





**PRA Technology and Regulatory Perspectives (P-111)**  
**Index**

Volume 1

Index

Syllabus

Module A - Introduction To PRA And Its Use At The NRC

Module B - Traditional Engineering Analysis And PRA

Module C - Overview Of PRA Process

Module D - Initiating Events

Module E - Event Trees

Module F - Fault Trees

Module G - Parameter Estimation

Module H - Common-Cause Failure

Module I - Human Reliability Analysis

Module J - Accident Sequence Quantification

Module K - External Events

Module L - Level 2 & 3 Analysis

Module M - Shutdown Risk

Module N - Importance Measures

Module O - Uncertainty

Module P - Plant-Specific, Risk-Informed Applications

Module Q - Configuration Risk Management

Module R - Maintenance Rule Implementation

Module S - Reactor Safety SDP Principles

Combustion Engineering Owners Group - AOT Pilot Program

Required Reading Assignments

    PRA Final Policy Statement

    ACRS Letter dated 4/11/97

    ACRS Letter dated 7/19/91

    ACRS Letter dated 12/16/97

    IMC 0609

    Part 9900 Inspection Guide

    Risk-Informed 10 CFR 50.59

Acronyms

C-1



# **PRA Technology and Regulatory Perspectives (P-111) Syllabus**

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

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

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

## Syllabus of topics

### Week 1

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

##### Objectives:

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

#### Module B - Traditional Engineering Analysis and PRA

##### Objectives:

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



## Module C - Overview of the PRA Process

### Objectives:

- Describe the major steps in the PRA process
- Describe the outputs of each of the “Levels” of PRA
- Describe why probabilistic models are used
- Give examples of disciplines required to perform a PRA
- Give examples of where traditional engineering inputs are used in the PRA process

## Module D - Accident Sequence Initiating Events

### Objectives:

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

## Module E - Accident Sequence Analysis Using Event Trees

### Objectives:

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

## Module F - Systems Analysis Using Fault Trees

### Objectives:

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

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

### Objectives:

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

## Module H - Common-Cause Failures

### Objectives:

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



## Module I - Human Reliability Analysis

### Objectives:

- Explain the role of HRA within the overall context of PRA
- Describe common error classification schemes used in HRA
- Describe how human interactions are incorporated into system models
- Identify strengths and limitations of HRA

## Module J - Accident Sequence Quantification

### Objectives:

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

## Module K - External Events

### Objectives:

- Define external events and differentiate them from the broader class of common cause events
- List several of the more significant external events, including those analyzed in the IPEEEs
- List the objectives of the IPEEE and the acceptable approaches for seismic events and fires
- Explain the ways in which external events may be evaluated and how this evaluation is related to the overall PRA task flow

## Module L - Level 2 & 3 Analysis

### Objectives:

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

## Module M - Shutdown Risk

### Objectives:

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

## Module N - Importance Measures

### Objectives:

- Identify and define (both mathematically and in words) 3 types of quantitative importance measures
- Discuss how importance measures are influenced by the value of the associated basic event, the values of other basic events, and modeling assumptions
- Explain why use of importance measures is considered valid for Maintenance Rule applications (i.e., binning SSCs into risk and non-risk categories)

## Module O – Uncertainty

### Objectives:

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



## Week 2

### Module P - Plant-Specific, Risk-Informed Applications

#### Objectives:

- Describe the objectives of the PRA Policy Plan and the scope of the Implementation Plan for the various NRC offices affected
- List the major elements of the decision logic used to review submittals containing changes to the current licensing basis and the role of the new draft Reg. Guides and SRPs in this process, including the numerical decision criteria related to CDF and LERF

### Module Q - Configuration Risk Management

#### Objectives:

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

### Module R - Maintenance Rule Implementation

#### Objectives:

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

### Module S - Reactor Safety Significance Determination Process

#### Objectives:

- Describe how initiating event (IE) frequency influences SDP result and how inspection finding could increase likelihood of IE
- Describe how remaining mitigation capability is estimated for a multi-train system (per Table 3) and why result is different for a system with two or more diverse trains
- Describe why SDP cannot assess significance of component with degraded reliability (component not completely failed)
- Describe mathematical meaning of estimated likelihood rating and remaining mitigation capability rating
- Describe conceptually how SDP result is considered a change in annualized CDF and why this risk metric was chosen
- Describe intended benefit of using SDP to foster better understanding and communication of probabilistic analyses and influential assumptions of specific analyses
- Describe how CCDP for an event differs from CCDP for degraded plant condition existing for specified period of time
- Describe how SDP is used as means for thinking about potential risk consequences of other equipment being degraded or unavailable and how this might improve chances of finding risk significant issues, even if inspection finding is “green”
- Describe benefit of involving inspectors in PRA vs. relying on PRA specialists to establish risk significance of each finding
- Describe difference between risk associated with degraded fire barrier and risk from fire initiators, and how this difference is treated in SDP
- Describe basis for shutdown risk phase 1 checklist in IMC 0609
- Describe difference between Type A and Type B findings related to containment integrity



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

Integrated Workshop #1 – Planning and Prioritizing Inspection Activities

Integrated Workshop #2 – Risk Significance of Findings and Events

Integrated Workshop #3 – SDP Evaluation of Fire Protection Findings

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



# DAILY REQUIRED READING ASSIGNMENTS FOR P-111

Note: The instructor will allow 30 minutes at the beginning of each day (7:30am - 8:00am) and 30-45 minutes at the end (~3:45pm - 4:30pm) for students to perform the reading assignments and IPE “lookups” assigned at the end of each days’ lecture material. Use the beginning of the next class (starting at 8:00am) to ask any questions about the previously assigned reading.

## Week 1

### Day 1

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

Module B - Traditional Engineering Analysis and PRA

Module C - Overview of PRA Process

#### Required Reading:

- 1) Review PRA Final Policy Statement  
Section III - Deterministic and Probabilistic Approaches to Regulation (pp. 18-21)
- 2) ACRS Letter dated April 11, 1997 “Risk-Based Regulatory Acceptance Criteria for Plant-Specific Application of Safety Goals”
- 3) IMC 0609, App. A, pp. A1-1 through A1-4.
- 4) Part 9900 Inspection Guidance  
Operability - Section 6.9  
Resolution of Degraded and Non-conforming Conditions - Section 4.5.3

#### Optional (Background) Reading:

- 1) PRA Final Policy Statement, all sections
- 2) NUREG 1560 pp. 14-4 to 14-5

### Day 2

Module D - Accident Sequence Initiating Events

Module E - Accident Sequence Analysis Using Event Trees

Module F - System Analysis Using Fault Trees

#### Required Reading:

- 1) IMC 0609, App. A, pp. A1-5 through A1-14
- 2) NUREG 1560 - Chapter 2 Tables (e.g., 2.1, 2.2, 2.3) applicable to the student’s chosen plant

#### Optional (Background) Reading:

- 1) NUREG 1560 - Sections 14.3.1, 14.3.2, 14.3.3 (pp. 14-6 to 14-22)



### Day 3

Module G - Estimation of Equipment Reliability and Unavailability

Module H - Estimation of Common-Cause Failure Probabilities

Module I - Human Reliability Analysis

Module J - Accident Sequence Quantification

Module K - External Events

#### Required Reading:

- 1) ACRS Letter dated July 19, 1991 (D910719) "The Consistent Use of PRA"
- 2) IMC 0609, App. A, pp. A1-15 through A1-23.
- 3) NUREG 1560 - Chapter 5 Tables (e.g., 5.1, 5.2, 5.3, 5.4) applicable to the student's chosen plant)

#### Optional (Background) Reading:

- 1) NUREG 1560 Sections 14.3.4, 14.3.5 (pp. 14-23 to 14-31)

### Day 4

Module L - Level 2 and 3 PRA

Module M - Shutdown Risk

Module N - Importance Measures

Module O - Uncertainty

#### Required Reading:

- 1) IMC 0609, App. A, pp. A1-24 through A1-27
- 3) NUREG 1560 Chapter 3 and 4 Tables applicable to the student's chosen plant

#### Optional (Background) Reading:

- 1) NUREG 1560 Sections 14.3.6 (pp. 14-32 to 14-35)

### Week 2

### Day 5

Module P - Plant-Specific, Risk-Informed Applications

Module Q - Configuration Risk Management

Module R - Maintenance Rule Implementation

Module S - Reactor Safety Significance Determination Process

#### Required Reading:

- 1) Reread NRC Final PRA Policy Statement, Section III.B. "Uncertainties and Limitations of Deterministic and Probabilistic Approaches"
- 2) ACRS Letter dated Dec 16, 1997 "Treatment of Uncertainties versus Point Values in the PRA-related Decision-making Process"
- 3) IMC 0609, Apps. F, G, and H.

Review for closed-book exam



Day 6

Closed-Book Exam (Time limit: 2 hours)

Integrated Workshop #1 – Planning and Prioritizing Inspection Activities

Reading: None - students are encouraged to use IPEs, NUREG 1560, and the Maintenance Rule Guidebook to formulate a list of questions for discussion with licensee PRA analysts for a plant of their choosing. Students may begin drafting a risk-informed inspection plan (optional).

Day 7

Integrated Workshop #2 – Risk Significance of Findings and Events

Reading: None - students are encouraged to use IPEs, NUREG 1560, and Maintenance Rule Guidebook to formulate a list of questions for discussion with licensee PRA analysts for a plant of their choosing. Students may begin drafting a risk-informed inspection plan (optional).

Day 8

Integrated Workshop #3 – SDP Evaluation of Fire Protection Findings

Review for open-book exam

Day 9

Open-Book Exam (Time limit: 2.5 hours)



## **Student Guidance on the use of IPE's and NUREG 1560 in P-111**

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

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

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



# Module A

## Introduction to PRA and Its Use by the NRC



# Introduction to PRA and Its Use by the NRC

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



# Objectives

- Upon completion of this module, students should be able to
  - Define risk
  - List the basic questions answered by PRA
  - List three potential uses of PRA by inspectors
  - Generally describe NRC's quantitative health objectives
  - List the subsidiary numerical goals derived from the NRC's quantitative health objectives
  - List three expected outcomes of the NRC PRA Policy Statement



# Objectives (cont.)

- Upon completion of this module, students should be able to
  - List one area explicitly precluded from PRA application
  - Describe NRC's framework for incorporating PRA into facility regulation
  - List two ways in which PRA is affecting plant licensing basis
  - List example PRA strengths and limitations
  - Discuss ways in which PRA limitations are addressed



# Outline of Topics

- Basic terminology
- Risk definition and examples
- How PRA is being used
- NRC quantitative health objectives and subsidiary numerical goals
- NRC PRA Policy Statement and Risk-Informed Regulation Implementation Plan
- Strengths and limitations of PRA
- How PRA limitations are addressed



# Basic PRA Terminology

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



# Risk Definition

- Risk - the frequency with which a given consequence occurs

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

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



# Risk Example - Death Due to Accidents

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



# Risk Example - Death Due to Cancer

- Societal Risk = 538,000 cancer-deaths/year  
(based on Center for Disease Control actuarial data)
- Average Individual Risk
  - = (538,000 Cancer-Deaths/Year)/250,000,000 Total U.S. Population
  - =  $2.2\text{E-}03$  Cancer-Deaths/Person-Year
  - $\approx 1/460$  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](http://www.cdc.gov) latest data (2001) 553,768 cancer deaths and 284,797,000 U.S. population, thus average individual risk  $\approx (553,768 \text{ deaths/year})/284,797,000$   
 $\approx 1.9\text{E-}03$  Deaths/Person-Year



# Basic PRA Terminology (cont.)

- Probabilistic risk assessment (PRA) - an analytical tool that answers three questions:
  - What can go wrong (accident scenario)
  - How likely is each scenario (frequency)
  - What are the effects (consequences)



# PRA Now Widely Used by Industry and NRC

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



# NRC Applications of PRA

- Monitoring reactor operations (e.g., Maintenance Rule)
- Value impact analysis for potential changes to licensed reactor design and operation (backfits)
- Licensing advanced reactor designs
- Reactor operations
  - Evaluation of changes to licensing basis
    - General guidance - R.G. 1.174
    - IST - R.G. 1.175
    - ISI - R.G. 1.178
    - Graded QA - R.G. 1.176
    - Tech. Specs. - R.G. 1.177
  - Inspections support (e.g., Senior Reactor Analyst in Regions)
    - Prioritization and planning of inspections
    - Evaluation of inspection findings
    - Evaluation of licensee use of PRA



# NRC Applications of PRA (cont.)

- Resource allocation
  - Regulatory requirements (e.g., NEI initiative)
  - Research (e.g., generic issue prioritization)
  - Regulatory analyses (e.g., generic issue resolution)
- Reactor design
  - Identify weaknesses in design
    - Risk-significant Systems, Structures, Components (SSCs)
    - Risk-significant accident scenarios
    - Risk-significant human actions
- Events analysis and significance (Accident Sequence Precursors)
- Non-reactor issues
  - Licensing high-level waste repository
  - Sealed sources
  - Spent fuel storage
  - Others



# Use of PRA by Inspectors

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



# 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 “background” (i.e., all risks)
  - Average individual (within 1 mile of plant) early fatality (accident) risk  $< 5\text{E-}7/\text{year}$
  - Average individual (within 10 miles of plant) latent fatality (cancer) risk  $< 2\text{E-}6/\text{year}$
- Lower level subsidiary goals were derived from the high-level QHOs
  - Frequency of significant core damage (CDF)  $< 1\text{E-}4/\text{year}$
  - Frequency of large early release of fission products from containment (LERF)  $< 1\text{E-}5/\text{year}$



# NRC Quantitative Health Objectives (cont.)

- Commission has approved guidelines for plant-specific application of QHOs and subsidiary objectives (R.G. 1.174, Module P)
- “Small” increases in risk are allowable in changing plant licensing basis (R.G. 1.174, Module P)



# Purposes of Individual Plant Examinations (IPE/IPEEE)

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



# IPEs (IPEEEs) Did Not Require PRA

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



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

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



# NRC PRA Policy Statement

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



# NRC PRA Policy Statement (cont.)

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



# NRC PRA Policy Statement (cont.)

- Expected outcomes (became expected outcomes of risk-informed regulation, too)
  - Improved risk-effective decision-making
    - Staff takes consistent approach to regulatory decisions
  - More efficient use of NRC resources
  - Reduce unnecessary regulatory burden on licensees
- Initially put into place through PRA Implementation Plan, now referred to as Risk-Informed Regulation Implementation Plan

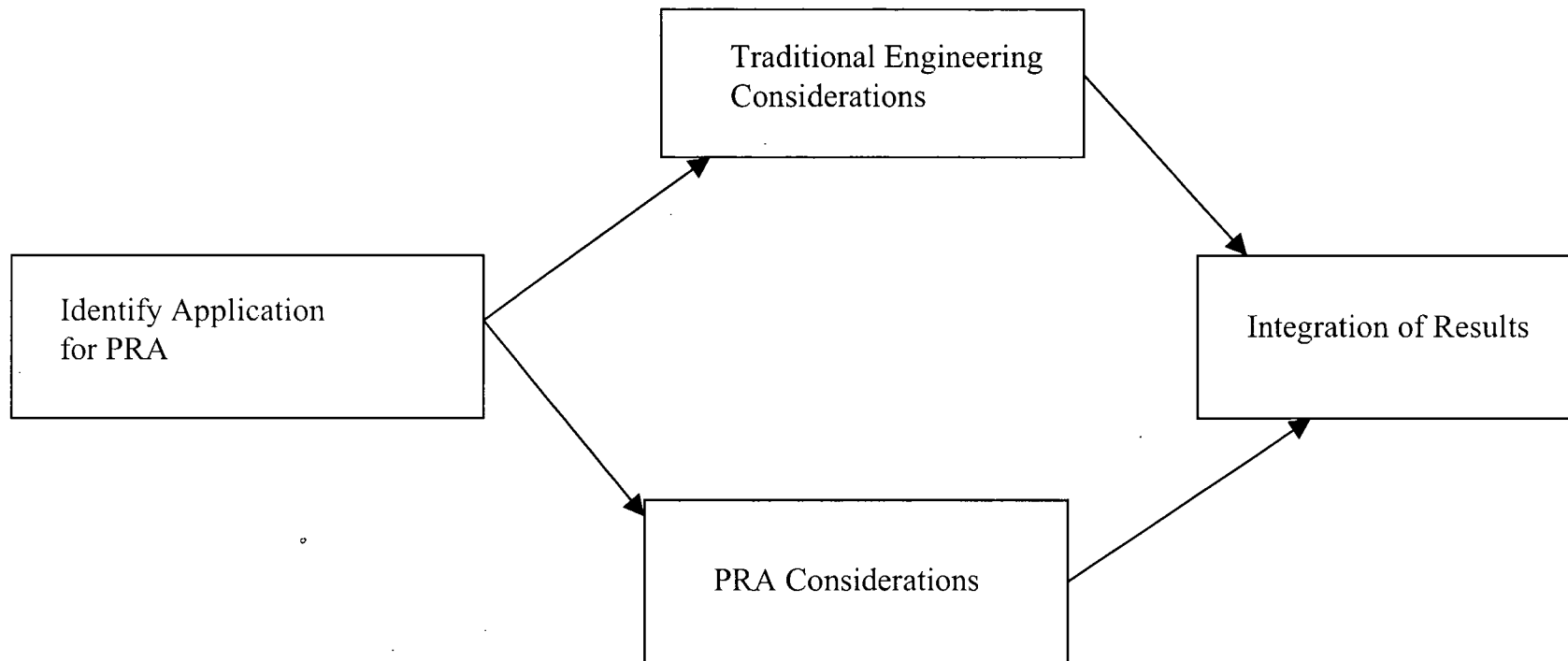


# Area Currently Excluded from PRA Application

- Equipment operability determination (for Tech. Specs.)



# NRC Framework for Applying PRA in Reactor Regulation



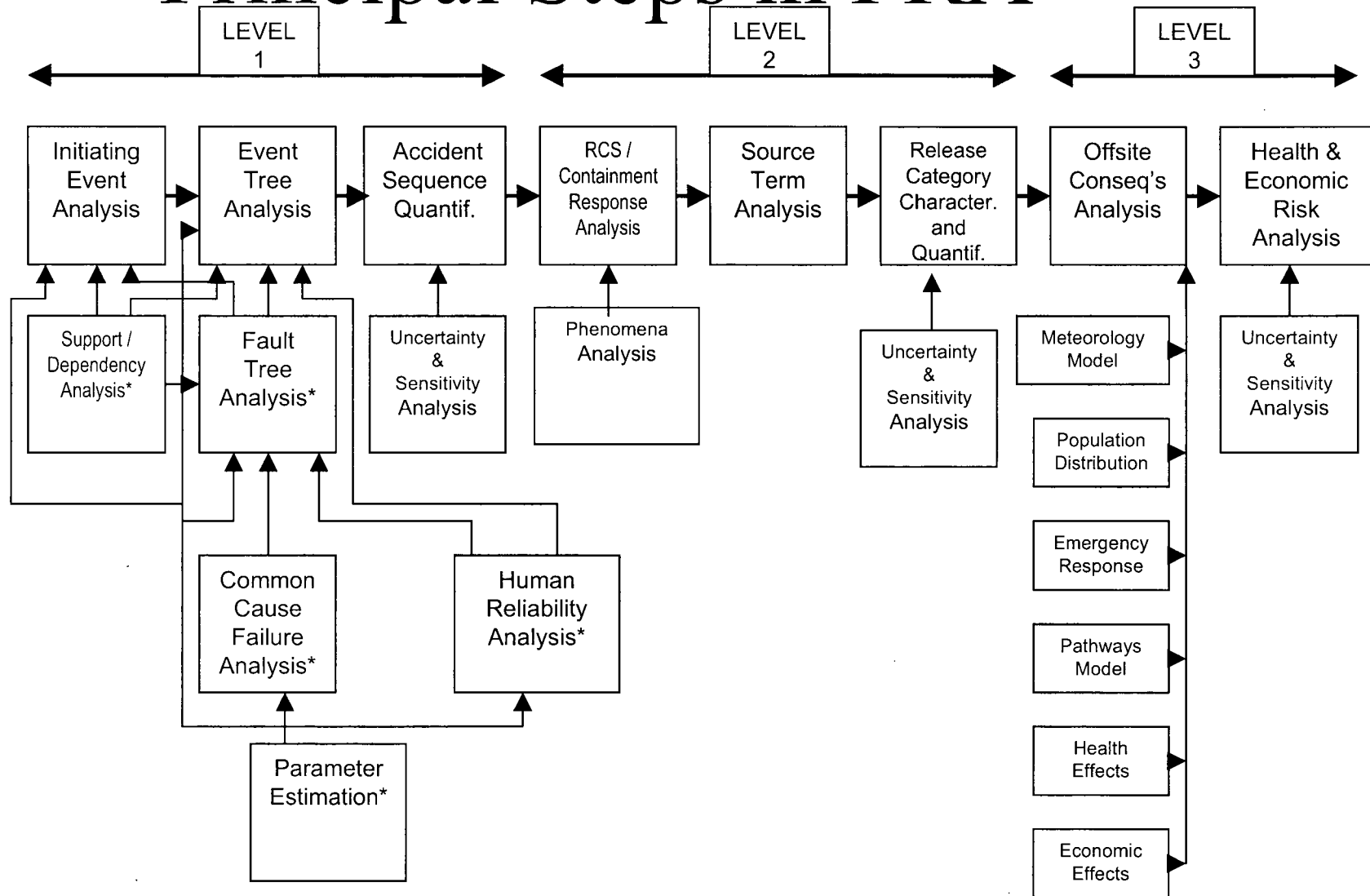


# PRA Is Impacting Licensing Basis

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

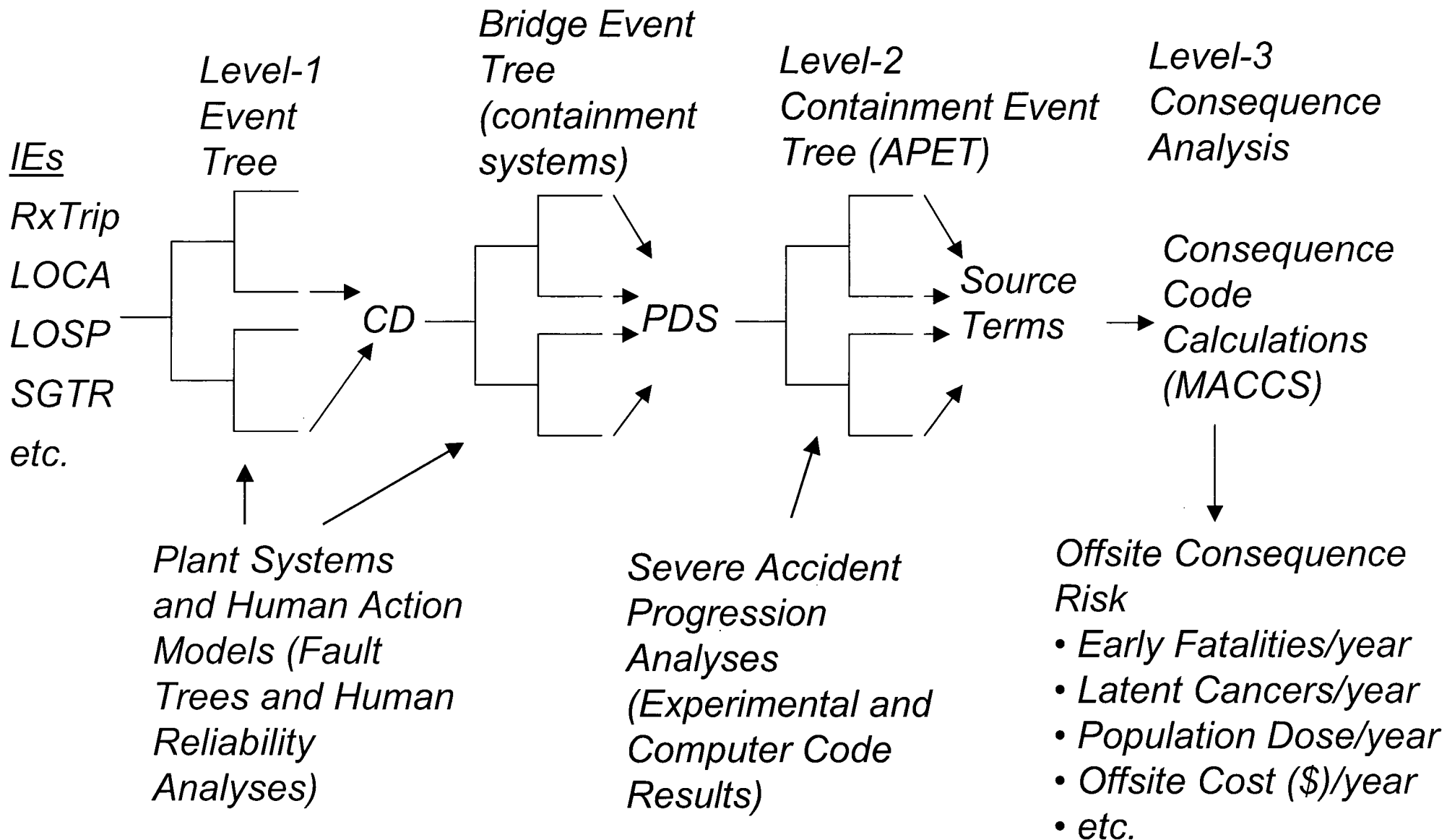


# Principal Steps in PRA





# Overview of Level-1/2/3 PRA





# PRA Strengths

- Rigorous, systematic tool for analyzing complex systems
- Information integration (multidisciplinary)
- Allows consideration of complex interactions
- Provides qualitative insights into plant vulnerabilities
- Provides quantitative results for use in decision-making
- Provides model structure which can be used for sensitivity studies
- Explicitly highlights and evaluates selected sources of uncertainty



# Principal PRA Limitations (see also Module O)

- Adequacy of data base for hardware and human performance
- Incomplete understanding of severe accident behavior
  - Results may be sensitive to analytical assumptions
- Modeling constraints and approximations, including truncation
- PRA only a snapshot analysis - need for “living” PRA
- 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
  - Less than full scope with respect to initiators, modes of operation
  - Not all scenarios included
    - Some missed by oversight
    - Some cannot be modeled at present



# Addressing PRA Limitations

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



# MODULE B

## TRADITIONAL ENGINEERING ANALYSIS AND PRA APPROACHES TO SAFETY ANALYSIS



# Traditional Engineering Analysis And PRA Approaches To Safety Analysis

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



# Objectives

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



# Outline

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



# Design Basis (Traditional) Approach to Risk

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



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

- Establishes requirements for
  - engineering margin
  - quality assurance
  - analysis methodology
- Requires redundancy and separation for critical systems
- Establishes principles for Defense-in-Depth



# Defense-In-Depth Provides Barriers (Physical,Procedural,Organizational) To Fission Product Release And Layers Of Protection



# Layers of Defense in Depth

## (Establishes Design & Operational Requirements)

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



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

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



# Examples of Layer 2 Barriers and Layer of Protection

## Control of Abnormal Operation and Detection of Failures

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



# Examples of Layer 3 Barriers and Layer of Protection Control of accidents within the design basis

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



# Examples of Layer 4 Barriers and Layer of Protection

Control Of Severe Plant Conditions, Including Prevention Of Accident Progression  
And Mitigation Of The Consequences Of Severe Accidents

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



# Examples of Layer 5 Barriers and Layer of Protection

Mitigation of radiological consequences of significant releases of radioactive materials

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



# Limitations of Traditional Approach

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



# The PRA Approach to Assessing Risk

- Focused on estimating the level of risk and risk-contributing features of design
  - PRA identifies accident initiators and inductively derives accident scenarios (i.e., not limited to predetermined set of accidents)
  - Analyzes multiple failures, including failures of redundant “barriers”
  - Non-safety equipment is credited
  - More extensive treatment of operator actions
  - Use of conservative margins avoided; focus on “best-estimate” analysis where possible
  - Goes beyond Design Basis



# Other PRA Approach Characteristics

- Assesses risk-significance of modeled elements
- Provides quantitative results and “model” for decision-making



## ECCS Single Failure Analysis Example

from FSAR Chapter 6, NUREG-0800 Requirements

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



# Single Failure Analysis Example (cont.)

## Contrast

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



# How PRA “Illustrates” Defense-in-Depth

(analyzes effectiveness of design/operational barriers)

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



# EXERCISE DEMONSTRATING TRADITIONAL ENGINEERING vs. PRA APPROACH TO SAFETY

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



# MODULE C

## OVERVIEW OF THE PRA PROCESS



# Purpose & Objectives

- Purpose: Provide an overview of the PRA process and describe why probabilistic models are used.
- Objectives: Upon completion of this module, students should be able to
  - Describe the major steps in the PRA process
  - Describe the outputs of each of the “Levels” of PRA
  - Describe why probabilistic models are used
  - Give examples of disciplines required to perform a PRA
  - Give examples of where traditional engineering inputs are used in the PRA process

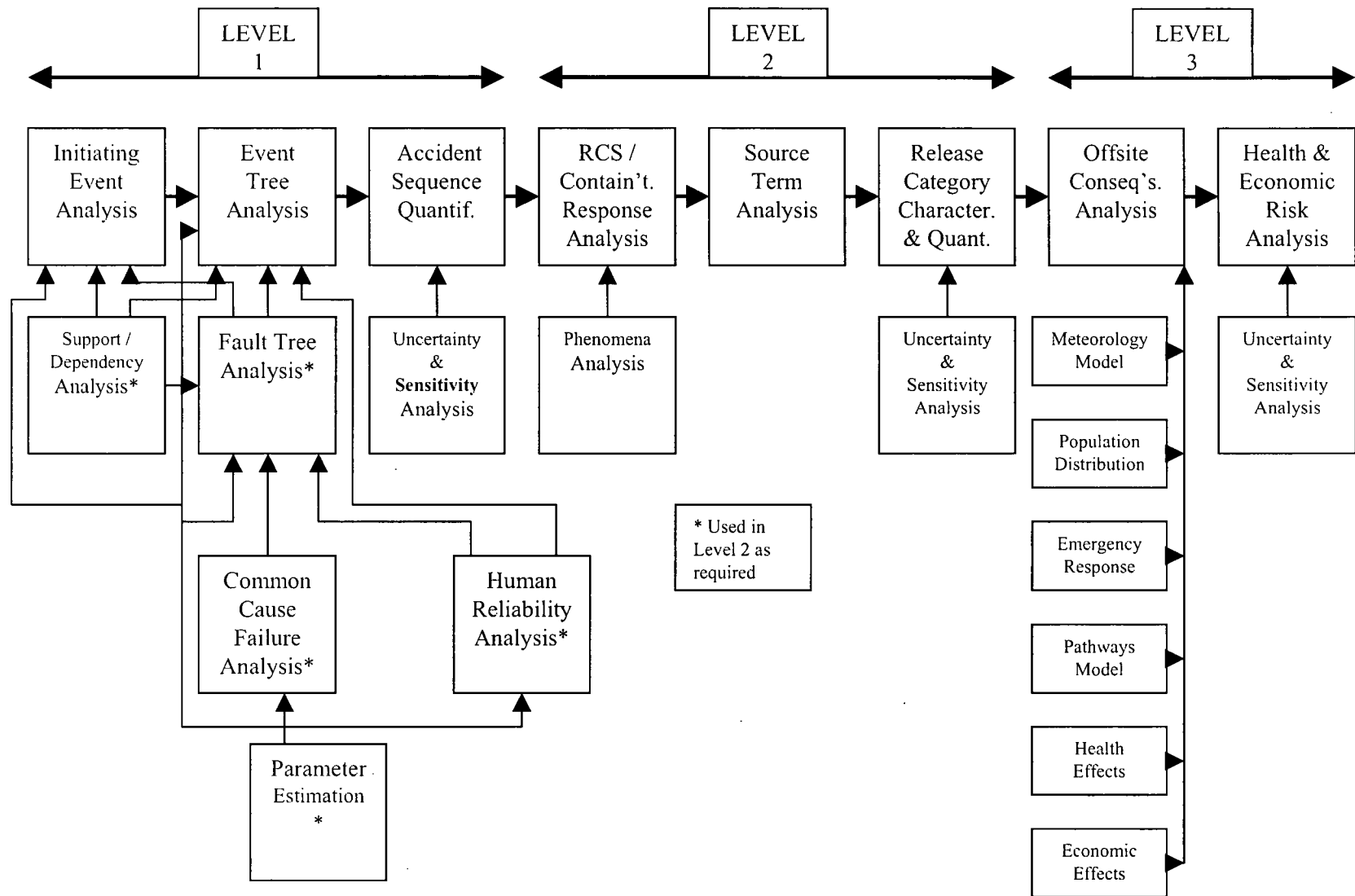


# Probabilistic Risk Assessment (PRA)

- PRA is a rigorous technical analysis that systematically attempts to answer three questions (also known as the risk triplet):
  - What can go wrong?
    - Identify accident scenarios
  - How likely is it?
    - Estimate likelihood of each accident scenario
  - What are the consequences?
    - Estimate consequences of each accident scenario



# Principal Steps in PRA





# Overview of PRA Process

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

<b><u>Level</u></b>	<b><u>An Assessment of:</u></b>	<b><u>Result</u></b>
1 (Systems Analysis)	Plant accident initiators and systems'/operators' response	Core damage frequency & contributors
2 (Containment Analysis)	Frequency and modes of containment failure	Categorization & frequencies of containment releases
3 (Radiological Consequences)	Public Health Consequences	Estimation of public & economic risks



# Level 1 PRA

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



# Level 2 PRA

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



# Level 3 PRA

- Level 3 PRA assesses public health and economic consequences of radiological releases
  - Comprises four major modeling processes (PRA specialists, meteorologists, health effects modelers...):
    - Atmospheric transport and deposition model to estimate
      - Direction and quantity of source-term plume release from containment
      - Area expected to be contaminated
      - Timing processes relative to emergency response
    - Pathways model considers:
      - Routes by which radiation enters body
      - Accumulated dose to various organs



# Level 3 PRA (cont.)

- Health effects model estimates:
  - Fatalities and injuries expected to occur within one year of accident (acute health effects)
  - Cancer deaths expected to occur over lifetime of exposed population (latent health effects)
- Models relating to other consequence factors such as:
  - Population distribution
  - Emergency response
  - Economic effects
- Integrated risk result is frequency with which a consequence of a particular magnitude will be exceeded
- NRC Quantitative Health Objectives (see Module A) constitute risk guidelines for commercial nuclear power plants



# Why Probabilistic Modeling?

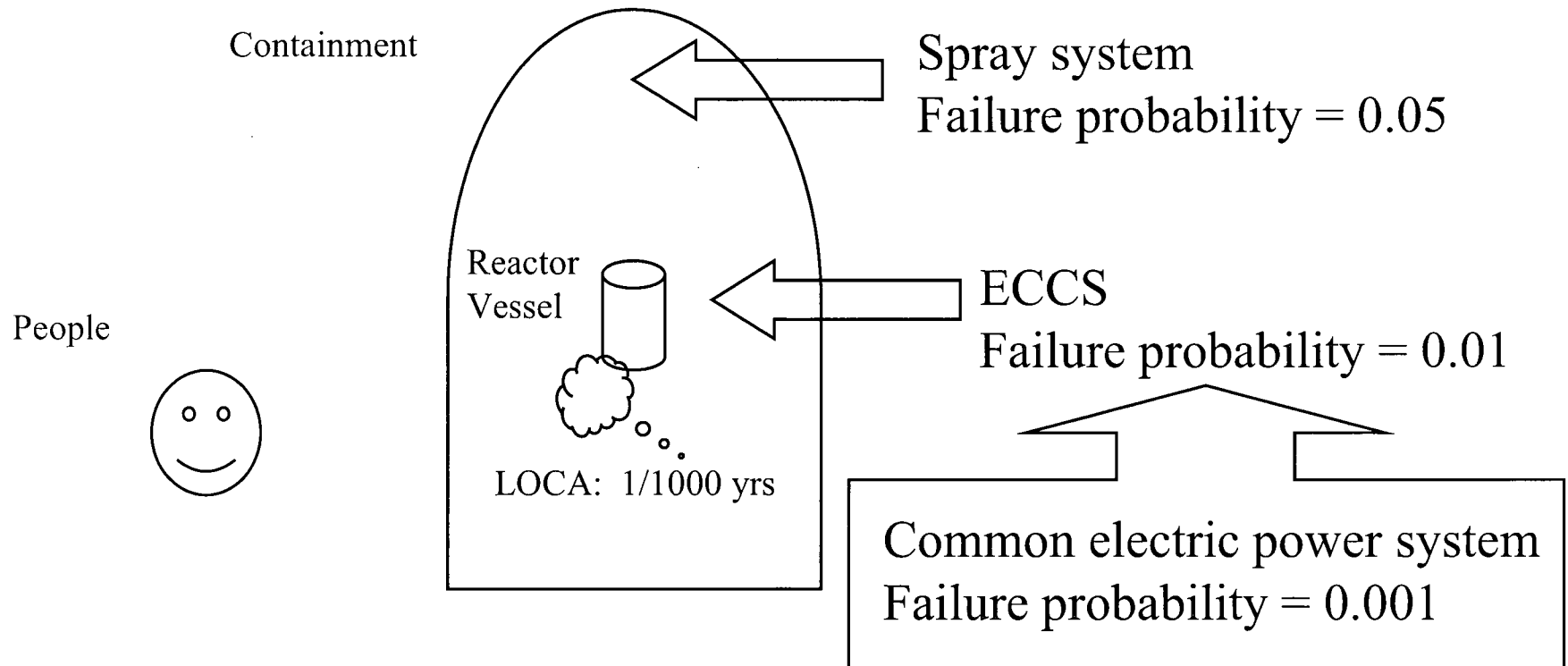
- Some problems/issues are too complex to treat deterministically; for example
  - Want to determine if emergency diesel generator (EDG) will start on next demand
  - Would require complete knowledge of initial and boundary conditions (e.g., how wearing of pieceparts affects start capability)
  - Our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



# Exercise Demonstrating PRA Process

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





**Assumptions:**

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



## \*\*\*\*IPE Exercise\*\*\*\*

- Using your choice of a plant's IPE, determine the following;
  - Level of PRA detail that was analyzed.
  - Estimated core damage frequency (CDF).  
Compare estimated CDF with  $1\text{E-}4$  goal.
  - Dominant (highest frequency) type of accident sequence.
  - Estimated large, early release frequency (LERF).  
Compare estimated LERF with  $1\text{E-}5$  goal.



