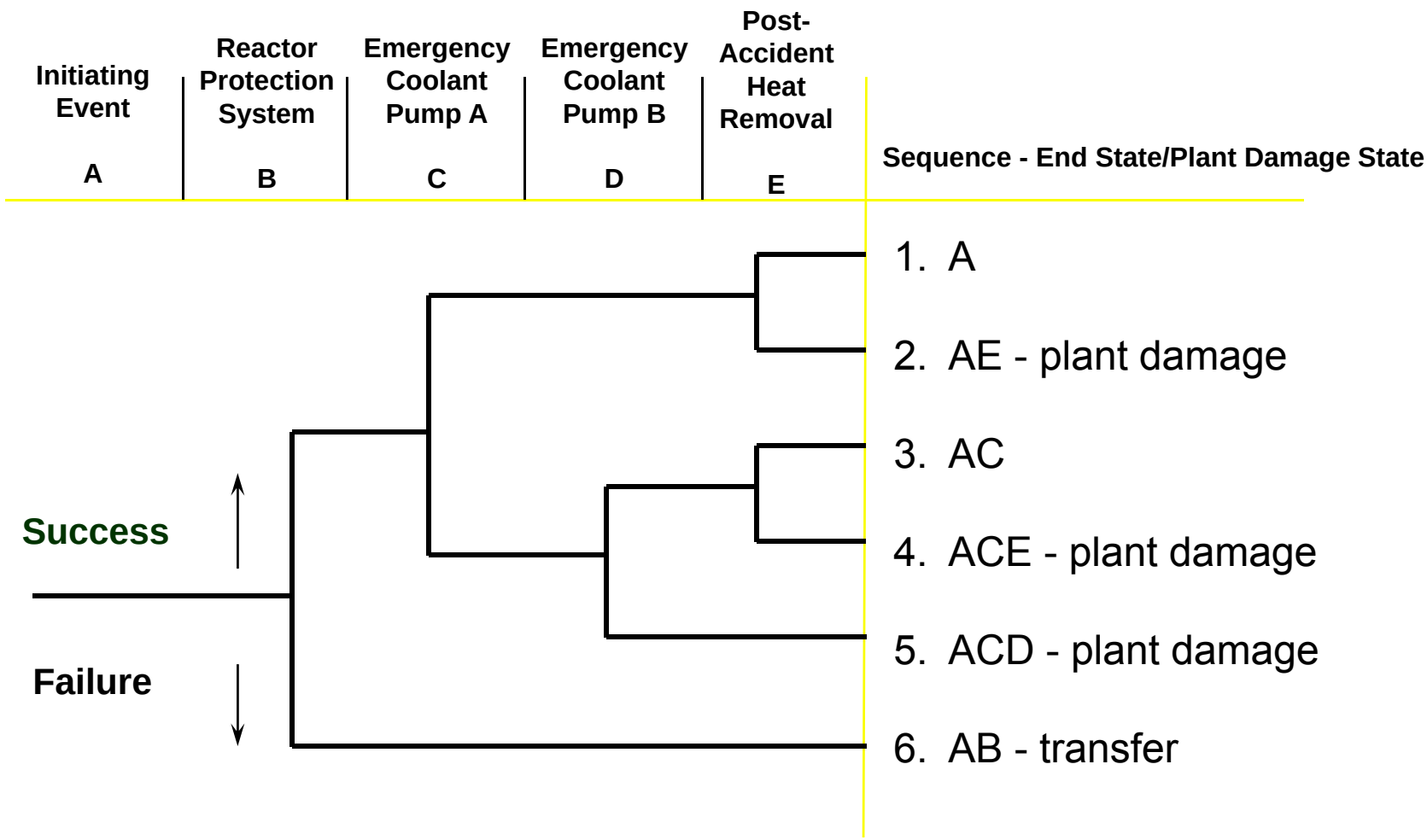
Accident Sequence Analysis

- Purpose: Students will learn purposes & techniques of accident sequence (event) analysis. Students will be exposed to the concept of accident sequences and learn how event tree analysis is related to the identification and quantification of dominant accident sequences.
- Objectives:
  - Understand purposes of event tree analysis
  - Understand currently accepted techniques and notation for event tree construction
  - Understand purposes and techniques of accident sequence identification
  - Understand how to simplify event trees
  - Understand how event tree logic is used to quantify PRAs
- References: NUREG/CR-2300, NUREG/CR-2728

Event Trees

- Typically used to model the response to an initiating event
- Features:
  - Generally, one system-level event tree for each initiating event group is developed
  - Identifies systems/functions required for mitigation
  - Identifies operator actions required for mitigation
  - Identifies event sequence progression
  - End-to-end traceability of accident sequences leading to bad outcome
- Primary use
  - Identification of accident sequences which result in some outcome of interest (usually core damage and/or containment failure)
  - Basis for accident sequence quantification

Simple Event Tree



Required Information

- Knowledge of accident initiators
- Thermal-hydraulic response during accidents
- Knowledge of mitigating systems (frontline and support) operation
- Know the dependencies between systems
- Identify any limitations on component operations
- Knowledge of procedures (system, abnormal, and emergency)

Principal Steps in Event Tree Development

- Determine boundaries of analysis
- Define critical plant safety functions available to mitigate each initiating event
- Generate functional event tree (optional)
  - Event tree heading - order & development
  - Sequence delineation
- Determine systems available to perform each critical plant safety function
- Determine success criteria for each system for performing each critical plant safety function
- Generate system-level event tree
  - Event tree heading - order & development
  - Sequence delineation

Determining Boundaries

- Mission time
  - Sufficient to reach stable state (generally 24 hours)
- Dependencies among safety functions and systems
  - Includes shared components, support systems, operator actions, and physical processes
- End States (describe the condition of both the core and containment)
  - Core OK
  - Core vulnerable
  - Core damage
  - Containment OK
  - Containment failed
  - Containment vented
- Extent of operator recovery

Critical Safety Functions

Example safety functions for core & containment

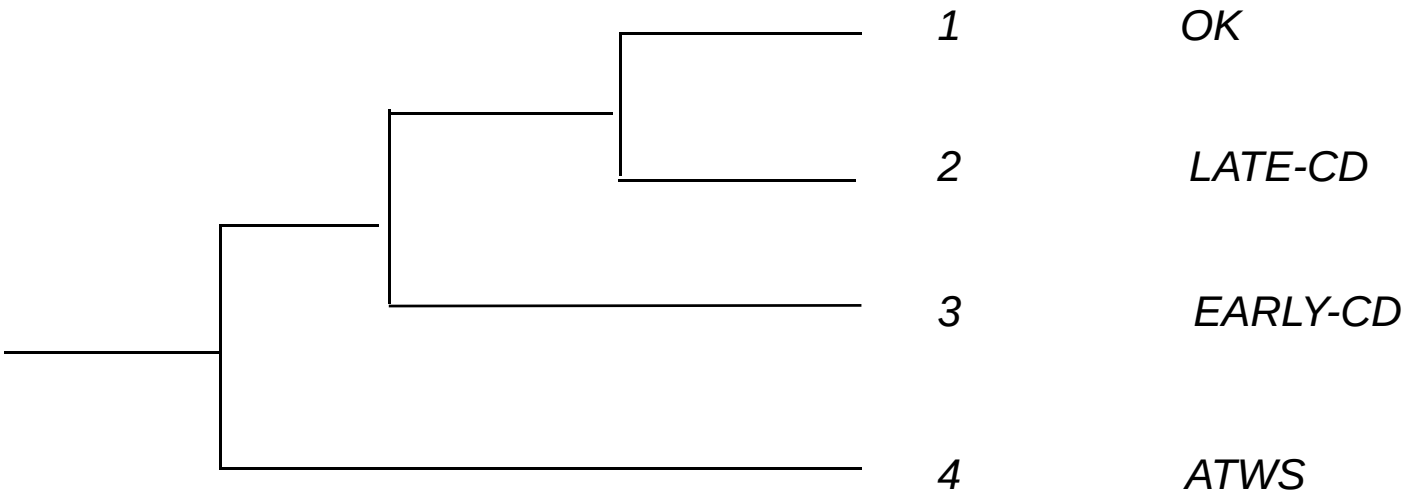
- Reactor subcriticality
- Reactor coolant system overpressure protection
- Early core heat removal
- Late core heat removal
- Containment pressure suppression
- Containment heat removal
- Containment integrity

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
- One functional event tree for transients and one for LOCAs
- Guides the development of more detailed system-level event tree model
- Generation of functional event trees not necessary; system-level event trees are the critical models
  - Could be useful for advanced reactor PRAs

Functional Event Tree

Initiating Event	Reactor Trip	Short term core cooling	Long term core cooling	SEQ #	STATE
IE	RX-TR	ST-CC	LT-CC		



System Success Criteria

- Identify systems which can perform each function
- Often includes if the system is automatically or manually actuated.
- Identify minimum complement of equipment necessary to perform function (often based on thermal/hydraulic calculations, source of uncertainty)
  - Calculations often realistic, rather than conservative
- May credit non-safety-related equipment where feasible

BWR Mitigating Systems

Function	Systems
Reactivity Control	Reactor Protection System, Standby Liquid Control, Alternate Rod Insertion
RCS Overpressure Protection	Safety/Relief Valves
Coolant Injection	High Pressure Coolant Injection, High Pressure Core Spray, Reactor Core Isolation Cooling, Low Pressure Core Spray, Low Pressure Coolant Injection (RHR) Alternate Systems- Control Rod Drive Hydraulic System, Condensate, Service Water, Firewater
Decay Heat Removal	Power Conversion System, Residual Heat Removal (RHR) modes (Shutdown Cooling, Containment Spray, Suppression Pool Cooling)

PWR Mitigating Systems

Function	Systems
Reactivity Control	Reactor Protection System
RCS Overpressure Protection	Safety valves, Pressurizer power-operated relief valves (PORV)
Coolant Injection	Accumulators, High Pressure Safety Injection, Chemical Volume and Control System, Low Pressure Safety Injection (LPSI), High Pressure Recirculation (may require LPSI)
Decay Heat Removal	Power Conversion System (main feedwater), Auxiliary Feedwater, Residual Heat Removal (RHR), Feed and Bleed (PORV + HPSI)

Example Success Criteria

IE	Reactor Trip	Short Term Core Cooling	Long Term Core Cooling
Transient	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
Medium or Large LOCA	Auto Rx Trip or Man. Rx Trip	1 of 2 ECI	1 of 2 ECR

Two Basic Approaches for Event Tree Models

- Two methods are generally used to develop detailed event trees
- Event trees with boundary conditions (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
- 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 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

Linked Fault Tree Approach

- Automatic treatment of shared event/system dependencies
  - Support system fault trees are linked into front-line and other support system fault trees
- One-step quantification
- Often use large, general-purpose fault trees
- Used by SPAR models and majority of utility PRAs
- Used in NUREG-1150 studies

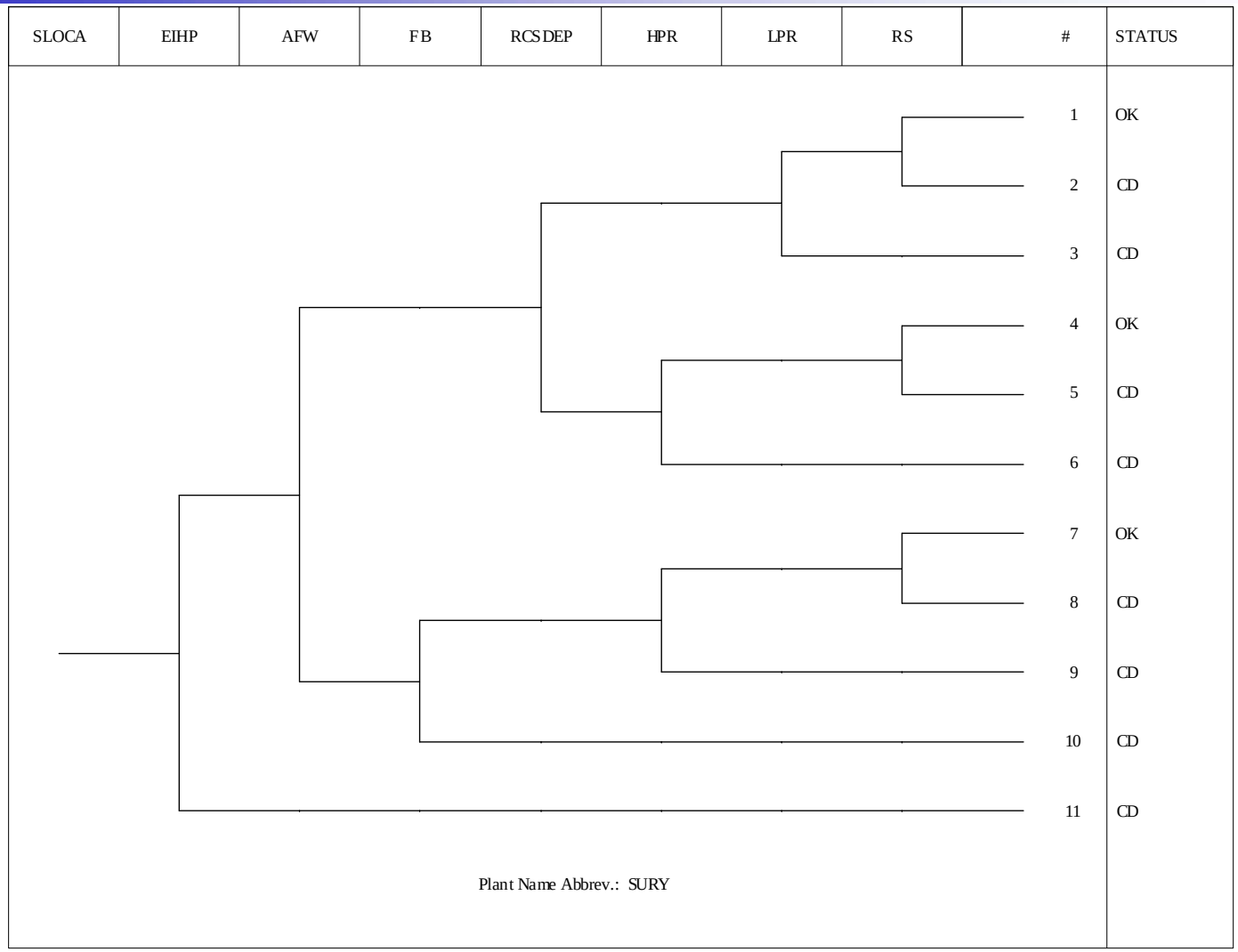
System-Level Event Tree Development

- A system-level event tree consists of an initiating event (one per tree), followed by a number of headings (top events), and a sequence of events representing the success or failure of the top events
- Top events represent the systems, components, and/or human actions required to mitigate the initiating event
- To the extent possible, top events are ordered in the time-related sequence in which they would occur
  - Selection of top events and ordering reflect emergency procedures
- Each node (or branch point) below a top event represents the success or failure of the respective top event
  - Logic is typically binary
    - Downward branch – failure of top event
    - Upward branch – success of top event
  - Logic can have more than two branches, with each branch representing a specific status of the top event

System-Level Event Tree Development (Continued)

- Dependencies among systems(needed to prevent core damage) are identified
  - Support systems can be included as top events to account for significant dependencies (e.g., diesel generator failure in station blackout event tree)
- Timing of important events (e.g., physical conditions leading to system failure) determined from thermal-hydraulic calculations
- Branches can be pruned logically (i.e., branch points for specific nodes removed) to remove unnecessary combinations of system success criteria requirements
  - This minimizes the total number of sequences that will be generated and eliminates illogical sequences
- Branches can transfer to other event tress for development
- Each path of an event tree represents a potential scenario
- Each potential scenario results in either prevention of core damage or onset of core damage (or a particular end state of interest)

Small LOCA Event Tree from Surry SDP Notebook

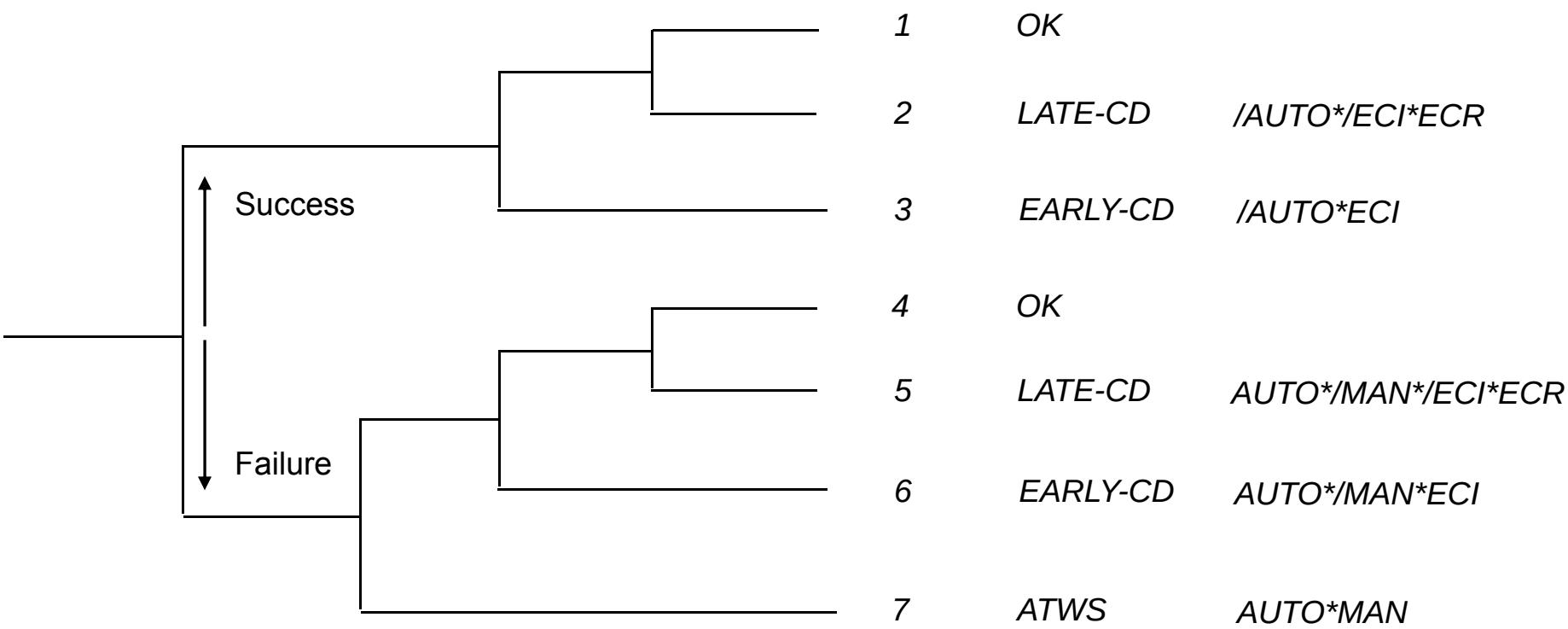


Event Tree Reduction and Simplification

- Single transient event tree can be drawn with specific IE dependencies included at the fault tree level
- Event tree structure can often be simplified by reordering top events
  - Example – Placing ADS before LPCI and CS on a BWR transient event tree
- Event tree development can be stopped if a partial sequence frequency at a branch point can be shown to be very small
- If at any branch point, the delineated sequences are identical to those in delineated in another event tree, the accident sequence can be transferred to that event tree (e.g., SORV sequences transferred to LOCA trees)
- Separate secondary event trees can be drawn for certain branches to simplify the analysis (e.g., ATWS tree)