# MODULE D

## ACCIDENT SEQUENCE INITIATING EVENTS

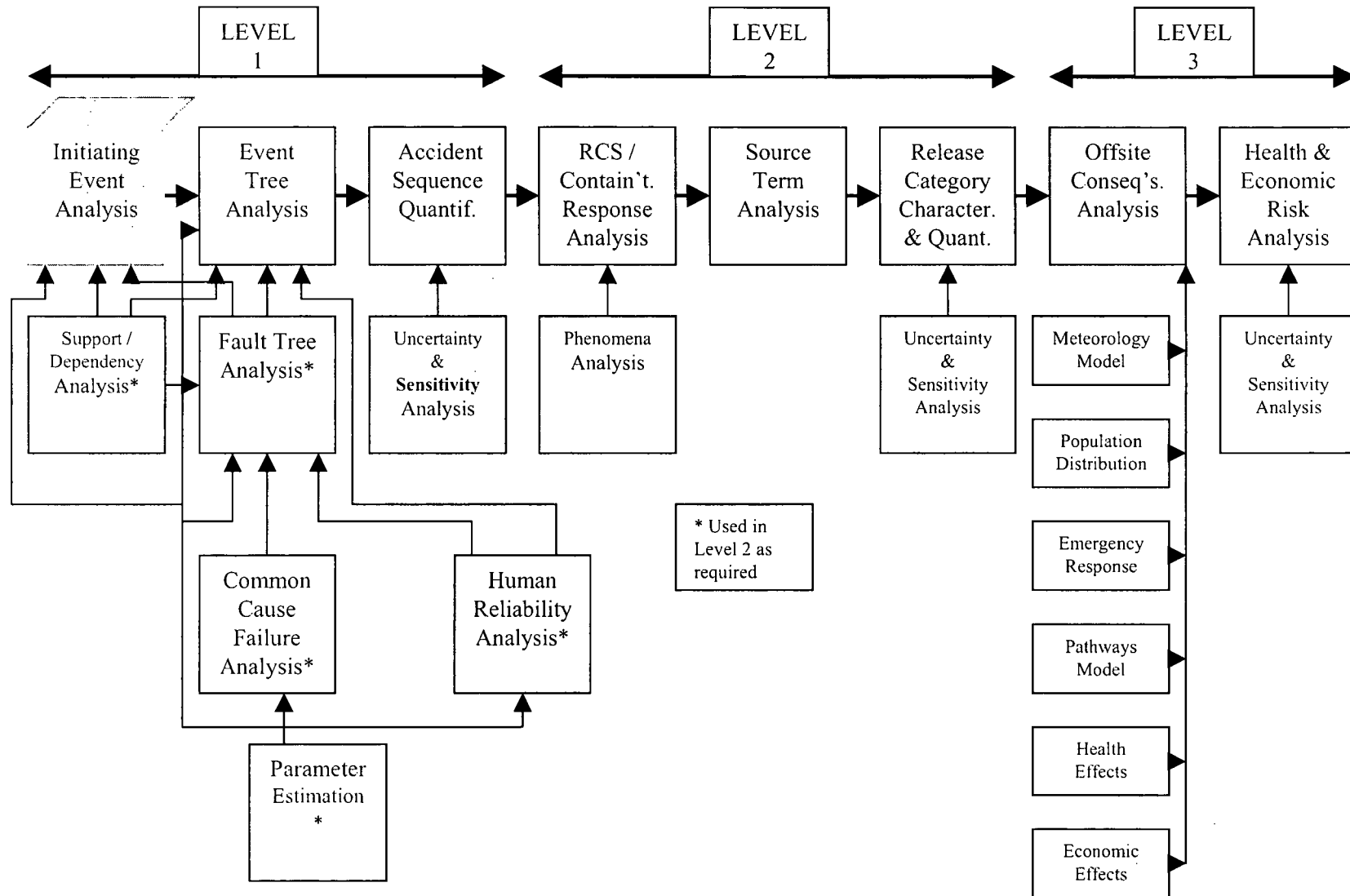


# Accident Sequence Initiating Events

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



# Principal Steps in PRA





# Initiating Events

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



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

Category	Initiating Event	Frequency (per Rx Yr)	Return Period (Rx Yr)
T1	Loss of offsite power	0.11	9.1
T2	Transient w/nonrecoverable loss of MFW	0.05	20
T2A	Transient w/recoverable loss of MFW	0.55	1.8
T3	Transient w/MFW available initially	1.35	0.75
T4	Loss of RCP seal cooling	6.0E-7	1,600,000
T5	Nonrecoverable loss of DC bus	0.006	167
T6	Loss of service water	6.3E-6	158,730



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

Category	Initiating Event	Frequency (per Rx Yr)	Return Period (Rx Yr)
T7	Steam generator tube rupture	0.01	100
T8	Loss of emergency switchgear room cooling	0.0066	152
T9	Loss of 4.1 kV emergency buses	0.018	56
A	Large LOCA	5.0E-4	2,000
S1	Medium LOCA	0.001	1,000
S2	Small LOCA	0.02	50
V	Interfacing system LOCA	1.6E-6	625,000



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

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



# Role of Initiating Events in PRA

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



## Example Categories of Initiating Events (SAR compared with PRA)

### In SAR

- Increase in secondary system heat removal
  - Increase in FW flow
  - Opening of SG relief valve
  - Balance-of-plant upsets
- Decrease in secondary system heat removal
  - Turbine trip
  - MSIV closure
  - Loss of FW flow
- Decrease in RCS flow rate
  - RCP trip
- Power anomalies
  - Uncontrolled rod withdrawal
  - Boron dilution
- Decrease in RCS inventory
  - SGTR
  - LOCAs

### In PRA

- T3 - transient w/MFW available
- T2A - transient w/MFW recoverable
- T3 - transient w/MFW available
- T3 - transient w/MFW available
- T2 - transient w/MFW not recoverable
- T3 - transient w/MFW available
- T3 - transient w/MFW available
- T3 - transient w/MFW available
- SGTR
- LOCAs



# Sources Used to Identify Initiating Events

- Review of Existing PRAs
- Review of Plant Experience and Procedures
- Feedback from other PRA Tasks
- Generic Databases
- Various NRC and Industry Sponsored Studies
- It should be noted that PRA initiators:
  - encompass all SAR initiators plus others and
  - are groupings of individual events with similar plant responses.



# Initiating Event Grouping

- For each identified initiating event:
  - identify the safety functions required to prevent core damage
  - identify the plant systems that can provide the required safety functions
- Group initiating events into categories that require the same plant response
- This is an iterative process, closely associated with the event tree construction task (see Module E). 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 (group)



# Initiating Event Grouping Example

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

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

\* Large LOCA success criteria based on calculations performed for (< 3 ft<sup>2</sup> equivalent area) credible pipe break, and realistic post-accident thermal hydraulic system performance.

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

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



# Initiating Event Quantification

- Use values based on type and frequency of events industry-wide (useful for rare events not expected to occur during the life of the plant)
- Use plant-specific data to update generic values when such data is available
- Modeling and/or analysis techniques (useful for very rare events)
- All of the above are used in a typical PRA



# Exercise: Initiating Event Frequency

- Calculate a transient initiating event frequency based on the following information;
  - A plant started operations four years ago, and the plant capacity factor was 85%.
  - Transients for the last four years:

<u>Year</u>	<u>Number of Transients</u>
1993	2
1994	0
1995	2
1996	1



# Generic Initiating Event Frequencies

- Generic initiating event frequencies can be obtained from the following sources.
  - NUREG/CR-4550 Vol.1 Methods and Data for NUREG-1150
  - NUREG/CR-2300 PRA Procedures Guide
  - NUREG/CR-2815 Probabilistic Safety Analysis Procedure Guide
  - NUREG/CR-3862 Development of Transient Initiating Event Frequencies (pre-1986)
  - NUREG/CR-5750 Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995
  - NUREG/CR-6365 Steam Generator Tube Failures
  - NUREG/CR-1032 Evaluation of Station Blackout accidents (pre-1988)
  - NUREG/CR-5946 Evaluation of Loss of Offsite Power Events: 1980-1996
  - NUREG/CR-4407 Pipe Break Frequency Estimation for Nuclear Power Plants
  - NSAC-154 ISLOCA Evaluation Guidelines
  - EPRI TR-100380 Pipe Failures in U.S. Commercial Nuclear Power Plants
- Note that the above cite industry-wide yearly averages. Plant-to-plant differences can and do exist, and on any given day can be dependent on existing plant configuration and environmental conditions. Therefore....



# A Cautionary Note

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



# Student Exercise

Given the following PRA results:

IE	IE Frequency (per yr)	IE Contribution to CDF
LLOCA	5E-5	3%
MLOCA	1E-4	10%
SLOCA	1E-3	15%
ISLOCA	2E-6	1%

(total internal/external CDF = 7E-5/yr)

The licensee finds that a number of RCS instrument lines are experiencing excessive mechanical fatigue due to lack of proper supports. Estimate the change in CDF if the frequency of SLOCA increases by a factor of 2 as a result of this condition.



# Student Exercise

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



# MODULE E

## ACCIDENT SEQUENCE ANALYSIS USING EVENT TREES

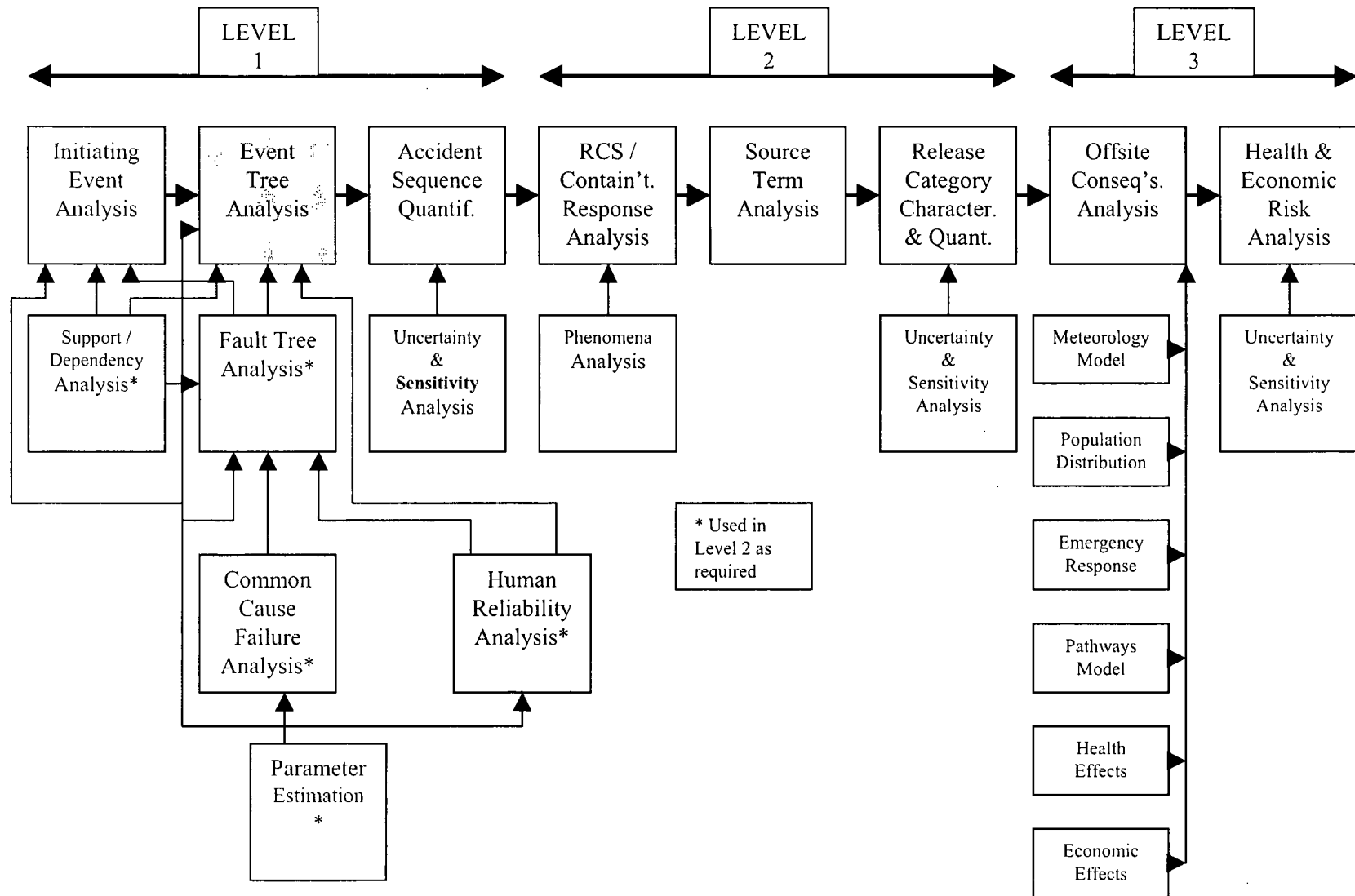


# Accident Sequence Analysis Using Event Trees

- Purpose: Students will learn purposes and techniques of event tree analysis. Students will learn how event tree analysis is related to the identification and quantification of accident sequences.
- Objectives:
  - Describe the purposes of event tree analysis
  - Describe techniques and notations employed in event tree construction
  - Describe the relationship between event tree construction and deterministically-identified success criteria
  - Compare PRA accident sequences (as depicted by the event trees) and the traditional SAR design basis accidents
- References: NUREG/CR-2300, NUREG-1489



# Principal Steps in PRA



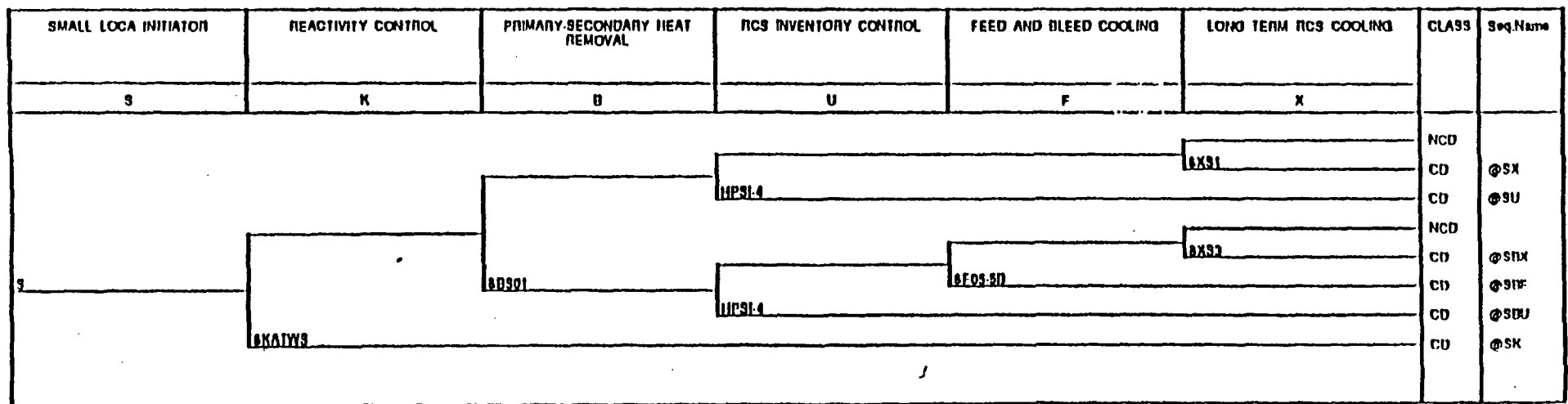


# Event Trees

- Typically used to model the response to an initiating event
- Features:
  - One event tree for each initiating event (or initiating event group)
  - Related to plant functions/systems/operations
  - Identifies relationships in event occurrence
  - Identifies relative timing of event occurrence
  - Provides event sequence progression
  - Provides end-to-end traceability of accident sequences
- Primary use
  - Identification of accident sequences which result in some outcome of interest (usually core damage and/or containment failure)
  - Forms the basis for accident sequence quantification



# (3.8): FCS SMALL LOCA EVENT TREE









# Principal Steps in Event Tree Development

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



# Determining Boundaries

- Mission time
- Dependencies among safety functions or systems
- Sequence end states - undesired outcome
  - Core damage
  - Core vulnerable
  - Containment vulnerable
- Extent of operator actions explicitly modeled in event tree



# Success Criteria

- Start with functional event tree showing the fundamental safety functions for the reactor core and containment
  - Reactor subcriticality
  - Core heat removal
  - Core inventory makeup
  - Primary coolant system integrity
  - Containment pressure suppression
  - Containment heat removal
  - Containment integrity



# Success Criteria (cont.)

- Identify which of the fundamental safety functions will be challenged or required to mitigate the accident initiator
- Identify systems which can perform each of the required fundamental safety functions
- Identify the minimum required equipment necessary to perform function (often based on thermal/hydraulic calculations, source of uncertainty)
  - Calculations often best-estimate, rather than conservative
- May credit non-safety-related equipment where feasible



# Example of Success Criteria Variability

- Examples from CEOG SIT AOT analyses for Large LOCAs
  - Fort Calhoun: Need 3 of 3 SITs to unbroken legs
  - Millstone 2: Need 2 of 3 SITs to unbroken legs
  - St. Lucie: Need 3 of 4 SITs to unbroken legs
  - Palo Verde 1, 2, 3: Need 2 of 3 SITs to unbroken legs



# Event Tree Development

- An event tree consists of an initiating event (one per tree), followed by a number of headings (or top events), and then the event tree structure or success/failure branching for the respective top events
- The top events represent the systems, components, and/or operations identified by success criteria
- To the extent possible, the top events are ordered in the time-related sequence in which they would occur
  - Selection of top events and their ordering reflects the EOPs
- Each node (or branch point) below a top event represents the success or failure of the respective top event.
  - Logic typically binary
    - Downward branch failure of top event
    - Upward branch success of top event
  - Logic can have more than binary branch, with each branch representing a specific status of the respective top event



# Event Tree Development (Continued)

- Branches can be pruned logically (branch points for specific nodes removed) to remove unnecessary combinations of system success requirements
  - This minimizes the total number of sequences that will be generated and eliminates illogical sequences
- Each path of an event tree represents a potential scenario
- Each potential scenario results in either plant success or core damage (or a particular end state of interest)



# Plant Damage States

- Also called “Accident Classes” or “Endstates.”
- Can use “indicators” to relate a core damage accident sequence to the existing status of plant safety function such as:
  - the status of the reactor coolant system at the onset of core damage,
  - the status of various systems’ operability,
  - the status of water inventories,
  - the status of the containment, and
  - the timing of the onset of core damage.
- Plant damage states are used to group accident sequences with similar outcomes for core damage analysis and to simplify subsequent use in Level 2/3 analysis.



# Event Tree Interpretation Exercise

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



**TABLE 3.1.1-1**  
**SOURCES OF INITIATING EVENT INFORMATION**

1. LERs for North Anna Unit 1 and 2 for 1986 - 1990.
2. NUREG/CR-3862, "Development of Transient Initiating Event Frequencies for use in PRA, May 1988".
3. NUREG/CR-4550, Volume 3.
4. Review of Support System Drawings for North Anna Units 1 and 2.
5. North Anna monthly operating reports 1980 - 1990.
6. Review of past PRAs on Westinghouse PWRs.



**TABLE 3.1.1-2**  
**LIST OF INITIATING EVENTS**

<u>Abbreviations</u>	<u>Descriptions</u>
T1	Loss of Offsite Power
T2	Transients with non-recoverable Loss of Main Feedwater
T2A	Transients with recoverable loss of Main Feedwater following FW Isolation
T3	Transients with Main Feedwater initially available
T4	Loss of RC Pump Seal Injection and Thermal Barrier Cooling
T5A	Non-recoverable Loss of DC Bus 1-I
T5B	Non-recoverable Loss of DC Bus 1-III
T6	Loss of Service Water System
T7	Steam Generator Tube Rupture
T8	Loss of Emergency Switchgear Room Cooling
T9A	Loss of 4160 V Bus 1H
T9B	Loss of 4160 V Bus 1J
A	Large LOCA      6" - 31"
S1	Medium LOCA     2" - 6"
S2	Small LOCA      3/8" - 2"
VX	Interfacing System LOCA
RX	Reactor Vessel Rupture



TABLE 3.1.1-7  
TRANSIENT INITIATING EVENT T2 SUB-GROUP

<u>Initiating Event Group</u>	<u>Representative Initiators</u>	<u>Comments</u>
T2 Non-recoverable Loss of Main FW	Failure of Main Feedwater. Loss of Instrument Air (IA) system. Main Feed- water Line Break.	Includes MFW failures (i.e., disabled pumps), failure in hotwell FW flow path, and insufficient condensate inventory, loss of IA.
T2A Recoverable Loss of MFW	Steam Generator Hi Hi Level. Inadvertent SI. Main Steamline Break.	FW recovered by start of 1 MFW pump and flow through 1 FRV or bypass valve.
	Lo Tavg coincident with Reactor Trip.	FW recovered by flow through 1 FW bypass valve and 1 MFW pump maintained on recirculation.



**TABLE 3.1.1-8**  
**CORRESPONDENCE BETWEEN NORTH ANNA IE GROUP AND EPRI CATEGORIES**

<u>North Anna IE Group(s)</u>	<u>EPRI Category</u>	<u>Title and Definition</u>
T2A, T3	1	<b>Loss of RCS Flow (1 loop)</b> - An inadvertent hardware or human error interrupts the flow in one loop of the reactor coolant system. SI*
T3	2	<b>Uncontrolled Rod Withdrawal</b> - One or more control rods are withdrawn inadvertently.
T3*	3	<b>CRDM Problems and/or Rod Drop</b> - Failures in the control rod drive mechanism (CRDM) occur that lead to out-of-tolerance conditions in the primary system. The transient may include dropping of one or more control rods into the core as part of the CRDM failure. [Assumes no turbine runback-use category 33 with turbine runback].
T3*	4	<b>Leakage from Control Rods</b> - Primary system leakage around the control rod drive mechanism is excessive and reactor shutdown is required.
T3*	5	<b>Leakage in Primary System</b> - Primary system leakage through various piping components is excessive and reactor shutdown is required. This transient does not include:  No. 4 - Leakage from control rods No. 7 - Pressurizer leakage No. 26 - Steam generator leakage
T3	6	<b>Low Pressurizer Pressure</b> - Pressurizer pressure falls below the lower operating limit.
T3*	7	<b>Pressurizer Leakage</b> - Pressurizer components allow excessive primary system leakage and reactor shutdown is required.



**TABLE 3.1.1-8 (Continued)**  
**CORRESPONDENCE BETWEEN NORTH ANNA IE GROUP AND EPRI CATEGORIES**

<u>North Anna IE Group(s)</u>	<u>EPRI Category</u>	<u>Title and Definition</u>
T3	8	<b>High Pressurizer Pressure -</b> Pressurizer pressure climbs above the upper operating limit.
T2A	9	<b>Inadvertent Safety Injection Signal -</b> Hardware or operator error initiates a safety injection.
T3	10	<b>Containment Pressure Problems -</b> Hardware or operator error results in containment pressure exceeding limits.
T3	11	<b>CVCS Malfunction - Boron Dilution -</b> Hardware or operator error results in a CVCS malfunctions such that reactor power is affected.
T3	12	<b>Pressure/Temperature/Power Imbalance - Rod Position Error -</b> Poor control rod positioning from mechanical or operator error causes a scram based on a pressure, temperature, or power imbalance.
Not Applicable	13	<b>Startup of Inactive Coolant Pump -</b> An inactive coolant pump is started at an improper power and flow condition. [Unit operation with inactive coolant loop is precluded by Technical specifications.]
T3	14	<b>Total Loss of RCS Flow -</b> A hardware or operator error causes a loss of reactor coolant system flow.
T3	15	<b>Loss or Reduction in Feedwater Flow (1 loop) -</b> One feedwater pump trips or another occurrence results in an overall decrease in feedwater flow.



**TABLE 3.1.1-8 (Continued)**  
**CORRESPONDENCE BETWEEN NORTH ANNA IE GROUP AND EPRI CATEGORIES**

<u>North Anna IE Group(s)</u>	<u>EPRI Category</u>	<u>Title and Definition</u>
T2, T2A	16	<b>Total Loss of Feedwater Flow (all loops)</b> - A simultaneous loss of all main feedwater occurs, excluding that due to loss of all offsite power (Category 35).
T2A	17	<b>Full or Partial Closure of MSIV (1 loop)</b> -One main steam isolation valve (MSIV) closes, the rest remaining open, or partial closure of one or more MSIV occurs. [Can result in Steam Generator Lo-Lo Level reactor trip.]
T3	18	<b>Closure of all MSIV</b> - One of various steam line or nuclear system malfunctions requires termination of steam flow from the vessel. The closure of one MSIV may cause an immediate closure of all other MSIVs; this occurrence is also included in this transient definition. However, any closure that is the result of another initiator is not included. [Can result in Steam Generator Lo-Lo Level reactor trip.]
T3*	19	<b>Increase in Feedwater Flow (1 loop)</b> - An increase in feedwater flow occurs in one loop. [Steam Generator Hi-Hi Level Turbine Trip/Reactor Trip causes Feedwater Isolation.]
T3*	20	<b>Increase in Feedwater Flow (All Loops)</b> - An increase in feedwater flow occurs in one loop.[Steam Generator Hi-Hi Level Turbine Trip/Reactor Trip causes Feedwater Isolation.]



**TABLE 3.1.1-8 (Continued)**  
**CORRESPONDENCE BETWEEN NORTH ANNA IE GROUP AND EPRI CATEGORIES**

<u>North Anna IE Group(s)</u>	<u>EPRI Category</u>	<u>Title and Definition</u>
T2A*, T3*,	21	<b>Feedwater Flow Instability - Operator Error</b> - Feedwater is being controlled manually, usually during startup or shutdown, and excessive or insufficient feedwater flow occurs.
T2A, T3*	22	<b>Feedwater Flow Instability - Miscellaneous Mechanical Causes</b> - Excessive or insufficient feedwater flow results from hardware failures in the feedwater system.
T2, T3	23	<b>Loss of Condensate Pumps (1 loop)</b> - One condensate pump fails, reducing feedwater flow. [Can result in Feedwater pump trip on low suction pressure]
T2	24	<b>Loss of Condensate Pumps (all loops)</b> - All condensate pumps fail, causing a loss of feedwater flow.
T3	25	<b>Loss of Condenser Vacuum</b> - Either a complete loss or decrease in condenser vacuum results from hardware or human error. Can use atmospheric steam dump without condenser, Feedwater pumps will not trip as long as hotwell inventory lasts.
T3*, T7	26	<b>Steam Generator Leakage</b> - Excessive primary system to secondary leakage occurs in the steam generator.
T3	27	<b>Condenser Leakage</b> - Excessive secondary system leakage occurs in the condenser. [Feedwater heater level Turbine Trip].



**TABLE 3.1.1-8 (Continued)**  
**CORRESPONDENCE BETWEEN NORTH ANNA IE GROUP AND EPRI CATEGORIES**

<u>North Anna IE Group(s)</u>	<u>EPRI Category</u>	<u>Title and Definition</u>
T3	28	<b>Miscellaneous Leakage in Secondary System</b> - Excessive leakage occurs in the secondary system other than in the condenser (see Category 27).
T2A, T3 <sup>+</sup>	29	<b>Sudden Opening of Steam Relief Valves</b> - A secondary system steam relief valve opens inadvertently, causing an unacceptably low pressure in the secondary system. [Can result in Feedwater Isolation from SI or Steam Generator Hi-Hi Level Turbine Trip/Reactor Trip.]
T2A <sup>+</sup> , T3 <sup>+</sup>	30	<b>Loss of Circulating Water</b> - Circulating water is not available to the plant. [Can result in loss of condenser vacuum - see Category 25.]
T3	31	<b>Loss of Component Cooling</b> - Excessive temperature of critical components is a result of a loss or decrease in component cooling water flow.
T3	32	<b>Loss of Service Water System</b> - The service water system fails to perform its function.
T2A <sup>+</sup> , T3 <sup>+</sup>	33	<b>Turbine Trip, Throttle Valve Closure, EHC Problems</b> - A turbine trip occurs; or turbine problems occur which in effect decrease steam flow to the turbine, causing a rapid change in the amount of energy removed from the primary system. [Turbine runback can result in Steam Generator Hi-Hi Level or Steam Generator Lo-Lo Level, causing Feedwater Isolation.]



**TABLE 3.1.1-8 (Continued)**  
**CORRESPONDENCE BETWEEN NORTH ANNA IE GROUP AND EPRI CATEGORIES**

<u>North Anna IE Group(s)</u>	<u>EPRI Category</u>	<u>Title and Definition</u>
T3	34	<b>Generator Trip or Generator Caused Faults</b> - The generator is tripped due to electrical grid disturbances or generator faults.
T1	35	<b>Loss of All Offsite Power</b> - All power to the plant from external sources (the grid or a dedicated transmission line to another plant) is lost.
T3	36	<b>Pressurizer Spray Failure</b> - The pressurizer spray system spuriously actuates or fails upon demand.
T3	37	<b>Loss of Power to Necessary Plant Systems</b> -Power is lost to a component or group of components such that plant shutdown is necessary. It does not include loss of power to those components whose failure causes another defined transient to occur.
T3	38	<b>Spurious Trips - Cause Unknown</b> - A scram occurs and no out-of-tolerance condition can be detected; the cause of the scram cannot be determined. [Use Category 9 if scram by SI reactor trip (and SI is spurious).]
T3	39	<b>Automatic Trip - No Transient Condition</b> - An auto scram is initiated by a hardware failure in instrumentation or logic circuits and no out-of-tolerance condition exists.



**TABLE 3.1.1-8 (Continued)**  
**CORRESPONDENCE BETWEEN NORTH ANNA IE GROUP AND EPRI CATEGORIES**

<u>North Anna IE Group(s)</u>	<u>EPRI Category</u>	<u>Title and Definition</u>
T3	40	<b>Manual Trip - No Transient Condition -</b> The operator initiates a scram for any reason when no out-of-tolerance condition exists.
T3	41	<b>Fire Within Plant -</b> A plant shutdown is necessitated by a fire in some part of the plant.

\* Evidenced in North Anna data  
+ Manual reactor trip only  
[ ] North Anna specific



**TABLE 3.1.1-9**  
**SOURCES OF DATA FOR PLANT-SPECIFIC INITIATORS**

1. North Anna Licensee Event Reports (LERs) for the period 1986 - 1990,
2. North Anna Power Station "Monthly Operating Report" for the period 1986 - 1990,
3. NUREG/CR-3862 for reactor trips within the interval 1978 through 1981, and for the power level of some reactor trip events over the interval 1982 through 1983. Note that North Anna "Monthly Operating Reports" were scanned to identify any unusual initiating events for the interval 1980 through 1990.

North Anna LERs were reviewed for the period 1984-1990 for the T9-related precursors involving loss of feeder power to the 4160 V buses 1H and 1J.