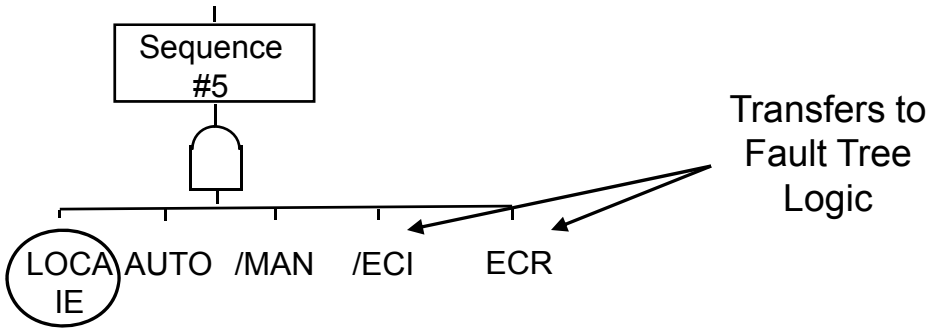
System Level Event Tree Determines Sequence Logic

Initiating Event	Rx Trip	Rx Trip	ST Core Cooling	LT Core Cooling	SEQ #	STATE	LOGIC
LOCA	AUTO	MAN	ECI	ECR			



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 the calculation (via “delete term”)
      - Sequence #5 cut sets ≈ (LOCA) * (AUTO cut sets) * (ECR cut sets) - any cut sets that contain MAN + ECI cut sets are deleted

Plant Damage State (PDS)

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

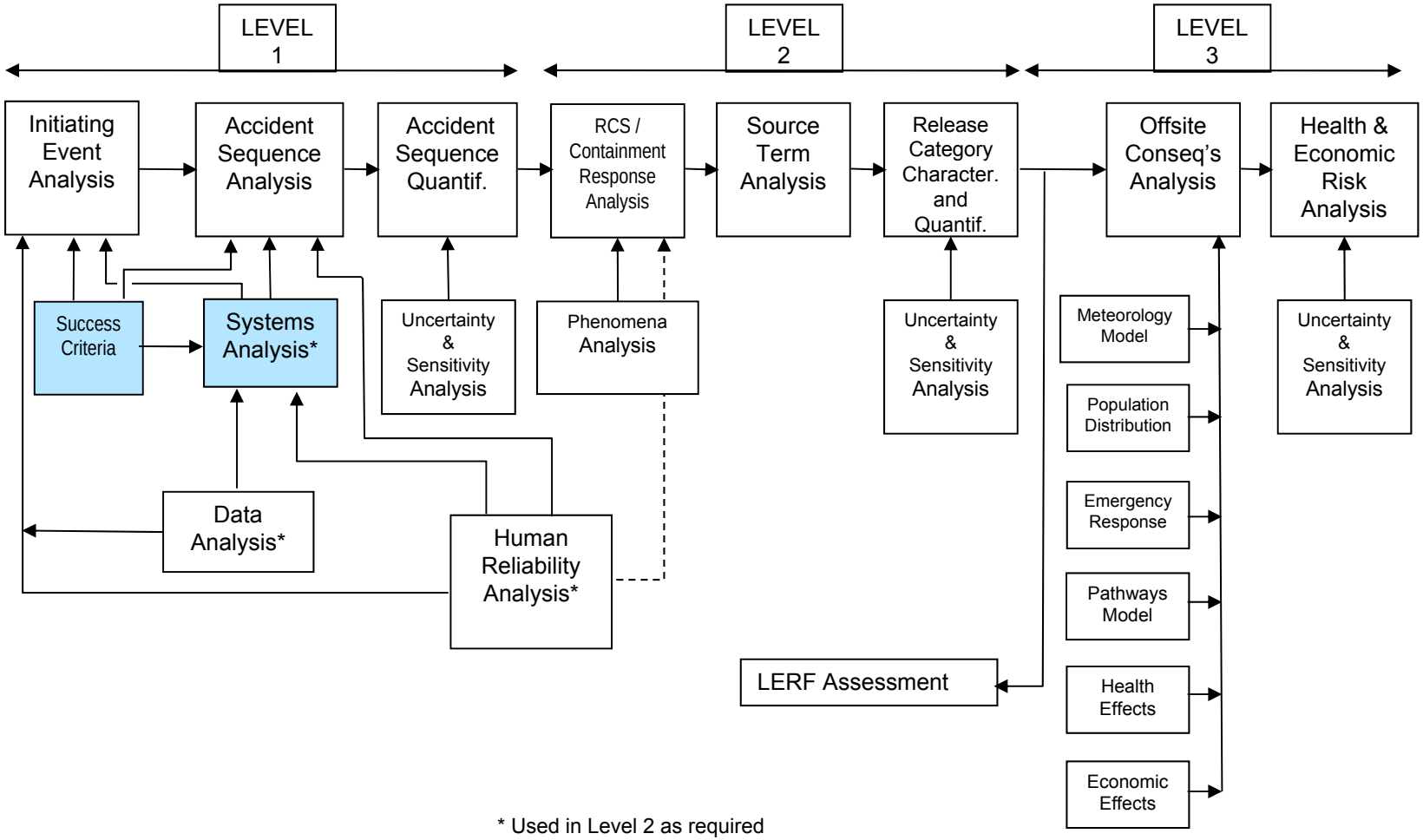
Example Category Definitions for PDS Indicators

1. Status of RCS at onset of Core Damage
   - T no break (transient)
   - A large LOCA (6” to 29”)
   - S1 medium LOCA (2” to 6”)
   - S2 small LOCA (1/2” to 2”)
   - S3 very small LOCA (less than 1/2”)
   - G steam generator tube rupture with SG integrity
   - H steam generator tube rupture without SG integrity
   - V interfacing LOCA
2. Status of ECCS
   - I operated in injection only
   - B operated in injection, now operating in recirculation
   - R not operating, but recoverable
   - N not operating and not recoverable
   - L LPI available in injection and recirculation of RCS pressure reduced
3. Status of Containment Heat Removal Capability
   - Y operating or operable if/when needed
   - R not operating, but recoverable
   - N never operated, not recoverable

Systems Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

Systems (Fault Tree) Analysis

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

Fault Tree Analysis Definition

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

NUREG-0492

Fault Trees

- Deductive analysis (event trees are inductive)
- Starts with undesired event definition
- Used to estimate system failure probability
- Explicitly models multiple failures
- Identify ways in which a system can fail
- Models can be used to find:
  - System “weaknesses”
  - System failure probability
  - Interrelationships between fault events

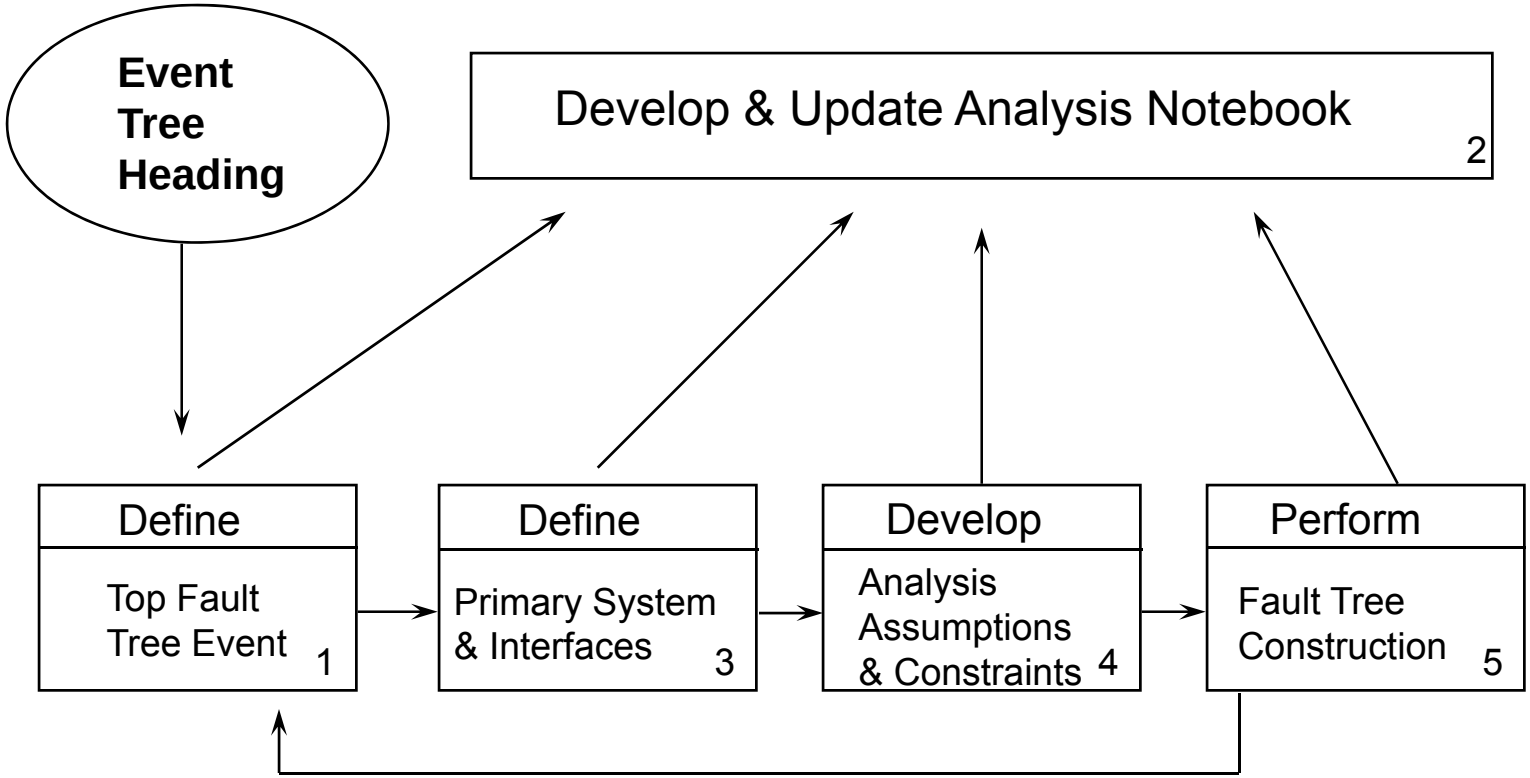
Fault Trees (cont.)

- Fault trees are graphic models depicting the various fault paths that will result in the occurrence of an undesired (top) event.
- Fault tree development moves from the top event to the basic events (or faults) which can cause it.
- Fault tree use gates to develop the fault logic in the tree.
- Different types of gates are used to show the relationship of the input events to the higher output event.
- Fault tree analysis requires thorough knowledge of how the system operates and is maintained.

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

Fault Tree Development Process



1. Define Top Event

- Undesired event or state of system
  - Often corresponds to an event on an event tree
  - Based on success criterion for system
    - Typically initiating event dependent (e.g., HPI would have different success criteria for small LOCA vs. medium LOCA)
    - Can be sequence dependent
    - Success criteria determined from thermal/hydraulic calculations (i.e., computer code runs made to determine how much injection is needed to keep core covered given particular IE)
  - Success criterion used to determine failure criterion
    - Fault tree top event
  - Success criterion must be precise (e.g., “Uninterupted flow from 2/3 HPIS pumps for 24 hours through 2/4 injection lines”

2. Develop & Maintain Analysis Notebook

- Scope of analysis and system definition
- Notebook should include system design and operation information (normal and abnormal), support system requirements, instrumentation and control requirements, technical specifications, test and maintenance data, pertinent analytical assumptions, component locations.
- Notebook reflects the iterative nature of fault tree analysis.

3. Define Primary System & Interfaces

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

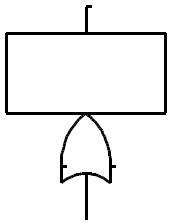
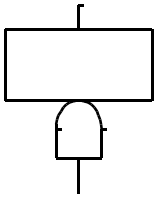
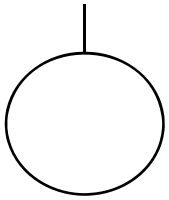
4. Develop Analysis Assumptions & Constraints

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

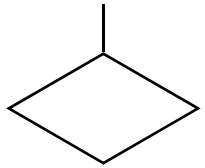
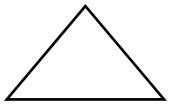
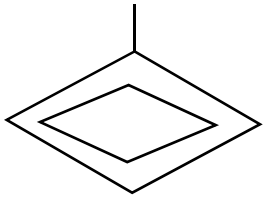
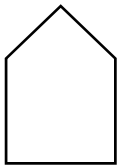
5. Fault Tree Construction

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

Fault Tree Symbols

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

Fault Tree Symbols (cont.)

Symbol		Description
	Undeveloped Event	A fault event whose development is limited due to insufficient consequence or lack of additional detailed information
	Transfer Gate	A transfer symbol to connect various portions of the fault tree
	Undeveloped Transfer Event	A fault event for which a detailed development is provided as a separate fault tree and a numerical value is derived
	House Event	Used as a trigger event for logic structure changes within the fault tree. Used to impose boundary conditions on FT. Used to model changes in plant system status.

Event and Gate Naming Scheme

- A consistent use of an event naming scheme is required to obtain correct results
- Example naming scheme: XXX-YYY-ZZ-AAAA
- Where:
  - XXX is the system identifier (e.g., HPI)
  - YYY is the event and component type (e.g., MOV)
  - ZZ is the failure mode identifier (e.g., FS)
  - AAAAA is a plant component descriptor
- A gate naming scheme should also be developed and utilized - XXXaaa
  - XXX is the system identifier (e.g., HPI)
  - aaa is the gate number

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
  - Fail to Open/Close/Operate
  - Unavailability
    - Test or Maintenance Outage

Typical Component Failure Modes (cont.)