**TABLE 3.1.1-10**  
**LIST OF NORTH ANNA REACTOR TRIP EVENTS, 1986-1990**

VaP Unit	EPRI Cat	Yr	Date	ID	IE Group	Pwr Lev	Bkr Cls	Description	Cause	SI	References
N1	15	90	01/23/90	1	T3	100	Y	RT ON STEAM/FEEDWATER FLOW MISMATCH DUE TO A FAILED DRIVER CARD ON A FRV.	NA 1 EXPERIENCED AN AUTO Rx TRIP FROM 100% POWER DUE TO LOW LEVEL IN THE C SG WITH STEAM FLOW/FW FLOW MISMATCH. THE MISMATCH RESULTED FROM THE CLOSURE OF THE C MF REG. VLV DUE TO A FA LED PCB DRIVER CARD IN THE VALVE CONTROLLER	N	LER 90-001-00
N1	21	89	12/05/89	2	T2A	90	Y	AUTO REACTOR TRIP RESULTING FROM EHC SYSTEM TRANSIENT. REACTOR WAS INITIALLY AT 90% POWER AND RAMPED DOWN UNTIL TRIP.	UNIT 1 EXPERIENCED AN AUTO REACTOR TRIP FROM 7% POWER DUE TO A LO LO LEVEL IN THE B SG CAUSED BY FW ISOLATION. PRIOR TO THE REACTOR TRIP, THE POWER WAS BEING REDUCED DUE TO EHC SYSTEM PRESSURE TRANSIENTS WHICH WAS CAUSED BY LEAKING TURBINE OPC VLVS.	N	LER 89-017-00
N1	33	89	07/19/89	3	T3	90	Y	REACTOR TRIP DUE TO A LOSS OF EHC SYSTEM PRESSURE.	UNIT 1 EXPERIENCED AN AUTO Rx TRIP FROM 90% POWER DUE TO A LOSS OF EHC SYSTEM PRESSURE WHICH WAS CAUSED BY A FAILED O-RING ON THE TURBINE TRIP SOV 20-ET, RESULTING IN THE CLOSURE OF THE TURBINE STOP VALVES GENERATING THE TURBINE TRIP SIGNAL.	N	LER 89-014-00
N1	15	89	02/25/89	4	T3	76	Y	REACTOR TRIP DUE TO A MAIN FEEDWATER REGULATING VALVE CLOSURE AND SUBSEQUENT SG TUBE LEAK.	UNIT 1 EXPERIENCED AN AUTO Rx TRIP FROM 76% POWER DUE TO 'C' SG STEAM FLOW/FW FLOW MISMATCH COINCIDENT WITH A LOW SG LEVEL. THE MISMATCH WAS CAUSED BY THE CLOSURE OF THE C MF REG. VALVE, ON THE LOSS OF AIR.	N	LER 89-005-00



**TABLE 3.1.1-10 (Continued)**  
**LIST OF NORTH ANNA REACTOR TRIP EVENTS, 1986-1990**

VaP Unit	EPRI Cat	Yr	Date	ID	IE Group	Pwr Lev	Bkr Cls	Description	Cause	SI	References
N1	15	88	08/06/88	5	19	100	Y	REACTOR TRIP ON STEAM FLOW/FEED FLOW MISMATCH COINCIDENT WITH A LOW LEVEL DUE TO MFRV CLOSURE.	AUTO Rx TRIP FROM 100% POWER DUE TO THE MISMATCH OF SG FEED FLOW/SG COINCIDING WITH A LOW LEVEL. THE MISMATCH RESULTED FROM A CLOSURE OF THE 'B' MF REG VLV WHICH WAS CAUSED BY A DEGRADED VOLTAGE CONDITION ON THE 1J EMERGENCY BUS, CAUSED BY AN RSST (RESERVE STATION SERVICE TRANSFORMER) FAULT.	N	LER 88-020-00
N1	33	88	03/19/88	6	13	004	N	TURBINE TRIP/REACTOR TRIP-EHC SYSTEM MALFUNCTION. NOT INCLUDED BECAUSE OF LOWER POWER LEVEL.	UNIT 1 EXPERIENCED AN AUTO Rx TRIP FROM 3.5% POWER DUE TO SPIKE IN THE TURBINE IMPULSE PRESSURE WHICH CAUSED A TURBINE TRIP & ENABLED THE LOGIC FOR A REACTOR TRIP WHEN A TURBINE TRIP CONDITION EXISTED.	N	LER 88-013-00
N1	33	88	01/13/88	7	12A	015	Y	AUTOMATIC REACTOR TRIP DUE TO HI-HI STEAM GENERATOR LEVEL.	AUTO TURBINE TRIP/Rx TRIP FROM 15% POWER DUE TO A TURBINE SOLENOID TRIP WHICH RESULTED WHEN A HI-HI LEVEL (>75%) WAS DETECTED ON 2/3 LEVEL CHANNELS IN THE 8 SG. THE HI-HI LEVEL CAUSED FW ISOLATION AND WAS THE RESULT OF SG LEVEL OSCILLATIONS.	N	LER 88-005-00
N1	30	88	01/08/88	8	12A	100	Y	MANUAL REACTOR TRIP IN ANTICIPATION OF LOSS OF THE MAIN CONDENSER.	Rx WAS MANUALLY TRIPPED FROM 100% POWER IN ANTICIPATION OF LOSS OF THE MAIN CONDENSER AFTER THE THREE RUNNING CW PUMPS TRIPPED SIMULTANEOUSLY & CONDENSER VACUUM WAS OBSERVED TO BE DECREASING RAPIDLY. CAUSE OF PUMPS FAILURE COULD NOT BE FOUND.	N	LER 88-002-00



**TABLE 3.1.1-10 (Continued)**  
**LIST OF NORTH ANNA REACTOR TRIP EVENTS, 1986-1990**

VaP Unit	EPRI Cat	Yr	Date	ID	IE Group	Pwr Lev	Bkr Cls	Description	Cause	SI	References
N1	22	87	11/23/87	9	T3	100	Y	REACTOR TRIP GENERATED FROM 5A FEEDWATER HI-HI LEVEL SIGNAL.	REACTOR TRIPPED FROM 100% POWER DUE TO A TURBINE SOLENOID TRIP WHICH RESULTED FROM A 5A FEEDWATER HEATER HI-HI LEVEL SIGNAL WHICH WAS GENERATED WHEN A LEVEL SWITCH FAILED.	N	LER 87-020-00
N1	26	87	07/15/87	10	T2A	100	Y	MANUAL REACTOR TRIP DUE TO INDICATIONS OF EXCESSIVE RCS LEAKAGE THROUGH STEAM GENERATOR TUBE.	REACTOR WAS MANUALLY TRIPPED FROM 100% POWER DUE TO INDICATIONS OF A SG TUBE LEAKAGE IN THE C SG. -20 MIN. LATER SAFETY INJECTION SYSTEM WAS AUTOMATICALLY INITIATED. THE ROOT CAUSE HAS BEEN LABELED A SG TUBE RUPTURE; HOWEVER, CONSIDERING SG REPLACEMENT, THIS EVENT WAS CATEGORIZED T3 AS A SG TUBE LEAK REQUIRING MANUAL REACTOR TRIP.	Y	LER 87-017-01
N1	33	87	06/29/87	11	T3	018	Y	REACTOR TRIP DUE TO 5A FEEDWATER HEATER HI-HI LEVEL.	Rx TRIPPED FROM 18% POWER DUE TO A TURBINE SOLENOID TRIP WHICH RESULTED FROM A 5A FW HEATER HI-HI LEVEL SIGNAL. THE HI-HI LEVEL IN THE 5A FW HEATER WAS CAUSED BY AN IMPROPER VLV LINE-UP FOLLOWING A REFUELING OUTAGE.	N	LER 87-015-01
N1	3	87	04/19/87	12	T3	067	Y	REACTOR TRIP CAUSED BY DROPPED CONTROL ROD.	REACTOR TRIPPED FROM 67% POWER DURING A CONTROLLED RAMPDOWN INTO A REFUELING OUTAGE DUE TO NUCLEAR INSTRUMENTATION SYSTEM POWER RANGE HIGH NEGATIVE FLUX RATE CAUSED BY A SINGLE DROPPED ROD.	N	LER 87-004-00



**TABLE 3.1.1-10 (Continued)**  
**LIST OF NORTH ANNA REACTOR TRIP EVENTS, 1986-1990**

VaP Unit	EPR Cat	Yr	Date	ID	IE Group	Pwr Lev	Bkr Cls	Description	Cause	SI	References
N1	33	86	08/27/86	13	13	100	Y	MANUAL TURBINE/REACTOR TRIP DUE TO HIGH TURBINE/GENERATOR VIBRATION.	TURBINE/REACTOR WERE MANUALLY TRIPPED WHEN NA1 WAS AT 100% POWER DUE TO HIGH VIBRATION OF TURBINE/GENERATOR BEARING VIBRATION. VIBRATION CAUSE WAS BREAKAGE OF A 13 INCH PIECE OF TURBINE BLADE FROM THE LAST STAGE OF THE 'A' LOW PRESSURE TURBINE.	N	LER 86-015-00
N1	16	86	05/20/86	14	13	100	Y	REACTOR TRIP FROM STEAM FLOW/FEED MISMATCH COINCIDENT WITH LOW STEAM GENERATOR LEVEL.	Rx TRIP OCCURRED FROM 100% POWER DUE TO A TRIP SIGNAL GENERATED FROM A STEAM FLOW/FEED FLOW MISMATCH (ALL 3 FW REG VLVS CLOSED BY SPURIOUS FW ISOLATION SIGNAL TO FRVS ONLY) CONCURRENT WITH A LOW LEVEL (2/3 LESS THAN/EQUAL TO 25% N.R. LEVEL) IN THE SG.	N	LER 86-008-00
N1	17	86	03/26/86	15	12A	100	Y	REACTOR TRIP DUE TO A SAFETY INJECTION TRIP SIGNAL.	Rx TRIPPED FROM 100% POWER DUE TO A SI CAUSED BY THE CLOSURE OF THE B MAIN STEAM LINE TRIP VALVE. THIS RESULTED IN REACTOR AND TURBINE TRIP. THE SI WAS INITIATED DUE TO HIGH STEAM FLOW COINCIDENT WITH LOW STEAM LINE PRESSURE IN 'A' & 'C' SGs.	Y	LER 86-006-00
N1	39	86	05/31/86	16	13	100	Y	REACTOR TRIP DUE TO LOSS OF A POWER TO 120 VAC VITAL BUS.	Rx TRIPPED FROM 100% POWER DUE TO FAILURE OF VITAL BUS WHICH POWERS THE RELAY THAT SENSES THE BREAKER POSITION OF 'A' RCP. DE-ENERGIZED RELAY, LEAD TO Rx TRIP SIGNAL BECAUSE THE RPS SENSED THE 'A' RCP BREAKER OPEN COINCIDENT WITH REACTOR POWER >30%.	N	LER 86-009-00



**TABLE 3.1.1-10 (Continued)**  
**LIST OF NORTH ANNA REACTOR TRIP EVENTS, 1986-1990**

VaP Unit	EPRI Cat	Yr	Date	ID	IE Group	Pwr Lev	Bkr Cls	Description	Cause	SI	References
N1	33	86	02/23/86	17	T3	100	Y	REACTOR/TURBINE TRIP - TURBINE CONTROL SYSTEM MALFUNCTION.	Rx TRIP/TURBINE TRIP OCCURRED FROM 100% POWER. THE REACTOR TRIP SIGNAL WAS GENERATED BY A LO-LO LEVEL IN 'B' SG, DUE TO CLOSURE OF THE TURBINE GOVERNOR VALVES, CAUSING SHRINKAGE IN ALL SG WITH 'B' SG REACHING THE Rx TRIP SETPOINT FIRST.	N	LER 86-002-00
N1	33	86	01/19/86	18	T3	004	Y	REACTOR/TURBINE TRIP DUE TO A TURBINE FIRST-STAGE IMPULSE PRESSURE SPIKE. NOT INCLUDED BECAUSE OF LOW POWER LEVEL.	TURBINE TRIP/REACTOR TRIP OCCURRED FROM 4% POWER DUE TO A TURBINE FIRST-STAGE IMPULSE PRESSURE SPIKE AS PLANT PERSONNEL WERE SETTING UP FOR A TURBINE-GENERATOR OVERSPEED TRIP TEST.	N	LER 86-001-00
N2	21	90	11/02/90	19	T3	15	Y	REACTOR TRIP FROM 9% POWER DUE TO LOSS OF NORMAL FEEDWATER. REACTOR WAS INITIALLY AT 15 % POWER.	AUTO REACTOR TRIP OCCURRED FROM 9% POWER DUE TO A LO-LO LEVEL IN 'A' SG WHILE RETURNING TO POWER OPER. THE REACTOR TRIP OCCURRED -8 MIN. FOLLOWING AN AUTO TURBINE TRIP FROM -15% POWER. THE CAUSE OF EVENT WAS PERSONNEL ERROR TO RESET FW BYPASS VALVE.	N	LER 90-010-00
N2	15	86	06/29/86	20	T9	100	Y	REACTOR TRIP DUE TO LOW STEAM GENERATOR LEVEL COINCIDENT WITH A STEAM FLOW/FEED FLOW MISMATCH.	Rx TRIP OCCURRED FROM 100% POWER DUE TO LOW SG LEVEL COINCIDENT WITH A STEAM FLOW/FEED FLOW MISMATCH DURING EMERGENCY RAMPDOWN, DUE TO LOSS OF 2/3 MFW PUMPS CAUSED BY A LOSS OF POWER TO 1 OF 2 500kV SWITCHYARD BUSES.	N	LER 86-009-00



**TABLE 3.1.1-10 (Continued)**  
**LIST OF NORTH ANNA REACTOR TRIP EVENTS, 1986-1990**

VaP Unit	EPRI Cat	Yr	Date	ID	IE Group	Pwr Lev	Bkr Cls	Description	Cause	SI	References
N2	34	86	04/11/86	21	T3	071	Y	UNIT 2 REACTOR TRIP DUE TO A TURBINE TRIP CAUSED BY A MAIN ELECTRICAL GENERATOR TRIP.	REACTOR TRIP OCCURRED FROM 71% POWER DUE TO A TURBINE TRIP CAUSED BY A MAIN ELECTRICAL GENERATOR TRIP, DUE TO ACTUATION OF A GENERATOR DIFFERENTIAL LOCKOUT RELAY UPON LOSS OF EXCITATION FIELD SIGNAL CAUSED BY FAILURE OF THE PERMANENT MAGNET GENERATOR.	N	LER 86-008-00
N2	33	86	04/16/86	22	T3	004	Y	REACTOR TRIP CAUSED BY TURBINE FIRST STAGE PRESSURE SPIKE. NOT INCLUDED BECAUSE OF LOW POWER LEVEL.	REACTOR TRIPPED FROM 4% POWER DUE TO TURBINE 1ST STAGE PRESS. SPIKE, CAUSED BY PERFORMING A THROTTLE VALVE/GOVERNOR VALVE TRANSFER WITH TURBINE IN AUTO CONTROL. THE PRESS. SPIKE CLEARED THE P-7 R <sub>x</sub> TRIP BLOCKS CAUSING R <sub>x</sub> TRIP DUE TO TURBINE TRIP.	N	LER 86-007-00
N2	3	86	05/29/86	23	T3	100	Y	UNIT 2 REACTOR TRIP OCCURRED FROM A NEGATIVE FLUX RATE TRIP.	R <sub>x</sub> TRIP OCCURRED FROM 100% POWER DUE TO A NEGATIVE FLUX RATE CAUSED BY THE OPENING OF THE STATIONARY COIL POWER SUPPLY DISCONNECTED TO ROD CONTROL POWER DISTRIBUTION CABINET 1AC, CAUSING 12 RODS TO DROP INTO THE CORE. PERSONNEL ERROR CAUSED THE EVENT.	N	LER 86-005-00



**TABLE 3.1.1-11**  
**SUMMARY OF NORTH ANNA SYSTEM REVIEW FOR INITIATING EVENTS**

<u>System</u>	<u>System Symbol</u>	<u>Front line or Support</u>	<u>Detailed Analysis</u>
Ambient Air Monitoring	AM	Neither	No
ATWS Mitigation System			
Actuation & Control			
(AMSAC)		Front line	No
Auxiliary Boilers	AB	Neither	No
Auxiliary Feedwater	AFW	Front Line	Yes
Auxiliary Steam	AS	Neither	No
Batteries, 125VDC	BY	Support	Yes
Bearing Cooling	BC	Support	Yes
Bearing Lube	BL	Neither	No
Blowdown	BD	Neither	No
Boron Recovery	BR	Neither	No
Building Structure	BLD	Neither	No
Chemical & Volume Control	CH	Front line	Yes
Chilled Water	CD	Neither	No
Circulating Water	CW	Support	Yes
Communications	CO	Neither	No
Component Cooling	CC	Support	Yes
Compressed Air	CA	Neither	No
Computer	CM	Neither	No
Condensate	CN	Support	Yes
Condensate Polishing	CP	Neither	No
Containment Access	CE	Neither	No
Containment Vacuum	CV	Neither	No
Control Rod Drive Power Supply	ED	Neither	No
Decay Heat Release	DHR	Neither	No
Decontamination	DC	Neither	No
Demineralizer Drain	WDR	Neither	No
Diesel Air	EB	Support	No
Drains (Aerated)	DA	Neither	No
Drains (Building Services)	DB	Neither	No
Drains (Gaseous)	DG	Neither	No
Domestic Water	DW	Neither	No
Early Warning	EW	Neither	No
Earthquake Reporting	ER	Neither	No
Electrical Calibration	EC	Neither	No
Electrical Equipment	PHP	Neither	No
Electrical Equipment (4KV & Above)	PH	Support	Yes
Electrical Equipment (600V & Below)	PL	Support	Yes
Electrical Hydraulic Control	EH	Neither	No
Electrical Instrumentation	EI	Neither	No
Electrical Power	EP	Support	Yes



C:\NAPS\IPE\TRES\T2A.EVT 8:00:40am 9-28-92 MUPRA 2.0 YPMR  
Quantification Date: 9-28-92 8:00:39am TOTAL CHF = 6.11E-005

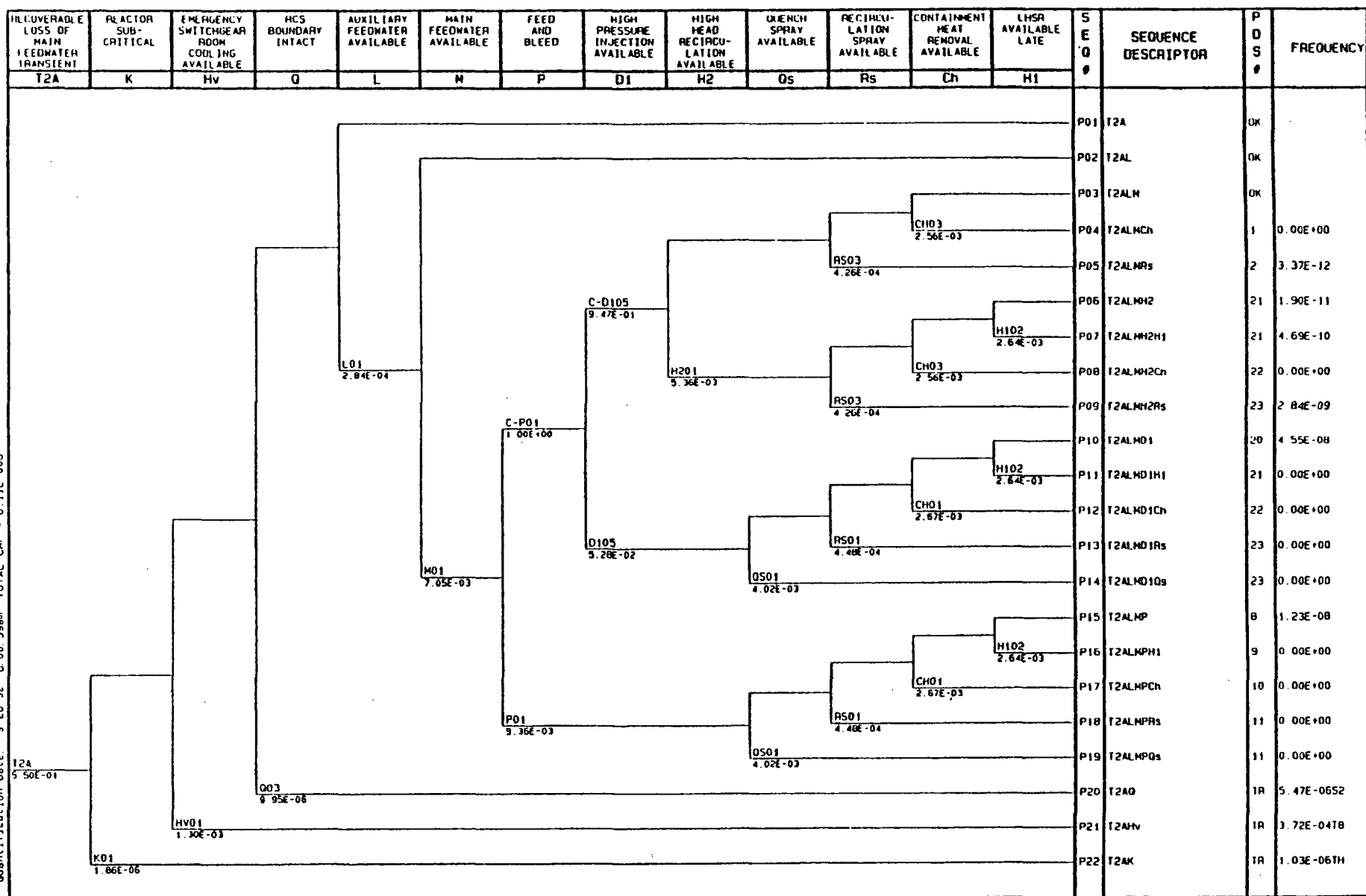


FIGURE 3.1-T2A

NORTH ANNA INDIVIDUAL PLANT EXAMINATION

T2A: RECOVERABLE LOSS OF MAIN FEEDWATER EVENT TREE



**TABLE 3.1.1-12**  
**SUMMARY OF LOSS OF SUPPORT SYSTEMS AS INITIATORS**

<u>Support System Loss Considered</u>	<u>Impact on Normal Operation</u>	<u>Attendant Important System Failures</u>	<u>Initiating Event Group</u>
4160 V Bus 1H	IRPI loss with total 4160 1H Bus loss could result in manual Reactor Trip or Shutdown	Charging Pump A ECCS Train A 480 V 1H 480 V 1H1 480 V 1H1-1 480 V 1H1-2S 480 V 1H1-4	Represented by the T9A Initiator. Impact on ESGR cooling also considered in the T8 Initiator.
4160 V Bus 1J	Isolation of RCP CC cooling could result in manual Reactor Trip or Shutdown	Charging Pump B ECCS Train B 480 V 1J 480 V 1J1 480 V 1J1-1 480 V 1J1-2S	Represented by the T9B Initiator. Impact on ESGR cooling also considered in the T8 Initiator.
480 V Bus 1H	IRPI loss with total 480 1H bus loss could result in manual Reactor Trip or Shutdown	Some ECCS Train A 480 V 1H1-1 480 V 1H1-4	Included within the T9A Initiator.
480 V Bus 1H1	No direct impact	Some ECCS Train A 480 V 1H1-2S	Not included as an Initiator. Disables some standby ECCS equipment, but doesn't cause transient or direct reactor trip.



**TABLE 3.1.1-12 (Continued)**  
**SUMMARY OF LOSS OF SUPPORT SYSTEMS AS INITIATORS**

<u>Support System Loss Considered</u>	<u>Impact on Normal Operation</u>	<u>Attendant Important System Failures</u>	<u>Initiating Event Group</u>
480 V Bus 1H1-1	IRPI loss with total 480 1H1-1 Bus loss could result in manual Reactor	ESGR Chiller Trains A & C	Included within the T9A Initiator.
480 V Bus 1H1-2S	No direct impact	Some ECCS Train A Same as 480 V Bus 1H1.	
480 V Bus 1H1-4	No direct impact	ESGR AHU 6 ESGR Chiller Train C	Included within the T9A Initiator. Impact on ESGR cooling also considered in the T8 Initiator.
480 V Bus 1J	Isolation of RCP cooling could result in manual Reactor Trip or Shutdown	Some ECCS Train B 480 V 1J1-1 480 V 1J1-2S	Included within the T9B Initiator.
480 V Bus 1J1	No direct impact	Some ECCS Train B	Same as 480 V Bus 1H1.



**TABLE 3.1.1-12 (Continued)**  
**SUMMARY OF LOSS OF SUPPORT SYSTEMS AS INITIATORS**

<u>Support System Loss Considered</u>	<u>Impact on Normal Operation</u>	<u>Attendant Important System Failures</u>	<u>Initiating Event Group</u>
480 V Bus 1J1-1	Isolation of RCP cooling could result in manual Reactor Trip or Shutdown	ESGR AHU 7 ESGR Chiller Train B	Included within the T9B Initiator.
480 V Bus 1J1-2S	No direct impact	Some ECCS Train B	Same as 480 V Bus 1H1.
120 VAC Vital Bus 1-I	Manual Reactor Trip on loss of RCP Cooling	MS Atmospheric Dump Valve A CC to RCP Thermal Barriers isolated	Included within the T3 Initiator.
120 VAC Vital Bus 1-II	No direct impact	MS Atmospheric Dump Valve B	None
120 VAC Vital Bus 1-III	Manual Reactor Trip on loss of RCP Cooling	MS Atmospheric Dump Valve C CC to RCP Thermal Barriers isolated	Included within the T3 Initiator.
125 VDC Bus 1-I	Reactor Trip on loss of MFW	ECCS Train A 4160 V switchgear MS Condenser Dump Valves	Represented by the T5A Initiator.



**TABLE 3.1.1-12 (Continued)**  
**SUMMARY OF LOSS OF SUPPORT SYSTEMS AS INITIATORS**

<u>Support System Loss Considered</u>	<u>Impact on Normal Operation</u>	<u>Attendant Important System Failures</u>	<u>Initiating Event Group</u>
125 VDC Bus 1-II	No direct impact	MFW Pump B Condensate Pump B	Not included as an Initiator. Standby MFW & Condensate Pumps available with autostart.
125 VDC Bus 1-III	Reactor Trip on loss of MFW	ECCS Train B 4160 V switchgear MS Condenser Dump Valves	Represented by the T5B Initiator.
Service Water	Manual Reactor Trip or Shutdown on loss of CC to RCPs, loss of Instrument Air or loss of ESGR cooling	Charging Pumps A/B/C CC Heat Exchangers ESGR Chillers A/B/C Instrument Air Compressors Recirculation Spray Heat Exchangers RCP Thermal Barriers RHR Pumps and Heat Exchangers cooling for SGTR	Represented by the T6 Initiator.
Component Cooling Water	Manual Reactor Trip or Shutdown on loss of RCP cooling	RCP Thermal Barriers RHR Pumps and Heat Exchangers cooling for SGTR	Impact on RCP Thermal Barriers considered in the T4 Initiator.



TABLE 3.1.1-12 (Continued)  
SUMMARY OF LOSS OF SUPPORT SYSTEMS AS INITIATORS

<u>Support System Loss Considered</u>	<u>Impact on Normal Operation</u>	<u>Attendant Important System Failures</u>	<u>Initiating Event Group</u>
Emergency Switchgear Room Cooling	Manual Reactor Trip or Shutdown due to switchgear thermal overload	All AC ECCS switchgear in ESGR	Represented by the T8 Initiator.
Containment Instrument Air	Manual Reactor Trip or Shutdown on loss of RCP cooling	Pressurizer PORV (backup nitrogen supply) RCP Thermal Barriers	Impact on RCP Thermal Barriers considered in the T4 Initiator.
Instrument Air Outside Containment	Reactor Trip on loss of MFW or MS isolation	RCP Thermal Barriers RHR Pump and Heat Exchanger cooling for SGTR MS Condenser Dump Valves MS Atmospheric Dump Valves (backup air (supply)	Included within the T2 Initiator. Impact on RCP Thermal Barriers considered in the T4 Initiator.
Bearing Cooling Water	Reactor Trip on loss of MFW	MFW Pumps Condensate Pumps	Included within the T2 Initiator.



**TABLE 3.1.1-15  
TRANSIENT SUCCESS CRITERIA**

<u>Reactivity Control</u>	<u>Core Heat Removal</u> <u>Early</u> <u>Late</u>	<u>Secondary Heat Removal</u>	<u>RCS (Integrity)</u>	<u>Containment Condition</u>
RPS Scram with < 2 rod failure to insert <sup>a</sup>	RCS - Natural Circ.	1/3 MFW pumps <sup>b,f</sup> OR 1/3 AFW pumps to 1/3 SGs <sup>c</sup>	RCS PORV Closure Note 1	Not Required
RPS Scram	1/3 Charging Pumps AND 1 RCS PORV (Feed & Bleed) <sup>e</sup>	Recirc. through 1/3 charging pumps - AND 1/2 Lo Head SI Pumps <sup>d</sup> (Note 3)	Not Required  Note 2	Recirculation through 1/2 IRS OR 1/2 ORS <sup>e</sup>

**Notes:**

1. Failure of RCS Integrity by failure of RCS PORV to close transfers to S2 event tree.
2. Feed & Bleed operation fails RCS Integrity through continued RCS PORV use.
3. For Transients, RCS depressurization before recirculation is not certain, so only high head safety recirculation is modeled. Also, ORS can be manually aligned to act as a backup for Lo Head Recirc for NAPS Unit 1.

**References:**

- |                      |                                 |
|----------------------|---------------------------------|
| a. WCAP-9691 p. A-11 | d. WCAP-9744                    |
| b. WCAP-9691 p. A-12 | e. Surry Analysis File 321MAF.1 |
| c. WCAP-9691 p. A-15 | f. NAPS UFSAR                   |



**TABLE 3.1.2-1 (Continued)**  
**LIST OF INITIATING EVENT CLASSES**

<u>INITIATING EVENT GROUP</u>	<u>DESCRIPTIONS</u>	<u>EVENT TREE</u>
A	Large LOCA 6" - 20"	A
S1	Medium LOCA 2" - 6"	S1
S2	Small LOCA 3/8" - 2"	S2
V	Interfacing System LOCA	Vx
R	Reactor Vessel Rupture	Rx
TL	Transient with failure to Scram at Power < 40 percent	TL
TH	Transient with failure to Scram at Power > 40 percent	TH

\* These event trees are discussed in one section of the report, as they are very similar.

\*\* T1A is not a true initiating event, but is a consequential event from T1.



**TABLE 3.1.2-2**  
**EVENT TREE HEADINGS**

<u>Abbreviation</u>	<u>Headings</u>	<u>Description of Event</u>
A	Large LOCA	Initiating Event-large LOCA
B	Offsite Power Recovery	Failure to recover an ESF bus following station black-out by recovering offsite power.
Ch	Containment Heat Removal	Failure of Service Water to an operable Recirculation Spray heat exchanger.
DG	EDG 1H or 1J Available	Failure of at least one diesel generator to start and run following loss of offsite power leading to station blackout.
Dh	Hot Leg Recirculation	Failure of the operator to switch to hot leg recirculation following a large LOCA.
D1	High Pressure Injection	Failure of Charging Pumps to inject in the appropriate mode.
D2	Accumulators Inject	Failure of Accumulators to inject in the appropriate mode.
D3	Low Head SI	Failure of low head SI pumps to inject.
D4	Emergency Boration	Failure to shutdown following ATWS by boron addition.
Fm	Break Size Partition	Percentage of small breaks not causing a CDA Hi Hi signal.
Hv	ESGR Cooling	Failure to provide HVAC to the ESGR using 1/2 AHUs and 1/3 chillers.
H1	Low Head Recirculation	Failure of low head pumps in the recirculation mode.



**TABLE 3.1.2-2 (Continued)**  
**EVENT TREE HEADINGS**

<u>Abbreviation</u>	<u>Headings</u>	<u>Description of Event</u>
H2	High Head Recirculation	Failure of low head and charging pumps in the high pressure recirculation mode.
K	Reactor Subcritical	Failure of control rods to insert as result of Reactor Protection System failure.
L	Auxiliary Feedwater System Available	Failure of Auxiliary Feedwater System for transients or small or medium LOCAs with reactor trip.
Lt	Turbine-Driven AFW available	Failure of the Turbine-Driven Auxiliary Feedwater Pump to start and run following station blackout.
M	Main Feedwater System Available	Failure of Main Feedwater.
MS1	Manual Scram	Failure of the operator to remove power from the control rod drive mechanisms.
O	Cooldown and Depressurize	Operator fails to cooldown and depressurize the reactor after a small break or in response to a loss of RCP seal cooling.
O2	Late Cooldown	Failure of operator to cooldown and depressurize in response to a ruptured steam generator.
P	Pressurizer PORVs	Failure of the operator to open 1/2 pressurizer PORVs to cause RCS feed and bleed.
Pr	Pressure Relief	Failure of adequate pressure relief following an ATWS event.



**TABLE 3.1.2-2 (Continued)**  
**EVENT TREE HEADINGS**

<u>Abbreviation</u>	<u>Headings</u>	<u>Description of Event</u>
Q	RCS Boundary Intact	Failure of pressurizer PORV to close after opening during a transient.
Qs	Quench Spray	Failure of 1/2 trains of Quench Spray.
Rc	Room Cooling Restored	Recovery of ESGR cooling or SW (resulting in reactor trip and loss of emergency power) prior to core uncover and vessel failure, or containment failure.
Rs	Recirculation Sprays Operable	Failure of at least one train of Recirculation Sprays to remove heat from Containment.
Rv	Reactor Vessel Integrity	Consideration of PTS following a rapid RCS cooldown.
RX	Reactor Vessel Rupture	Initiating event is a Reactor Vessel rupture.
SGI	Steam Generator Isolation	Failure to isolate the ruptured Steam Generator.
Slc	No Potential for RCP Seal Failure	Failure to establish seal cooling from operable Unit 2 CC pumps.
S1	Medium LOCA	Initiating event is a medium LOCA (2" to 6").
S2	Small LOCA	Initiating event is a small LOCA (3/8" to 2").
T	Transients	Representative initiating event for general transient event tree.
Tt	Turbine Trip	Turbine fails to trip.



**TABLE 3.1.2-2 (Continued)**  
**EVENT TREE HEADINGS**

<u>Abbreviation</u>	<u>Headings</u>	<u>Description of Event</u>
T1	Loss of Offsite Power	Initiating event is Loss of of all Offsite Power.
T1A	Station Blackout	Loss of diesel generators 1H and 1J leading to station blackout at Unit 1.
T1Tr	Loss of ESGR Cooling Transfer from T1 Event Tree	Transfer of T1Hv sequence, Loss of Offsite Power with consequential loss of Emergency Switchgear Room Cooling.
T2	Loss of MFW	Initiating event is non-recoverable loss of Main Feedwater.
T2A	Recoverable Loss of MFW	Initiating event is recoverable loss of Main Feedwater following Feedwater isolation.
T2ATr	Loss of ESGR Cooling Transfer from T2A Event Tree	Transfer of T2AHv sequence, recoverable loss of Main Feedwater with coincidental loss of Emergency Switchgear Room Cooling.
T2Tr	Loss of ESGR Cooling Transfer from T2 Event Tree	Transfer of T2Hv sequence, non-recoverable loss of Main Feedwater with coincidental loss of Emergency Switchgear Room Cooling.
T3	Transient with MFW Available	Initiating event is Transient with Main Feedwater available.
T3Tr	Loss of ESGR Cooling Transfer from T3 Event Tree	Transfer of T3Hv sequence, transient with Main Feedwater available, with coincidental loss of Emergency Switchgear Room Cooling.
T4	Loss of RC Pump Seal Cooling	Initiating event is loss of RCP seal injection and thermal barrier cooling.