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

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
  - Operator action may be needed to actuate
- Support systems might be required for component to function
  - AC and/or DC power
  - Service water or component water cooling
  - Room cooling

Definition of Dependent Failures

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

Common Cause Failures (CCFs)

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

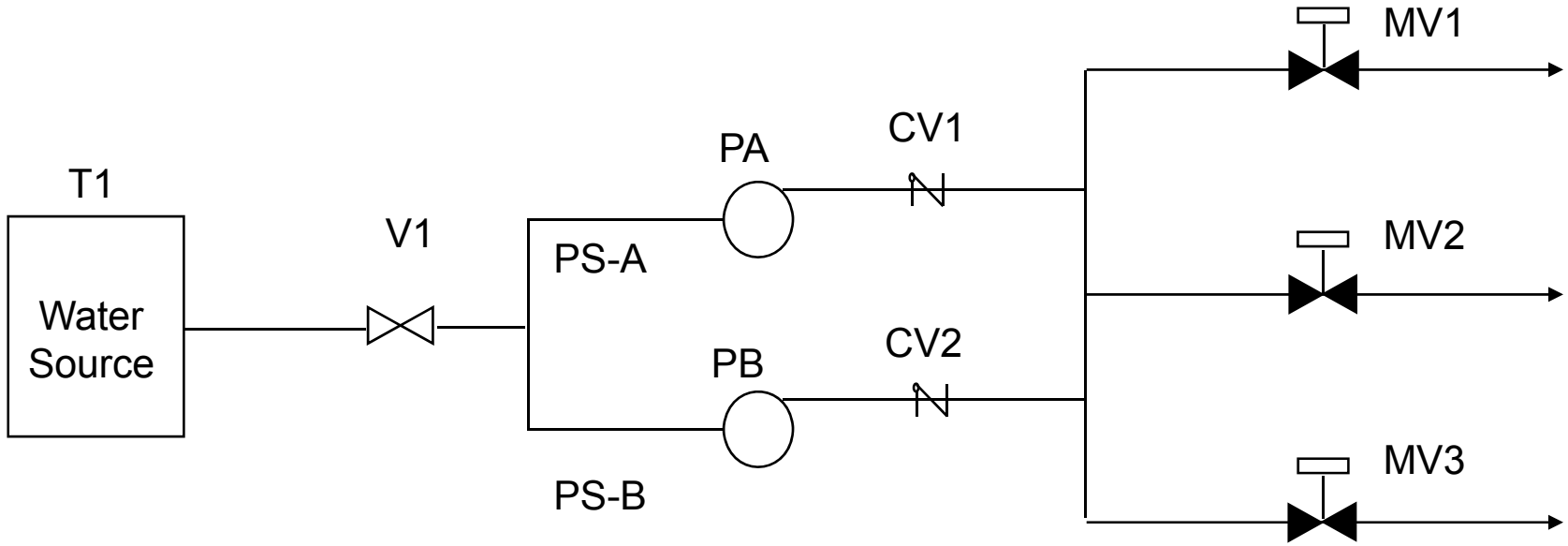
Common Cause Failure Mechanisms

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

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

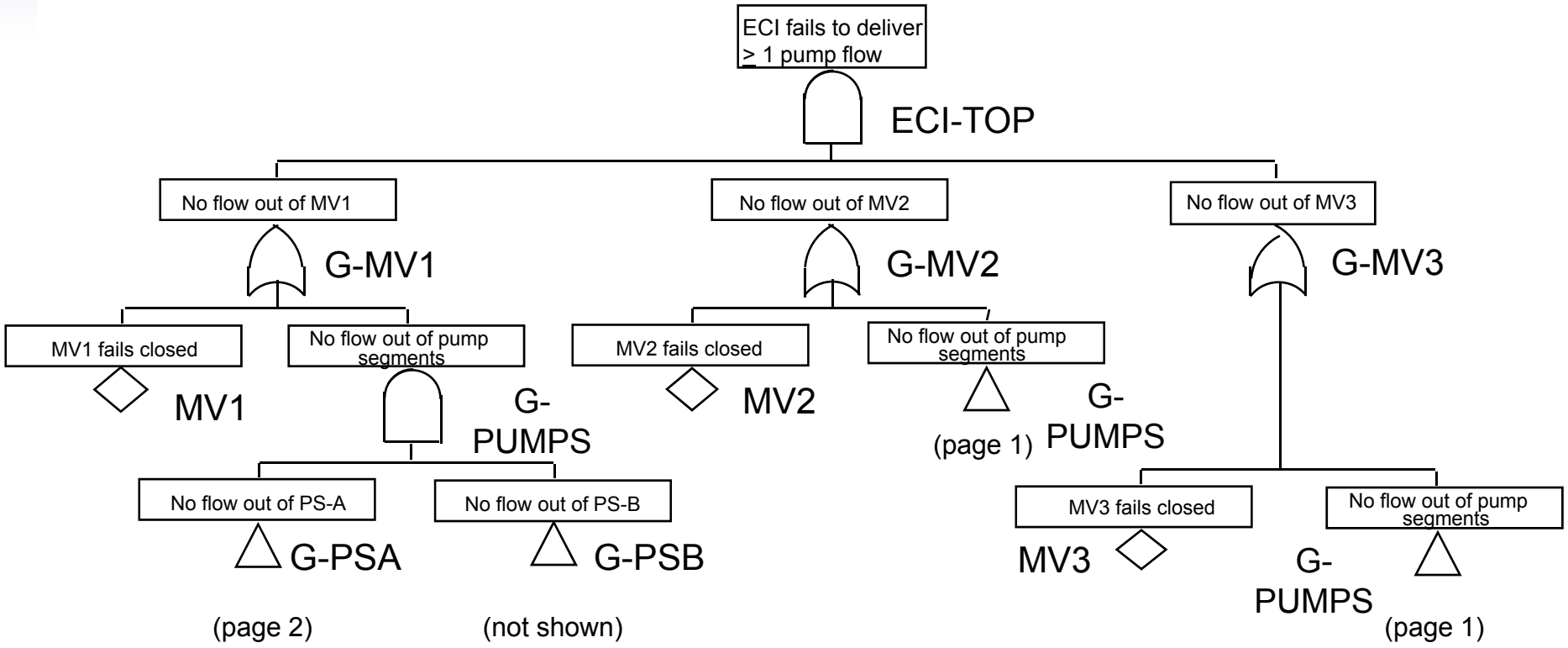
Example - ECI



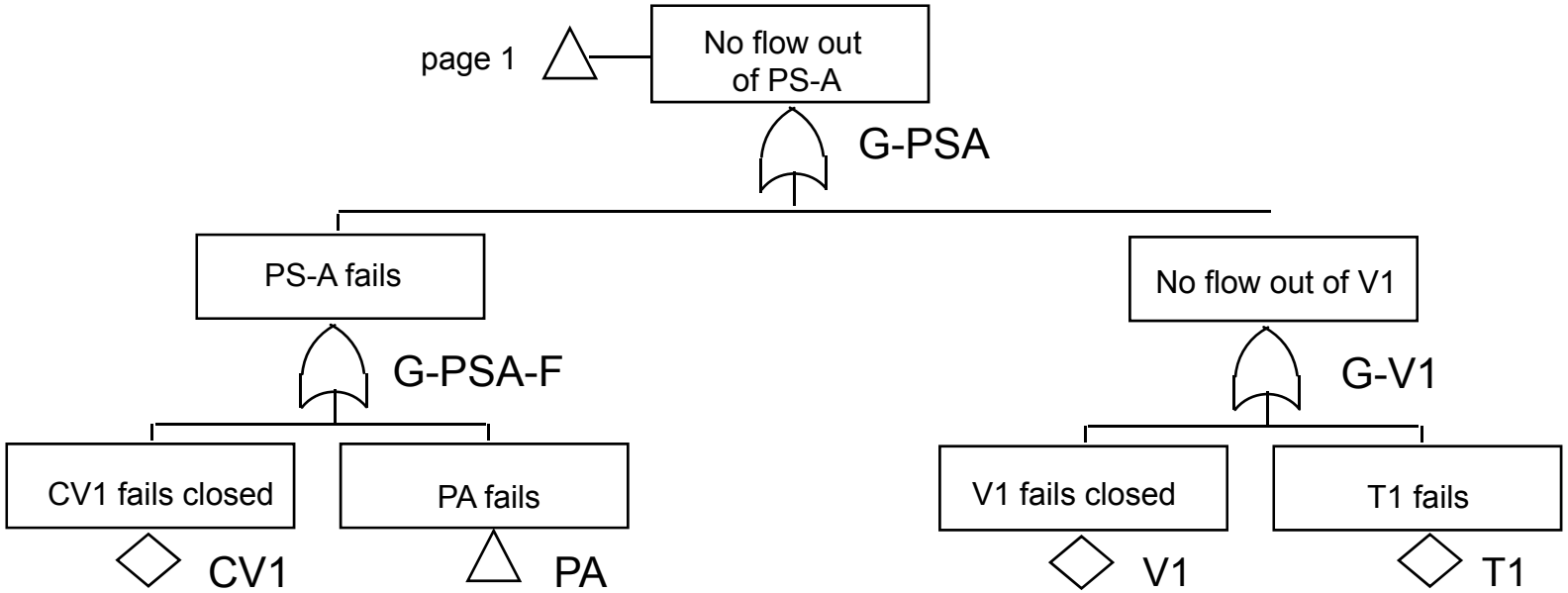
***Success Criteria**: Flow from any one pump through any one MV*

T_ tank
V_ manual valve, normally open
PS-_ pipe segment
P_ pump
CV_ check valve
MV_ motor-operated valve, normally closed

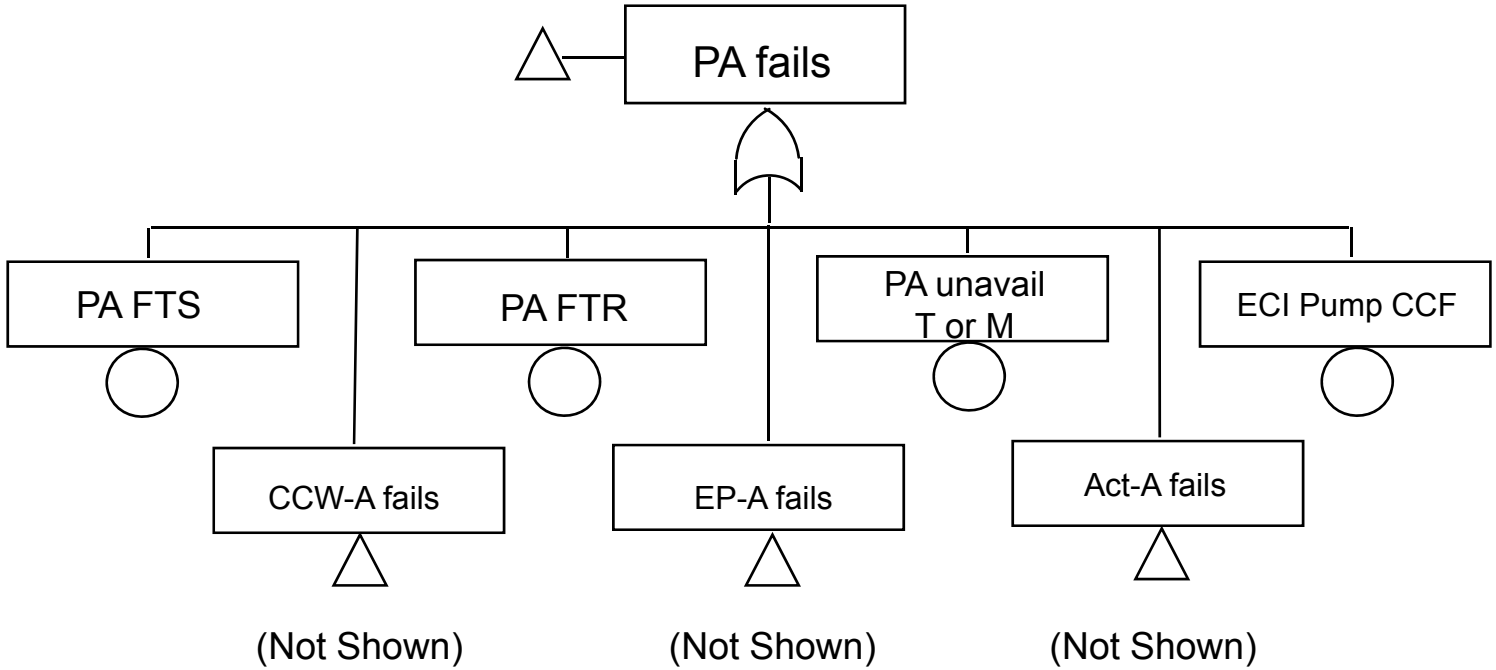
ECI System Fault Tree – "Sink to Source Method" (page 1)



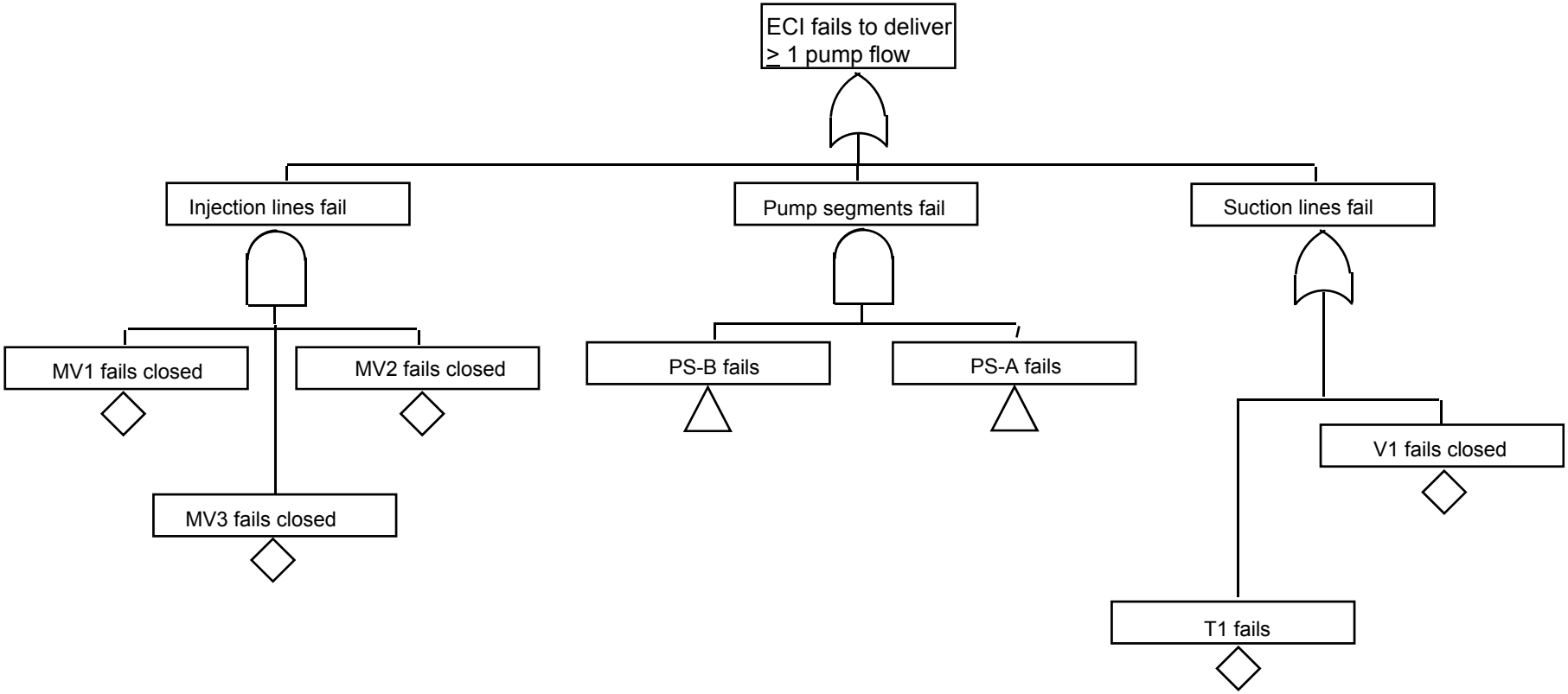
ECI System Fault Tree – "Sink to Source Method" (page 2)



ECI System Fault Tree – "Sink to Source Method" (page 3)



ECI System Fault Tree - Block Diagram Method



Boolean Fault Tree Reduction

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

Rules of Boolean Algebra

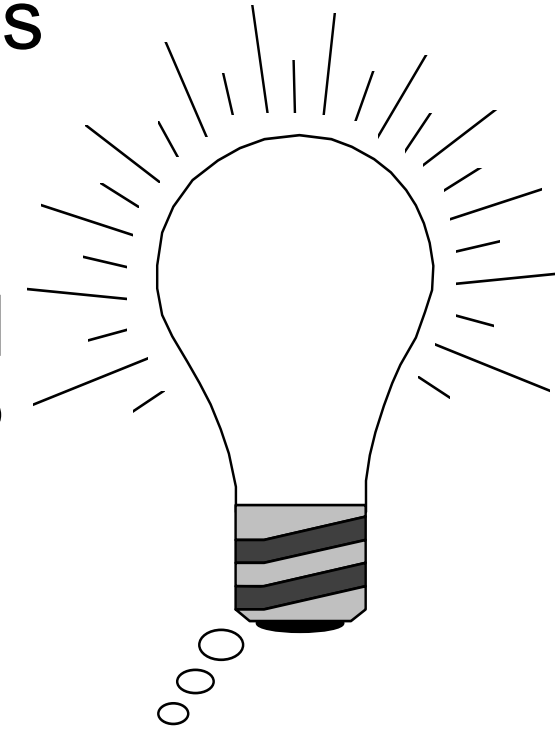
Mathematical Symbolism	Engineering Symbolism	Designation
(1a) $X \cap Y = Y \cap X$	$X \cdot Y = Y \cdot X$	Commutative Law
(1b) $X \cup Y = Y \cup X$	$X + Y = Y + X$	
(2a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$	$X * (Y * Z) = (X * Y) * Z$ $X(YZ) = (XY)Z$	Associative Law
(2b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X + (Y + Z) = (X + Y) + Z$	
(3a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	$X * (Y + Z) = (X * Y) + (X * Z)$ $X(Y+Z) = XY + XZ$	Distributive Law
(3b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X + (Y * Z) = (X + Y) * (X + Z)$	
(4a) $X \cap X = X$ **Important!**	$X \cdot X = X$	Idempotent Law
(4b) $X \cup X = X$	$X + X = X$	
(5a) $X \cap (X \cup Y) = X$	$X \cdot (X + Y) = X$	Law of Absorption
(5b) $X \cup (X \cap Y) = X$	$X + X * Y = X$	
(6a) $X \cap X' = \Phi = 0$	$X \cdot /X = \Phi = 0$	Complementation
(6b) $X \cup X' = \Omega = I$	$X + /X = \Omega = I$	
(6c) $(X')' = X$	$/(/X) = X$	
(7a) $(X \cap Y)' = X' \cup Y'$	$/(X \cdot Y) = /X + /Y$	DeMorgan's Theorem
(7b) $(X \cup Y)' = X' \cap Y'$	$/(X + Y) = /X * /Y$	

Algebra

Important During Cut Set Generation

Minimal Cutset

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



Reduction of Example Fault Tree

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

Start Substituting

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

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).

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 * MV2 * MV3) +
(G-PUMPS * MV2) +
(G-PUMPS * MV3) +
(G-PUMPS).

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

Reduction of Example Fault Tree (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.