**TABLE 3.1.2-2 (Continued)**  
**EVENT TREE HEADINGS**

<u>Abbreviation</u>	<u>Headings</u>	<u>Description of Event</u>
T5A	Loss of DC Bus I	Initiating event is loss of DC Bus 1-I.
T5B	Loss of DC Bus III	Initiating event is loss of DC Bus 1-III.
T6	Loss of Service Water	Service Water is lost from both the reservoir and Lake Anna.
T7	Steam Generator Tube Rupture	Initiating event is a steam generator tube rupture.
T8	Loss of Emergency Switch- gear Room Cooling	Loss of HVAC to the Emergency Switchgear Room.
T9A	Loss of Power from 4160 V Emergency Bus 1H	Loss of feeder power to or failure of 4160 V emergency bus 1H.
T9ATr	Loss of ESGR Cooling Transfer from T9A Event Tree	Transfer of T9AHv sequence, loss of feeder power to or failure of 4160 V Emergency Bus 1H, with consequential loss of Emergency Switchgear Room Cooling.
T9B	Loss of Power from 4160 V Emergency Bus 1J	Loss of feeder power to or failure of 4160V emergency bus 1J.
T9BTr	Loss of ESGR Cooling Transfer from T9B Event Tree	Transfer of T9BHV sequence, loss of feeder power to or failure of 4160 V Emergency Bus 1J, with consequential loss of Emergency Switchgear Room Cooling.
TL	Low power transients (for ATWS)	Initiating event is all transients at power lower than or equal to 40 percent.
TH	High power transients (for ATWS)	Initiating event is all transients at power greater than or equal to 40 percent.



**TABLE 3.1.2-2 (Continued)**  
**EVENT TREE HEADINGS**

<u>Abbreviation</u>	<u>Headings</u>	<u>Description of Event</u>
VX	Interfacing System LOCA	Initiating event is an Inter- facing System LOCA.
Vi	Isolation of LOCA	Failure to isolate interfacing LOCA.
W	RHR Cooling	Failure of 1/2 Residual Heat Removal Trains.
Y	Core Cooling Recovery	Failure of the operator to use steam to rapidly cooldown and depressurize the RCS as directed by 1-FR-C.1 or C.2.



**TABLE 3.3.1-1**  
**DEFINITION OF PROBABILITY MODELS AND THEIR PARAMETERS**

<u>Basic Event</u>	<u>Probability Models</u>	<u>Data Required</u>
Initiating Event	Poisson Model  $P(r) = \frac{(ft)^r e^{-ft}}{r!}$ <p>f: frequency</p>	Number of events r in time t
Standby component fails on demand	1) Constant probability failure on demand, or $U = \frac{n}{N}$	1) Number of events n in total number of demands N
Standby component fails in time, or component changes state between tests (faults revealed on functional test only)	2) Constant standby failure rate  $U = 1 - \frac{1 - e^{-\lambda_s T_1}}{\lambda_s T_1}$ <p><math>T_1</math> : Time between tests  <math>\lambda_s</math>: Standby failure rate</p>	2) Number of events n in total time in standby $T_s$
Component in operation fails to run, or component changes state during mission (state of component continuously monitored)	Constant failure rate $U = 1 - \exp(-\lambda_o T_m) \approx \lambda_o T_m$ <p><math>T_m</math>: Mission time  <math>\lambda_o</math>: Operating failure rate</p>	Number of events n in total exposure time $T_e$ (Time standby component is operating, or time the component is on line)



# MODULE F

## SYSTEMS ANALYSIS USING FAULT TREES

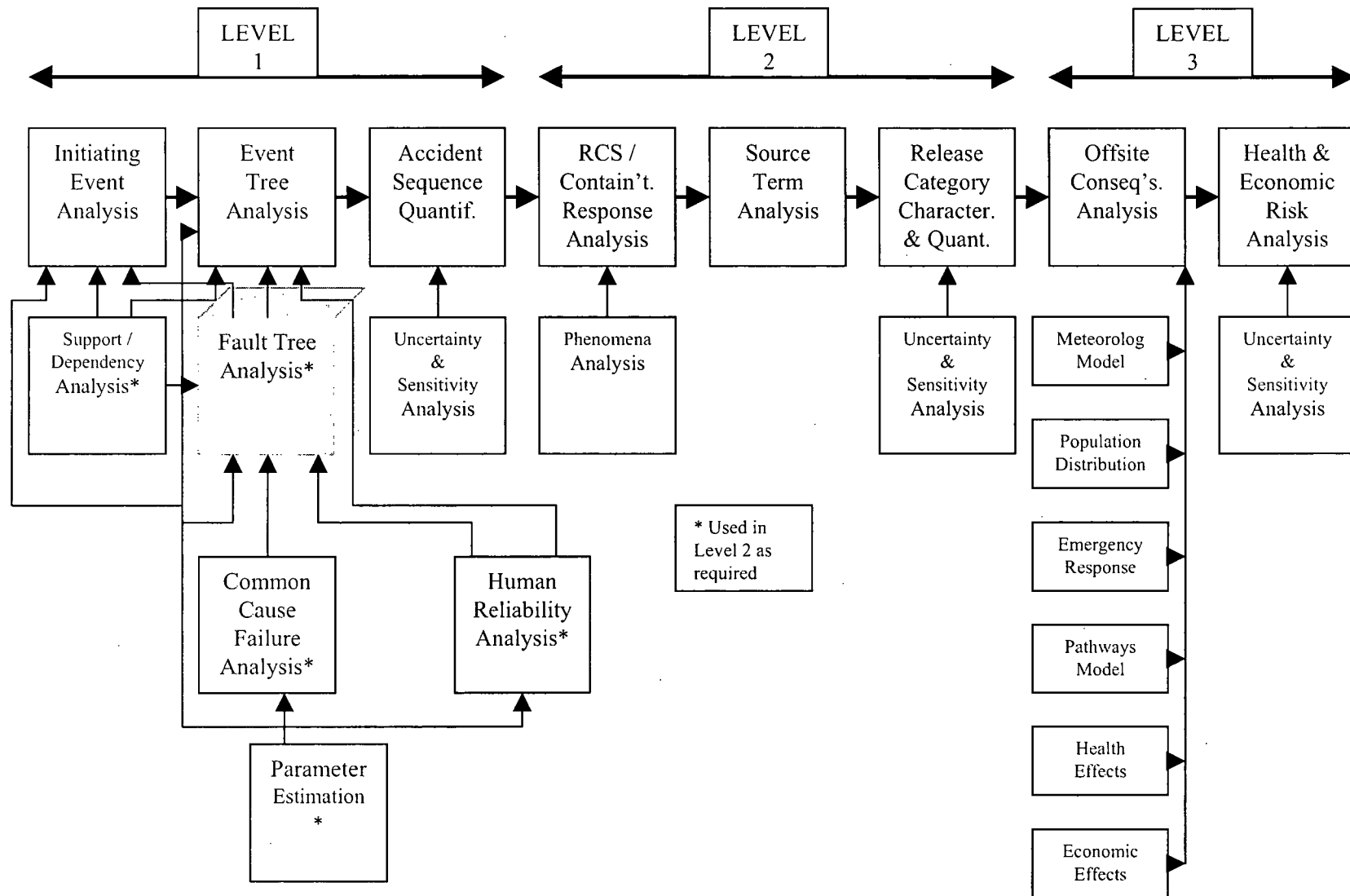


# Fault Tree Concepts

- Purpose: Students will learn the purposes of fault tree analysis. Students will learn how the appropriate level of detail for a fault tree analysis is established. Students will become familiar with the terminology, notation, and symbology employed in fault tree analysis.
- Objectives:
  - List the purposes of fault tree analysis.
  - Define the terminology, notation, and symbology used in fault tree analysis.
  - Interpret the results of fault tree reduction
  - Define and correctly apply the definition of “minimal cut sets”
- References: NUREG-0492, NUREG/CR-2300, NUREG-1489



# Principal Steps in PRA





# Fault Tree Analysis Definition

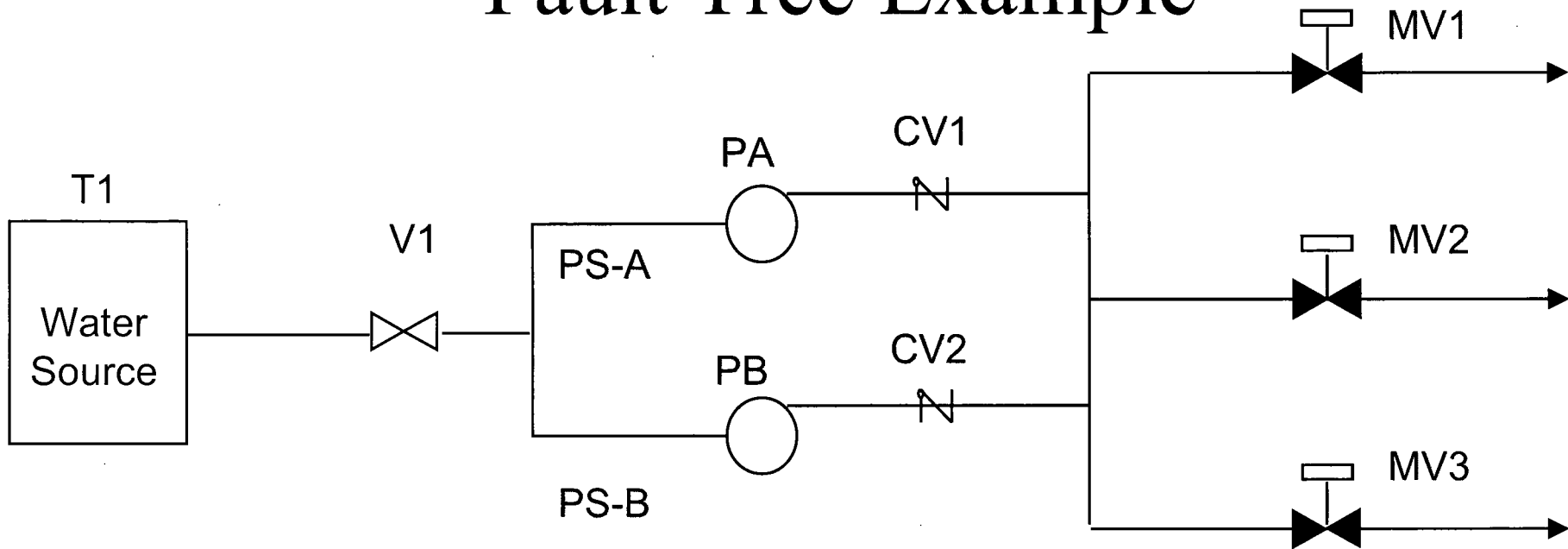
*“An analytical technique, whereby an **undesired state** of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed **in the context of its environment and operation** to find all **credible** ways in which the undesired event can occur.”*

NUREG-0492



# Emergency Cooling Injection System

## Fault Tree Example



*Flow from any one pump through any one MV is success*

*T\_ tank*

*V\_ manual valve, normally open*

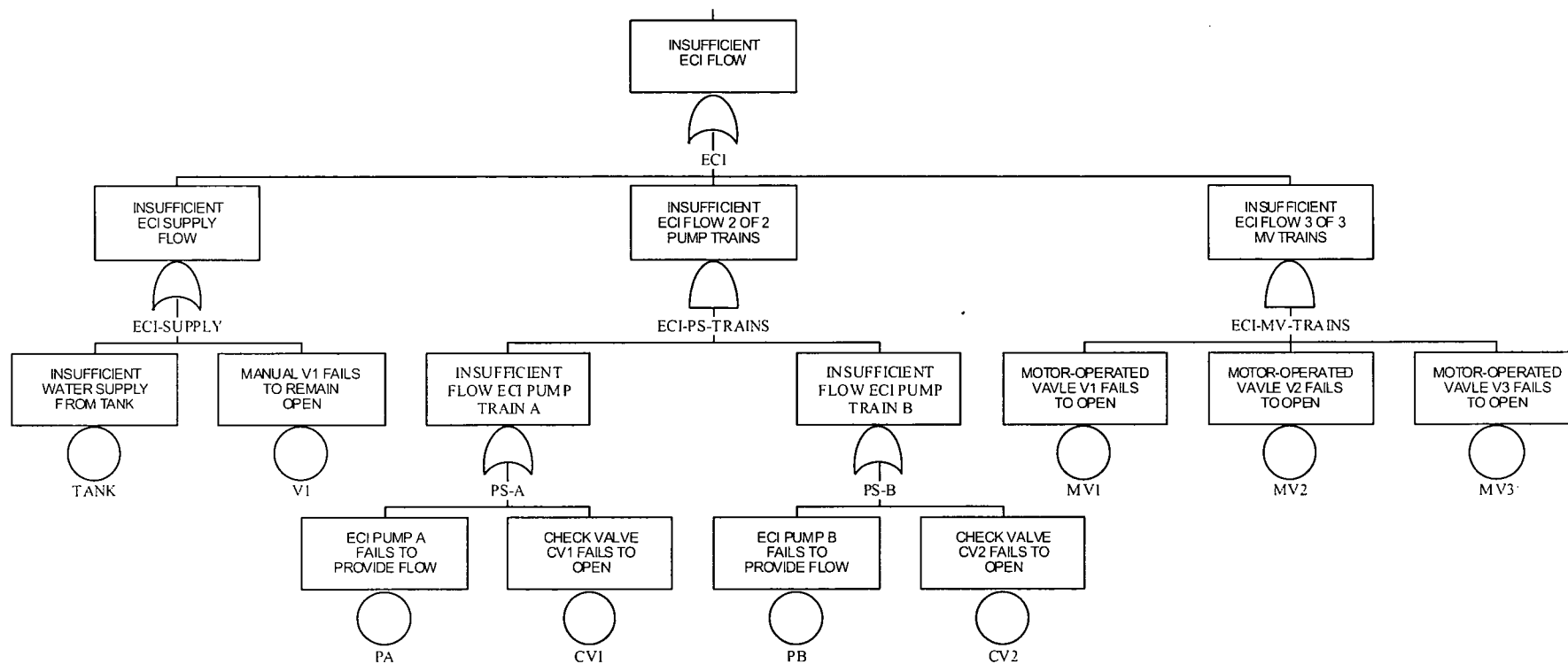
*PS\_ pipe segment*

*P\_ pump*

*CV\_ check valve*

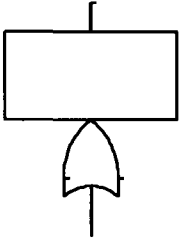
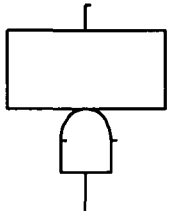
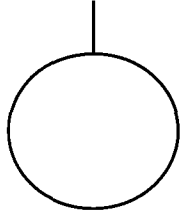
*MV\_ motor-operated valve, normally closed*





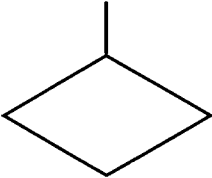
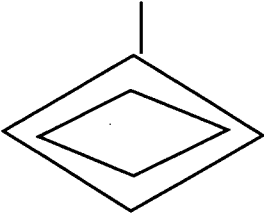
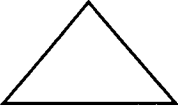
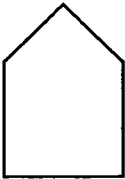


# Fault Tree Symbols

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



# Fault Tree Symbols (cont.)

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



# Relationship Between Fault Trees and Event Trees

- As discussed in Module E, event trees consist of a series of nodes. Each node represents the success or failure of a particular system, component, or operation.
- For complex systems, fault tree models are used to model system failure and estimate the system's probability of failure.
- Therefore, the top event of a fault tree corresponds to the failure branch of its associated event tree node.



# Fault Trees

- Deductive analysis (event trees are inductive)
- Top down approach starting with undesired event (top event) definition
- Explicitly models multiple failures
- Provides event relationships (i.e., combinations of events leading to undesired event)
- Used to estimate top event unreliability (i.e., probability top event fails to perform intended function)

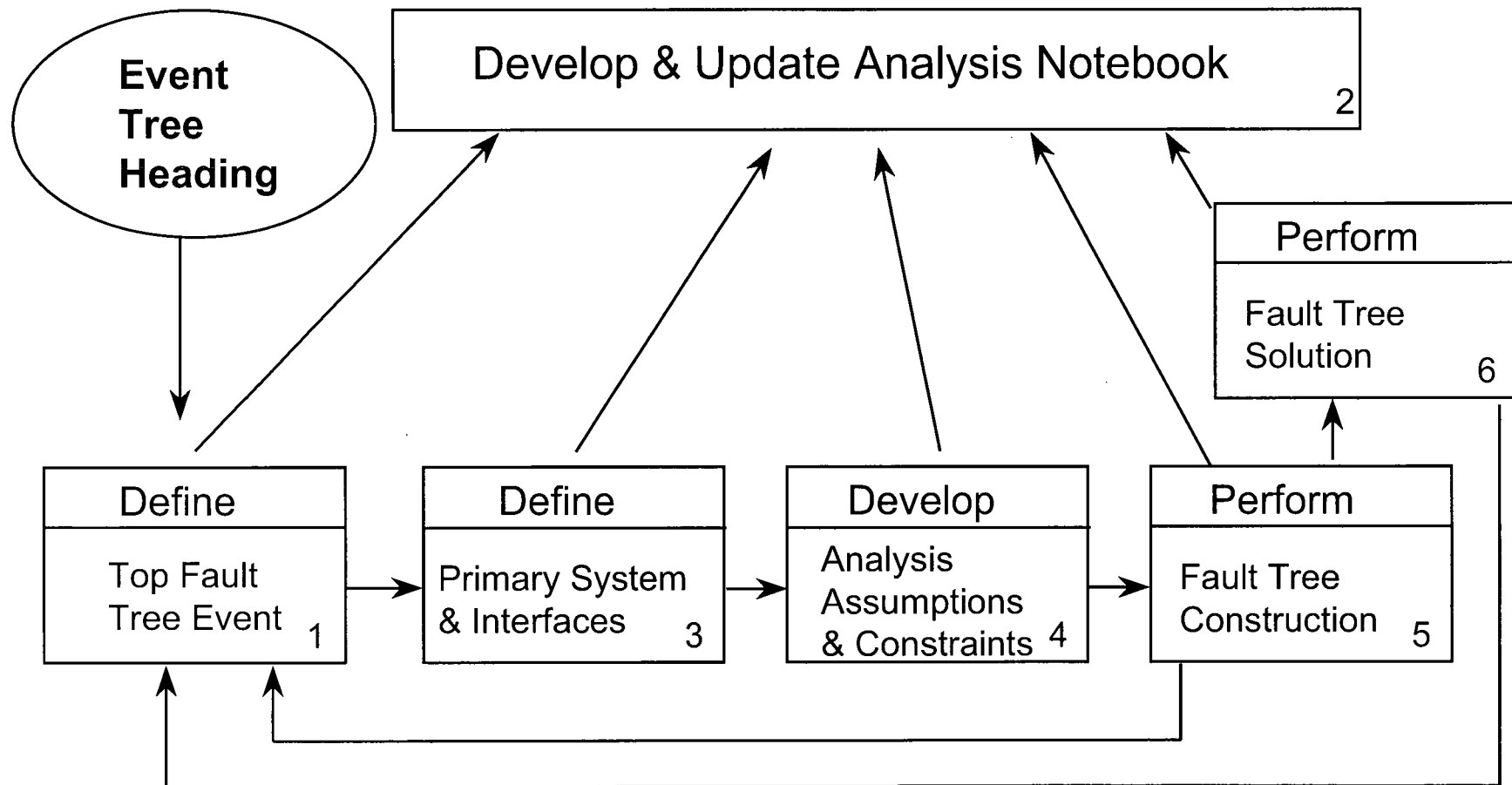


# Purpose of Fault Tree Analysis

- Fault trees can be used to identify the ways in which a system, component, function, or operation can fail.
- Fault tree models can be used to determine:
  - Interrelationships between fault events, failure combinations producing undesired event
  - System “weaknesses”
    - Qualitative
    - Quantitative
  - System unreliability (system failure probability)



# Fault Tree Development and Analysis Process





# 1. Define Top Event

- Undesired event or state of system
  - Often corresponds to an event on an event tree
  - Based on success criterion for system
    - Typically initiating event dependent (e.g., HPI would have different success criteria for small LOCA vs. medium LOCA)
    - Success criteria determined from thermal/hydraulic calculations (i.e., computer code runs made to determine how much injection is needed to keep core covered given particular IE)
  - Success criterion used to determine failure criterion
    - Fault tree top event
  - Will often have multiple versions of system failure fault tree
    - For different IEs



## 2. Develop and Update System Notebooks

- Fault tree development is an iterative process, that is related to the other PRA processes. A system notebook should be started at the onset of fault tree development; it should be maintained and updated periodically.
  - A system notebook should contain the following:
    - scope of analysis,
    - system definition and boundaries,
    - system design information,
    - the drawings or diagrams used for model development,
    - system operational information,
    - applicable Technical Specifications,
    - test and maintenance information and data,
    - analytical assumptions,
    - component failure rate data, and
    - fault tree results.
  - System notebooks were typically developed during the IPE process. Although the system notebooks are not generally included in the IPE submittal, the system notebooks should be available for review by the inspectors.



### 3. Define the System and Interfaces

- Define system/component boundaries based on:
  - the information required from the analysis and
  - the basic event level (i.e., the level of resolution of available data)
  - function of the system being modeled
  - Note: boundaries may not be consistent with those used in the plant
- Identify shared components with other systems.
- Identify dependencies on other systems.



## 4. Develop Analysis Assumptions and Constraints

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



## 5. Fault Tree Construction

- Fault tree construction requires the step-by-step postulation of system faults, starting at the top event and working down to the basic events whose failures contribute to the top event failure.
- A standardized symbology is employed.
- Postulation should be consistent with the level of resolution in the available data and the analytical assumptions.
- Fault tree construction is an iterative process requiring constant feedback from the other PRA processes as well as the other steps in the fault tree development process.



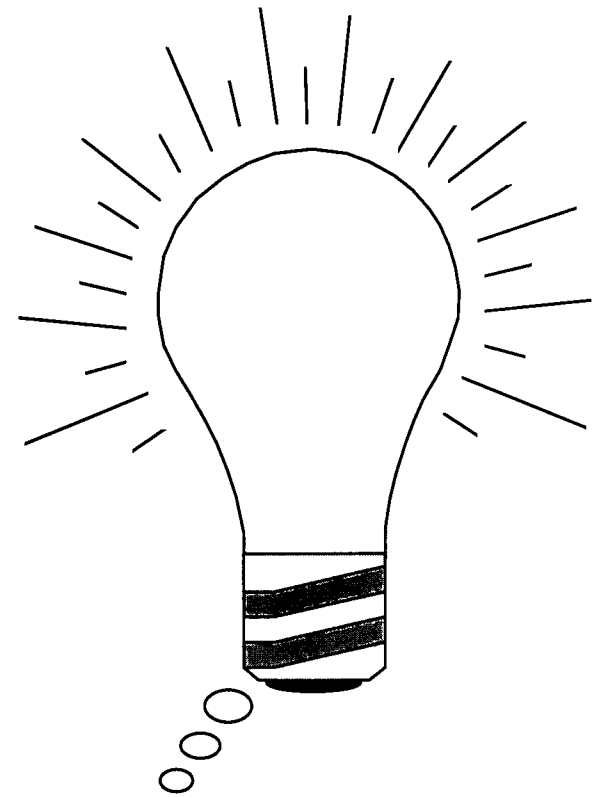
## 6. Fault Tree Solution

- Due to the complexity of most fault trees, computers are used to generate results. This produces a list of the various combinations of basic event failures that cause the top event to occur.
- Fault tree results - the list of various combinations are called Minimal Cut Sets.
- Solution relies on “laws” of Boolean algebra.
- Because typical models are very large, solution most often approximated by performing minimal cut set truncation.



# Minimal Cut Set

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



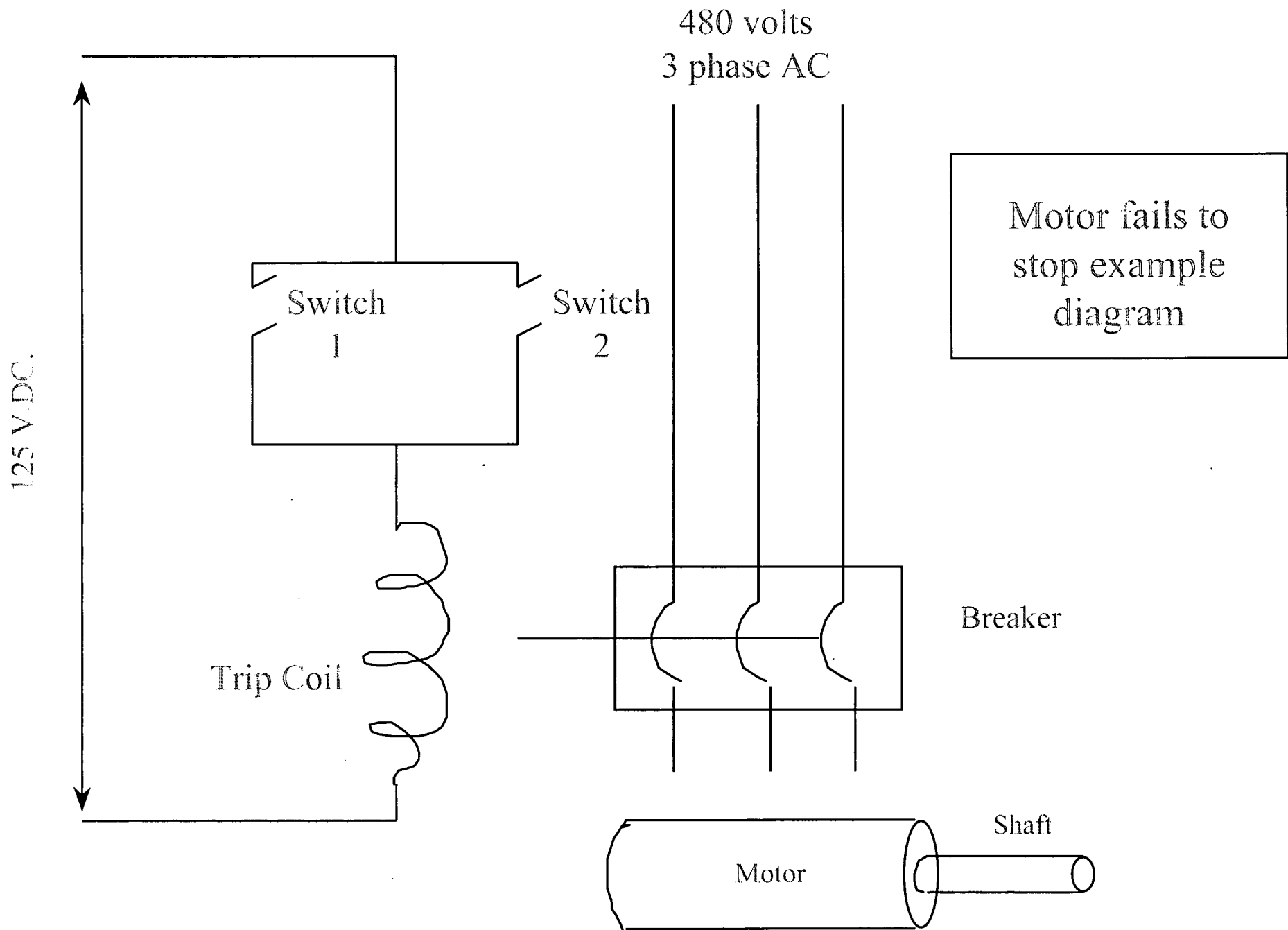
Understanding the concept of minimal cut sets is one of the most important steps in understanding PRA



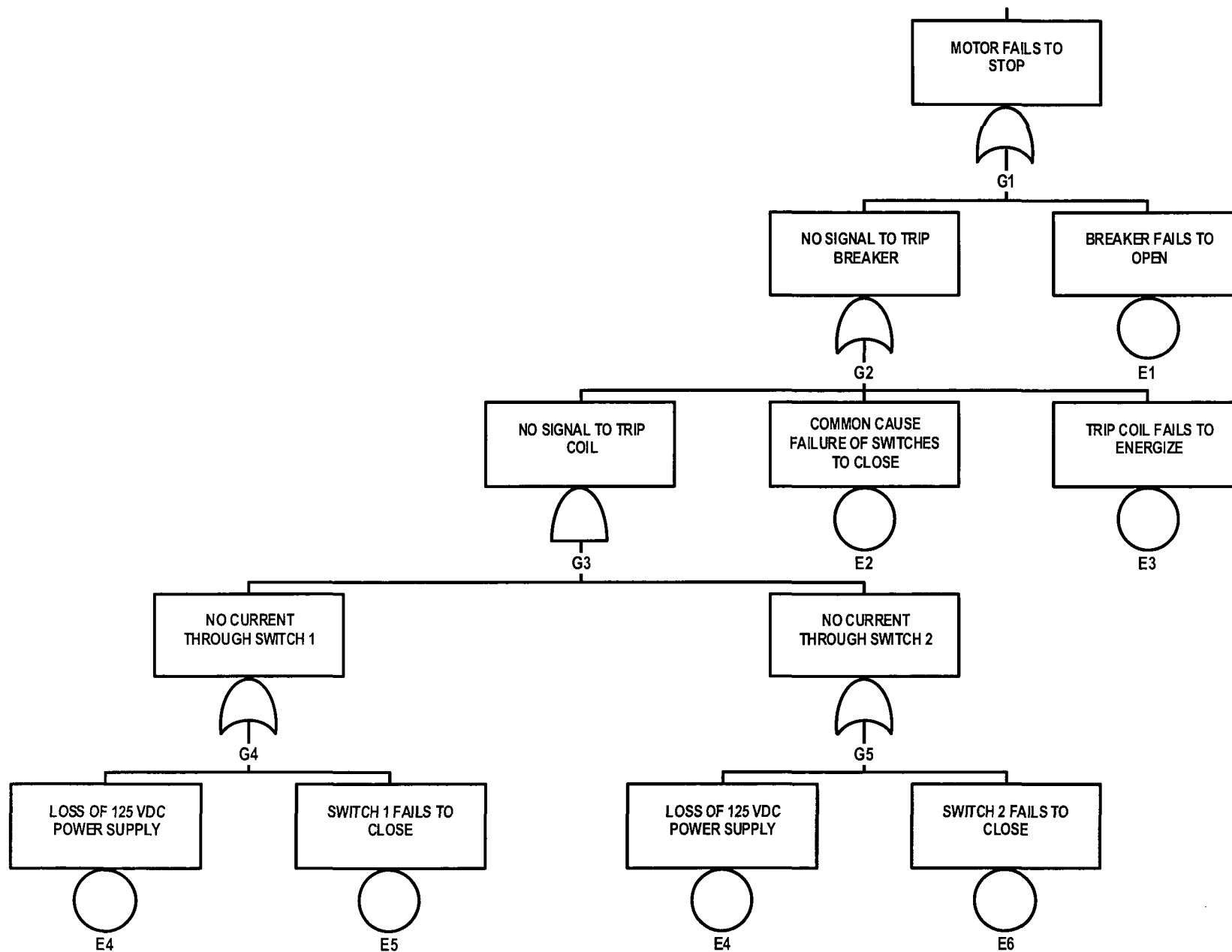
# Demonstration of the Fault Tree Construction & Solution Process

- Build fault tree for the schematic provided
- Some assumptions:
  - Ignore wire faults
  - Do not model details of 125 V DC power supply
- Will solve fault tree and discuss “meaning” of the solution process











# Boolean Fault Tree Reduction

- First, express a fault tree's logic as a Boolean Equation.
- Then, apply the rules of Boolean Algebra to reduce the terms.
- This results in a reduced form of the Boolean Equation, which can be used to quantify the fault tree in terms of its minimal cut sets.
- Boolean reduction is typically done automatically by the fault tree software during the quantification process.



# Fault Tree Results

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



# Rules of Boolean Algebra

Mathematical Symbolism	Engineering Symbolism	Designation
(1a) $X \cap Y = Y \cap X$ (1b) $X \cup Y = Y \cup X$	$X * Y = Y * X$ $X + Y = Y + X$	Commutative Law
(2a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ (2b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X * (Y * Z) = (X * Y) * Z$ $X + (Y + Z) = (X + Y) + Z$	Associative Law
(3a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ (3b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X * (Y + Z) = (X * Y) + (X * Z)$ $X + (Y * Z) = (X + Y) * (X + Z)$	Distributive Law
(4a) $X \cap X = X$ (4b) $X \cup X = X$	$X * X = X$ $X + X = X$	Idempotent Law
(5a) $X \cap (X \cup Y) = X$ (5b) $X \cup (X \cap Y) = X$	$X * (X + Y) = X$ $X + (X * Y) = X$	Law of Absorption



# Reduction of Example Fault Tree

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

$$G1 = G2 + E1$$

$$G2 = E2 + G3 + E3$$

$$G3 = G4 * G5$$

$$G4 = E4 + E5$$

$$G5 = E4 + E6$$

- Back-substitute

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

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

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



## Reduction of Example Fault Tree (cont.)

- Expand parentheses

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

- Reduce terms using rules of Boolean algebra

Idempotent Law applies to  $E4 * E4 = E4$

Law of Absorption applies to  $E4 + (E4 * \text{"Y"}) = E4$

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

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

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

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

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

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

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

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

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



## \*\*\*\* Fault Tree Exercise \*\*\*\*

- Using the AFW fault tree from North Anna IPE (provided in Volume 2 of course material), identify various fault tree elements;
  - top event,
  - the various types of logic gates and gate names,
  - the use of house events,
  - transfers (including transfers to support systems),
  - undeveloped events, and
  - basic events and basic event names, noting examples of human error and common cause failure.
- Review your IPE for fault tree models and note the various fault tree elements.