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
- Modeling T&M unavailability can result in illegal cutsets
- Putting recovery in FT might give optimistic results
- Logic loops

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

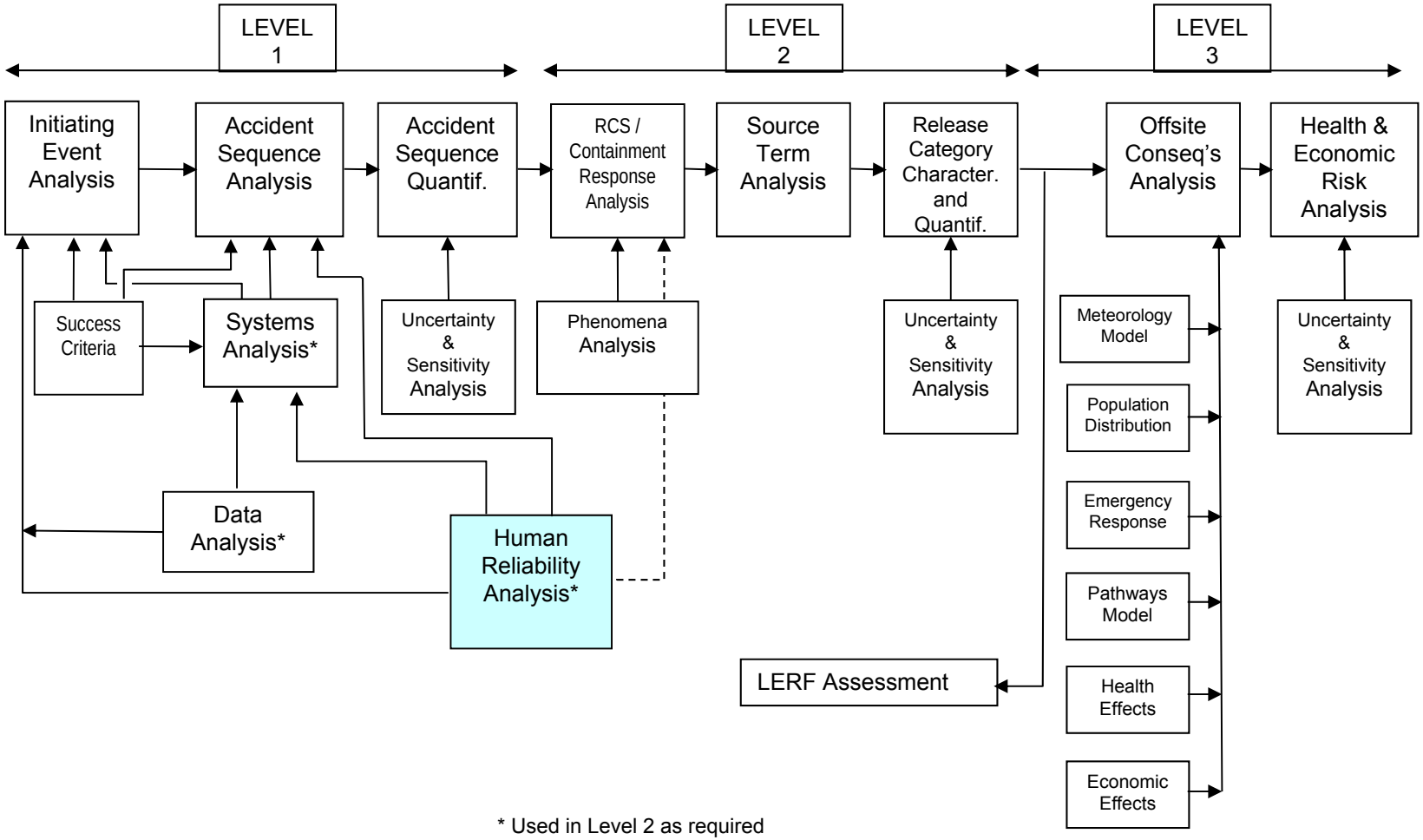
Results

- 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?

Human Reliability Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

Human Reliability Analysis

Purpose: This session will provide a generalized, high-level introduction to the topic of human reliability and human reliability analysis in the context of PRA.

Objectives: Provide students with an understanding of:
- The goals of HRA and important concepts and issues
- The basic steps of the HRA process in the context of PRA
- Basic aspects of selected HRA methods

HRA Purpose

Why Develop a HRA?

- **PRA reflects the as-built, as-operated plant**
  - **HRA models the "as-operated" portion**

Definition of HRA

- A **structured approach** used to **identify** potential human failure events (HFEs) and to systematically **estimate the probability** of those errors using data, models, or expert judgment

HRA Produces

- Qualitative evaluation of the factors impacting human errors and successes
- Human error probabilities (HEPs)

Human Reliability Analysis

- Starts with the basic premise that the humans can be represented as either:.
  - A component of a system, or
  - A failure mode of a system or component.
- Identifies and quantifies the ways in which human actions initiate, propagate, or terminate fault & accident sequences.
- Human actions with both positive and negative impacts are considered in striving for realism.
- A difficult task in a PRA since need to understand the plant hardware response, the operator response, and the accident progression modeled in the PRA.

Human Reliability Analysis Objectives

Ensure that the **impacts of plant personnel** actions are reflected in the assessment of risk in such a way that:

a) both **pre-initiating event and post-initiating event** activities, including those modeled in support system initiating event fault trees, are addressed.

b) logic model elements are defined to represent the effect of such personnel actions on **system availability**/unavailability and on **accident sequence** development.

c) **plant-specific and scenario-specific factors** are accounted for, including those factors that influence either what activities are of interest or human performance.

d) human performance issues are addressed in an integral way so that **issues of dependency are captured**.

Ref. ASME RA-Sb-2005

Modeling of Human Actions

- Human Reliability Analysis provides a structured modeling process
- HRA **process steps**:
  - Identification & Definition
    - Human interaction identified, then defined for use in the PRA as a Human Failure Event (HFE)
    - Includes HFE categorization as to the type of action
  - Qualitative analysis of context & performance shaping factors
  - Quantification of Human Error Probability (HEP)
  - Dependency
  - Documentation

Categories Of Human Failure Events in PRA

- Operator actions can occur throughout the accident sequence
  - **Pre-initiator errors** (latent errors, unrevealed) occur before the initiating event.
    - May occur in or out of the main control room
    - Failure to restore from test/maintenance
    - Miscalibration
    - Often captured in equipment failure data
    - For HRA the focus is on equipment being left unavailable or not working exactly right.
  - Operator actions contribute or **cause initiating events**
    - Usually implicitly included in the data used to quantify initiating event frequencies.

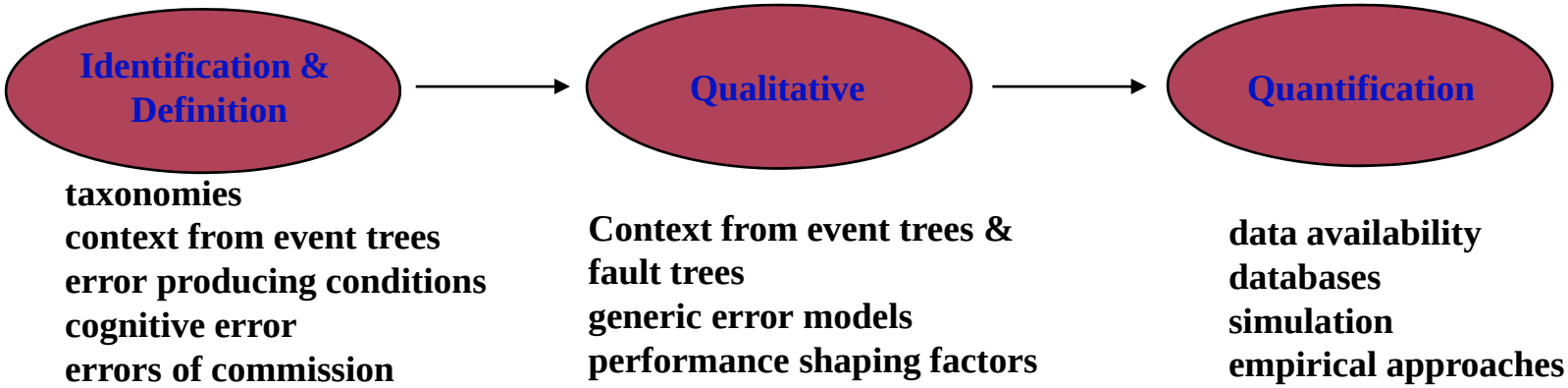
Categories Of Human Failure Events in PRA (cont'd)

– **Post-initiator errors** occur after reactor trip. Examples:
  - Operation of components that have failed to operate automatically, or require manual operation.
  - "Event Tree top event" operator actions modeled in the event trees (e.g., failure to depressurize the RCS in accordance with the EOPs)
  - Recovery actions for hardware failures (example - aligning an alternate cooling system, subject to available time)
  - Recovery actions following crew failures (example - providing cooling late after an earlier operator action failed)
  - Operation of components from the control room or locally.

Categorization & Definition of Human Failure Events in PRA (cont'd)

- Additional "category", error of commission or aggravating errors of commission, typically out of scope of most PRA models.
  - Makes the plant response worse than not taking an action at all
- Within each operator action, there are generally, two types of error:
  - Diagnostic error (cognition) – failure of detection, diagnosis, or decision-making
  - Execution error (manipulation) – failure to accomplish the critical steps, once they have been decided, typically due to the following error modes.
    - Errors of omission (EOO, or Skip) -- Failure to perform a required action or step, e.g., failure to monitor tank level
    - Errors of commission (EOC, or Slip) -- Action performed incorrectly or wrong action performed, e.g., opened the wrong valve, or turned the wrong switch.

Human Reliability Analysis is the Combination of Three Basic Steps



From about 1980 on, some 38 different HRA methods have been developed - almost all centered on quantification.

There is no universally accepted HRA method (to date).

The context of the operator action comes directly from the event trees and fault trees although some techniques have recently ventured beyond.

Identification & Definition Process

- **Identify** Human Failure Events (HFEs) to be considered in plant models.
  - Based on PRA event trees, fault trees, & procedures.
    - Includes front line systems & support systems.
  - Often done in conjunction with the PRA modelers (Qualitative screening)
  - Normal Plant Ops-- Identify potential errors involving miscalibration or failure to restore equipment by observing test and maintenance, reviewing relevant procedures and plant practices
    - Guidelines for pre-initiator qualitative screening
  - Post-Trip Conditions-- Determine potential errors in diagnosing and manipulating equipment in response to various accident situations

Identification & Definition Process (cont.)

- PRA model identifies component/system/function failures
- HRA requires **definition** of supporting information, such as:
  - for post-initiating events, the cues being used, timing and the emergency operating procedure(s) being used.
- ATHEANA – identify the "base case" for accident scenario
  - Expected scenario – including operator expectations for the scenario
  - Sequence and timing of plant behavior – behavior of plant parameters
  - Key operator actions

Identification Process (cont'd)

- Review emergency operating procedures to identify potential human errors
- Flow chart the EOPs to identify critical decision points and relevant cues for actions
- If possible, do early observations of simulator exercises
- List human actions that could affect course of events (qualitative screening)

Qualitative Analysis

- **Context**, a set of plant conditions based on the PRA model
  - Initiating event & event tree sequence
    - includes preceding hardware & operator successes/failures
  - Cues, Procedure, Time window
- Qualitatively examine factors that could influence performance (**Performance Shaping Factors, PSFs**) such as
  - Training/experience
  - Clarity of cues
  - Task complexity
  - Environmental cond.
  - Human-machine interface
  - Management and organizational factors
  - Scenario timing
  - Workload
  - Crew dynamics
  - Accessibility
- Note ATHEANA models "Error Forcing Context" consisting of plant context & scenario-specific factors that would influence operator response.

Performance Shaping Factors (PSFs)

- Are people-, task-, environmental-centered influences which could affect performance.
- Most HRA modeling techniques allow the analyst to account for PSFs during their quantification procedure.
- PSFs can Positively or Negatively impact human error probabilities
- PSFs are identified and evaluated in the human reliability task analysis

Quantifying the Human Error Probability

- Quantifying is the process of
  - selecting an HRA method then
  - calculating the Human Error Probability for a HFE
    - based on the qualitative assessment and
    - based on the context definition.
- The calculation steps depend on the methodology being used.
- Data sources – the input data for the calculations typically comes operator talk-throughs &/or simulations, while some methods the data comes from databanks or expert judgment.
- The result is typically called a Human Error Probability or HEP

Levels of Precision

- Conservative (screening) level useful for determining which human errors are the most significant contributors to overall system error
- Those found to be potentially significant contributors can be profitably analyzed in greater detail (which often lowers the HEP)

Screening

- Too many HFEs to do detailed quantification?
  - Trying to reduce level of effort, resources
  - Used during IPE era for initial model development
- ASME PRA Standard
  - Pre-initiators: screening pre-initiators is addressed in High Level Requirement HLR-HR-B
  - Post-initiators: screening is not addressed explicitly as a High Level Requirement
    - Supporting requirement HR-G1 limits the PRA to Capability Category I if conservative/screening HEPs used.
- Thus, screening is more appropriate to Fire PRA.

Detailed Quantification

- Point at which you bring all the information you have about each event
  - PSFs, descriptions of plant conditions given the sequence
  - Results from observing simulator exercises
  - Talk-throughs with operators/trainers
  - Dependencies
- Quantification Methods
  - Major problem is that none of the methods handle all this information very well
- Assign HEPs to each event in the models

HRA Methods

- Attempt to reflect the following characteristics:
  - plant behavior and conditions
  - timing of events and the occurrence of human action cues
  - parameter indications used by the operators and changes in those parameters as the scenario proceeds
  - time available and locations necessary to implement the human actions
  - equipment available for use by the operators based on the sequence
  - environmental conditions under which the decision to act must be made and the actual response must be performed
  - degree of training, guidance, and procedure applicability

Common HRA Methodologies in the USA

- Technique for Human Error Rate Prediction (THERP)
- Accident Sequence Evaluation Program (ASEP) HRA Procedure
- Cause-Based Decision Tree (CBDT) Method
- Human Cognitive Reliability (HCR)/Operator Reliability Experiments (ORE) Method
- Standardized Plant Analysis Risk HRA (SPAR-H) Method
- A Technique for Human Event Analysis (ATHEANA)

Caused Based Decision Tree (CBDT) Method (EPRI)

Series of decision trees address potential causes of errors, produces HEPs based on those decisions.

- Half of the decision trees involve the man-machine cue interface:
  - Availability of relevant indications (location, accuracy, reliability of indications);
  - Attention to indications (workload, monitoring requirements, relevant alarms);
  - Data errors (location on panel, quality of display, interpersonal communications);
  - Misleading data (cues match procedure, training in cue recognition, etc.);
- Half of the decision trees involve the man-procedure interface:
  - Procedure format (visibility and salience of instructions, place-keeping aids);
  - Instructional clarity (standardized vocabulary, completeness of information, training provided);
  - Instructional complexity (use of "not" statements, complex use of "and" & "or" terms, etc.); and
  - Potential for deliberate violations (belief in instructional adequacy, availability and consequences of alternatives, etc.).
- For time-critical actions, the CBDT is supplemented by a time reliability correlation

EPRI HRA Calculator

- Software tool
- Uses SHARP1 as the HRA framework
- Post-initiator HFE methods:
  - For diagnosis, uses CBDT (decision trees) and/or HCR/ORE (time based correlation)
  - For execution, THERP for manipulation
- Pre-Initiator HFE methods:
  - Uses THERP and ASEP to quantify pre-initiator HFEs

ATHEANA

- Experience-based (uses knowledge of domain experts, e.g., operators, pilots, trainers,etc.)
- Focuses on the error-forcing context
- Links plant conditions, performance shaping factors (PSFs) and human error mechanisms
- Consideration of dependencies across scenarios
- Attempts to address PSFs holistically (considers potential interactions)
- Structured search for problem scenarios and unsafe actions

Dependencies

Dependency refers to the extent to which failure or success of one action will influence the failure or success of a subsequent action.

1) Human interaction depends on the accident scenario, including the type of initiating event
2) Dependencies between multiple human actions modeled within the accident scenario,
3) Human interactions performed during testing or maintenance can defeat system redundancy,
4) Multiple human interactions modeled as a single human interaction may involve significant dependencies. (from SHARP1)

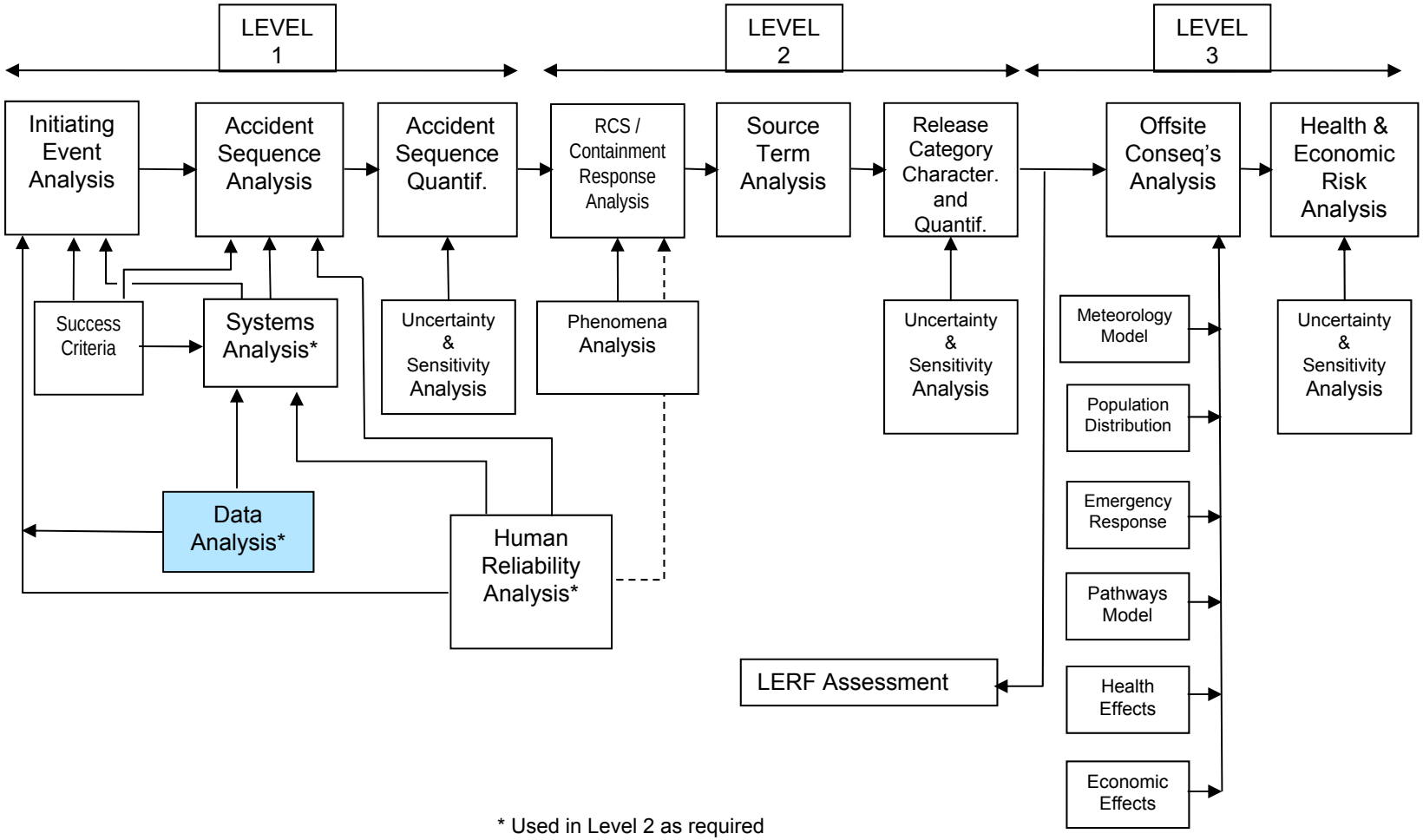
HRA Process Summary

- Human Reliability Analysis provides a structured modeling process
- Human Interactions are incorporated as Human Failure Events in a PRA, **identification & definition** finds the HFEs
- Post-initiator operator actions consist of:
  - **Qualitative analysis** of Context and Performance Shaping Factors
    - Operator action must be feasible (for example, sufficient time, sufficient staff, sufficient cues, access to the area)
  - Then **Quantitative assessment (using an HRA method**)
    - Includes dependency evaluation
- Two Parts of the Each Human Failure Event (HFE)
  - Operator must recognize the need/demand for the action (**cognition**) AND
  - Operator must take steps (**execution**) to complete the actions.

Data Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

Data Analysis

- Purpose: Students will be introduced to sources of initiating event data; and hardware data and equipment failure modes, including common cause failure, that are modeled in PRAs.

- Objectives: Students will be able to:
  - Understand parameters typically modeled in PRA and how each is quantified.
  - Understand what is meant by the terms
    - Generic data
    - Plant-specific data
    - Bayesian updating
  - Describe what is meant by common-cause failure, why it is important, and how it is included in PRA

References

- NUREG/CR-6823 PRA Data Handbook
- NUREG/CR-5750 IE Frequency Data
- NUREG/CR-5500 Reliability Study (multiple systems)
- NUREG/CR-6928 IE and Component Data
- NUREG/CR-2300 PRA Procedures Guide
- NUREG-1489 (App. C) NRC Use of PRA
- NUREG/CR-5485, Guidelines on modeling Common-Cause failures in PRA
- NUREG/CR-5497, Common-Cause Failure Parameter Estimations
- NUREG/CR-6268, Common-Cause Failure Database and Analysis System: Event Definition and Classification
- N. Siu and D. Kelly, "Bayesian Parameter Estimation in PRA," tutorial paper in Reliability Engineering and System Safety 62 (1998) 89-116.
- Martz and Waller, "*Bayesian Reliability Analysis*."

PRA Parameters

- Initiating Event Frequencies
- Basic Event Probabilities
  - Hardware
    - component reliability (fail to start/run/operate/etc.)
    - component unavailability (due to test or maintenance)
  - Common Cause Failures
  - Human Errors (discussed in previous session)

Categories of Data

- Two basic categories of data: plant-specific and generic
- Some guidance on the use of each category:
  - Not feasible or necessary to collect plant-specific data for all components in a PRA (extremely reliable components may have no failures)
  - Some generic data sources are non-conservative (e.g., LERS do not report all failures)
  - Inclusion of plant-specific data lends credibility to the PRA
  - Inclusion of plant-specific data allows comparison of plant equipment performance to industry averages
- Should use plant-specific data whenever possible, as dictated by the availability of relevant information

Initiating Event Frequencies

- Typically combination of:
  - Generic data for rare events (e.g., LOCAs)
  - Plant-specific data for more common events (most transients)
- An IE frequency is a failure rate (λ)
  - Poisson: prob(r failures in time t) = $(1/r!)\, e^{-\lambda t}(\lambda t)^r$

    prob(r >0, in time t) = $1-e^{-\lambda t} \approx \lambda t$ (for $\lambda t << 1$)
- Parameters required are number of plant scrams and total time
  - For at-power PRAs, time parameter is the number of years plant is critical

Basic Events Probabilities

- Probability of failure depends on mission and failure rate (i.e., the λ or p)
  - 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 set of failure events and set of demands (or time) must be consistent with each other

Failure Probability Models

- Demand Failures
  - Binomial: prob(r failures in n demands)

    $= \quad p^r(1-p)^{n-r}$

    prob(1 failure|1 demand) = p = Q_d
- Failures in Time
  - Poisson: prob(r failures in time t) = $(1/r!)\, e^{-\lambda t}(\lambda t)^r$

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

Q = Failure probability (unreliability or unavailability)	t_i = surveillance test interval
p = Failure rate (per demand)	λ_m = maintenance frequency
λ_s = Failure rate (per hour) standby	d_m = maintenance duration
λ_h = Failure rate (per hour) operating	t_{OOS} = total time out of service
t_m = mission time	t_{total} = total time

Component Failure Modes

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

Boundary Conditions and Modeling Assumptions Affect Form of Data

- Clear understanding of component boundaries and missions needed to accurately use raw data or generic failure rates. For example:
  - Do motor driven components include circuit breakers? (Are CB faults included in component failure rate?)
- Failure mode being modeled also impacts type and form of data needed to quantify the PRA.
  - FTR – failures while operating and operating time
  - FTS/FTO – failures and demands (successes)

Data Sources for Parameter Estimation

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

Generic Data Sources

- NUREG-1150 supporting documents (NUREG/CR-4550 series, pre-1987)
- WASH-1400 (pre-1975)
- IEEE Standard 500 (1990)
- NUREG/CR-3862 for initiating events (pre-1986)
- NUREG/CR-5750 for initiating events (1987-1995)
- NUREG/CR-5500 for system reliability (1984-1998)
- NUREG/CR-6928 for components and initiating events (1998-2002)
- NUREG-1032 for loss of offsite power(pre-1988)
- NUREG-5496 loss of offsite power (1980-1996)
- SECY 04-0060 Loss-of-Coolant Accident Break Frequencies for the Option III Risk-Informed Reevaluation of 10 CFR 50.46, Appendix K to 10 CFR Part 50, and General Design Criteria (GDC) 35 (April 2004)
- NUREG-1829 Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process (June 2005)
- Institute of Nuclear Power Operations Nuclear Plant Reliability Data System (NPRDS) – archival only (no longer maintained)
- Institute of Nuclear Power Operations Equipment Performance Information Exchange (EPIX) – replaced NPRDS

Generic Data Issues

- Key issue is whether data is applicable for the specific plant being analyzed
  - Most generic component data is mid-1980s or earlier vintage
  - Some IE frequencies known to have decreased over the last decade
    - Frequencies updated in NUREG/CRs 5750 and 5496
  - Criteria for judging data applicability not well defined (do not forget important engineering considerations that could affect data applicability)
  - ASME PRA Standard requirements

Plant-Specific Data Sources

- Licensee Event Reports (LERs)
  - Can also be source of generic data
- Post-trip SCRAM analysis reports
- Maintenance reports and work orders
- System engineer files
- Control room logs
- Monthly operating status reports
- Test surveillance procedures

Plant-Specific IE and Component Data Collection and Analysis

- Gather data to obtain raw information needed for estimating event parameters
  - Determine period of time for obtaining plant data
    - Entire plant history can be used minus first year of operation
    - Most recent data should be used to represent current maintenance practices and component performance
    - Five to seven years of data is desirable
  - Collect plant information from plant records and documents listed on previously
  - Sort data by IE category; component, failure mode, and severity
    - Plant changes can affect the categorization of a scram event
  - Pool data from several like components in same system
  - Screen data
    - Events that can no longer occur due to plant change can be eliminated
  - Obtain exposure estimates
  - Interpret the information to obtain variables of interest (e.g., failures, demands, operating hours)
  - Estimate parameter values from data
  - Scram data can be used to estimate some conditional event probabilities (e.g., relief valve sticking open)

Component Failure Severity Classification

- Raw data is classified by severity of the component failure
- Example severity classes:
  - Catastrophic - the component would have failed to perform its function
  - Degraded – component degraded to point where it can not meet required success criteria and was taken out of operation for repair

  Incipient - component degraded but could still function and was taken out of operation for repair
- The class of failure severity determines if raw data is used in calculating a specific data parameter
  - Catastrophic and degraded failures are used in calculating failure rates and probabilities and maintenance outage unavailabilities
  - Incipient failures are used to calculate maintenance outage unavailabilities

Component Exposure Estimates

- "Exposures" refers to the amount of component operating time (failure rates) and the number of demands (failure probabilities)
- Sources of component exposure include:
  - Tests – Tech Specs, procedures, test records used to estimate frequency and duration of tests
  - Actuations – actual equipment usage
  - Failure-related actuations – operability test after maintenance event (ASME Standard says not to include this)
  - Interface-related actuations – increased test frequency per Tech Spec (e.g., DGs) and closure of valves to isolate failed components
  - Operation time meter

Plant-Specific Data Issues

- Combining data from different sources can result in:
  - double counting of the same failure events
  - inconsistent component boundaries
  - inconsistent definition of “failure”
- Plant-specific data is typically very limited
  - small statistical sample size
- Inaccuracy and non-uniformity of reporting
  - LER reporting rule changes
- Difficulty in interpreting “raw” failure data
  - administratively declared inoperable, does not necessarily equate to a “PRA” failure

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)

Bayes' Theorem is Basis for Bayesian Updating of Data

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

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

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

Bayesian 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

Common Cause Failures (CCFs)

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

Common Cause Failure Mechanisms

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

Common Cause Modeling in PRA

- Three parametric models used
  - Beta factor (original CCF model)

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

  - Multiple Greek Letter (MGL) model
    - (β = 2 failures, $\gamma = 3$ failures, $\delta = 4$ failures)
  - Alpha factor model (addressed uncertainty concerns in MGL)
    - $\alpha_k \equiv$ conditional probability that a failure event involves k components failing due to a shared cause, given a failure event
- Apply to cut sets containing same failure mode for sample component type
  - Diesel generators
  - MOVs, AOVs, PORVs, SRVs
  - Pump
  - Batteries

Beta Factor Example

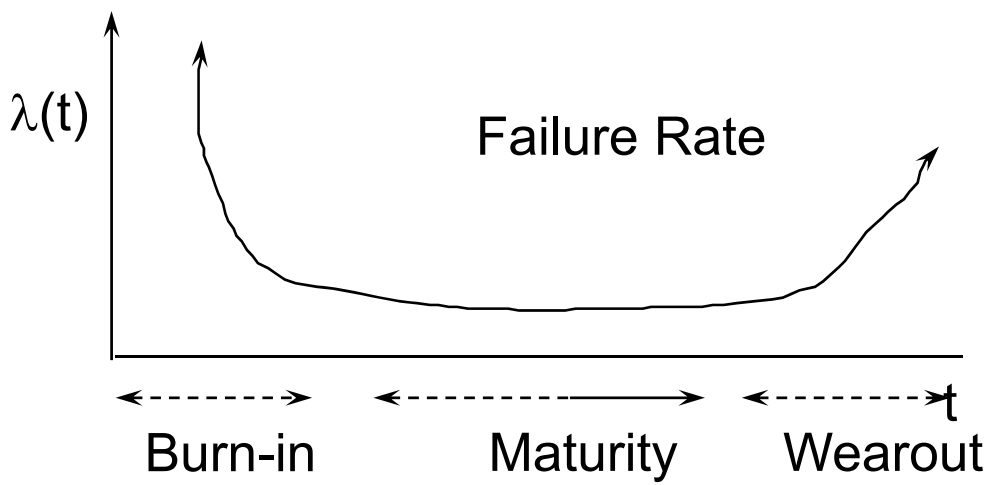
- High pressure pumps
  - β = 10 CCF $\div$ 47 total failures $\approx$ 2.1E-1
  - Motor-driven pump fail to start = 3.0E-3 per demand
- Cut set: HPI-MDP-FS-A * HPI-MDP-FS-B
  - Independent failure $\approx$ 3E-3 * 3E-3 = 9E-6
- Cut set: HPI-MDP-CF-CCFAB
  - CCF = 3E-3 * β = 6E-4

Limitations of CCF Modeling

- Limited data, hence generic data often used
  - Applicability issue for specific plant
- Screening values may be used
  - Potential to skew the results
- Not typically modeled across systems since data is collected/analyzed for individual systems
- Not typically modeled for divers components (e.g., motor-driven pump/turbine-driven pump)
- Causes not explicitly modeled (i.e., each failure mechanism not explicitly modeled)

Component Data Not Truly Time Independent

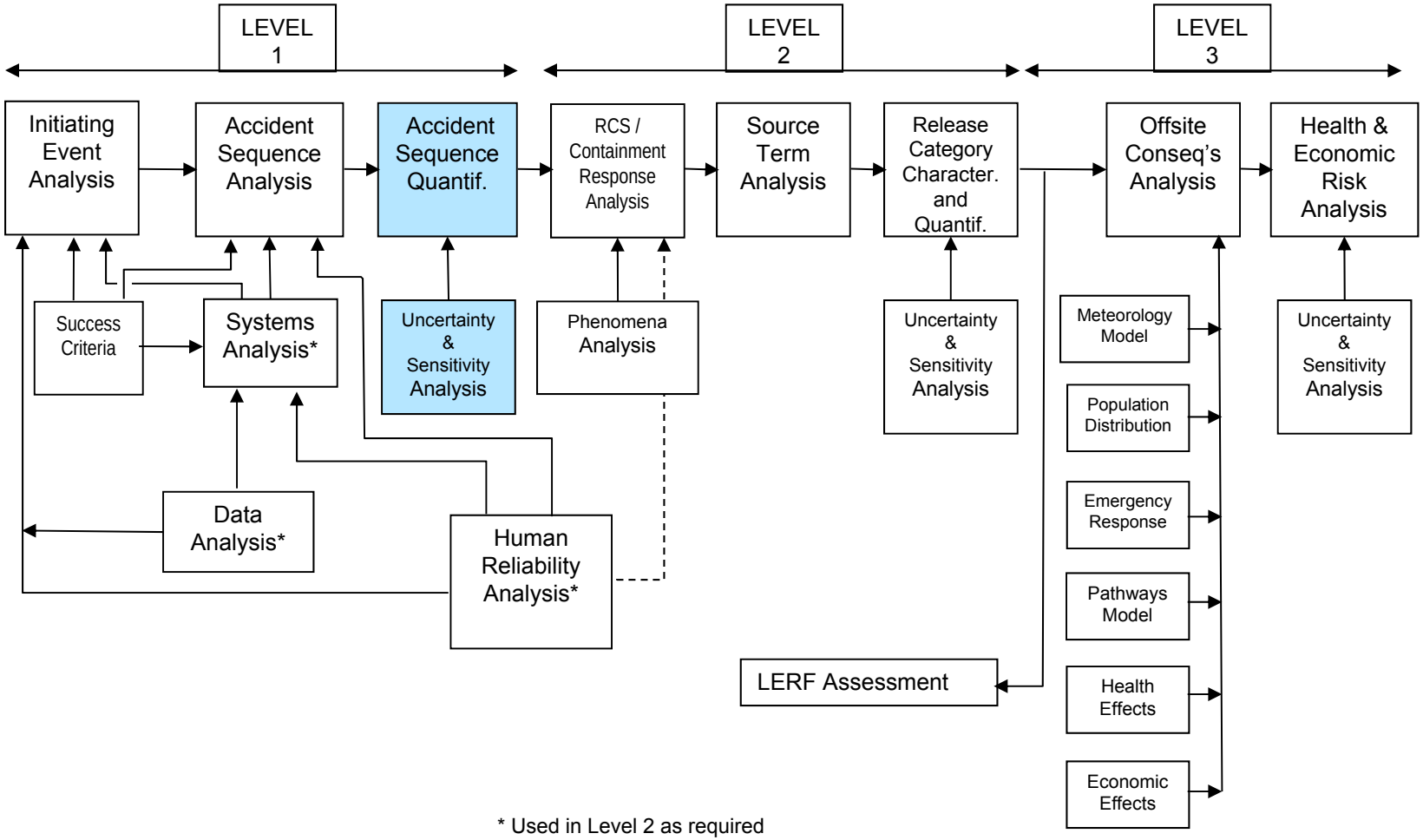
- PRAs typically assume time-independence of component failure rates
  - One of the assumptions for a Poisson process (i.e., failures in time)
- However, experience has shown aging of equipment does occur
  - Failure rate (λ) = $\lambda(t)$
  - "Bathtub" curve



Accident Sequence Quantification

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

Purpose and Objectives

- Purpose
  - Present elements of accident sequence quantification and importance analysis and introduce concept of plant damage states
- Objectives
  - Become familiar with the:
    - process of generating and quantifying cut sets
    - different importance measures typically calculated in a PRA
    - impact of correlation of data on quantification results
    - definition of plant damage states
- References: NUREG/CR-2300 and NUREG/CR-2728