# MODULE G

## EQUIPMENT FAILURE MODES AND DATA SOURCES FOR PARAMETER ESTIMATION

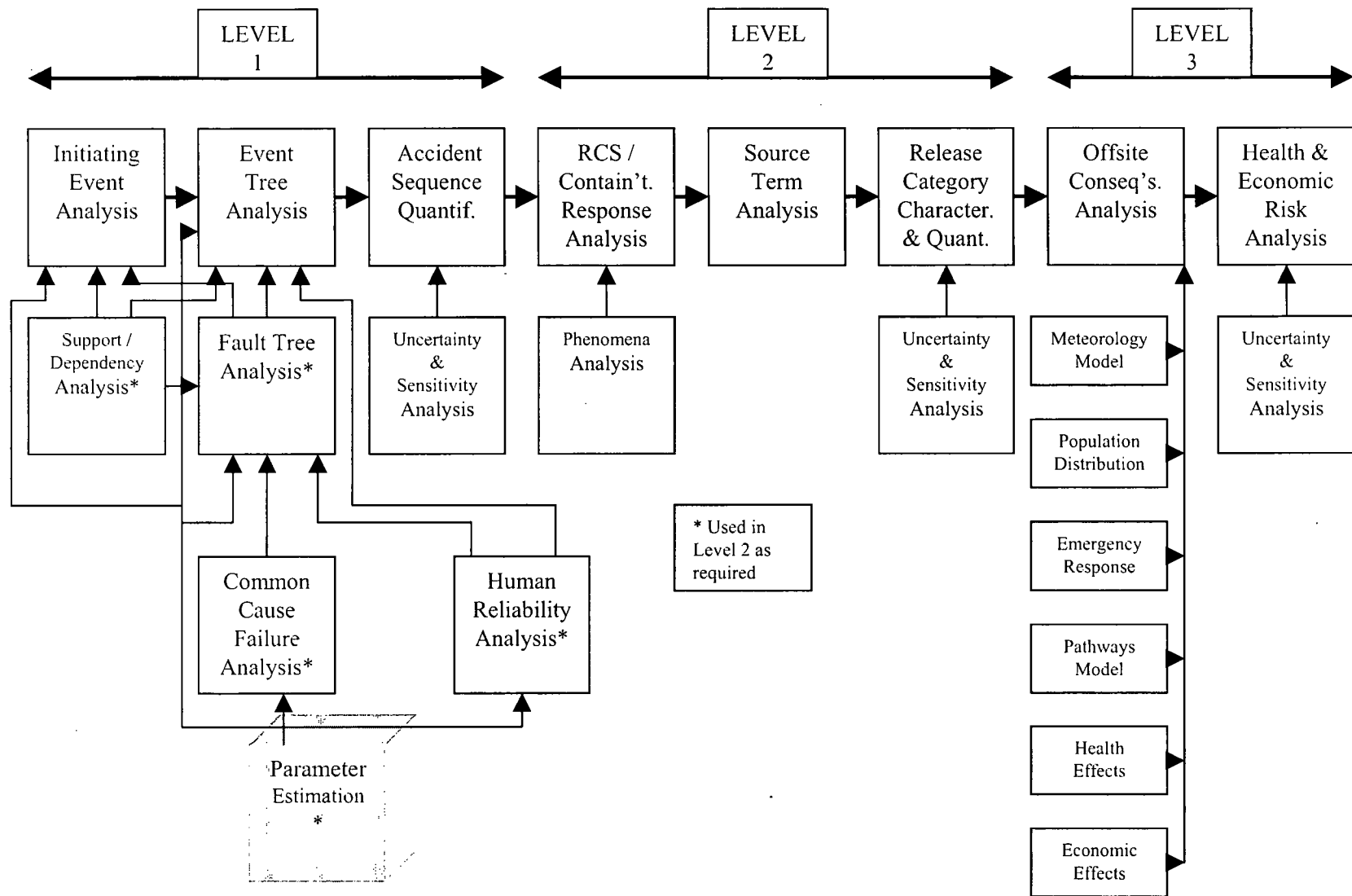


# Equipment Failure Modes and Data Source for Parameter Estimation

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



# Principal Steps in PRA





# Parameter Estimation

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

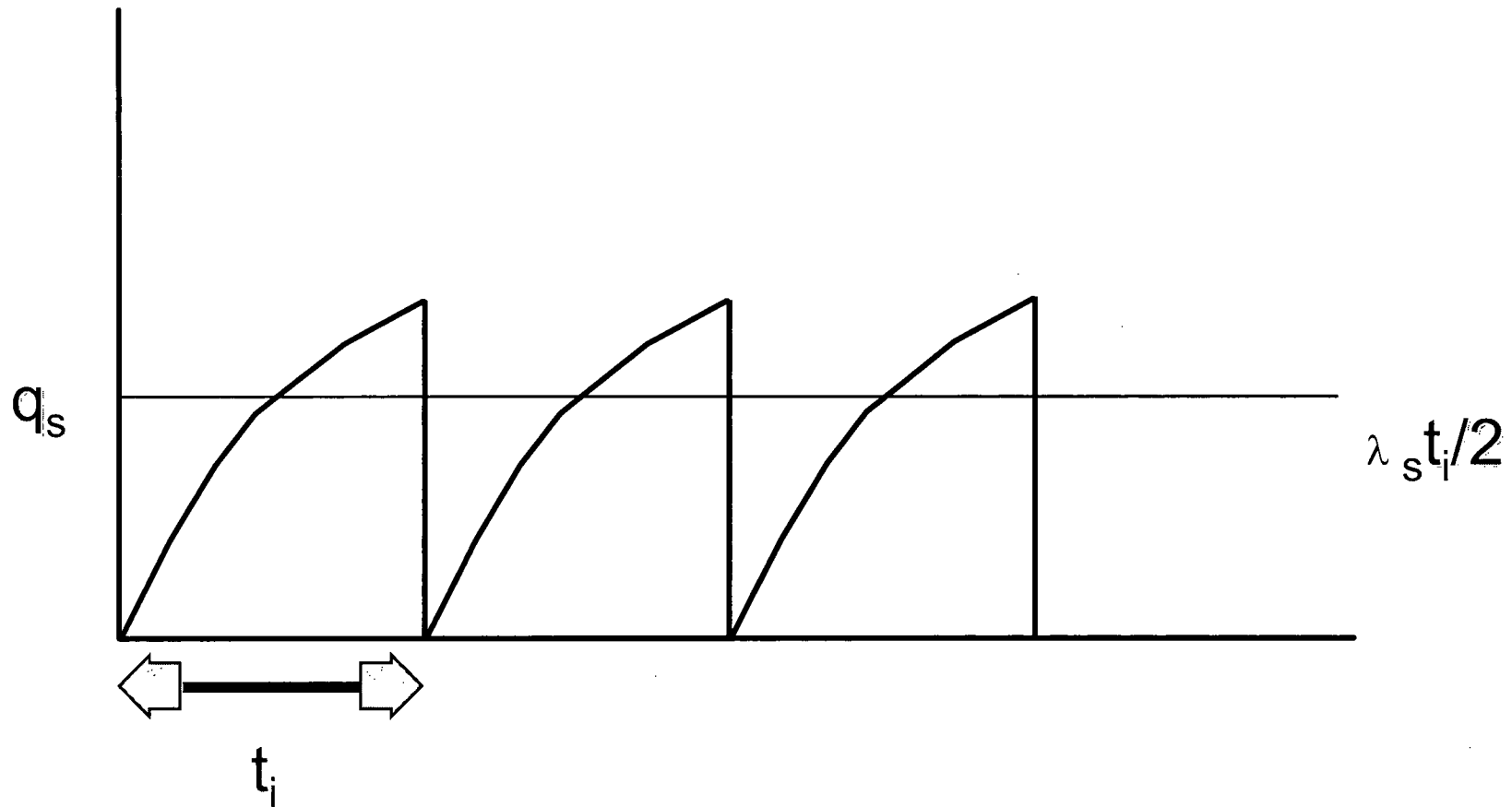


# System Models Need Following Types of Component Parameter Estimates

<b><u>Failure Contribution</u></b>	<b><u>Type of Measure</u></b>	<b><u>Calculational Formula</u></b>	<b><u>Parameter Definition</u></b>
Hardware Failure on Demand	Demand failure probability	$q_d = p$	$p$ = Demand failure probability; need number of failures and number of demands
Hardware Failure of Operating Component	Unreliability (mission failure)	$q_r = 1 - e^{-\lambda_o t_m}$ $q_r \approx \lambda_o t_m$ (for small $\lambda t$ ; when $\lambda t < 0.1$ )	$\lambda_o$ = Operating failure rate; need number of failures and total operating time $t_m$ = Mission time
Test/Maintenance Outage	Unavailability (Average)	$q_m = f_m J_m$	$f_m$ = Frequency of test or maintenance $J_m$ = Test or maintenance outage time
Hardware Failure while in standby of Standby Component	Standby failure probability Unavailability (Average)	$q_s \approx 1/2 \lambda_s t_i$	$\lambda_s$ = Standby failure rate; need number of failures and total time in standby $t_i$ = Test interval



On the average, standby equipment can be unavailable for 1/2 the test interval





## \*\*\*\*Parameter Estimation Exercise\*\*\*\*

Over five years, a standby component has the following operating history:

- 60 test/maintenance outages (test interval is 720 hours and each outage has a demand) and 4 unplanned demands
- Failures: 1 demand failure, 1 failure in standby (failure uncovered during testing), and 1 failure to run
- Total run time is 200 hours
- Average test/maintenance outage time is 1.8 hours

From this history, estimate:

- Demand failure probability
- Standby failure rate and standby unavailability
- Operating failure rate and unreliability for a mission time of 12 hours
- Test/maintenance unavailability



# Data Collection and Analysis to Support Parameter Estimation

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



# Data Sources

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



# Generic Data Sources

- NUREG-1150 supporting documents (NUREG/CR-4550 series, pre-1987)
- WASH-1400 (pre-1975)
- IEEE Std. 500
- NUREG/CR-3862 for initiating events (pre-1986)
- NUREG/CR-5750 for initiating events (1987-1995)
- NUREG-1032 for loss of offsite power (pre-1988)
- NUREG/CR-5496 for loss of offsite power (1980-1996)
- Institute of Nuclear Power Operations Nuclear Plant Reliability Data System (NPRDS) – archival only (no longer maintained)
- Institute of Nuclear Power Operations Equipment Performance Information Exchange (EPIX) – replaced NPRDS



# Generic Data Issues

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



# Plant-Specific Data Collection and Analysis

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



# Plant-Specific Data Issues

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



# Bayes' Theorem is Basis for Bayesian Updating of Data

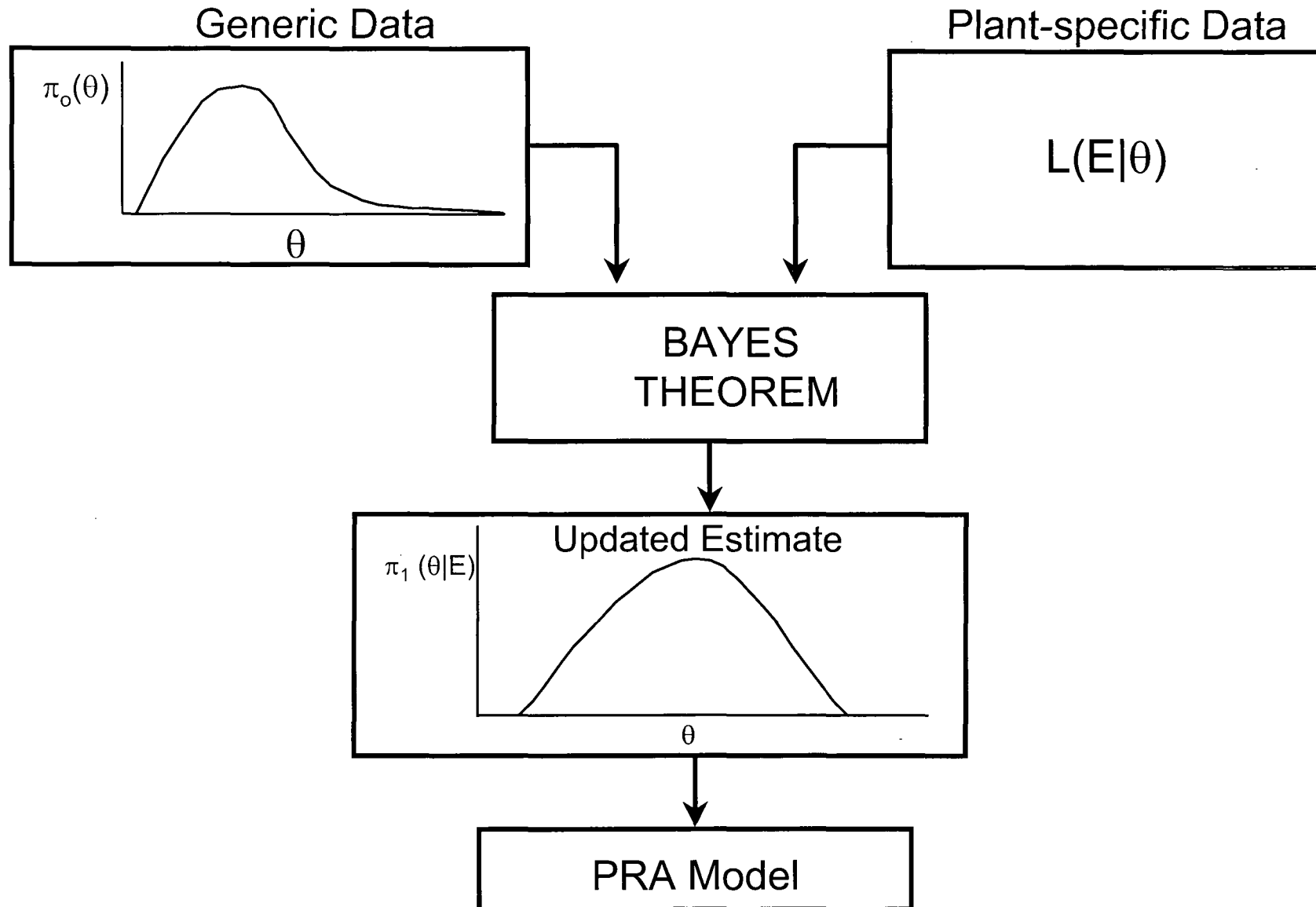
- Typical use: sparse plant-specific data combined with generic data using Bayes' Theorem:

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

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



# Bayesian Updating



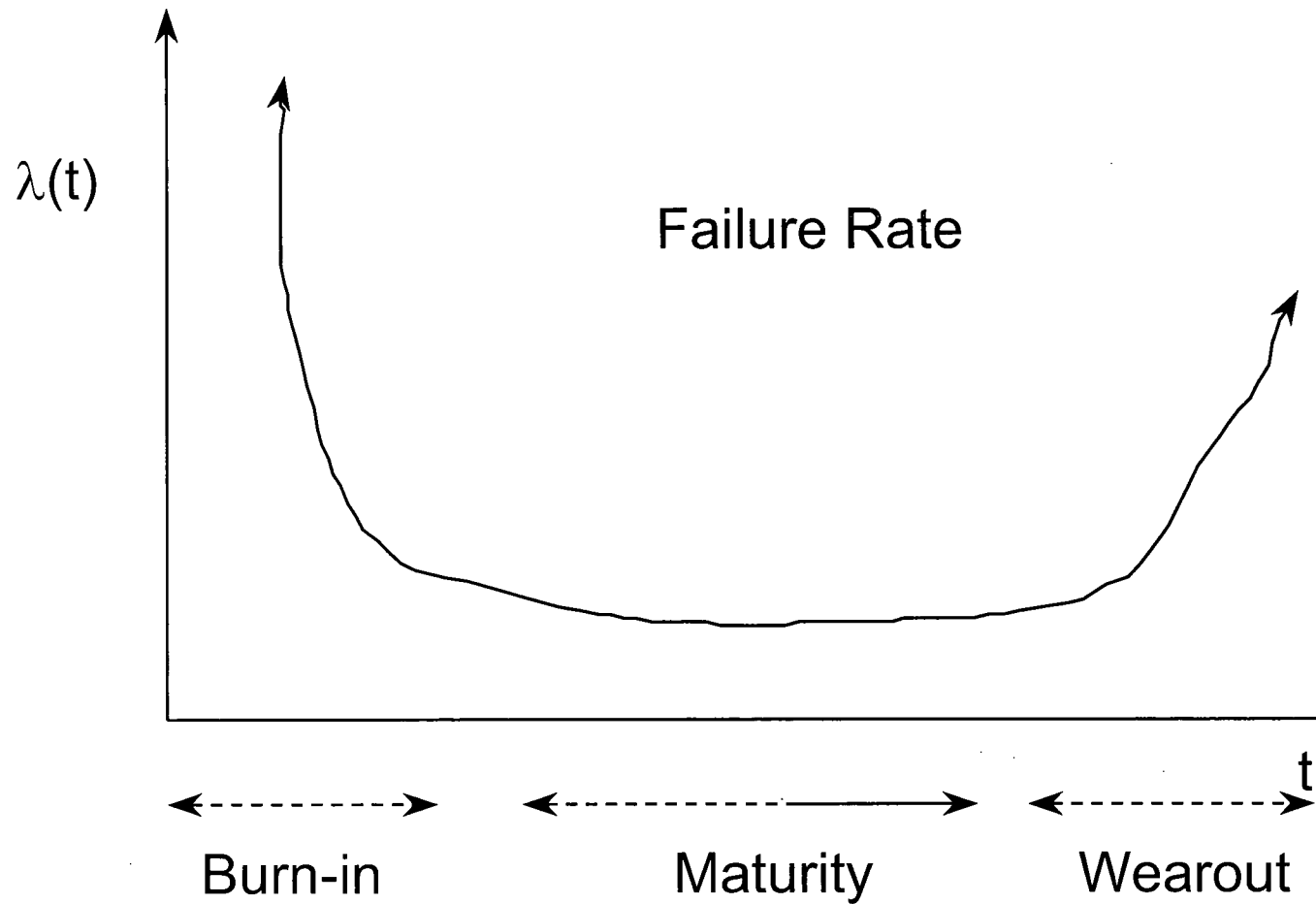


# Component Data Not Truly Time Independent

- 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 ( $\lambda$ ) =  $\lambda(t)$
  - “Bathtub” curve



# The “Bathtub” Curve





# The “Bathtub” Curve (cont.)

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



# Class Exercise on PRA Component Failure Data

- As a class - Based on experience, determine a consensus ranking of the following component failure modes (highest to lowest)
  - Diesel generator fails to start on demand
  - Check valve fails to open on demand
  - Motor-operated valve fails to open on demand
  - Motor-driven pump fails to start on demand
  - Turbine-driven pump fails to start on demand
- Individually - Based on typical values found in your IPE/PRA, how does the class qualitative ranking agree with the a quantitative ranking? Any comments on the PRA values?



# MODULE H

## COMMON CAUSE FAILURES

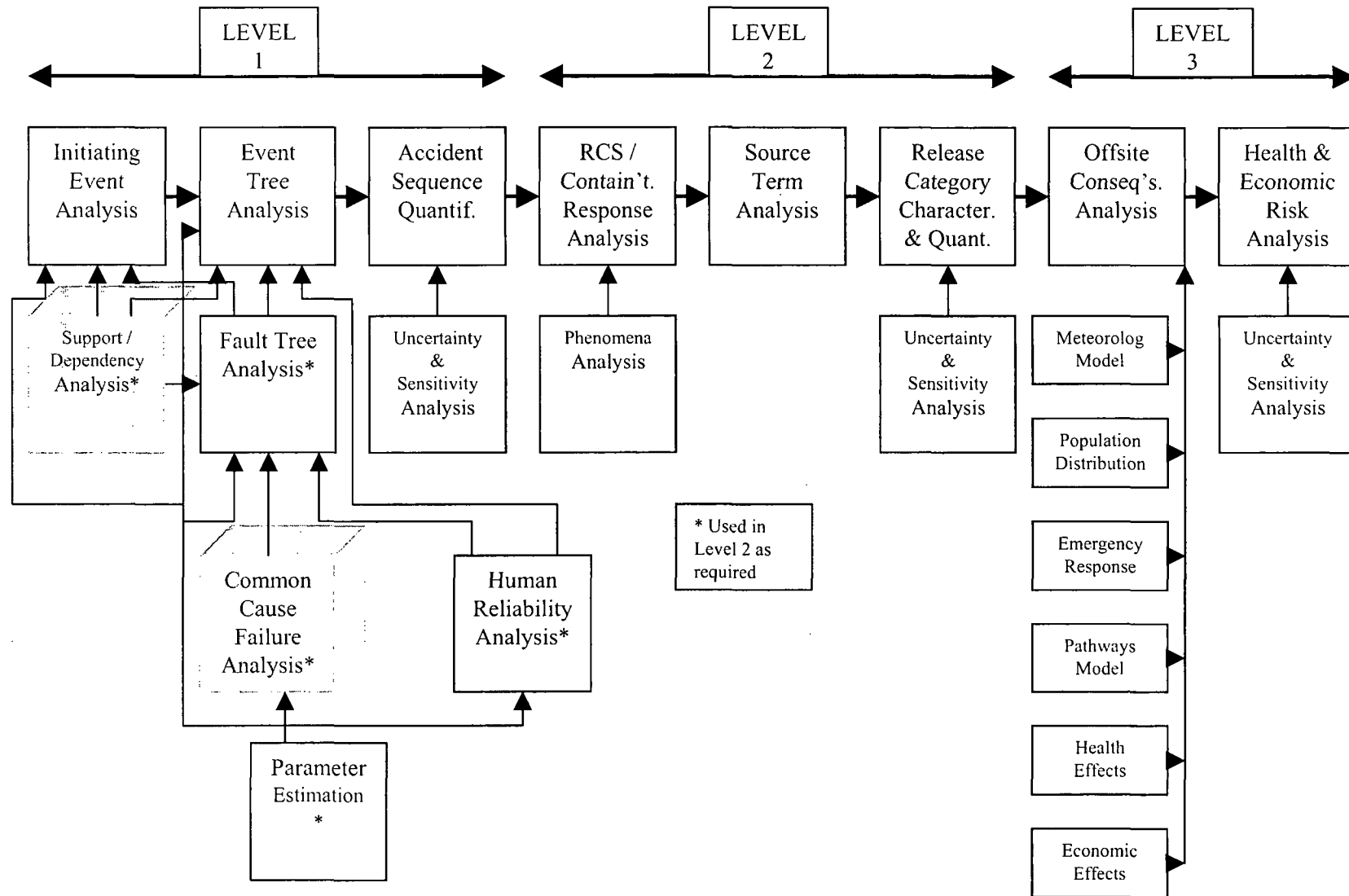


# Common Cause Failures

- Purpose: Students will be introduced to the concept of how common cause failures and other dependencies are treated in the PRA
- Objectives: Students will be able to:
  - Define several types of dependent failures and how they are modeled
  - Give examples of dependent and common cause failures
  - Describe the importance of modeling common cause failure in PRA
- References:
  - NUREG/CR-4780, Procedures for Treating CCF in Safety & Reliability Studies
  - EPRI NP-3967, Classification and Analysis of Reactor Operating Experience Involving Dependent Events
  - NUREG/CR-5485, Guidelines on Modeling Common-Cause Failures in PRA
  - NUREG/CR-5497, Common-Cause Failure Parameter Estimations
  - NUREG/CR-6268, Common-Cause Failure Database and Analysis System: Event Definition and Classification



# Principal Steps in PRA





# Definition of Dependent Failures

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



# Common Cause Failures

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



# Common Cause Failure Mechanisms

- Environment
  - Radioactivity
  - Temperature
  - Corrosion
- Design deficiency
- Manufacturing defect
- Test or Maintenance error
- Operational error



# Common Cause Modeling in PRA

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

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

- Multiple Greek Letter (MGL) model (expanded on beta-factor)
  - Alpha factor model (addressed uncertainty concerns in MGL)
- Apply to cut sets containing same failure mode for sample component type
  - Diesel generators
  - MOVs, AOVs, PORVs, SRVs
  - Pump
  - Batteries



# Beta Factor Example

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



## Current Limitations of CCF Modeling

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

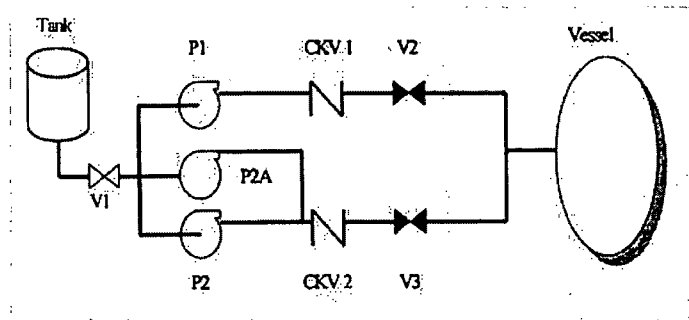


# Student Exercise

- Using the North Anna AFWS fault tree pages and schematic;
  - Identify the CCFs modeled by identifying all basic events with the following labels in the basic event names;
    - XXXXXX-LEAKAGE
    - XXXXXX-CC-XXXXXX
  - Postulate why (i.e., causes) such CCFs might exist.
  - Compare the CCF basic event failure probability with the corresponding component independent failure probability.



# Common Cause Student Exercise



- Injection system has a tank with a line through a normally open valve V1 to two pump trains. Pump train 1 has a pump P1, a check valve CKV1, and normally closed valve V2. Pump train 2 has two pumps P2 and P2A, CKV2, and normally closed valve V3. Both pump trains discharge to a common header to the reactor vessel.
  - Assuming the system is a standby injection system with 2 – 100 % including 3 - 100% pumps...
    - Which components and what corresponding hardware failure modes would you expect to be modeled in the PRA as Common Cause Failure (CCF) events?
    - If the CCF Beta-factor for valves failing to open is 0.05 and the valve failure-to-open probability is 0.005, what are the CCF and independent failure probabilities for the combined failure of V2 and V3 both failing to open?



# MODULE I

## HUMAN RELIABILITY ANALYSIS

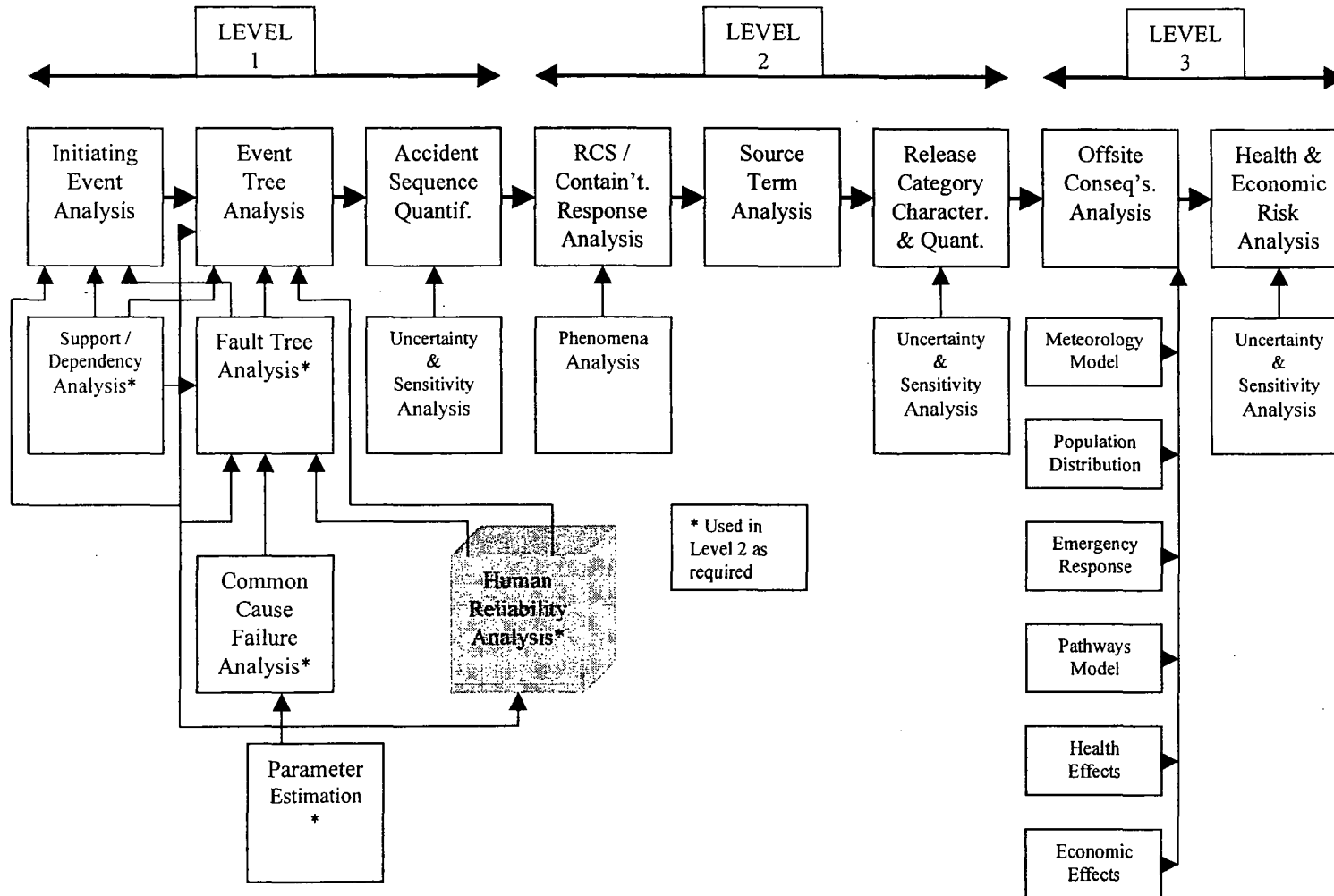


# Human Reliability Analysis

- Purpose: To expose the student to how human actions are treated in a PRA.
- Objectives - the student will be able to:
  - Explain the role of HRA within the overall context of PRA
  - Describe common error classification schemes used in HRA
  - Describe how human interactions are incorporated into system models
  - Identify strengths and limitations of HRA
- References:
  - NUREG/CR-1278, Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Application (“Swain & Guttman”)
  - Gertman, D.I. and Blackman, Harold S., Human Reliability & Safety Analysis Data Handbook (1994).
  - EPRI-NP-3583, Systematic Human Action Reliability Program, 1984



# Principal Steps in PRA





# Human Error Contribution to Risk Can Be Large

- Human error has been shown to be a significant contributor to overall plant risk:
  - Past studies have indicated that operator error may contribute a large percentage of total nuclear plant risk
  - Human errors may have significantly higher probabilities than hardware failures
  - Humans can circumvent the system design (e.g., shutting off safety injection)



# Human Reliability Analysis (HRA)

- Starts with the basic premise that the humans are, in effect, part of the system. Thus, nuclear power plants and systems which comprise them are “person-machine systems.”
- Identifies and quantifies the ways in which human actions contribute to the initiation, propagation, or termination of accident sequences.



“Human Reliability” is the probability that a person will:

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



# Categories Of Human Error

- Errors can occur throughout the accident sequence
  - Pre-initiator errors (latent errors that may occur in or out of the main control room)
    - Failure to restore
    - Miscalibration
  - As a contribution or cause to initiating events





# Categories Of Human Error (Cont.)

## – Post-initiator errors

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



# Typical Human Error Probabilities Span a Significant Range of Values

Failure Probability	Comment	Typical Characteristics
0.1 or greater (success = 90% or less)	Some post-initiator events may lie in this range	Very short time available Complex task Multiple actions outside control room High degree of burden Little or confusing plant status information Little training High stress
0.001 - 0.1 (success - 90% - 99.9%)	Where most human error lies with the exception of most pre-initiator events and some human post-initiators	<div>   </div> As these vary, so does the human error probability
Less than 0.001 (success = 99.9% or more)	Where most pre-initiator events lie and some "automatic" post-initiator events	Lots of time Straight forward task steps No burden Lots of training or routinely performed Performed "automatically" Low or no stress



# Types Of Human Error

- Generally, two types of human errors are defined:
  - Errors of omission --Failure to perform a required action or step; e.g., failure to initiate feed-and-bleed
  - Errors of commission-- Action performed incorrectly or wrong action performed; e.g., opening the wrong valve, turning off safety injection
- Normally only the first type is modeled due to uncertainty in being able to identify errors of commission, and lack of modeling and quantification methods to address such errors.



# Types Of Human Error (continued)

## ATHEANA (A Technique for Human Event ANAlysis):

- Current NRC Research project to develop a methodology and implementation guidance for addressing errors of commission
- Draft documentation exists; will become a NUREG in 1998
- Method has been tried at Seabrook as a demonstration project
- Is a structured “brain-storming” technique to identify important errors of commission and the combinations of plant conditions and performance shaping factors that enhance the probability of such commission errors



# **ATHEANA Project Notes These Parallels for the Two Worst Nuclear Plant Accidents**

- TMI-2 and Chernobyl-4
- Operators entered an “unusual” plant condition
  - TMI: violated emergency feedwater requirements & instituted a workaround using instrument air to unblock resin beds
  - Chernobyl: violated rules on power & reactivity requirements
- Operators did not understand subsequent plant response
  - TMI: did not recognize nor fully understand the implications of reaching a saturation regime
  - Chernobyl: plant entered a regime where the core physics were not well-understood
- Operators did not fully account for the indications of the actual plant state
  - TMI: alternative rationalizations used to explain instruments
  - Chernobyl: instrumentation & eyewitness reports were dismissed



## **Other Experience Tells Us That While Plant Staff Normally Perform Appropriately, Unsafe Acts Do Occur**

- Auto-initiation/arming is bypassed/defeated
- Manual startup or backup to auto-initiation does not occur when required
- Equipment is inappropriately terminated, isolated, actuated, re-started, its output diverted...
- Equipment is inappropriately operated, controlled, its status changed...
- Equipment is not stopped when required



# **The More Serious Events Appear to Demonstrate...**

- Unsafe human actions, when most significant, typically involve:
  - plant behavior outside “expected” range
  - plant behavior not fully understood
  - indications of the actual plant state are not recognized
  - prepared plans or procedures may not be particularly helpful
- ATHEANA is a brainstorming process designed to identify those plant conditions and operator performance shaping factors that together produce an “error-forcing context” with the characteristics cited above.



# **The Underlying Steps for Applying ATHEANA**

- Identify scenarios in which operators may inappropriately disable operating equipment or fail to actuate necessary equipment
- Identify combinations of plant conditions and weaknesses in the human-machine interface that could mislead operators
- Estimate the likelihood of these conditions and weaknesses
- Estimate the likelihood of incorrect operator actions under these conditions/weaknesses
- Incorporate results into the PRA to obtain overall risk significance
- Develop “fixes” as appropriate



# **ATHEANA Searches for Conditions or Factors Observed in Past Events That Licensees and Inspectors Should be Watchful Of...**

- Entering troublesome or unusual condition
- Possible misleading or inaccessible indications & alarms
- Previous experience or training biases including written & unwritten rules & practices
- Procedure shortcomings (e.g., ambiguous, complicated...)
- Conditions causing poor communications
- Unclear or ambiguous safety function “start” and “termination” criteria
- Circuitry design that could hamper desired actions (e.g., protective trips, “lock-in” circuits...)
- Conditions when new or unfamiliar equipment would be used
- Conditions when environmental factors would interfere with the ability to perform
- When certain instrument failures or multiple equipment failures could be particularly troublesome



# HRA Process

- Identify Human Errors to be considered in plant models:
  - Normal Plant Ops-- Identify potential errors involving miscalibration or failure to restore equipment by observing test and maintenance / reviewing procedures
  - Upset Conditions-- Determine potential errors in manipulating equipment in response to various accident situations
    - Review of emergency and abnormal operating procedures to identify potential human errors
      - List human actions that could affect course of events



# HRA Process (cont..)

- Conduct Human Reliability Task Analyses
  - Breakdown system-required actions (tasks) into each of the physical or mental steps to be performed
  - Develop and quantify HRA model of event
    - Assign nominal human error estimates
    - Determine plant-specific adjustments to nominal human error estimates
    - Account for dependence between tasks



# Performance Shaping Factors (PSFs)

- Are people-, task-, environmental-centered influences which serve to alter base error rates.
- Most HRA modeling techniques allow the analyst to account for PSFs during their quantification procedure.
- PSFs can *Positively* or *Negatively* impact human error probabilities
- PSFs are identified in human reliability task analysis



## What to look for in evaluating PSFs: Brief Examples

Stress	Knowledge of consequences of act performed improperly, insufficient time, etc.
Training	How frequent does it cover the task being evaluated
Skill level	What is time in grade (master tech)
Motivation, morale	Unkept facility, lack of procedures, compliance, high absenteeism
Procedures	Labels which don't exist, steps which are incomplete or confusing, placement and clarity of caution statements
Interface	Indicator and control switch design and layout
Noise	Evaluate in terms of Db



# How Human Actions Are Incorporated Into PRA Model

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



# HRA Strengths and Limitations

- Major Strength: HRA identifies areas where improvements may be made in training, procedures, and equipment to reduce risk
- Limitations:
  - Lack of consensus as to which modeling and quantification approach to use (several exist)
  - Lack of data on human performance forces reliance on subjective judgment
  - Skill and knowledge of those performing the HRA
- These limitations result in a wide variability in human error probabilities and make human contribution to risk a principal source of uncertainty



# Student Exercise 1

- Find examples of human error modeling in the North Anna AFW fault tree used in the previous module (find “HEP” type events).
- Are the human error events identified, pre- or post-initiator errors?



## Student Exercise 2

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



# MODULE J

## ACCIDENT SEQUENCE QUANTIFICATION

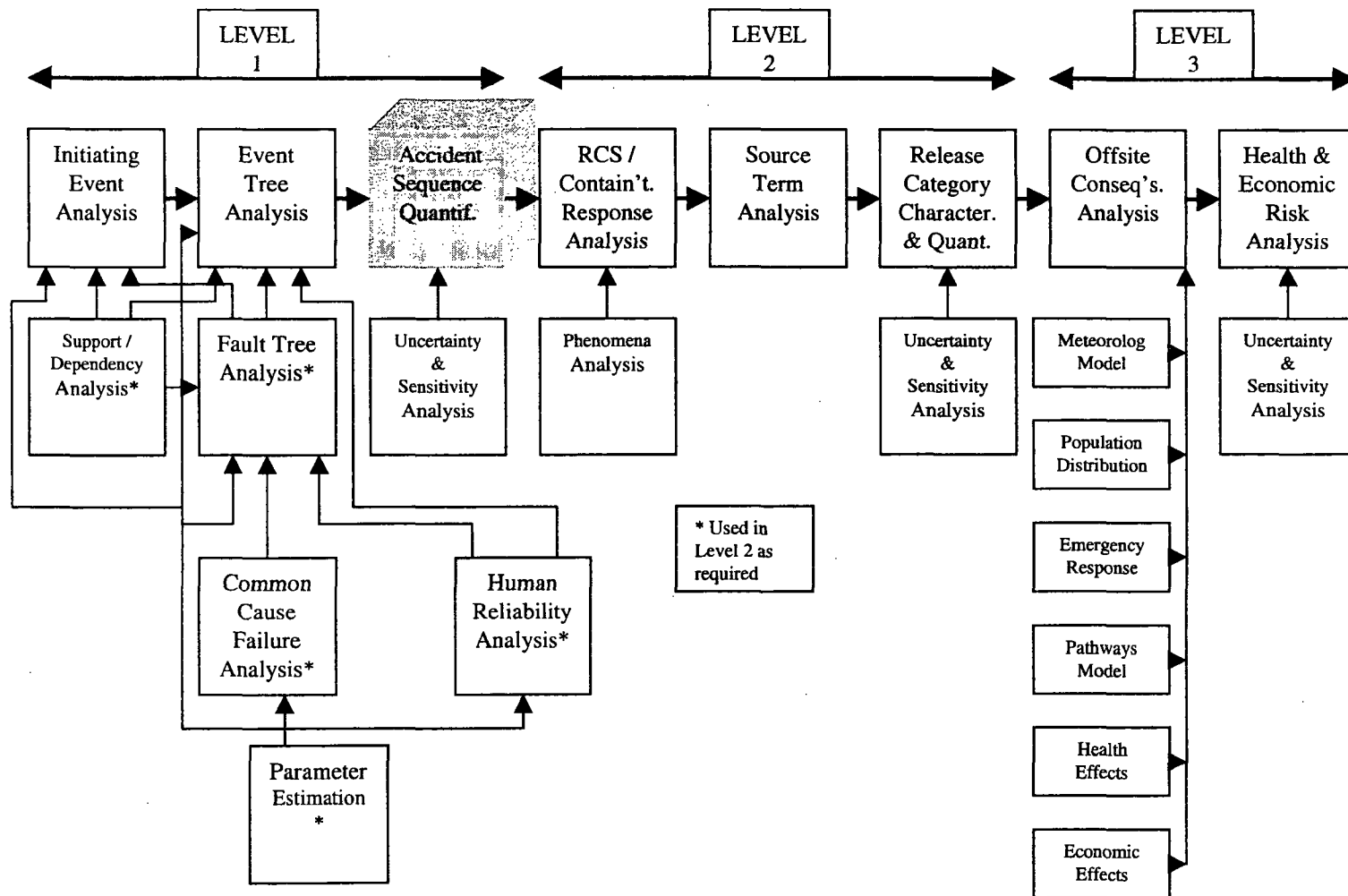


# Accident Sequence Quantification

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



# Principal Steps in PRA





# Purpose of Accident Sequence Quantification

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



# Generalized Quantification Procedure

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



# Accident Sequence Quantification

- There are two basic approaches:
  - Fault Tree Linking – Fault trees are linked to their corresponding event tree top events
    - Support system dependencies included in fault tree models
    - Tends to make fault trees complex, but simplifies event trees
  - Event Trees with Boundary Conditions – Support system dependencies explicitly included in event tree models
    - Tends to make fault trees much simpler but complicates event trees.



# Fault Tree Linking

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

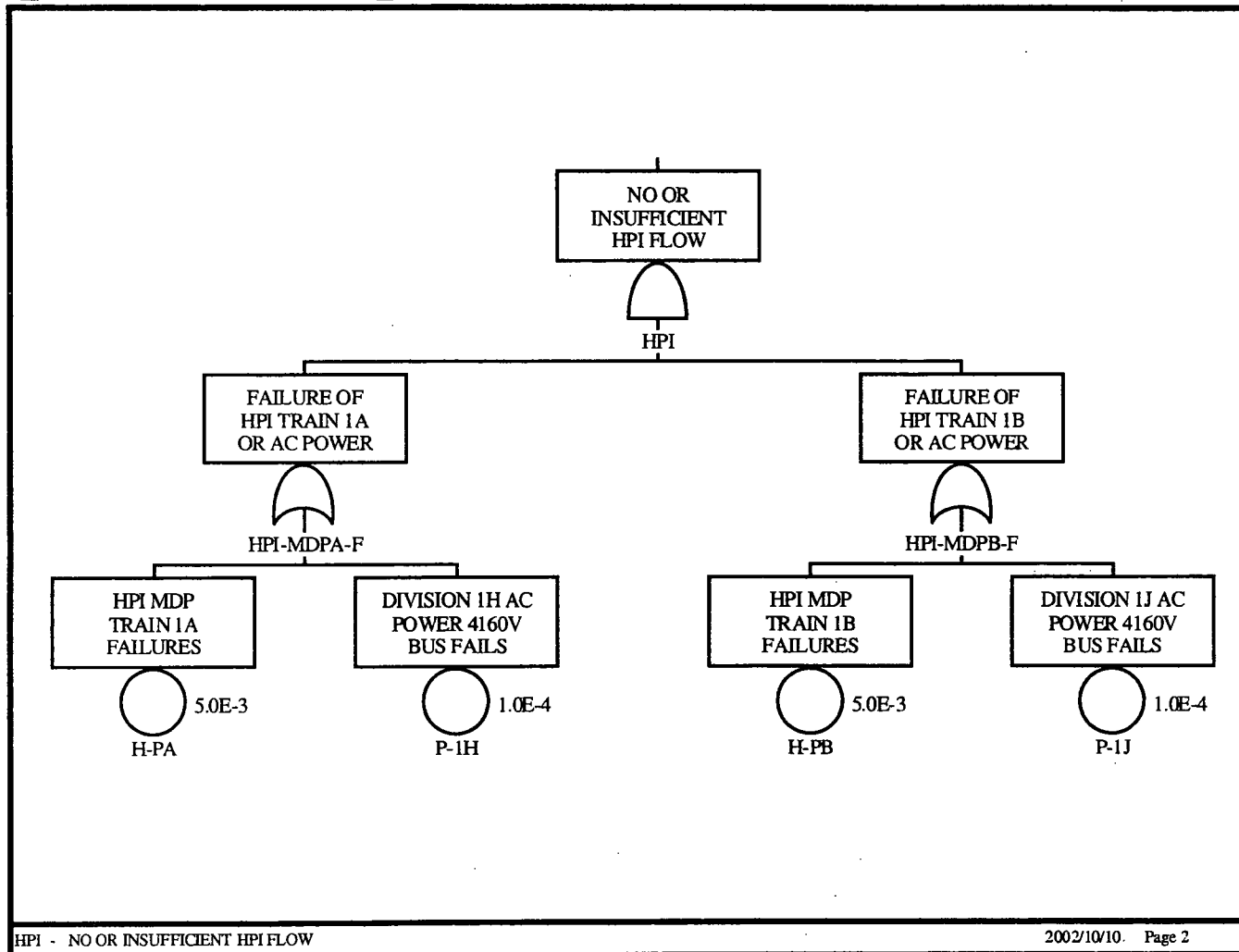


# Simplified Example of Quantification Process

SMALL LOCA	HIGH PRESSURE INJECTION AVAILABLE	AUXILIARY FEEDWATER AVAILABLE		
IE-SLOCA	HPI	AFW	#	END-STATE
<pre> graph LR     A[IE-SLOCA] --&gt; B1[OK]     A --&gt; B2[CD-PDS1]     A --&gt; B3[CD-PDS2]         </pre>				<p>1 OK</p> <p>2 CD-PDS1</p> <p>3 CD-PDS2</p>
SLOCA - Small Loss of Coolant Accident event tree				2002/10/10 Page 1

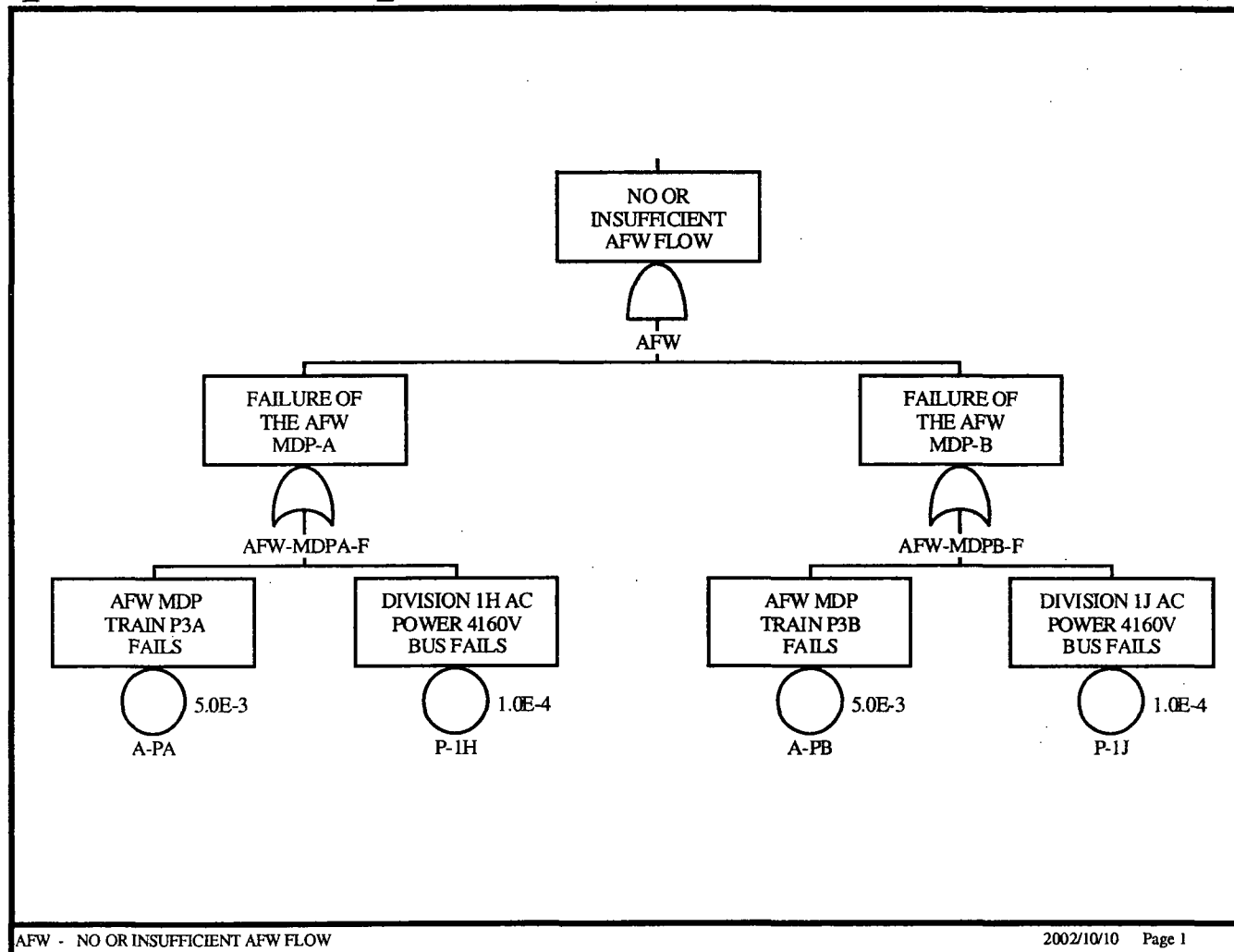


# Simplified Example of Quantification Process (cont.)



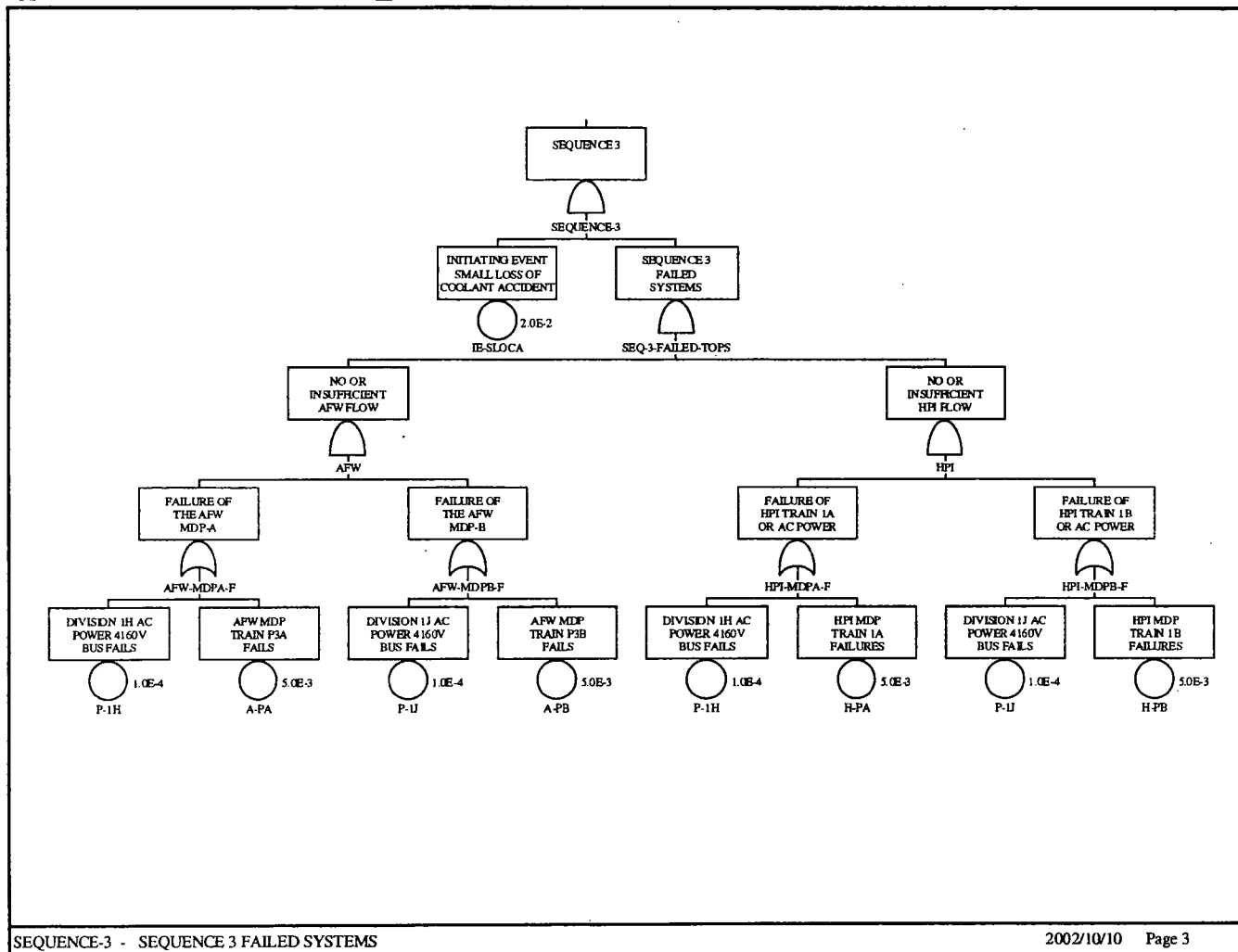


# Simplified Example of Quantification Process (cont.)





# Simplified Example of Quantification Process (cont.)





## Simplified Example of Quantification Process (cont.)

Seq3= IE-SLOCA \* System HPI Fails \* System AFW Fails

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

$$= (IE-SLOCA) *$$

$$[(H-PA * H-PB * A-PA * A-PB + H-PA * H-PB * A-PA * P-1J + H-PA * H-PB * A-PB * P-1H + H-PA * H-PB * P-1H * P-1J)$$

$$+ (P-1J * H-PA * A-PA * A-PB + P-1J * H-PA * A-PA * P-1J + P-1J * H-PA * A-PB * P-1H + P-1J * H-PA * P-1H * P-1J)$$

$$+ (P-1H * H-PB * A-PA * A-PB + P-1H * H-PB * A-PA * P-1J + P-1H * H-PB * A-PB * P-1H + P-1H * H-PB * P-1H * P-1J)$$

$$+ (P-1H * P-1J * A-PA * A-PB + P-1H * P-1J * A-PA * P-1J + P-1H * P-1J * A-PB * P-1H + P-1H * P-1J * P-1H * P-1J)]$$

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

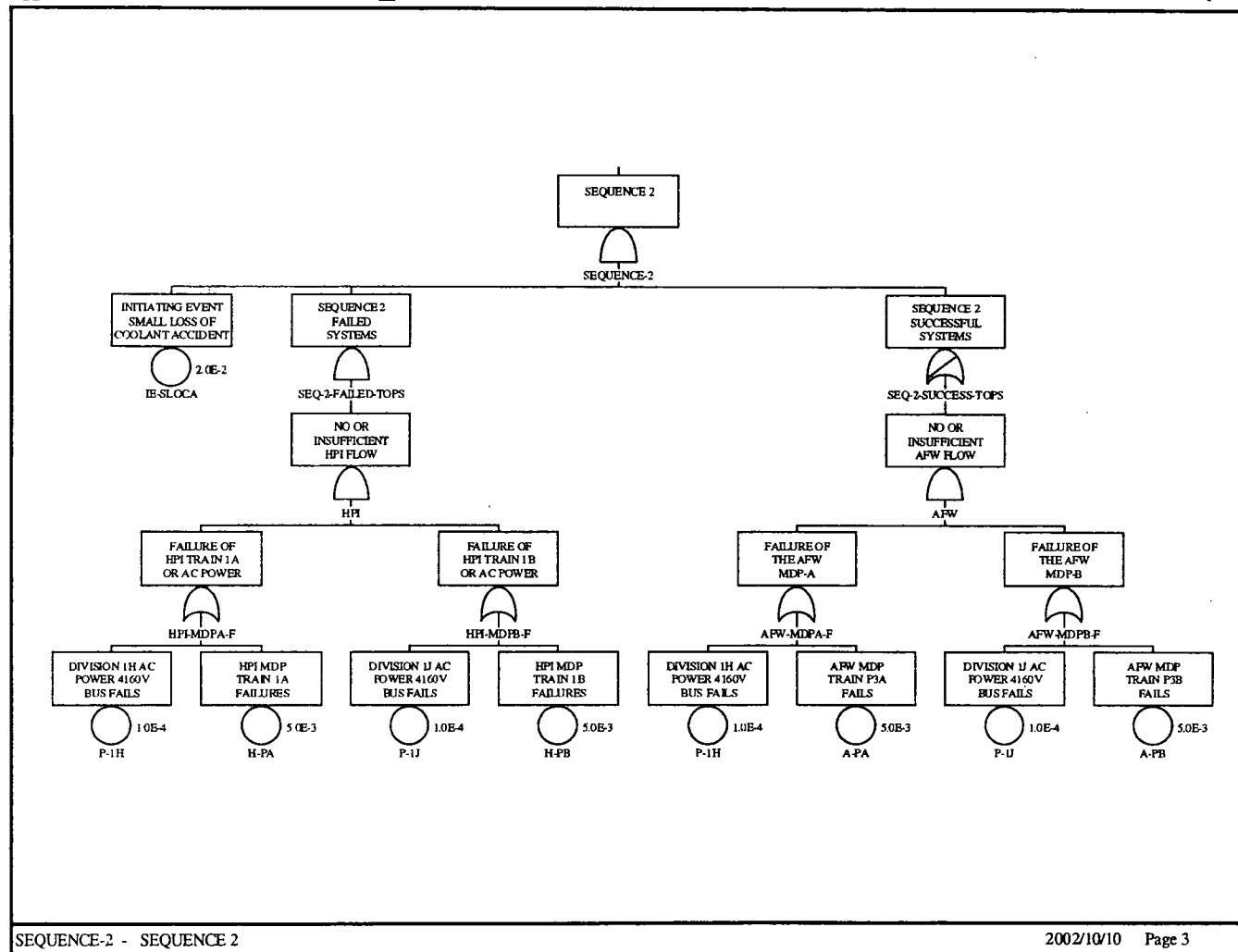
$$Seq3 = (2E-2/Year) * (1E-4 * 1E-4 + 5E-3 * 5E-3 * 1E-4 + 5E-3 * 5E-3 * 1E-4 + 5E-3 * 5E-3 * 5E-3 * 5E-3)$$

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

$$= 3.125E-10/Year$$



# Simplified Example of Quantification Process (cont.)





## Simplified Example of Quantification Process (cont.)

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

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



# Simplified Example of Quantification Process

SMALL LOCA	HIGH PRESSURE INJECTION AVAILABLE	AUXILIARY FEEDWATER AVAILABLE			
IE-SLOCA	HPI	AFW	#	END-STATE	FREQUENCY
<pre> graph LR     A[ ] --- B[ ]     B --- C1[1 OK]     B --- C2[2 CD-PDS1]     C2 --- C3[3 CD-PDS2]             </pre>			1	OK	
			2	CD-PDS1	5.200E-007
			3	CD-PDS2	3.125E-010

SLOCA - Small Loss of Coolant Accident event tree

2002/10/10 Page 1



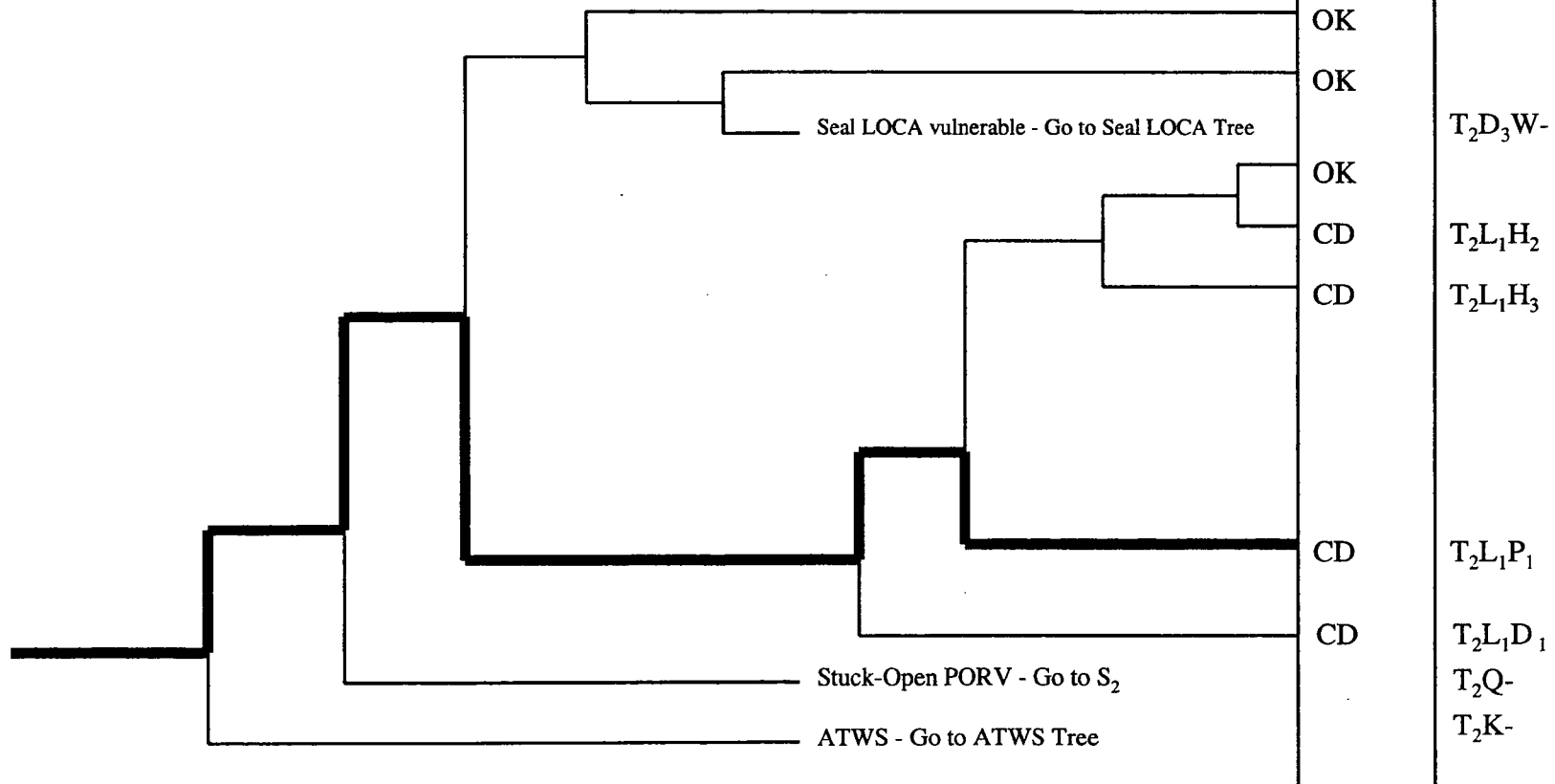
# Truncation and Minimal Cut Sets

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



# Event Tree for T<sub>2</sub> - Loss of Main Feedwater

Initiator	RPS	RVC	AFW	SIF	CCW	HPI	PRV	LPI/ LPR	HPR	STATUS	SEQUENCE
T <sub>2</sub>	K	Q <sub>1</sub>	L <sub>1</sub>	D <sub>3</sub>	W	D <sub>1</sub>	P <sub>1</sub>	H <sub>3</sub>	H <sub>2</sub>		





# Summary of Sequence T<sub>2</sub>L<sub>1</sub>P<sub>1</sub>

- This sequence is initiated by a loss of main feedwater (T<sub>2</sub>), followed by failure of the auxiliary feedwater (AFW) system, and failure of feed and bleed cooling due to the inability to open both power operated relief valves (PORVs).
- The loss of main feedwater initiator places a demand on auxiliary feedwater to remove core decay heat. Failure of the AFW system causes a demand for feed and bleed cooling. Failure to initiate feed and bleed and various failures which prevent one of the two PORVs from opening contribute to this sequence. Success criteria require that two PORVs open for successful feed and bleed.
- The dominant contributors to AFW failure are common cause failure of the air-operated steam generator level control valves and the common cause failure of all three AFW pumps due to steam binding. The dominant contributor to failure of feed and bleed is operator failure to open PORVs, followed by mechanical failures of the PORV block valves and PORVs.



# Identifiers for T<sub>2</sub> Event Tree

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



# Dominant Contributors to Sequence $T_2L_1P_1$

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

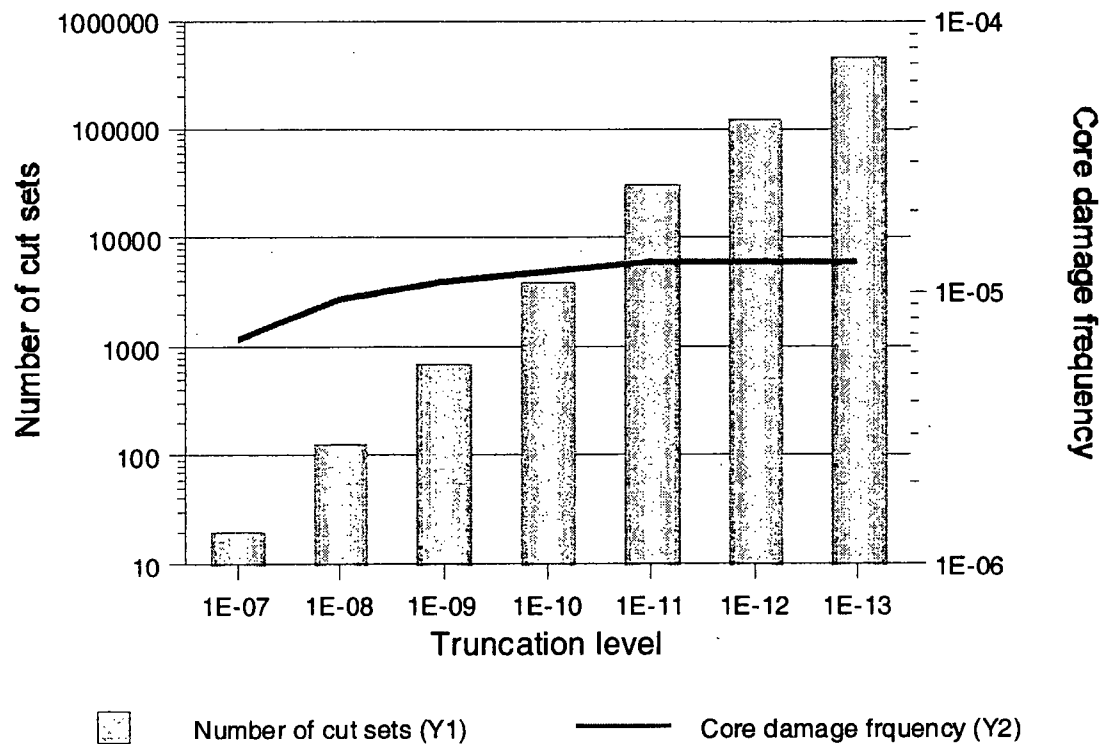


# Term Descriptions

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



# Core Damage Frequency and Number of Cutsets Sensitive to Truncation Limits





# Event Trees with Boundary Conditions

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



# Simplified Example of Quantification Process

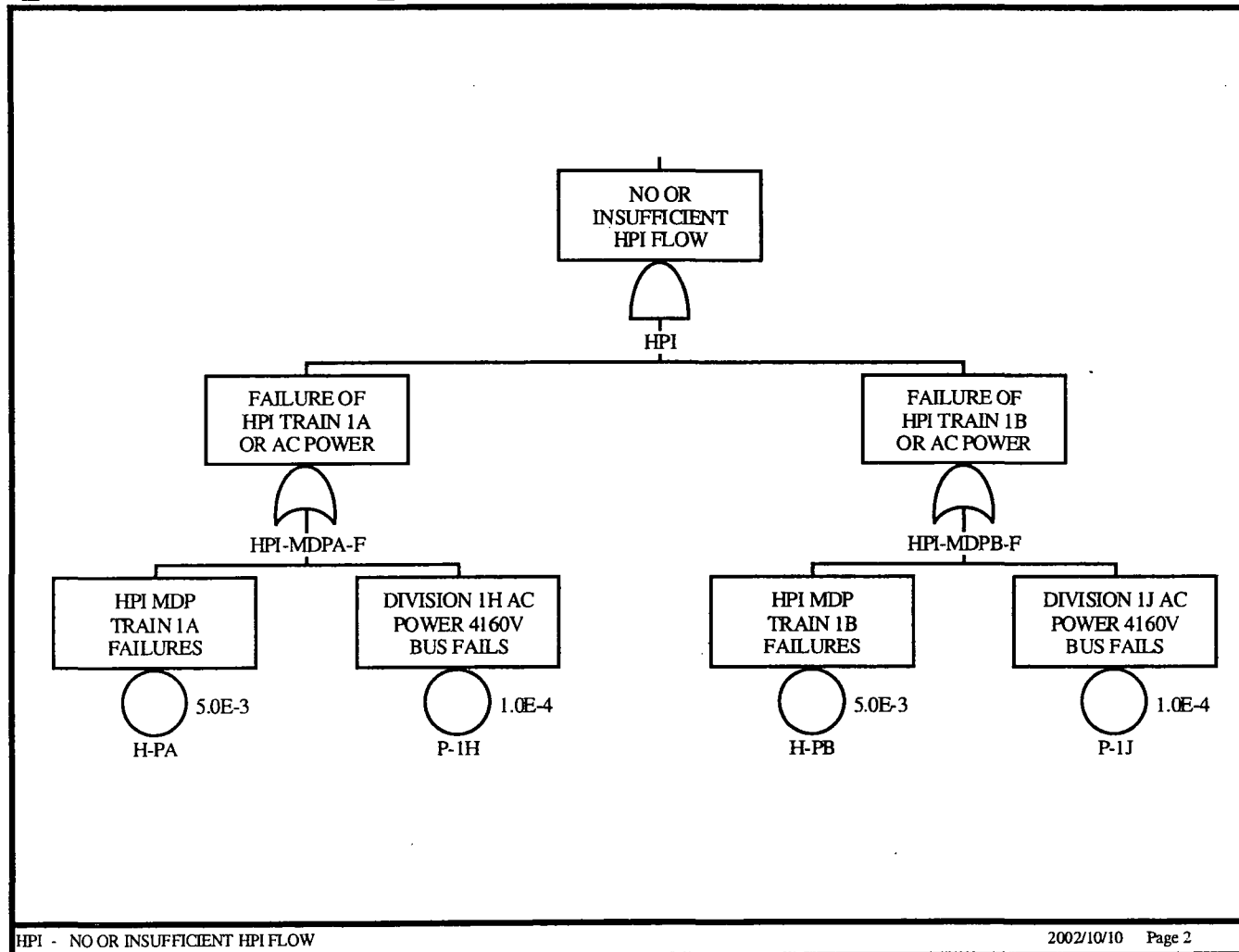
	SMALL LOCA	DIVISION 1H AC POWER 4160V BUS FAILS	DIVISION 1J AC POWER 4160V BUS FAILS	HIGH PRESSURE INJECTION AVAILABLE	AUXILIARY FEEDWATER AVAILABLE		
	IE-SLOCA	P-1H	P-1J	HPI	AFW	#	END-STATE
<pre> graph LR     Start(( )) --- B1[ ]     B1 --- B2[ ]     B1 --- B3[ ]     B1 --- B4[ ]     B2 --- HPI1[HPI-1]     B2 --- HPI2[HPI-2]     B3 --- HPI3[HPI-3]     B3 --- HPI4[HPI-4]     HPI1 --- AFW1[AFW-1]     HPI1 --- AFW2[AFW-2]     HPI2 --- AFW3[AFW-3]     HPI2 --- AFW4[AFW-4]     HPI3 --- AFW5[AFW-5]     HPI3 --- AFW6[AFW-6]     HPI4 --- AFW7[AFW-7]     HPI4 --- AFW8[AFW-8]     </pre>							1 OK
							2 CD-PDS1
							3 CD-PDS2
							4 OK
							5 CD-PDS1
							6 CD-PDS2
							7 OK
							8 CD-PDS1
							9 CD-PDS2
							10 OK
							11 CD-PDS1
							12 CD-PDS2