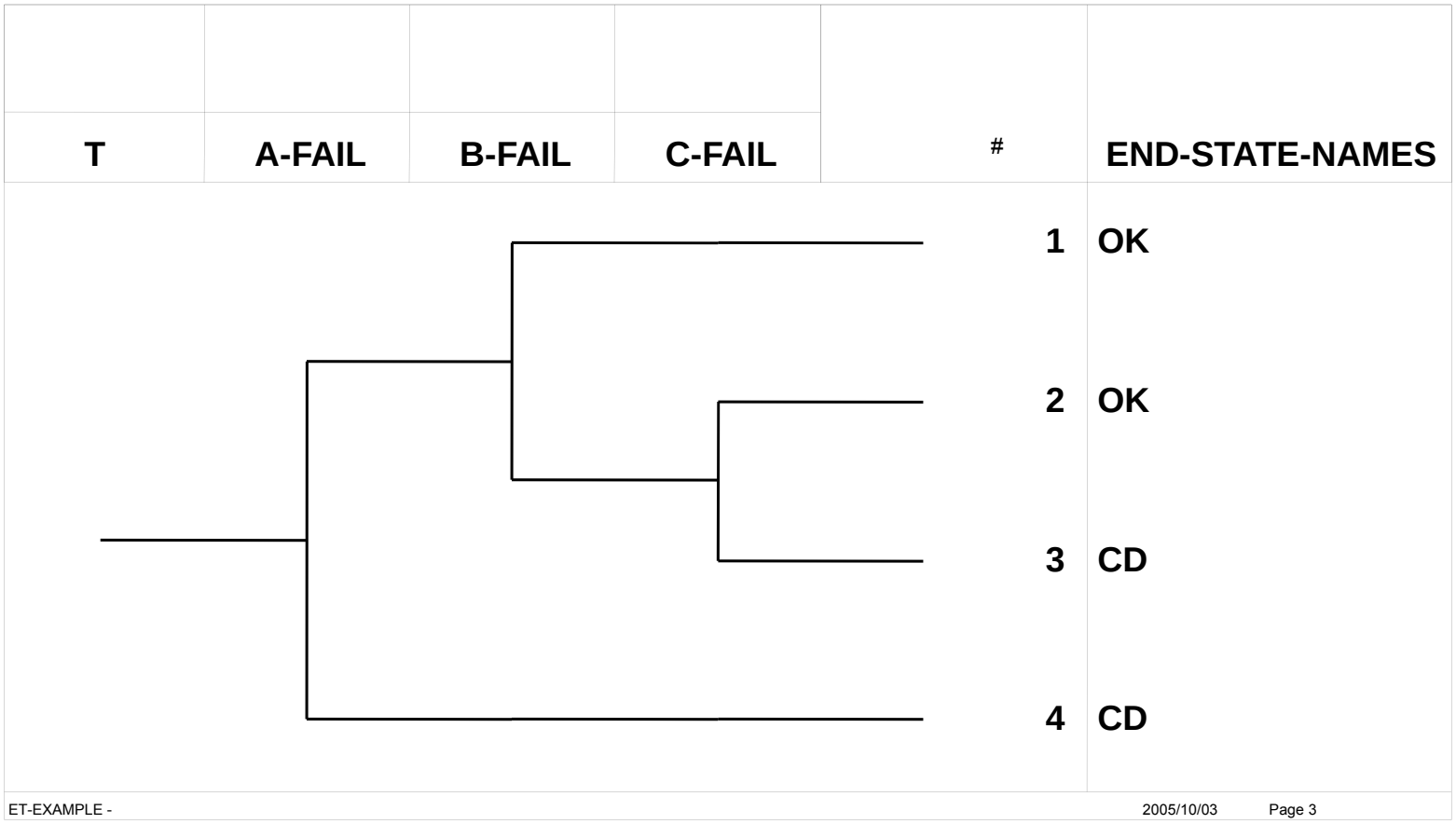
Prerequisites for Generating and Quantifying Accident Sequence Cut Sets

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

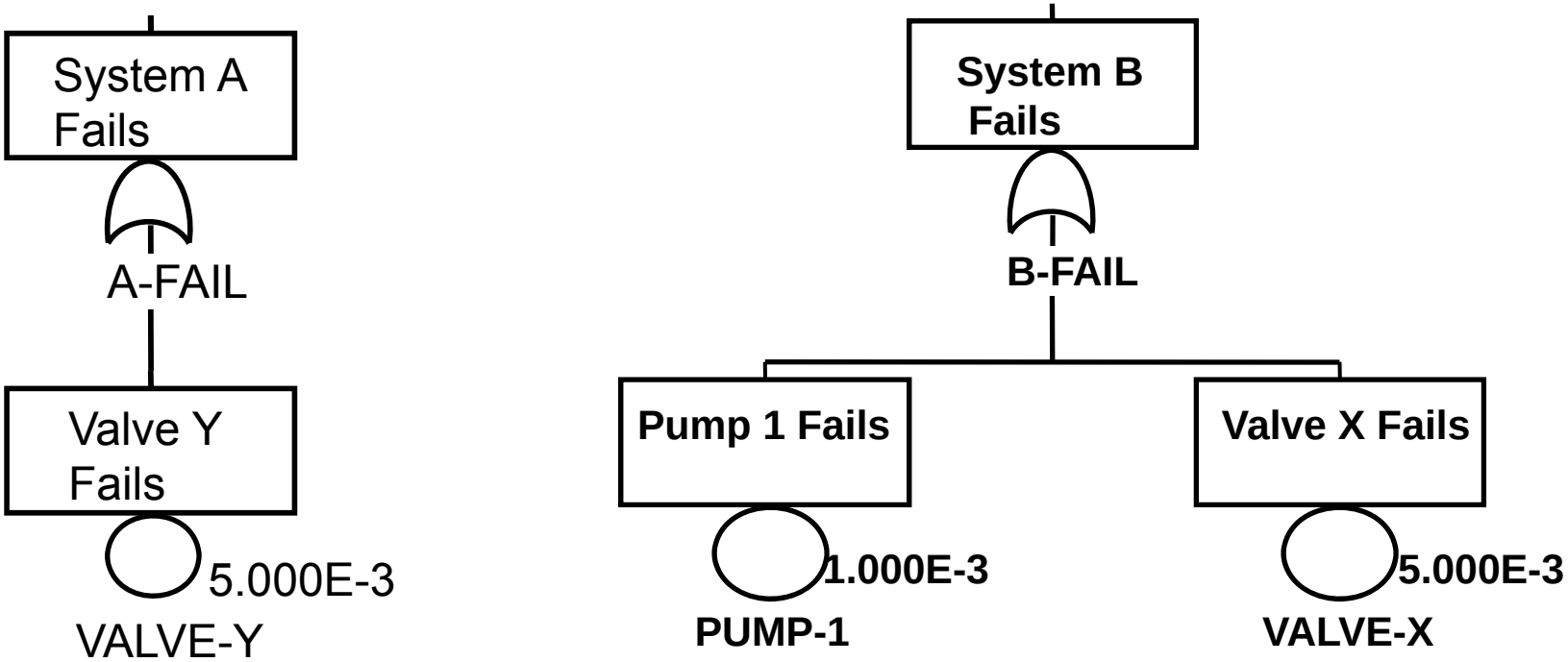
Accident Sequence Quantification (Fault-Tree Linking Approach)

- Link fault tree models on a sequence level using event trees (i.e., generate sequence logic)
- Generate minimal cut sets (Boolean reduction) for each sequence
- Quantify sequence minimal cut sets with data
- Eliminate inappropriate cut sets, add operator recovery actions, and requantify
- Determine dominant accident sequences
- Perform sensitivity, importance, and uncertainty analysis

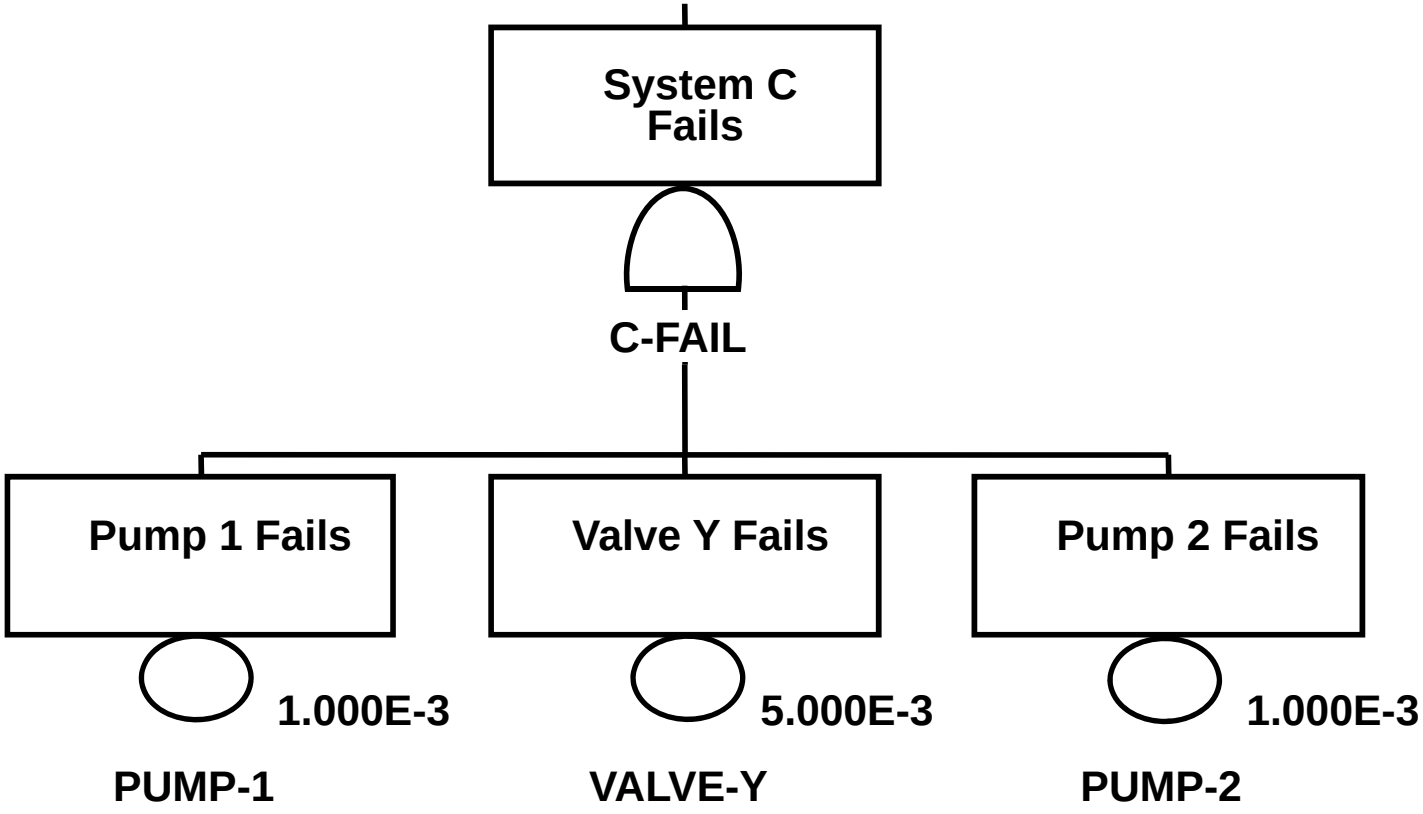
Example Event Tree



Example Fault Trees



Example Fault Trees (Concluded)



Generating Sequence Logic

- Fault trees are linked using sequence logic from event trees. From the example event tree two sequences are generated:
  - Sequence # 3: T * /A-FAIL * B-FAIL * C-FAIL
  - Sequence #4: T * A-FAIL

Generate Minimal Cut Sets for Each Sequence

- A ***cut set*** is a combination of events that cause the sequence to occur
- A minimal cut set is the smallest combination of events that causes to sequence to occur
- Cut sets are generated by "ANDing" together the failed top event fault trees, and then, if necessary, eliminating (i.e., deleting) those cut sets that contain failures that would prevent successful (i.e., complemented) top events from occurring. This process of elimination is called *Delete Term*
- Each cut set represents a failure scenario that must be "ORed" together with all other cut sets for the sequence when calculating the total frequency of the sequence

Sequence Cut Set Generation Example

- Sequence #3 logic is T * /A-FAIL * B-FAIL * C-FAIL
- ANDing failed top events yields

B-FAIL * C-FAIL = (PUMP-1 + VALVE-X) * (PUMP-1 * VALVE-Y * PUMP-2)

= (PUMP-1 * PUMP-1 * VALVE-Y * PUMP-2) + (VALVE-X * PUMP-1 * VALVE-Y * PUMP-2)

= (PUMP-1 * VALVE-Y * PUMP-2) + (VALVE-X * PUMP-1 * VALVE-Y * PUMP-2)

= PUMP-1 * VALVE-Y * PUMP-2

- Using Delete Term to remove cut sets with events that would fail top event A-FAILS (i.e., VALVE-Y) results in the elimination of all cut sets
- Sequence #4 logic is T * A-FAIL, resulting in the cut set

  T *VALVE-Y

Quantification of Sequence Cut Sets

- Exact Solution for Top = A + B:

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

  - Cross terms become unwieldy for large lists of cut sets.
- Thus, sequences typically quantified using either:
  - Rare-Event Approximation
    - P(Top) = sum of probabilities of individual minimal cut sets (MCSs) = P(A) + P(B)
    - P(AB) judged sufficiently small (rare) that it can be ignored (i.e., cross-terms are simply dropped)

$$\mathbf{P(Top\ Event)} \leq \sum \mathbf{P(MCS_k)}$$

Or

  - Minimal Cut Set Upper Bound (min-cut) Approximation
    - P(Top) = 1 - product of cut set success probabilities

$$\mathbf{P(Top\ Event) \leq 1- \Pi(1-P\{MCS_k\})}$$

Comparison of Quantification Methods for P(A+B)

	Small values for P(A) & P(B), A & B independent	**Large values for P(A) & P(B), A & B independent**	**A & B dependent**
Values	P(A) = 0.01 P(B) = 0.03	P(A) = 0.4 P(B) = 0.6	B = /A P(A) = 0.4 P(B) = P(/A) = 0.6
Exact	0.01 + 0.03 - (0.01 * 0.03) = 0.0397	0.4 + 0.6 - (0.4 * 0.6) = 0.76	0.4 + 0.6 - P(A*/A) = 1.0
Rare Event	0.01 + 0.03 = 0.04	0.4 + 0.6 = 1.0	0.4 + 0.6 = 1.0
MinCut UB	1 - [(1-0.01) * (1-0.03)] = 0.0397	1 - [(1-0.4) * (1-0.6)] = 0.76	1 - [(1-0.4) * (1-0.6)] = 0.76

Eliminating "Inappropriate" Cut Sets

- When solving fault trees to generate sequence cut sets it is likely that "inappropriate" cut sets will be generated
- "Inappropriate" cut sets are those containing *invalid* combinations of events. An example would be:
  - … SYS-A-TRAIN-1-TEST * SYS-A-TRAIN-2-TEST ….
- Typically eliminated by searching for combinations of invalid events and then deleting the cut sets containing those combinations

Adding “Recovery Actions” to Cut Sets

- Cut sets are examined to determine whether the function associated with a failed event can be restored; thus “recovering” from the loss of function
- If the function associated with an event can be restored, then a “Recovery Action” is ANDed to the cut set to represent this restoration
- The probability assigned to the “Recovery Action” will be the probability that the operators fail to perform the action or actions necessary to restore the lost function
- Probabilities are derived either from data (e.g., recovery of off-site power) or from human reliability analysis (e.g., manually opening an alternate flow path given the primary flow path is failed)

Dominant Accident Sequences (Examples)

Surry (NUREG-1150)

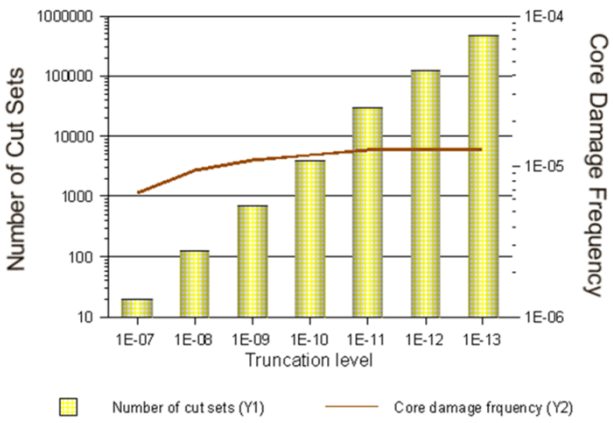
Seq	Description	% CDF	Cum
1	Station Blackout (SBO) - Batt Depl.	26.0	26.0
2	SBO - RCP Seal LOCA	13.1	39.1
3	SBO - AFW Failure	11.6	50.7
4	SBO - RCP Seal LOCA	8.2	58.9
5	SBO - Stuck Open PORV	5.4	64.3
6	Medium LOCA - Recirc Failure	4.2	68.5
7	Interfacing LOCA	4.0	72.5
8	SGTR - No Depress - SG Integ'ty 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)

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

Truncation Issues Affect Quantification

- Two types of truncation
  - Cut set frequency
  - Cut set order
    - Truncating on number of basic events in a cut set generally limited to vital area analyses
- Becoming less of a concern with increased computer/software capabilities
- 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 cutoff value should be decreased until change in total frequency becomes stable

Importance Measures for Basic Events

- Provide a quantitative perspective on risk and sensitivity of risk to changes in input values
- Three are encountered most commonly:
  - Fussell-Vesely (F-V)
  - Birnbaum
  - Risk Reduction (RR)
  - Risk Increase (RI) or Risk Achievement (RA)

Importance Measures
(Layman Definitions)

- Risk Achievement Worth (RAW)
  - Relative risk increase assuming failure
- Risk Reduction Worth (RRW)
  - Relative risk reduction assuming perfect performance
- Fussell-Vesely (F-V)
  - Fractional reduction in risk assuming perfect performance
- Birnbaum
  - Difference in risk between perfect performance and assumed failure

Importance Measures
(Mathematical Definitions)

R = Baseline Risk

R(1) = Risk with the element always failed or unavailable

R(0) = Risk with the element always successful

RAW = R(1)/R or R(1) - R

RRW = R/R(0) or R - R(0)

F-V = [R-R(0)]/R

Birnbaum = R(1) – R(0)

Limitations of Importance Measures

- Risk rankings are not always well-understood in terms of their issues and engineering interpretations
  - That is, high importance does not necessarily mean dominant contributor to CDF
- RAW provides indication of risk impact of taking equipment out of service but full impact may not be captured
  - That is, taking component out of service for test and maintenance may increase likelihood of initiating event due to human error
- F-V and RAW rankings can differ significantly when using different risk metrics
  - Such as, core damage frequency due to internal events versus external events, shutdown risk, etc.
- Individual F-V or RAW measures cannot be combined to obtain risk importance for combinations of events

Uncertainty Must be Addressed in PRA

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

PRAs Identify Two Types of Uncertainty

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

Aleatory Uncertainty

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

Epistemic Uncertainty

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

Types of Epistemic Uncertainties

- Parameter uncertainty
- Modeling uncertainty
  - System success criteria
  - Accident progression phenomenology
  - Health effects models (linear versus nonlinear, threshold versus non-threshold dose-response model)
- Completeness
  - Complex errors of commission
  - Design and construction errors
  - Unexpected failure modes and system interactions
  - All modes of operation not modeled

Addressing Epistemic Uncertainties

- Parameter uncertainty addressed by propagating parameter uncertainty distributions through model
- Modeling uncertainty usually addressed through sensitivity studies
  - Research ongoing to examine more formal approaches
- Completeness addressed through comparison with other studies and peer review
  - Some issues (e.g., design errors) are simply acknowledged as limitations
  - Other issues (e.g., errors of commission) are topics of ongoing research

Prerequisites for Performing a Parameter Uncertainty Analysis

- Cut sets for individual sequence or groups of sequences (e.g., by initiator or total plant model) exist
- Failure probabilities for each basic event, including distribution and correlation information (for those events that are uncertain or are modeled as having uncertainty)
- Frequencies for each initiating event, including distribution information

Performing A Parameter Uncertainty Analysis

- Select cut sets
- Select sampling strategy
  - Monte Carlo: simple random sampling process/technique
  - Latin Hypercube: stratified sampling process/technique
- Select number of observations (i.e., number of times a variable's distribution will be sampled)
- Perform calculation

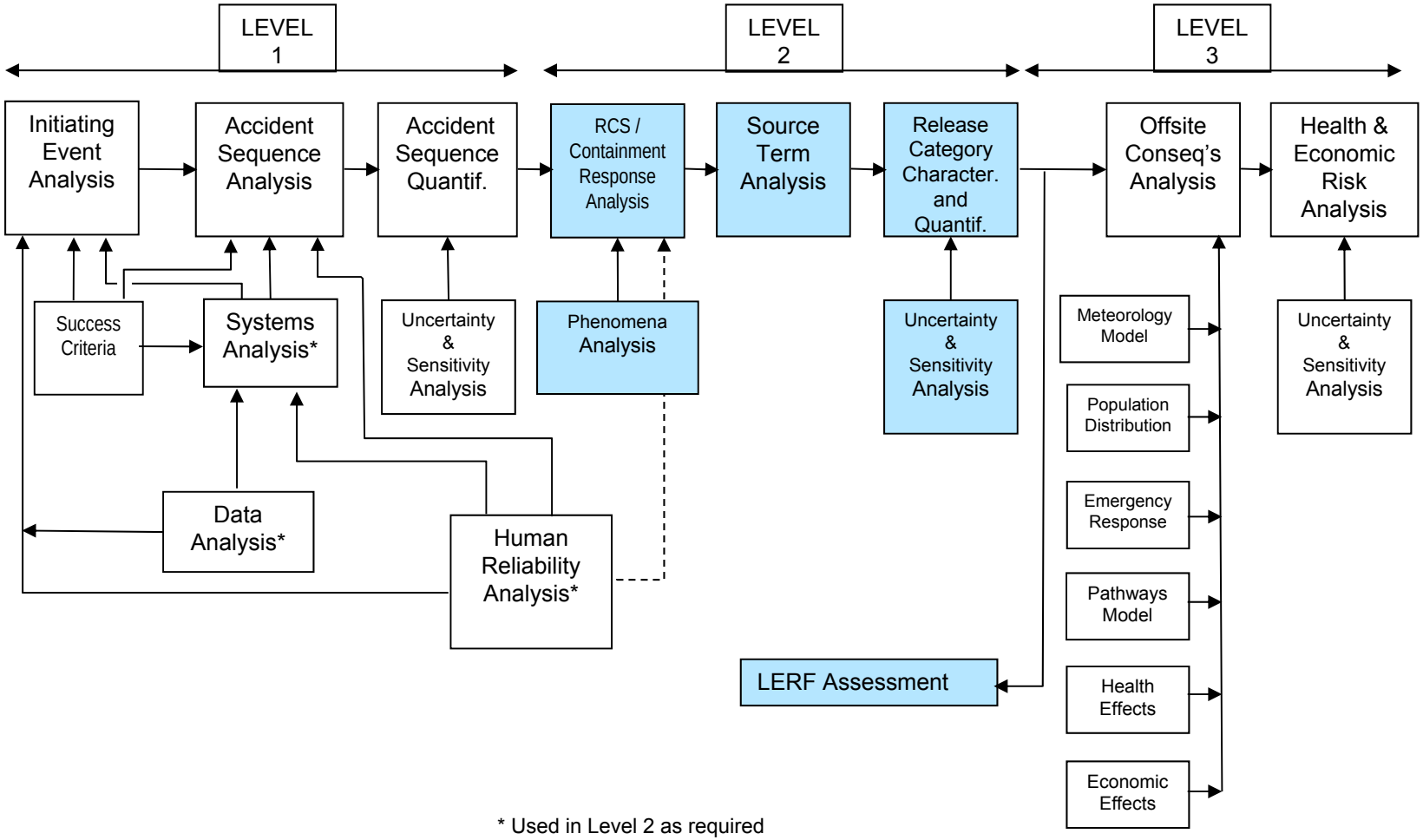
Correlation: Effect on Results

- 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

LEVEL 2/LERF Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

Purpose and Objectives

- Purpose: Students receive a brief introduction to accident progression (Level 2 PRA).
- Objectives: At the conclusion of this topic, students will be able to:
  - List primary elements which comprise accident phenomenology
  - Explain how accident progression analysis is related to full PRA
  - Explain general factors involved in containment response
- Reference: NUREG/CR-2300, NUREG-1489 (App. C)

Level 2 PRA Risk Measures

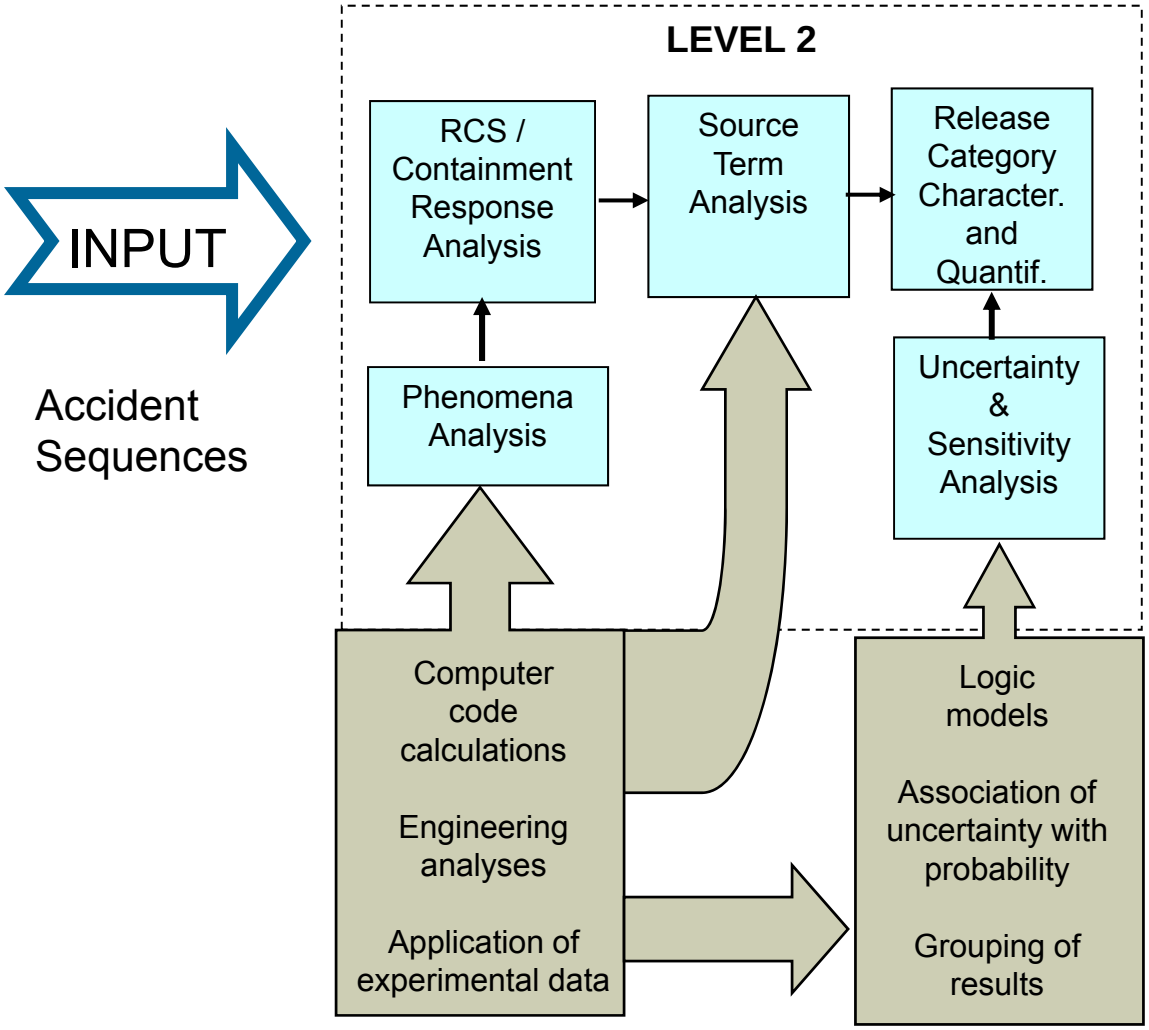
- Current NRC emphasis on LERF
  - Risk-informed Decision-Making for Currently Operating Reactors
  - Broader view expected for new reactors
- Some discussion of alternative risk acceptance criteria
  - Goals for frequency of various release magnitudes
  - Release often expressed in units of activity (not health consequences)
- Full-scope Level 2 offers Complete Characterization of Releases to Environment
  - Frequency of large/small, early/late releases

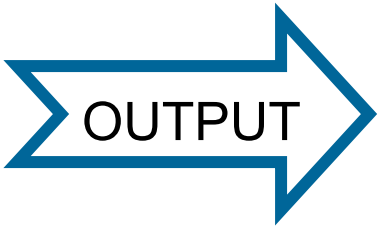
LERF Definition

- A LERF definition is provided in the PSA Applications Guide:

Large, Early Release: A radioactive release from the containment which is both large and early. Large is defined as involving the rapid, unscrubbed release of airborne aerosol fission products to the environment. Early is defined as occurring before the effective implementation of the off-site emergency response and protective actions.

Level 2 PRA is a Systematic Evaluation of Plant Response to Core Damage Sequences





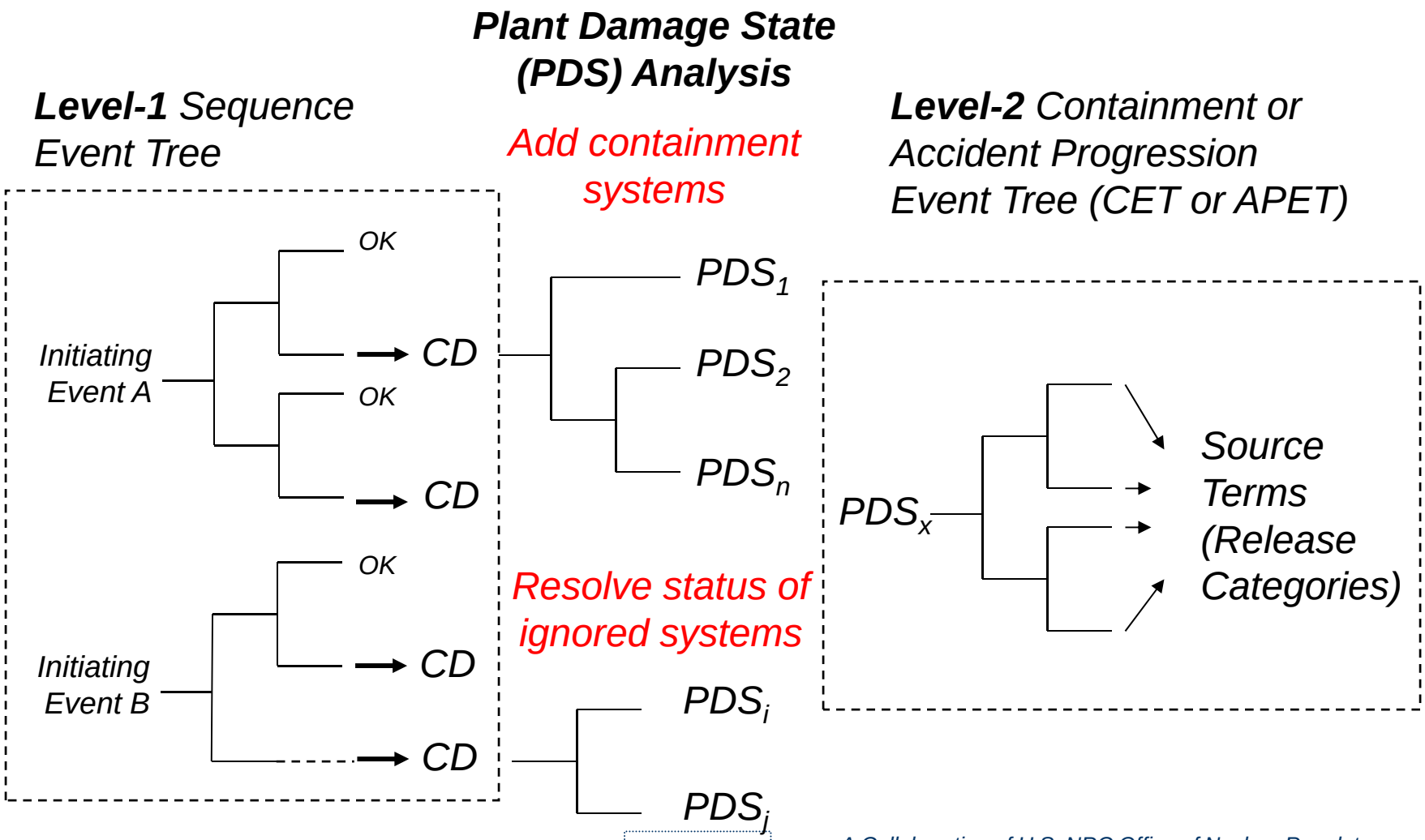
Deterministic:
- Reactor transient
- Containment response
- Core damage progression
- Fission product inventory released to environment

Probabilistic:
- Relative likelihood of (confidence in) alternative responses for each sequence
- Frequency of fission product release categories

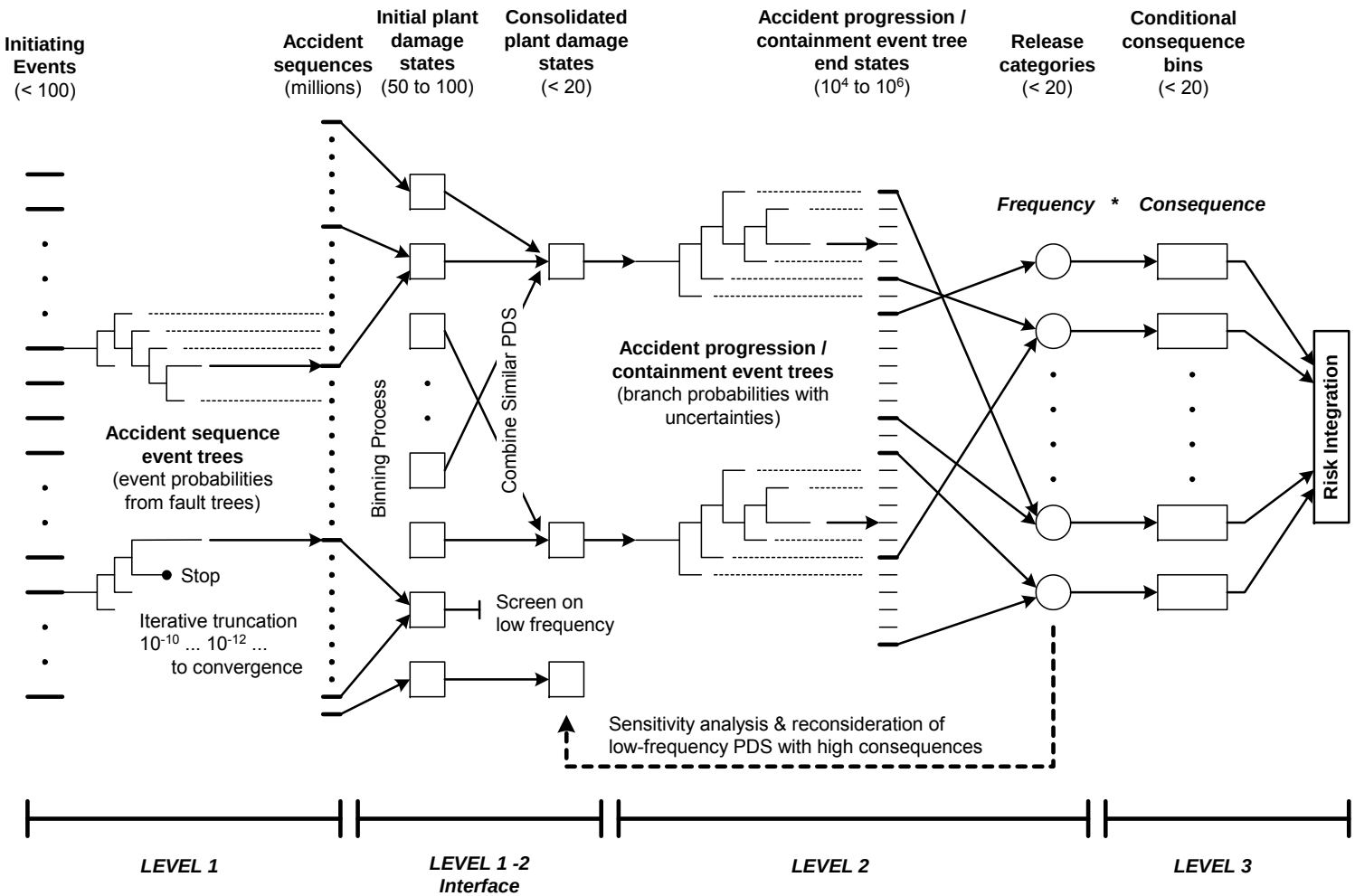
Some Subtle Features of the Level 2 PRA Process