SLOCA - Small Loss of Coolant Accident event tree

2002/10/10 Page 1

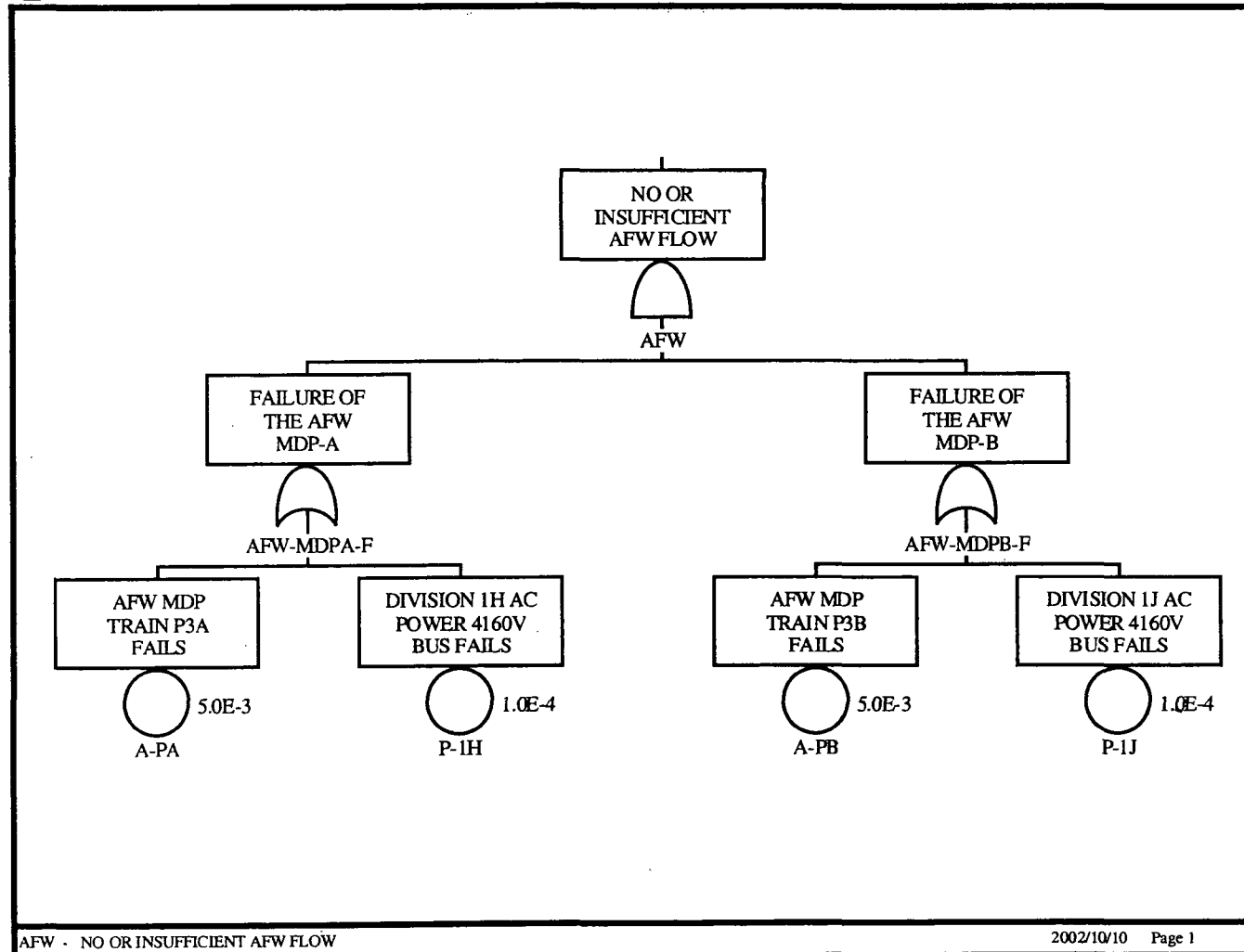


# Simplified Example of Quantification Process (cont.)





# Simplified Example of Quantification Process (cont.)





## Simplified Example of Quantification Process (cont.)

- Fault Tree      Split Fraction
- AFW-1          2.500E-005
- AFW-2          5.000E-003
- AFW-3          5.000E-003
- AFW-4          1.000E+000
  
- HPI-1          2.500E-005
- HPI-2          5.000E-003
- HPI-3          5.000E-003
- HPI-4          1.000E+000
  
- P-1H          1.000E-004
- P-1J          1.000E-004
  
- IE-SLOCA      2.000E-2/year



## Simplified Example of Quantification Process (cont.)

Sequence 2= IE-SLOCA \* /P-1H \* /P-1J \* HPI-1\* /AFW-1  
 Sequence 3= IE-SLOCA \* /P-1H \* /P-1J \* HPI-1 \* AFW-1  
 Sequence 5= IE-SLOCA \* /P-1H \* P-1J \* HPI-2\* /AFW-2  
 Sequence 6= IE-SLOCA \* /P-1H \* P-1J \* HPI-2\* AFW-2  
 Sequence 8= IE-SLOCA \* P-1H \* /P-1J \* HPI-3\* /AFW-3  
 Sequence 9= IE-SLOCA \* P-1H \* /P-1J \* HPI-3\* AFW-3  
 Sequence 11= IE-SLOCA \* P-1H \* P-1J \* HPI-4\* /AFW-4  
 Sequence 12= IE-SLOCA \* P-1H \* P-1J \* HPI-4\* AFW-4

Sequence 2=  $4.999\text{E-}007 = 2\text{E-}2/\text{YEAR} * 0.9999 * 0.9999 * 2.5\text{E-}5 * 0.999975$   
 Sequence 3=  $1.250\text{E-}011 = 2\text{E-}2/\text{YEAR} * 0.9999 * 0.9999 * 2.5\text{E-}5 * 2.5\text{E-}5$   
 Sequence 5=  $9.949\text{E-}009 = 2\text{E-}2/\text{YEAR} * 0.9999 * 1.0\text{E-}4 * 5.0\text{E-}3 * 0.995$   
 Sequence 6=  $4.999\text{E-}011 = 2\text{E-}2/\text{YEAR} * 0.9999 * 1.0\text{E-}4 * 5.0\text{E-}3 * 5.0\text{E-}3$   
 Sequence 8=  $9.949\text{E-}009 = 2\text{E-}2/\text{YEAR} * 1.0\text{E-}4 * 0.9999 * 5.0\text{E-}3 * 0.995$   
 Sequence 9=  $4.999\text{E-}011 = 2\text{E-}2/\text{YEAR} * 1.0\text{E-}4 * 0.9999 * 5.0\text{E-}3 * 5.0\text{E-}3$   
 Sequence 11=  $0.000\text{E-}000 = 2\text{E-}2/\text{YEAR} * 1.0\text{E-}4 * 1.0\text{E-}4 * 1.0\text{E+}0 * 0.0\text{E+}0$   
 Sequence 12=  $2.000\text{E-}010 = 2\text{E-}2/\text{YEAR} * 1.0\text{E-}4 * 1.0\text{E-}4 * 1.0\text{E+}0 * 1.0\text{E+}0$

Total =  $5.201\text{E-}7/\text{Year}$



# Simplified Example of Quantification Process (cont.)

	SMALL LOCA	DIVISION 1H AC POWER 4160V BUS FAILS	DIVISION 1J AC POWER 4160V BUS FAILS	HIGH PRESSURE INJECTION AVAILABLE	AUXILIARY FEEDWATER AVAILABLE			
	IE-SLOCA	P-1H	P-1J	HPI	AFW	#	END-STATE	FREQUENCY
<pre> graph LR     Start(( )) --- B1[ ]     B1 --- B2[ ]     B1 --- B3[ ]     B1 --- B4[ ]     B2 --- HPI1[HPI-1]     B2 --- HPI2[HPI-2]     B3 --- HPI3[HPI-3]     B4 --- HPI4[HPI-4]     HPI1 --- AFW1[AFW-1]     HPI2 --- AFW2[AFW-2]     HPI3 --- AFW3[AFW-3]     HPI4 --- AFW4[AFW-4]         </pre>						1	OK	
						2	CD-PDS1	4.999E-007
						3	CD-PDS2	1.250E-011
						4	OK	
						5	CD-PDS1	9.949E-009
						6	CD-PDS2	5.000E-011
						7	OK	
						8	CD-PDS1	9.949E-009
						9	CD-PDS2	5.000E-011
						10	OK	
						11	CD-PDS1	0.000E+000
						12	CD-PDS2	2.000E-010
SLOCA - Small Loss of Coolant Accident event tree						2002/10/10 Page 1		



# Quantification Results

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



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

## Code/Developer:

- CAFTA/SAIC - FT-linking with ETs
- Riskman/PL&G - ETs with boundary conditions
- SETS/Worrell Inc. - FT-linking
- SAPHIRE (IRRAS)/INEEL - FT-linking/ETs with BCs
- Nupra/NUS & Sciencetech - FT linking with ETs
- Graftor/Westinghouse - FT-linking/ETs with BCs
- Rebeca/Erin Engineering - FT-linking with ETs



# Student Exercise

- Answer the following from your plant's IPE/PRA
  - Which accident sequence quantification approach (i.e., Fault Tree Linking or Event Tree with Boundary Conditions) was used in your plant's IPE/PRA?
  - What are the two initiating event groups that contribute the most to the plant's CDF (from a percentage contribution basis
  - What two classes of accidents (or specific accident sequences if that is what is presented) contribute the most to the plant's CDF?



# MODULE K

## EXTERNAL EVENTS

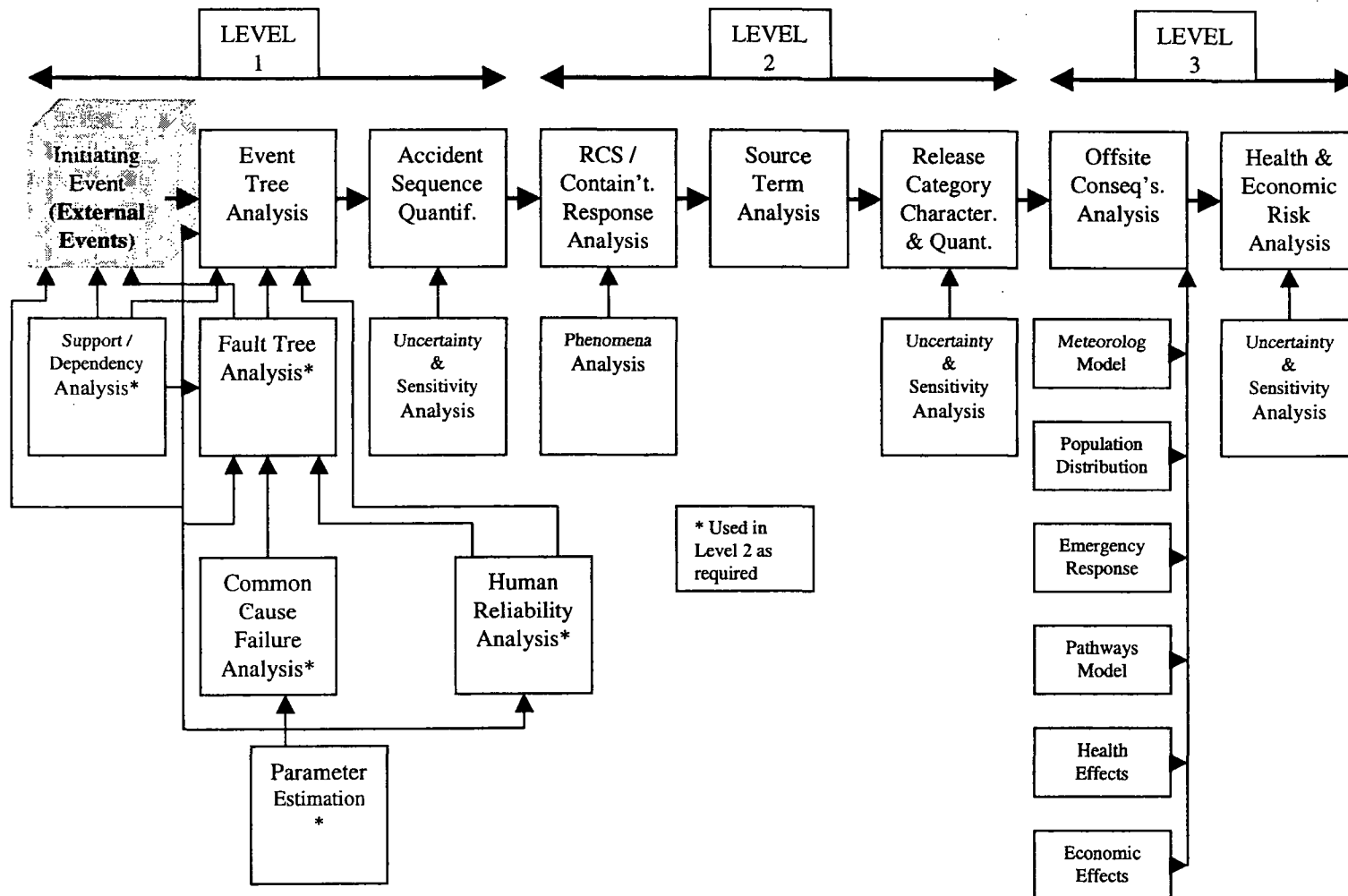


# External Events

- **Purpose:** This topic will acquaint students with the definition of external events and the IPEEEs.
- **Objectives:**
  - Define external events and differentiate them from the broader class of dependent events
  - List several of the more significant external events, including those analyzed in the IPEEEs
  - Know the objectives of the IPEEE and the acceptable approaches for seismic events and fires
  - Explain the ways in which external events may be evaluated and how this evaluation is related to the overall PRA task flow.
- **References:** PRA Procedures Guide (NUREG/CR-2300), Generic Letter 88-20, Supplements 4 and 5, NUREG-1407



# Principal Steps in PRA





# Possible External Events

(\*External Initiating Events Assessed in IPEEEs)

Event	Usual cause for exclusion
<ul style="list-style-type: none"><li>• Aircraft</li><li>• Avalanche</li><li>• *Earthquake</li><li>• *Fire in plant</li><li>• Fire outside plant but on site</li><li>• Fire off site</li><li>• Flammable fluid release</li></ul>	<ul style="list-style-type: none"><li>• --</li><li>• Physically impossible for most sites</li><li>• --</li><li>• --</li><li>• --</li><li>• No means to propagate to plant</li><li>• Considered under fire (onsite) or pipeline accident (offsite)</li></ul>
<ul style="list-style-type: none"><li>• Fog</li><li>• *Flooding, <i>external</i> (including seiche, storm surge, dam failure, and tsunami)</li><li>• Flooding, <i>internal</i></li></ul>	<ul style="list-style-type: none"><li>• Included in aircraft or ship impact</li><li>• --</li><li>• --</li></ul>



# Possible External Events (cont.)

(\*External Initiating Events Assessed in IPEEEs)

Event	Usual cause for exclusion
<ul style="list-style-type: none"><li>• *High winds (including tornadoes)</li><li>• Hurricane</li><li>• Ice</li></ul>	<ul style="list-style-type: none"><li>• --</li><li>• Wind damage covered under high winds, water damage covered under flooding</li><li>• Ice formation on aircraft covered under aircraft impact; ice formation on transmission lines covered under loss of offsite power; ice blockage of river or lake covered in plant design -- loss of cooling</li></ul>
<ul style="list-style-type: none"><li>• Industrial or military accident offsite</li><li>• Landslide</li><li>• Lightning</li><li>• Meteorite impact</li></ul>	<ul style="list-style-type: none"><li>• --</li><li>• Physically impossible for most sites</li><li>• Included in plant design</li><li>• Frequency less than earthquake or tornado</li></ul>



# Possible External Events (cont.)

(\*External Initiating Events Assessed in IPEEEs)

Event	Usual cause for exclusion
<ul style="list-style-type: none"><li>• Pipeline accident</li><li>• Sabotage</li><li>• Ship impact</li></ul>	<ul style="list-style-type: none"><li>• --</li><li>• Outside scope - impossible to assess</li><li>• Impossible to damage more than water intake</li></ul>
<ul style="list-style-type: none"><li>• Toxic gas release</li><li>• Transportation accident</li><li>• Turbine missile</li><li>• Volcanic activity</li></ul>	<ul style="list-style-type: none"><li>• --</li><li>• --</li><li>• --</li><li>• Geologic setting of most sites makes this extremely difficult</li></ul>
<ul style="list-style-type: none"><li>• War</li><li>• *Transportation and nearby facility accidents</li><li>• *Other plant-specific hazards</li></ul>	<ul style="list-style-type: none"><li>• Outside scope - impossible to assess</li><li>• --</li><li>• --</li></ul>



## External events excluded because they occur slowly enough that mitigative action may be taken or their effects are inconsequential

Event	Remarks
• Blizzard/Snow	• Runoff due to melting considered under flooding, external; winds less than tornado
• Drought	• --
• Erosion	• --
• Hail	• --
• Heavy rain	• Runoff considered under flooding, external
• High temperature	• Considered in design
• Low Temperature	• Considered in design
• River diversion or change in lake level	• --



# Importance of External Events

- External events can initiate a core damage accident
- External events can negate or compromise the systems or procedures used to prevent or mitigate accident consequences



# History of External Events PRA in U.S.

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



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

- NRC/industry-sponsored PRA Procedures Guide (NUREG/CR-2300) includes methods for analyzing external events - 1983
- Extensive research sponsored by NRC and EPRI on methods for analyzing external events
- GL 88-20 issued - 1988, includes requirements for assessing vulnerabilities to internal floods
- NUREG-1150 - 1989, contains analyses of external events for Peach Bottom and Surry
- GL 88-20, Supplement 4 - 1991, contains IPEEE requirements for other external events



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

- NUREG-1407 issued containing IPEEE submittal guidance - 1991
- Originally requested IPEEE submittal date was June 1994
- GL 88-20, Supplement 5 revised IPEEE seismic requirements - 1995



# IPEEE Requirements

- External hazards to be assessed
  - Internal fires
  - Seismic events
  - High winds and tornadoes
  - External floods
  - Transportation and nearby facility accidents
  - Other plant-specific hazards



# Acceptable Methods for Analysis of Internal Fires

- Level 1 fire PRA
- Fire-Induced Vulnerability Evaluation (FIVE)



# Acceptable Methods for Analysis of Seismic Events

- Level 1 seismic PRA plus containment performance analysis (required for high seismicity sites)
  - Use of revised LLNL seismic hazard curves permitted by Supplement 5 to GL 88-20
- Seismic margin assessment (either EPRI or NRC methodology with enhancements)



# Acceptable Methods for Analysis of Other External Events

- Screening analysis with assessment of containment performance
- Use of judgment to define scope and depth of analysis
- Comparisons against 1975 SRP criteria are acceptable first step



#### 4. PLANT IMPROVEMENTS

As a result of the IPEEE-Seismic walkdowns, several issues/outliers not meeting EPRI NP-6041-SL caveats and/or criteria were determined. These issues were resolved by analysis and where needed, by performing modifications (including those for USI A-46) to improve the seismic capacity of components and plant. The resolved issues/outliers are grouped by Electrical/Mechanical components, Tanks and Heat Exchangers, and Supporting Components (i.e. Cable Trays and Conduits). Listed below are the resolved issues/outliers which required modifications to improve their seismic performance. Issues resolved by analyses are not included in this section.

##### 4.1 ELECTRICAL AND MECHANICAL EQUIPMENT

Issues not meeting the established screening criteria of Appendix F of EPRI NP-6041-SL were resolved. In several cases, the resolution required modification. Table 4-1 below provides the list of the resolved issues/outliers for Electrical/Mechanical components which required modifications.

Table 4-1

##### Resolution of Issues/Outliers Resulting in Modifications

ITEM NO.	CLASS	MARK NUMBER	DESCRIPTION OF ISSUE/OUTLIER	RESOLUTION
1	01	1-EP-MC-21,22 2-EP-MC-21,22 2-EP-MC-50,51	Motor Control Centers (MCC) contain essential relays, causing interaction between cabinets, and in some cases, with the adjacent wall	MCCs were connected to each other or to the wall, as required, by DCP 95-017
2	04	1-EE-ST-1H, 1J 1-EE-ST-1H1, 1J1 2-EE-ST-2H,2H1	Transformer mounting nuts were found loose and required tightening	Transformer mounting nuts were tightened
3	07	1-GN-PCV-125A-3, 125B-3	Loose nuts attaching PCV's to baseplates were found	Nuts tightened per station issued Work Orders
4	07	2-RC-PCV-2455C	Seismic interaction concern with adjacent structure	DCP 94-012 corrected interaction concerns
5	08B	2-RC-SOV-2455C-1,2	Seismic interaction with adjacent SOV's	Interaction resolved per DCP 94-012



Table 4-1 (Continued)

ITEM NO.	CLASS	MARK NUMBER	DESCRIPTION OF ISSUE/OUTLIER	RESOLUTION
6	08B-	2-RC-SOV-2456	Seismic interaction with adjacent SOV's	SOV was replaced with Nuclear Grade ASCO and fixed to prevent interaction
7	10	2-HV-AC-9	One anchor bolt missing on 2-HV-AC-9	Missing anchor bolt installed on 2-HV-AC-9.
8	16	1-VB-I-04	Transformer was missing two bolts	Missing Bolts replaced
9	20	1(2)-EI-CB-23A,B,C 1-EI-CB-44 1(2)-EI-47A,C,E,F 1-EP-28A,B,C,E,F,G,H,J 2-EP-28A,B,E,F 1(2)-EP-48A 1(2)-EI-64A,B	All Cabinets contain essential relays and were not attached to adjacent cabinets, therefore were interaction outliers due to essential relays	All cabinets connected together by DCP 93-015-3.
10	7	1-BD-TV-100H	During the field walkdown of Steam Generator Blowdown valves inside Containment, it was noted that these valves have long operator in the horizontal direction and are heavier than the valves in the seismic data base. These valves were analyzed and it was found that the valve operator yoke ( cast iron) stress will exceed the allowable if the yoke was oriented such that the operator dead load bending stress was along the yoke weak axis. The valve operator yoke strong axis for 1-BD-TV-100H was found to be oriented at 45 degrees. The evaluation indicated that the yoke stress during a seismic event will result in low seismic capacity for this valve.	An Engineering Transmittal CEM-95-049, Rev. 0 was written to reorient the yoke such that the operator dead load bending stress is along the yoke strong axis. The valve was rotated, leading to a higher seismic capacity. The transmittal also indicated that a procedure be written to ensure that the operator yoke orientation is maintained correctly at all times.



**Table 4-1 (Continued)**

ITEM NO.	CLASS	MARK NUMBER	DESCRIPTION OF ISSUE/OUTLIER	RESOLUTION
11	23 -	1-ND-IIST*	Support rack for Incore Thimble guide tubes above seal table was found not welded to frame.	The issue was corrected per Work Order No. 159918.

## **4.2 TANKS AND HEAT EXCHANGERS**

The tanks and heat exchangers included in the SSEL were evaluated in accordance with the guidelines of EPRI NP-6041 SL.

A total of 110 tanks and heat exchangers in the SSEL were evaluated, including the rule-of-the-box items. The evaluation of tanks and heat exchangers was performed by screening and analysis, and HCLPF values were calculated for the weaker and critical components. Modifications of the anchorage/support of three tanks - Component Cooling Surge Tank (1-CC-TK-1) - which serves as a make-up tank to Units 1 and 2, and Steam Generator Blowdown Tanks (not in the SSEL), were required. The details of these modifications are discussed below.

### **Component Cooling Surge Tank (1-CC-TK-1)**

The tank is a 7'-6" diameter x 10'-6" high cylindrical overhead steel tank supported on four W6x20 column legs at elevation 298', in the auxiliary building, Unit 1. The tank is common to Units 1 and 2. The tank was originally designed by Stone & Webster Engineering Corporation (SWEC). An evaluation of the tank support legs concluded that the existing supports did not meet the plant design basis. Further evaluation and necessary hardware modifications to the supports have been performed via Design Change Package (DCP) 96-020 to meet the design basis with ample of margin. A HCLPF calculation was performed on the tank with the modified supports and anchorage, and the capacity was found to be greater than 0.3g.

### **Steam Generator Blowdown Tanks (1/2 - BD-TK-1)**

During the field inspection of Component Cooling Surge Tank (1-CC-TK-1) which is in the SSEL, similarly supported Steam Generator Blowdown (SGBD) tanks (1 and 2 -BD-TK-1) were identified. The evaluation of Surge Tank supports had indicated that the tank supports would fail during a seismic event with tank filled with water. SGBD tanks are not safety related and they are not in the SSEL. However, the failure of these tank legs would impact the safety related systems in the collapse envelope of the tanks. The tank supports were evaluated and found that they would fail during a seismic event with the tank filled with water. The tank supports were therefore modified



to ensure the structural integrity of the supports during a seismic event. The tank support legs were modified under DCP 94-010.

### **4.3 CABLE AND CONDUIT RACEWAY SYSTEMS**

In accordance with Section 5.2 of the Generic Implementation Procedure (GIP) for the resolution of USI A-46, and the IPEEE guidelines, the outliers in this group are classified as not meeting inclusion rules, seismic performance concerns, or not meeting the Limited Analytical Review process. As a result of the walkdowns of Cable tray and Conduit Raceway Systems, several issues/outliers were identified and categorized. Those which were resolved via modification are listed below.

- 1) Cable tray splice connection plates were missing in 12 cable trays at different elevations in the annulus of the Unit 1 containment. The cable trays were, however, adequately supported so that they could continue to perform their function during a seismic event. Work Requests 8458 and 8501 were issued and these splice plates have since been installed.
- 2) Vertical cable tray cover approximately 6' above floor elevation near column 13 in the Unit 1 Containment was found to be not adequately clamped. Work request 8492 to clamp the cover was issued and the cover was properly clamped.
- 3) Loose conduit support clamps were noticed - one (1) in the Unit 1 Containment and two (2) in the Unit 2 Containment. Work Requests 8465 and 8490 were issued to correct this deficiency and the clamps have been tightened.
- 4) Conduit support clamps were missing at 3 locations inside the Unit 1 containment. Work Requests 8462, 8463, and 8466 were issued to install the missing clamps and the missing clamps were installed.
- 5) Spare conduit next to conduit 1CK903XC against the loop room C wall in Unit 1 Containment was found to be broken at one place. Work Request 8467 was issued and the broken conduit was replaced.
- 6) Conduits at four locations inside the Unit 2 Containment was found to have long spans. Work requests 8495 and 8497 were issued to add additional supports to reduce the unsupported length of conduits. Additional supports have since been installed.
- 7) Seven long cantilever conduit spans in the Unit 2 Containment were noticed. Work Requests 8494 and 8497 were issued to install additional supports. The installation of new supports has been completed.
- 8) Armor cable at two locations in the Unit 2 Containment were found to have broken armor cover



at the connection to the junction box. Work Requests 8491 and 6498 were issued to correct these deficiencies. The armor cables have been repaired.

- 9) In the Unit 2 Containment, JB-3599-2 located in loop room B had some cover screws missing. Work Request 8496 was issued to install the missing screws and they were installed.

All of the above issues were reviewed to ensure that they do not compromise the structural integrity of raceway systems and do not impact any safety functions of the equipment and structures in their vicinity. The review indicated that these issues do not compromise the structural integrity of the raceway systems or impact other safety related items functions during a seismic event. These issues were, however, resolved to enhance the seismic capacity of the raceway systems.



# MODULE L

## LEVEL 2 & 3 ANALYSIS

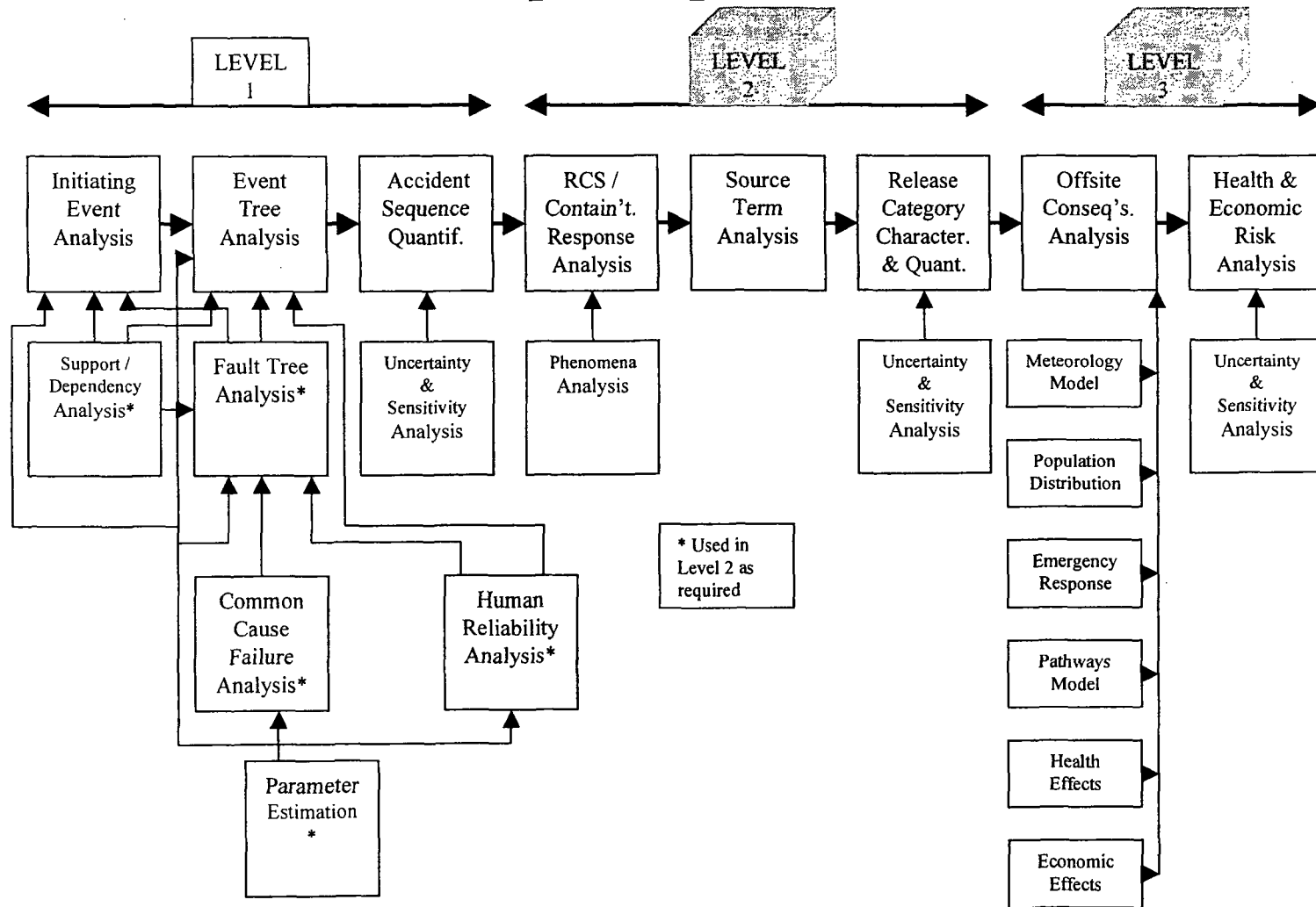


# Level 2 & 3 Analysis

- ☞ Purpose: Introduce the students to the purposes and scope of level 2 and 3 analyses.
- ☞ Objectives:
  - ❖ Describe the general purpose of Level 2 and 3 analyses
  - ❖ List typical types of consequences from a Level 3 PRA
- ☞ References: NUREG/CR-2300, NUREG-1489



# Principal Steps in PRA





# Purpose of Level 2 & 3 Analyses

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



# Level 2 Analysis Overview

- ☞ A Level 2 Analysis evaluates the radionuclide releases from accidents that result in a severely damaged core. It considers the following elements:
  - ❖ fission product transportation, deposition, and release in the reactor coolant system,
  - ❖ fission product transportation, deposition, and release in the containment.
  - ❖ determining source terms from the containment



# Plant Damage State Binning

- ☞ Plant-damage states are groups of accident sequences with certain similarities regarding plant response, timing, and equipment status. The containment analyst provides guidance as to which types of sequences are aggregated into which plant-damage states.



# Transportation, Deposition, and Release in the Reactor Coolant System

- ☞ The following issues concerning the transportation through, deposition in, and release of radionuclides from the reactor coolant system needed to be considered in the level 2 analysis:
- ❖ vessel pressure and inventory,
  - ❖ recovery of injection prior to or after vessel breach,
  - ❖ hydrogen released prior to or after vessel breach, and
  - ❖ hydrogen burn prior to or after vessel breach.



# Transportation, Deposition, and Release in the Containment

- ☞ The following issues concerning the transportation through, deposition in, and release of radionuclides from the containment needed to be considered in the level 2 analysis:
- ❖ debris coolability,
  - ❖ pressure increase due to hydrogen burn,
  - ❖ interactions between molten fuel and water,
  - ❖ debris-concrete interaction, and
  - ❖ containment pressure control.



# Source Term from the Containment

☞ The release of radionuclides from the containment is dependent upon radionuclide chemistry, the physical form of the fuel, and the environment into which it is released. Therefore, the source term specification should include: the magnitude of the release, the release rate, and the chemical and physical forms of the release material. The following potential release processes need to be considered:

- ❖ cladding-rupture release,
- ❖ diffusion release,
- ❖ leach release,
- ❖ melt release,
- ❖ melt/concrete release, and
- ❖ fragmentation release.



# Level 3 Analysis Overview

- ☞ A Level 3 Analysis evaluates the effects of the release of radioactive materials on the surrounding population and environment. It can consider the following adverse impacts (commonly referred to as “public risk”):
  - ❖ early and long-term deaths,
  - ❖ early and long-term injuries,
  - ❖ contamination of property, land, or water,
  - ❖ economic impacts



# Major Areas of a Level 3 Analysis

- ☞ The following areas are the major considerations that must be taken into account during a level 3 analysis:
  - ❖ atmospheric transportation and deposition model, including meteorology
  - ❖ pathways model,
  - ❖ dosimetry model,
  - ❖ health effects model,
  - ❖ population distribution model,
  - ❖ emergency response model, and
  - ❖ economic effects model.