- Level 2 Requires More Information than a Level 1 PRA Generates
  - Containment safeguards systems not usually needed to determine 'core damage'
  - Level 1 event trees built from success criteria can ignore status of front-line systems that influence extent of core damage
- Event Trees Create Very Large Number of Scenarios to Evaluate
  - Grouping of similar scenarios is a practical necessity
- Quantification Involves Considerable Subjective Judgment
  - Uncertainty, Sensitivity and Uncertainty in Uncertainty

Additional Work is Often Required to Link Level 1 Results to Level 2



Typical Steps in Level 2 Probabilistic Model



Major Tasks:

- Plant Damage State (PDS) Analysis
  - Link to Level 1
- Deterministic Assessments of Plant Response to Severe Accidents
  - Containment performance assessment
  - Accident progression & source term analysis
- Probabilistic Treatment of Epistemic Uncertainties
  - Account for phenomena not treated by computer codes
  - Characterize relative probability of alternative outcomes for uncertain events
- Couple Frequency with Radiological Release
  - Link to Level 3

Major Steps of Level 2 Analysis

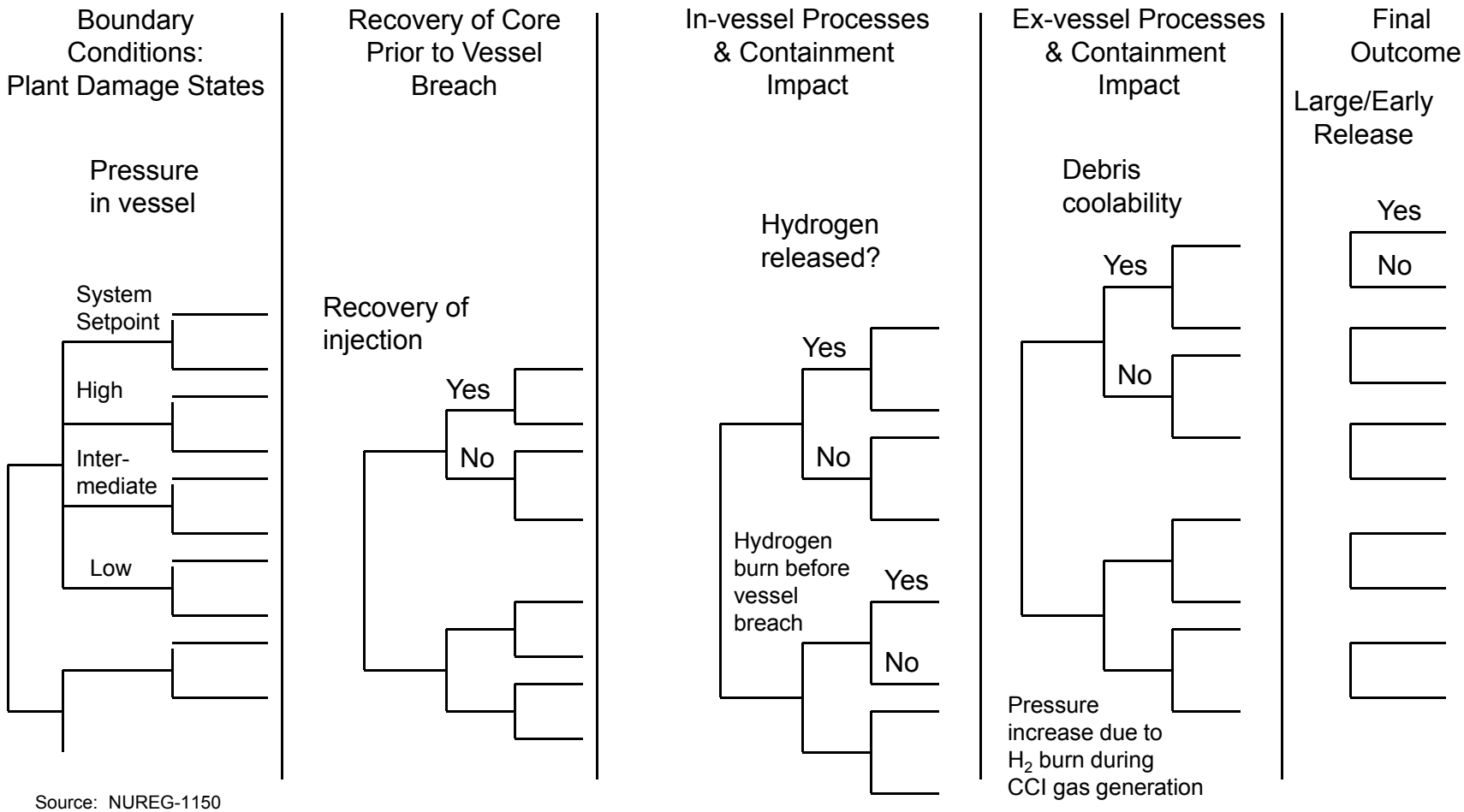
- Level 1 -2 Interface
  - Enhance Level 1 accident sequence models to meet Level 2 needs
  - Group cut sets into “plant damage state” (PDS) bins.
  - Output - Frequency of each PDS bin (5 to 25 PDSs).
- Accident Progression Analysis
  - Run preliminary MELCOR runs to establish source term Release Categories
  - Build Containment Event Tree (CET)
    - Sequence of events that lead to containment failure and fission product release.
  - Run PDSs through CET
  - Output - Frequency of each CET end-state.
- Source Term Binning
  - Develop criteria for source term binning of CET end-states
  - Run additional MELCOR runs to refine source term Release Categories
  - Group CET end-states into source term “Release Categories”
  - Output - Frequency of each Release Category.

Level 1-2 Interface

- Enhance Level 1 accident sequence models to address Level 2 information needs
  - Add front line systems excluded from core damage sequences but relevant to the progression of core damage.
  - Add containment system response to Level 1 models
  - Requantify Level 1 results
  - Accomplished using either a Containment Safeguards Tree or Bridge Tree

- Consolidate Level 1 results for Level 2 (PDS Analysis)
  - Identify post-core damage attributes important to containment response
  - Group Level 1 Sequences (or cut sets) into bins defined in terms of common accident attributes relevant to containment response.
  - Output - Frequency of PDSs.

Schematic of Accident Progression Event Tree



Source: NUREG-1150

Accident Progression Analysis

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

Severe Accident Analysis

Computer Code (e.g., MAAP or MELCOR) Calculations Provide Foundation Information for Design-Specific Information --

- Thermal-hydraulic response/success criteria
  - Primary coolant inventory management, reactor pressure control & heat removal
- Time of major events
  - Onset of core damage
  - Time to exceed containment failure criteria
  - Available time for operator actions
- Evolution of severe accident phenomena
  - RCS & containment pressure/temperature signatures
  - Fission product release/transport (source term)
- Containment Ultimate Pressure

Containment Response

- How does the containment system deal with physical conditions resulting from the accident?
  - Pressure
  - Heat sources
  - Fission products
  - Steam and water
  - Hydrogen
  - Other non-condensables
- Typical failure modes:
  - Isolation failure or bypass
  - Over-pressure (global)
  - Creep (axial growth)
  - Corium-concrete interaction
  - Blowdown reaction forces
  - Local heating of pressure boundary penetrations or seals
  - Localized dynamic loads

Deterministic Analysis Results Useful for APET/CET Quantification

- Probability of containment failure at vessel breach hinges on likelihood of hydrogen ignition in containment.
  - Possibilities for ignition sources?
  - Flame propagation from drywell?
  - Debris transport from pedestal?

  } *Questions the APET/CET should consider*
- Containment over-pressure from large burn can also fail drywell wall
  - Suppression pool bypass for late in-vessel F.P. releases
- Reactor vessel failure at low pressure depends on failure of safety valve
  - Valve failure criteria?
  - Single cycling valve?

  } *Questions the APET/CET should consider*

APET/CET Quantification

- System failure events quantified in manner consistent with Level 1
  - Most system issues handled prior to PDS Analysis
- Dependencies and Data (Aleatory) Uncertainties Accompanying Level 1 systems analysis must be carried forward through PDS:
  - Support system failures, if any.
  - Prior operator performance, if any.
  - PDS frequency as distribution, if any.
- Most CET events cannot be quantified as randomly occurring events
  - Fundamental nature of uncertainty is NOT stochastic (random) behavior of the 'system'
  - Epistemic or 'state-of-knowledge' uncertainty
  - Probability represents analysts' degree of confidence that a particular outcome is true
  - Evidence may point to one outcome over another
- Many events are quantified using engineering judgment

Uncertainty Analysis in Level 2 PRA

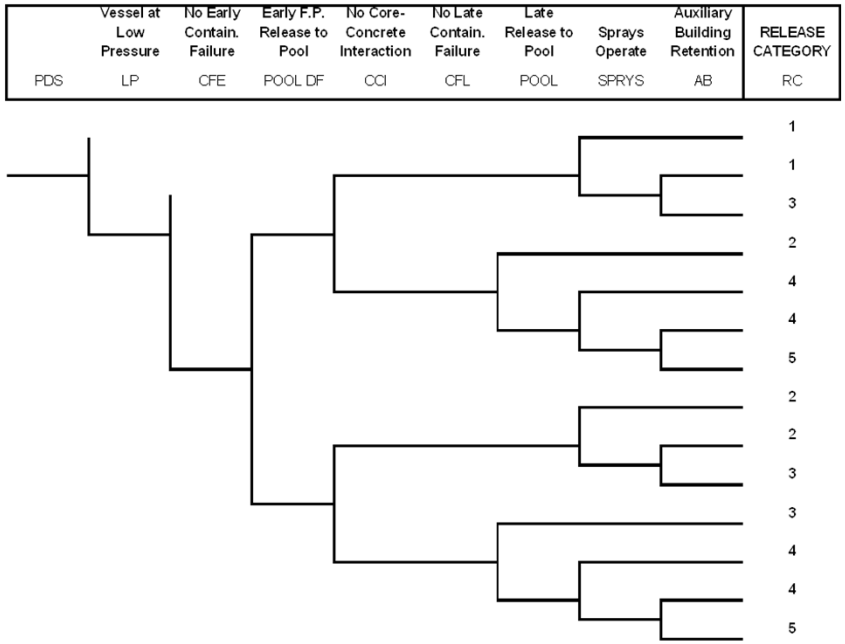
- Event Quantification in CET Predominantly Reflects Epistemic Uncertainty
  - Subjective judgment about a particular outcome
- Most CET probabilities are estimated as point estimates:
  - From deterministic calculations, or
  - Engineering judgment.
- Distributions Can Be Defined and Sampled to model epistemic uncertainties

Issues to Tackle in Propagating Uncertainty through Level 2 APET/CET

- Large Values of Probability (> 0.1) Are Common
  - Eliminates Use of Some Quantification Techniques common to Level 1.
- Correlation Among Events Can be Complicated
  - Event chronology:
    - Example: Hydrogen Combustion
      - Probability of early burn correlated with in-vessel generation
      - Probability of burn at vessel breach correlated with early burn
      - Probability of late burn correlated with all earlier burns
  - Circular Dependence
    - H2 Generation → RPV Pressure → SRV Behavior → H2 Generation

Source Term Binning

- **Rather than calculate a source term for each end-state of the CET, rules are generated to group end-states with similar source terms.**
  - **Each group is referred to as a source term 'bin' or release category**
  - **Rules (binning criteria) are based on knowledge gained from multiple source term calculations**



Process similar to PDS analysis

- **Define binning criteria from results of calculations**
- **Link each CET end-state to a unique Category**

Typical Source Term Binning Characteristics

- Timing, size & location of containment failure
- Plant or accident features that attenuate airborne fission product concentration
  - Release path through auxiliary building(s)
  - Atmosphere sprays
- Effectiveness of ex-vessel debris cooling
- Availability of water after RPV lower head failure
  - Cover debris with pool of water (scrubbing)
  - Cool RPV surfaces reduces revolatilization

Release Fraction as a Measure for Comparing Source Terms

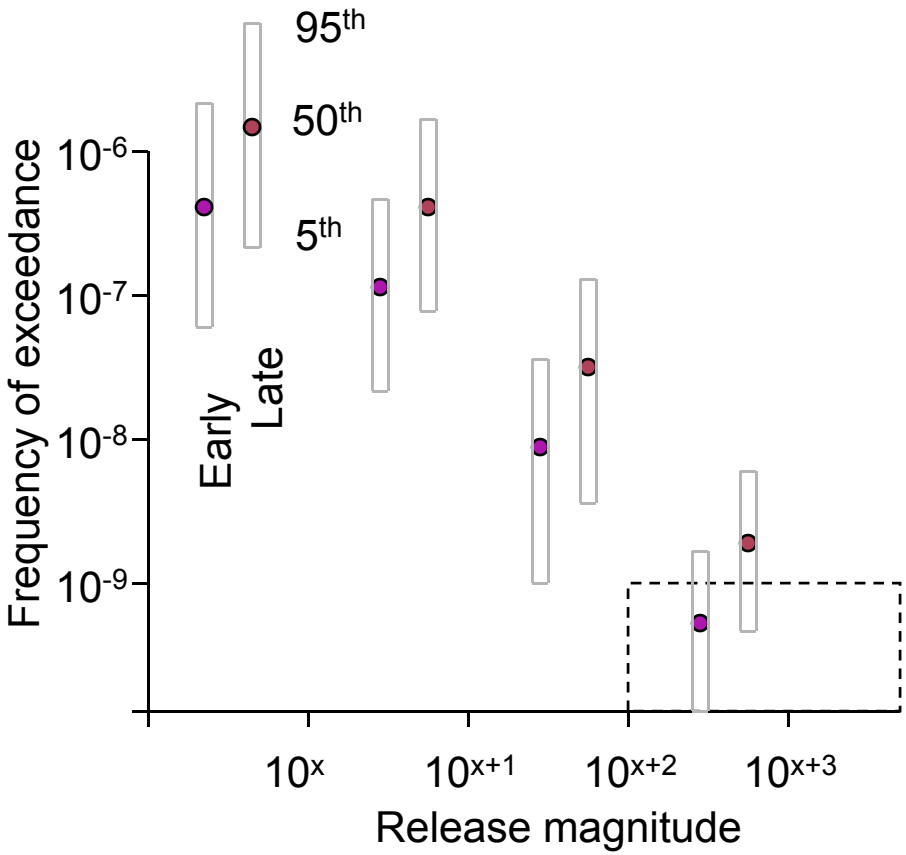
- "Bin" or group calculated source terms into broad classes based on magnitude and timing of release to the environment
  - Release fractions for Iodine (I-131) and Cesium (Cs-137) are established measures of early and long-term health effects, respectively
  - Binning criteria can be based on one, or both measures

Fractional Release of Initial Core Inventory

Release Category	Lower Bound	Upper Bound
RC1	1.0	0.1
RC2	0.1	0.01
RC3	1.E-2	1.E-3
RC4	1.E-3	1.E-4
RC5	1.E-4	1.E-5
RC6	1.E-5	1.E-6
RC7	1.E-6	1.E-7
RC8	No release	

Full Scope Level 2 PRA: Wide Range of Possible Accidental Releases to Environment

- Characterization of Releases to the Environment of all Types
  - Large/Small
  - Early/Late
  - Energetic/Protracted
  - Elevated/Ground level
- Frequency of Each Type Describes Full Spectrum of Releases Associated with Core Damage Events



Bounding or Screening Models for U.S. Risk-Informed Applications (LERF)

- NUREG/CR- 6595 (Brookhaven 2004)
  - Provides simplified approach designed to supplement Level-I PRAs submitted in support of risk-informed decision making.
  - Accident sequence information provided in the Level-I PRA is used to estimate the frequencies of various containment failure modes."

- A Simplified Model Can Be Used to Estimate Bounding Value of LERF
  - Simple method outlined in NUREG/CR-6595
  - Pre-quantified "CETs" with paths leading to LERF
  - Avoids expensive of plant-specific deterministic analysis
  - Avoids source term (MELCOR) calculations
  - Only useful if bounding values for conditional containment failure probability are tolerable