# Dominant Risk Contributors Sometimes Not Dominant With Respect to CDF

- ☞ For PWRs, SGTR and bypass sequences (e.g., ISLOCA) dominate LERF and therefore early fatalities
- ☞ SGTR and bypass not dominant contributors to core damage frequency
  - ❖ If SGTR or bypass occur, consequences are large
  - ❖ Remember:  $\text{risk} = \text{frequency} \times \text{consequence}$



# Student Exercise

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



# MODULE M

## SHUTDOWN RISK



# Shutdown Risk

- ❖ Purpose: To understand why shutdown modes of operation are thought to be of concern from a risk perspective, and to become familiar with approaches to analyzing shutdown risk.
- ❖ Objectives:
  - ▶ Describe how shutdown modes can be risk-significant
  - ▶ Describe why PRA must treat separate modes of operation during shutdown
  - ▶ Discuss the risk importance of systems available to maintain plant safety functions and the effect of maintenance outages on shutdown risk
- ❖ References:
  - ▶ NUREGs 1449, 6143, 6144, 6166



# Shutdown Risk

- ❖ Shutdown (S/D) and low power encompasses operation when the reactor is subcritical or in transition between subcriticality and power operations up to ~15% of rated power
- ❖ S/D risk studies examine events that could occur during low power or shutdown operations
- ❖ In initial risk studies, risk from full power operations was assumed to be dominant since during shutdown:
  - ▶ Reactor is subcritical
  - ▶ Decay heat is decreasing with time
  - ▶ Adequate time is available to respond to accidents



# Shutdown Risk (Cont.)

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



# Background

- ❖ In response to concerns about safety of operations during shutdown, NRC initiated studies of potential risks during low power and shutdown operations
- ❖ Precursor events implied that potential generic vulnerabilities existed:
  - ▶ April 87 Diablo Canyon event resulting in loss of RHR while in midloop operation (and numerous similar events at other plants)
  - ▶ March 90 Vogtle plant loss of all AC power while shutdown
  - ▶ Two generic letters were subsequently issued relating to low-power and shutdown operations:
    - ✓ GL 87-12-- Loss of RHR while the RCS is partially filled
    - ✓ GL 87-17-- Loss of Decay Heat Removal



# Background (Cont.)

- ❖ Study included following activities:
  - ▶ Review of operating experience for domestic and foreign reactors
  - ▶ Analysis of selected significant events to estimate conditional probability of core damage using ASP models
  - ▶ Review of PRAs that included shutdown operations
  - ▶ Commissioned preliminary Level 1 PRAs for S/D and low power operations for Surry and Grand Gulf
  - ▶ Evaluated thermal/hydraulic studies of loss of RHR under S/D conditions and identified alternative methods of providing RHR



# NUREG-1449

## ❖ Shutdown And Low-power Operation At Commercial Nuclear Power Plants In The U. S.

- ▶ Study published in 1993 documented significant technical findings including:
  - ✓ Outage planning is crucial to safety during S/D
  - ✓ Significant maintenance activities increase potential for fires during shutdown
  - ✓ PWRs are more likely to experience events than BWRs; dominant contributor to PWRs is loss of RHR during operations with reduced inventory (midloop operation)
  - ✓ Extended loss of RHR in PWRs can lead to LOCAs caused by failure of temporary pressure boundaries in RCS or rupture of RHR system piping



# Precursor Events

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



# Precursor Events (cont.)

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



**OPERATING REACTORS EVENTS BRIEFING 95-06**

**LOCATION: 0-10 B11, WHITE FLINT  
WEDNESDAY, MARCH 1, 1995, 11:00 A.M.**

**WOLF CREEK, UNIT 1**

**REACTOR COOLANT SYSTEM  
INVENTORY CONTROL PROBLEMS  
WHILE SHUT DOWN (UPDATE)**

**MILLSTONE, UNIT 2**

**PRESSURE LOCKING OF  
CONTAINMENT SUMP  
RECIRCULATION VALVES**

**FERMI, UNIT 2**

**INACCURATE REACTOR LEVEL  
INDICATION CAUSED BY DATA  
COLLECTION EQUIPMENT**

---

**PRESENTED BY:**

**EVENTS ASSESSMENT AND GENERIC COMMUNICATIONS BRANCH  
DIVISION OF PROJECT SUPPORT, NRR**



WOLF CREEK, UNIT 1  
BLOWDOWN EVENT WHILE ON RHR (UPDATE)  
SEPTEMBER 17, 1994

PROBLEM

REACTOR COOLANT SYSTEM (RCS) BLOWDOWN THROUGH THE RESIDUAL HEAT REMOVAL (RHR) SYSTEM TO THE REFUELING WATER STORAGE TANK (RWST).

CAUSE

OVERLAPPING OPERATIONS AND MAINTENANCE ACTIVITIES.

SAFETY SIGNIFICANCE

- APPROXIMATELY 9,000 GALLONS OF RCS INVENTORY BLOWN DOWN IN ABOUT ONE MINUTE.
- POTENTIAL FOR 90% VOIDING IN RWST HEADER THAT IS SUCTION FOR ALL EMERGENCY CORE COOLING SYSTEM (ECCS) PUMPS IF BLOWDOWN IS NOT TERMINATED IN 3-5 MINUTES.
- MITIGATION OF AN EXTENDED BLOWDOWN MAY BE DIFFICULT BECAUSE OF POTENTIAL COMMON-MODE FAILURE OF ALL ECCS PUMPS.

DISCUSSION

- EVENT ORIGINALLY BRIEFED ON SEPTEMBER 28, 1994.

---

CONTACTS: S. ISRAEL, AEOD/SPD/RAB  
J. KAUFFMAN, AEOD/SPD/RAB

AIT: NO

REFERENCE: AEOD TECHNICAL REVIEW REPORT

SIGEVENT: YES



- AEOD STAFF VISITED WOLF CREEK IN NOVEMBER 1994.
- PLANT IN-MODE 4 AT 350 PSIG AND 300F.
- OPERATORS WERE STROKING VALVE HV8716A AFTER PACKING ADJUSTMENT AND OPENING VALVE 8717 TO BORATE RHR TRAIN B.
- THESE OVERLAPPING ACTIVITIES CREATED A FLOW PATH FROM THE RCS TO RWST THROUGH THE RHR-RWST DISCHARGE LINE.
- THE BLOWDOWN WAS STOPPED BY CLOSING HV8716A IN ONE MINUTE BEFORE RHR COOLING WAS LOST.

#### TECHNICAL REVIEW

LICENSEE CALCULATIONS SHOW 90% VOID IN RWST HEADER LINE IN 3 MINUTES IF FLOW PATH NOT ISOLATED.

- THERE ARE NO AUTOMATIC SYSTEMS TO MITIGATE SUCH AN EVENT. MUST RELY ON MANUAL OPERATOR ACTION.
- ECCS PUMPS SUSCEPTIBLE TO FAILURE IF OPERATED IN STEAMBOUND ENVIRONMENT.
- PROCEDURES NOT WELL SUITED FOR THIS DEGRADED SCENARIO.
- OPERATOR ACTIONS ARE UNCERTAIN IN THIS SCENARIO.
- LICENSEE ESTIMATED CORE UNCOVERY IN 50 MINUTES IF \_\_\_\_\_ BLOWDOWN NOT ISOLATED.



CONCLUSIONS

- UNRECOGNIZED DESIGN VULNERABILITY THAT COULD RESULT IN A LOSS OF COOLANT EVENT WITH POTENTIAL COMMON-MODE FAILURE OF ECCS PUMPS.
- MITIGATION FROM EXTENDED BLOWDOWN UNCERTAIN BECAUSE OF DEGRADED CONDITIONS, PROCEDURE MAY NOT ADDRESS SITUATION WELL, AND POTENTIAL IMPROMPTU OPERATOR ACTIONS.
- INSUFFICIENT WORK CONTROLS TO PRECLUDE THE EVENT.
- THERE HAVE BEEN OTHER RELATED LOSS OF COOLANT EVENTS WHILE PWRs WERE ON SHUTDOWN COOLING.

FOLLOWUP

- LICENSEE REOPENED HIS INVESTIGATION OF THE EVENT.
- LICENSEE HAS INVOLVED WESTINGHOUSE OWNERS GROUP.
- LICENSEE HAS REMOVED USE OF RHR-RWST LINE FROM RHR BORATION PROCEDURES.
- LICENSEE IS MODIFYING SHUTDOWN LOCA PROCEDURES BASED ON RECENT THERMAL-HYDRAULIC CALCULATIONS.
- INFORMATION NOTICE 95-03 ISSUED JANUARY 1995.
- ENFORCEMENT ACTION EA 94-251.



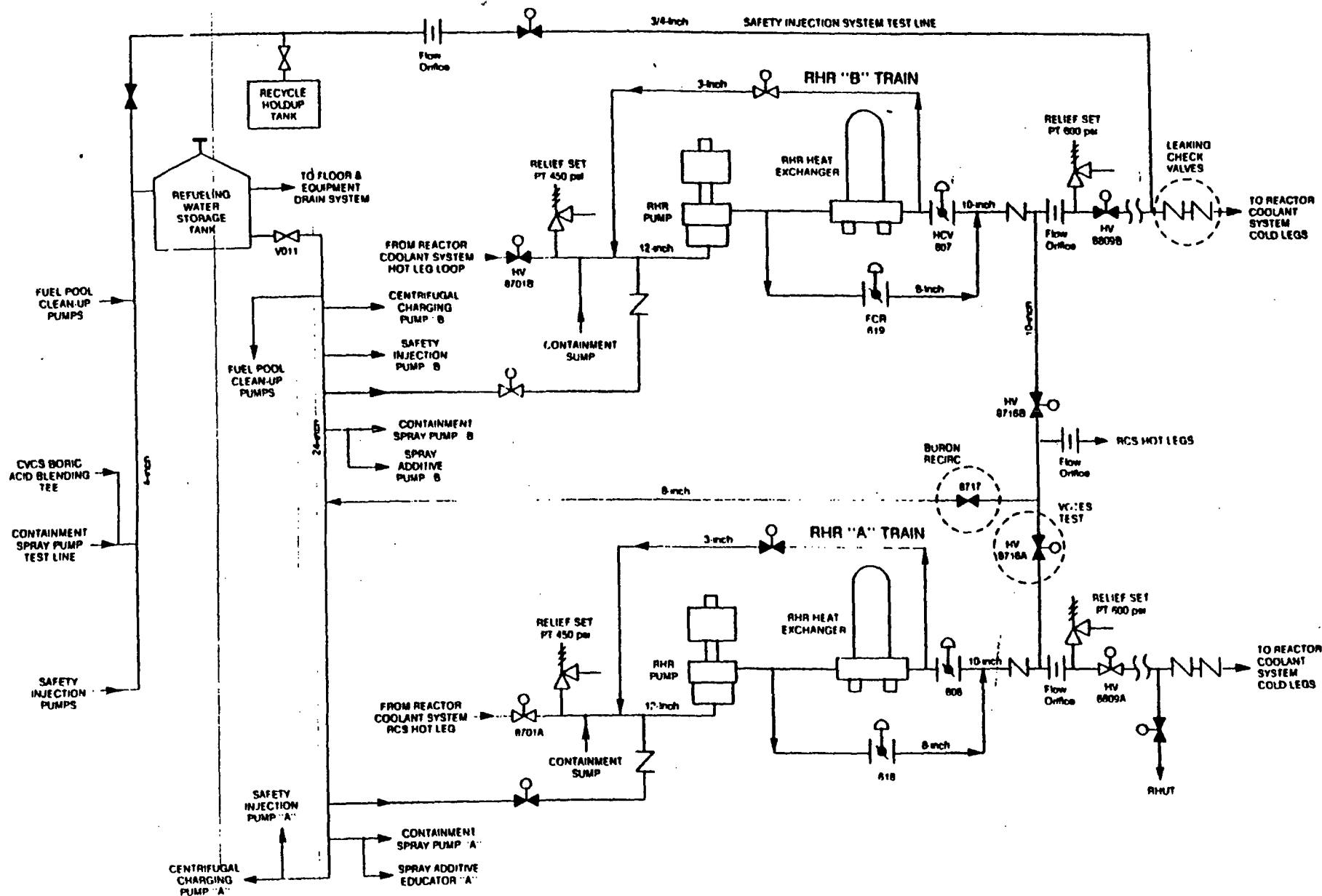


Figure 1 Valve Lineup Before Event



## D.2 LER No. Inspection Report 482/94-18

Event Description: Reactor Coolant System Blows Down to Refueling Water Storage Tank During Hot Shutdown

Date of Event: September 17, 1994

Plant: Wolf Creek

### D.2.1 Summary

On September 17, 1994, about 28 h after shutting down to begin a refueling outage, an inappropriate alignment of the residual heat removal (RHR) system allowed the rapid transfer of about 9,200 gal of water from the reactor coolant system (RCS) to the refueling water storage tank (RWST). Operators corrected the misalignment within about 66 s. Subsequent analyses have shown that, had the operators not acted within about 3 min, the RCS could have been voided down to the loop piping elevation, potentially rendering all emergency core cooling systems (ECCSs) inoperable. With the RCS vented to the environment through the RWST, core uncover could have occurred in as little as 30 min. The conditional core damage probability estimated for this event is  $3.0 \times 10^{-3}$ .

### D.2.2 Event Description

At 0400 hours on September 17, 1994, Wolf Creek was in Mode 4 preparing to begin a refueling outage with an RCS pressure of 340 psig and temperature of 300°F. Two reactor coolant pumps (RCPs) were in service, the steam generators (SGs) were filled, and the condenser and condensate systems were secured. The safety injection (SI) pumps and one of two centrifugal charging pumps were out of service with breakers open to prevent low-temperature overpressurization. RHR train A was in service to provide shutdown cooling.

Activities in progress included monitoring RCS cooldown and depressurization, performing a 24-h emergency diesel generator test run, and responding to alarms caused by minor component cooling water (CCW) system problems. Maintenance work was being performed on RHR valve 8716A, the A RHR to SI system hot leg recirculation isolation valve, and efforts were in progress to ready RHR train B for use.

RHR train B was being lined up for recirculation back to the RWST in order to raise boron concentration before placing the train in service. This required the opening of valve 8717, a manual valve in the 8-in. common line from the RHR pump discharge headers to the RWST ECCS pump suction header. A nuclear station operator (NSO) was dispatched to locally open valve 8717.

The reactor operator was controlling the chemical and volume control system (CVCS) in preparation for taking the RCS solid. This effort was complicated by failure of the volume control tank's nitrogen cover gas pressure regulator. The balance of plant (BOP) operator was lining up the B RHR train for service and adjusting the CCW system to deal with incoming alarms. The operators then received a call from a plant electrician requesting that valve 8716A be stroked (closed and reopened) in support of a test procedure. Meanwhile, the NSO had arrived at valve 8717 and prepared to open it.

Approximately 3 ft from the NSO, the electrician was working on valve 8716A, but neither he nor the NSO recognized the significance of opening valves 8717 and 8716A simultaneously. When opened together, valves 8716A and 8717 provide a direct pathway from the RHR pump discharge to the RWST ECCS suction header. When the control room operator closed valve 8716A from the control room, the operator stationed at valve 8717 apparently had only begun opening it. As water flowed from the RCS to the RWST, pressurizer level dropped about 2%, but this was not noted until the event was reviewed later. After valve 8716A closed, the control room operator waited about 30 s and then reopened it.



Valve 8717 was fully open by this time, and reactor coolant inventory began rapidly flowing to the RWST. The operator stationed at 8717 observed loud flow and water hammer noises, called the control room to report them, and was instructed to close the valve. This instruction was apparently based on good operating practice to reclose a valve when unexpected flow and noise results from opening it, rather than from an understanding of the circumstances of the event. At the same time, control room personnel received a high RWST level alarm, the pressurizer level high annunciator cleared, and the pressurizer level instrumentation "pegged low."

Operators responded by tripping the RCPs, increasing charging flow, and manually isolating letdown. A relief supervising operator who was present at the time identified the flow path through valves 8716A and 8717 to the RWST. Operators closed valve 8716A, isolating the blowdown about 66 s into the event.

During the time that the blowdown was in progress, about 9,200 gal flowed from the RCS to the RWST causing the RWST to overflow. Approximately 650 gal overflowed from the RWST to the waste holdup tank.

The RHR and charging systems remained in service, and RCS level was gradually restored.

Additional information related to this event is contained in LER 482/94-013, "Personnel Error Resulted in an Unanticipated Loss of Reactor Coolant Level."

### D.2.3 Additional Event-Related Information

Subsequent analysis determined that, had the blowdown not been quickly isolated, the primary system could have drained down to the RCS loop elevation in as little as 3 min. The RWST ECCS suction header could have been filled with steam shortly thereafter. It was further determined that an operating RHR pump could have been damaged by as little as 0.5 min of operation after the primary system drained down to the RCS loop elevation. Unisolated, the blowdown could have led to core uncover in as little as 30 min, based on a Westinghouse analysis of the event.

The Westinghouse analysis, performed after the event, suggests that once the RWST ECCS suction header voided, operation of the multistage SI pumps would have resulted in their failure. Isolation of the blowdown path would have allowed water to flow back from the RWST into the suction header; however, there is no assurance that the ECCS pumps could fulfill their functions while drawing water from the RWST following such an event.

The Westinghouse analysis also indicates that if the suction header voided, recovery would be problematic even if the RHR pumps were shut off in time. In less than the time required to fill, vent, and restart an RHR pump, reactor pressure could exceed the RHR reactor high-pressure shutoff point.

Also noteworthy in this event is the fact that the containment was bypassed. Had the blowdown not been isolated, core damage could have occurred in as little as 30 min. A direct pathway would have existed via the RHR return line to the RWST and to the environment via the RWST vent. Off-site doses could be expected to exceed technical specification limits under such conditions.

### D.2.4 Modeling Assumptions

Evaluation of this event is strongly influenced by assumptions regarding human reliability, the time and degree of effort required to recover ECCSs, and the viability of the "reflux" cooling method, wherein steam from a boiling core may be condensed in the SG tubes with the condensate draining back to the reactor. Substantial uncertainty is associated with each of these assumptions.

Approximately 3 min was available for the operators to diagnose and isolate the blowdown before all RHR and ECCS pumps were rendered inoperable. Even though procedures did not address the response to this condition, the operators' understanding of the existing system alignment allowed them to rapidly diagnose and correct the problem. During the event, the blowdown was isolated after a period of 66 s.



To estimate the likelihood that operators would fail to isolate the blowdown prior to uncovering the RCS loops, the time reliability correlation (TRC) models from *Human Reliability Analysis* (Dougherty and Fragola, Wiley, 1988) were employed. Operator response within the first 3 min was assumed to be rule-based and without hesitancy. This is considered appropriate based on the indications available to the operators at the time. Assuming the median response time to be the response time observed in this event (~60 s), and using Table 10-8 of Dougherty and Fragola, a crew error probability of 0.06 is estimated.

Had operators failed to isolate the blowdown path within 3 min, a direct vent path would have been established from the RCS through the RWST. Analyses were performed showing that core damage could have occurred as little as 27 min later.

After the RCS loops voided at 3 min, the ECCS common suction header would have begun to void. Additional consequences of a failure to terminate the event prior to this point would require more difficult operator actions. These actions were considered recovery (general diagnosis that must be used in the absence of rules) with hesitancy (due to conflict, burden, and uncertainty) within the context of the TRC model. Based on Table 10-11 in Dougherty and Fragola, a crew failure probability of 0.05 is estimated for the 27-min time period.

If the blowdown had been isolated after the loops voided (after 3 min, but before 30 min), substantial time and effort would have been required to refill and vent the RWST ECCS suction header and the ECCS pump suction that are aligned to it. An analysis performed by Westinghouse indicates that significant voids entrained in the suction supply (5 to 20%) would guarantee a loss of ECCS prime [Reference 3], and other analyses have shown that operation in that condition for more than a minute or two would cause pump failure.

Without extensive venting and priming, the high-pressure pumps would be expected to fail after loop voiding. A report concerning the event indicated that there was no assurance that the ECCS pumps would fulfill their function while drawing water from the RWST following the event [Reference 4]. Further, questions have been raised regarding the structural integrity of the RWST, if it were subjected to the water hammer effects from a blowdown. The high-pressure ECCS pumps were, therefore, assumed in this analysis to be unavailable once the RWST ECCS suction header voided.

A conservative analysis (without consideration of SG secondary-side inventory that existed during the event) showed that, without some form of decay heat removal, pressure in the RCS could exceed the RHR shutoff head within as little as 15 min. This is less than the time that would likely be required to restore the RHR system to service. Because the power-operated relief valves were found to be inoperable subsequent to this event, it was assumed that depressurization of the RCS would have been difficult to achieve. The RHR pumps were, therefore, assumed to be inoperable once the RWST ECCS suction header voided. The only remaining decay heat removal path would be reflux cooling via the SGs. The SGs were available during the event, and reflux cooling was considered a viable core cooling method. In the short term, the water inventory in the SG would provide decay heat removal. Eventually, SG makeup and the opening of atmospheric vent valves would be required for continued heat removal via this method. Reflux cooling was assumed to require two SGs and one source of feedwater for success (consistent with SBO requirements). Assuming both motor-driven auxiliary feedwater pumps and all four SGs and their atmospheric dump valves are available, a failure probability of  $\sim 7.0 \times 10^{-4}$  is estimated for reflux cooling based on component failure probabilities used in the IRRAS-based ASP models for Wolf Creek. It should be noted that this estimate addresses equipment availability only and not the uncertainty in the viability of the reflux cooling method. Since consideration of such uncertainty is beyond the scope of this analysis, the potential impact of reflux cooling being unavailable or ineffective was addressed in a sensitivity analysis.

The analysis of this event follows the simple event tree in Figure D.2.1. The tree includes the following branches:

**BLOWDN.** Blowdown. Blowdown of RCS inventory via valves 8717 and 8716A.

**ISOS-S.** Isolation in the short term (3 min). Isolation of the blowdown within 3 min is assumed to prevent voiding of the RCS. After the RCS loops voided at 3 min, RCS pressure would have rapidly dropped, and the ECCS common suction header would have begun to void. It was assumed that once the RWST ECCS suction header voided, the high-pressure ECCS pumps would be unavailable.



*ISOS-L.* Isolation in the long term (within the next 27 min). Had operators failed to isolate the blowdown path within 3 min, a direct vent path would have been established from the RCS through the RWST. Analyses were performed showing that core damage could have occurred as little as 27 min later.

*REFLUX.* Successful use of SG reflux cooling. If the blowdown is successfully isolated 3 to 30 min after the initiating event, SG reflux cooling must be successful to prevent core damage. ECCS is assumed to be unavailable due to voiding in the suction header.

## D.2.5 Analysis Results

The probability of core damage for this event is the probability of sequence 3 (failure to isolate the RCS blowdown before voiding the RCS loops, successful isolation before core uncover, and failure of reflux cooling) plus the probability of sequence 4 (failure to isolate the RCS blowdown before voiding the RCS loops and failure to isolate the blowdown before core uncover):

$$0.06 \times (1-0.05) \times 7.0 \times 10^{-4} + 0.06 \times 0.05 = 3.0 \times 10^{-3}.$$

If reflux cooling is assumed to be viable, a core damage probability of 0.003 is estimated. This estimate is probably conservative because it assumes that all ECCS pumps are unavailable once significant voiding occurs in the ECCS common suction header. Assumptions concerning the viability of reflux cooling play an important role in the core damage probability estimated for this event. For example, it may be of interest to consider what reflux cooling failure probability would lead to a doubling of the estimated core damage probability. An assumed failure probability of ~0.05 for reflux cooling raises the estimated core damage probability by a factor of 2, to  $6.0 \times 10^{-3}$ .

## D.2.6 References

1. LER 482/94-013, "Personnel Error Resulted in an Unanticipated Loss of Reactor Coolant Level," January 4, 1995.
2. NRC Inspection Report 482/94-18, "Drain-down event of September 17, 1994," December 9, 1994.
3. Wolf Creek RCS Draindown Event Analysis, NTD-NSRLA-95-083, Westinghouse Electric Co., February 1995.
4. Reactor Coolant System Blowdown at Wolf Creek on September 17, 1994, AEOD/S95-01, J. Kauffman and S. Israel, USNRC, March 1995.



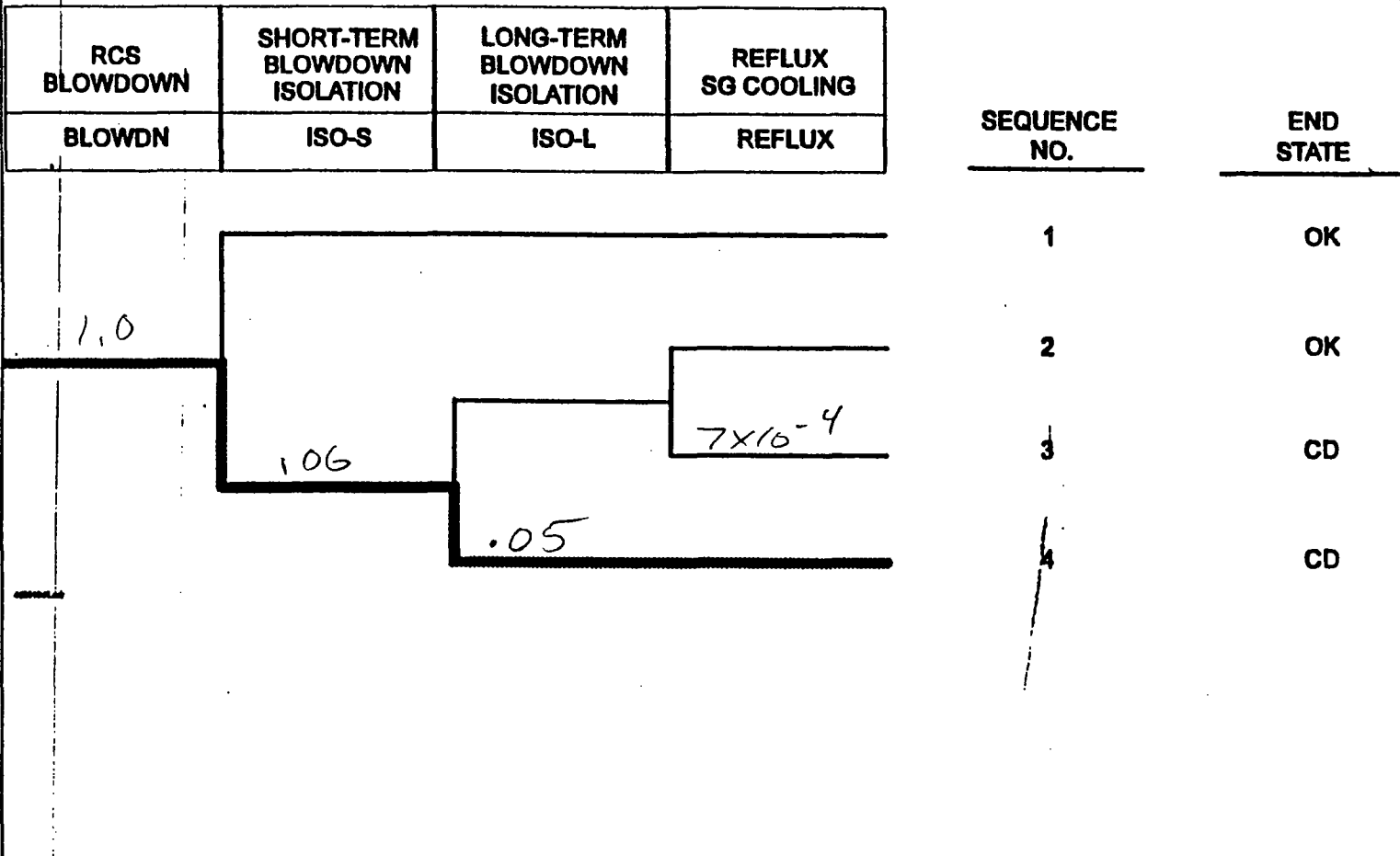


Figure D.2.1. Dominant core damage sequence for Inspection Report 482/94-18.



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
OFFICE OF NUCLEAR REACTOR REGULATION  
WASHINGTON, D.C. 20555-0001

January 18, 1995

NRC INFORMATION NOTICE 95-03: LOSS OF REACTOR COOLANT INVENTORY AND POTENTIAL  
LOSS OF EMERGENCY MITIGATION FUNCTIONS WHILE IN  
A SHUTDOWN CONDITION

Addressees

All holders of operating licenses or construction permits for nuclear power reactors.

Purpose

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice (IN) to alert addressees to a recent incident involving a loss of reactor coolant inventory while in a shutdown condition at a Westinghouse pressurized-water reactor. The incident is unique because the initiating event has the potential to create an accident and cause a loss of accident mitigation capability. It is expected that recipients will review the information for applicability to their facilities and consider actions, as appropriate, to avoid similar problems. However, suggestions contained in this notice do not constitute NRC requirements; therefore, no specific action or written response is required.

Background

NRC has issued a number of generic communications describing events at reactor facilities involving inadvertent loss of reactor coolant inventory while the facility was in a shutdown condition. In Generic Letter 88-17, "Loss of Decay Heat Removal (DHR)," the staff requested several actions to address loss of DHR events that occurred while the reactor was in a shutdown condition. In two information notices (IN 90-55, "Recent Operating Experience on Loss of Reactor Coolant Inventory While in a Shutdown Condition," and IN 91-42, "Plant Outage Events Involving Poor Coordination Between Operations and Maintenance Personnel During Valve Testing and Manipulations"), the staff discussed inadvertent loss of inventory events. A document issued by the NRC Office for Analysis and Evaluation of Operational Data (AEOD/E704), "Discharge of Primary Coolant Outside of Containment at PWRs While on RHR Cooling," reported six additional events having similar characteristics.

This IN deals with the Wolf Creek draindown event of September 17, 1994. A similar event occurred at Braidwood in 1990. Both events involved operators inadvertently transferring more than 9000 gallons of reactor coolant system (RCS) inventory to the refueling water storage tank (RWST) while preparing to shift operation of the residual heat removal (RHR) trains. However, the Wolf Creek event occurred when the RCS was pressurized to 340 psi at a temperature

9501110412



of 300 °F. As a result, more than 9000 gallons of RCS inventory was drained from the RCS to the RWST in about 1 minute.

The Wolf Creek design incorporates a 24 inch header pipe from the RWST from which the RHR pumps, the charging pumps, the high-head injection pumps, and the containment spray pumps take suction. If an RCS to RWST fluid transfer filled the 24 inch header with steam and pump operation were attempted, the pump could have been severely damaged and lost as a means of supplying RCS makeup and core cooling. In addition, such steam would create conditions favoring water hammer, which could be destructive to involved components.

#### Description of Circumstances

On September-17, 1994, the Wolf Creek Generating Station experienced a loss of reactor coolant inventory while in a shutdown condition when operators performed two incompatible activities concurrently. Preceding the event, operators were controlling the reactor coolant system in Mode 4 (hot shutdown) at approximately 300 °F and 340 psig. Operations personnel found that during the latter part of the cycle leaking check valves had diluted the boron concentration in the RHR train B piping. Licensee procedures require that the water in the piping be reborated before the RHR B train is put into operation in this circumstance. This was routinely done by recirculating the RHR piping water through the RWST using a containment spray pump.

Maintenance personnel were repairing a packing leak and performing valve motor-operator diagnostic testing on the train A RHR discharge crossover isolation valve. The shift supervisor decided that it would be acceptable to stroke the train A discharge crossover isolation valve provided that the RHR train B discharge crossover isolation valve and the RHR crossover return to the RWST manual isolation valve remained shut. To continue the cooldown to Mode 5, operators began preparations to start RHR train B so that reactor coolant pumps could be secured. While personnel continued the repair and valve motor-operator diagnostics on the train A crossover isolation valve, an auxiliary operator opened the RHR crossover return to the RWST manual isolation valve for the reboration. When both valves were opened, the reactor coolant system had a draindown flowpath through RHR train A into the 24-inch pipe that leads from the RWST. After approximately 1 minute, operators recognized an unintended flowpath and shut the train A discharge crossover isolation valve to terminate the draindown. The event transferred approximately 9200 gallons of RCS water to the RWST, depressurized the RCS to approximately 225 psig, and allowed the RCS temperature to increase by approximately 7 °F.

#### Discussion

The Office for Analysis and Evaluation of Operational Data (AEOD) reviewed this event at the Wolf Creek site from November 7 through 10, 1994, and plans to issue a report. The following discussion is, in part, based on the AEOD review and, in part, on the Office of Nuclear Reactor Regulation (NRR) and regional staff view of the potential safety implications.



Two incompatible activities were performed concurrently, causing this event: (1) alignment of the RHR train B crossover isolation valve (to adjust the boron concentration) required the valve to be opened and (2) motor-operator diagnostic testing required the train A RHR discharge crossover isolation valve to be stroked open and closed. These two activities inadvertently created the flow path for the draindown. The failure of several individuals, including the reactor operator, supervising operator, and shift supervisor, to recognize that these activities were incompatible resulted in a loss of control of plant configuration and directly caused the draindown event.

The shift supervisor initially recognized the potential for diverting RHR flow from the RCS to the RWST; however, the shift supervisor failed to establish a positive barrier, such as tagging or padlocking, to ensure that the manual crossover return to the RWST manual isolation valve remained shut. Repair and diagnostic testing of the train A discharge crossover isolation valve represented work on the only available train of a safety system. These decisions permitted work on a safety system required for safe operation of the plant without proper controls in place to prevent an inappropriate system configuration.

In recognition of additional challenges to plant operators during outage conditions, the licensee had established an outage emergent work process to evaluate unscheduled work. This process was intended to relieve some of the additional burden that might distract the operators from properly monitoring the safe condition of the plant. It was also intended to provide additional assurance that potential adverse impacts on plant operation were fully considered. However, this emergent work process was not used to evaluate the motor-operated valve work on RHR train A.

The presence of the deborated water in the RHR train B piping, the attempt to reborate, and the concurrent repair and testing of the RHR train A crossover isolation valve raises the following concerns:

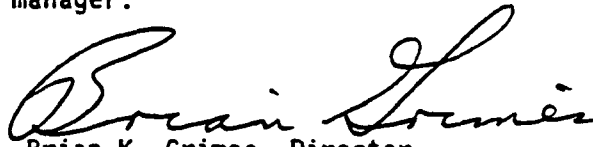
1. There is a possibility of introducing hot RCS water into the common 24-inch suction header supplied from the RWST. The RHR pumps, the charging pumps, the high-head injection pumps, and the containment spray pumps take suction from this header. Introducing hot RCS water into this header could create steam conditions and interfere with RHR pump operation. If the RHR pump were lost, alignment of the other pumps to this header as a response to the loss of RHR cooling could have also interfered with the operation of these other pumps.
2. There is the potential that if the draindown continued, the RHR piping could become filled with steam. This would create conditions favoring water hammer, which could damage valves, pumps, piping, or pipe supports. The RWST supply to the ECCS and containment spray could be jeopardized.



3. There was the possibility for inadvertent injection of relatively cold, lightly borated water from the RHR train B piping into the RCS. In the hot shutdown condition (Mode 4), where the reactor is being borated as it cools down, introduction of cold, lightly borated water reduces the margin to criticality. The licensee determined that the injection of the water from the RHR train B piping into the RCS would not have brought the reactor to a critical state. However, the potential for criticality may exist at other facilities under similar conditions.

The Wolf Creek draindown event has been classified by the NRC staff as a significant event for the NRC Performance Indicator Program.

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please contact one of the technical contacts listed below or the appropriate Office of Nuclear Reactor Regulation project manager.



Brian K. Grimes, Director  
Division of Project Support  
Office of Nuclear Reactor Regulation

Technical contacts: J. Frederick Ringwald, RIV  
(316) 364-8653

Lambros Lois, NRR  
(301) 504-3233

Attachment:  
List of Recently Issued NRC Information Notices



LIST OF RECENTLY ISSUED  
NRC INFORMATION NOTICES

Information Notice No.	Subject	Date of Issuance	Issued to
95-02	Problems with General Electric CR2940 Contact Blocks in Medium-Voltage Circuit Breakers	01/17/95	All holders of OLs or CPs for nuclear power reactors.
95-01	DOT Safety Advisory: High Pressure Aluminum Seamless and Aluminum Composite Hoop-Wrapped Cylinders	01/04/95	All U.S. Nuclear Regulatory Commission licensees.
94-90	Transient Resulting in a Reactor Trip and Multiple Safety Injection System Actuations at Salem	12/30/94	All holders of OLs or CPs for nuclear power reactors.
94-89	Equipment Failures at Irradiator Facilities	12/28/94	All U.S. Nuclear Regulatory Commission irradiator licensees.
94-88	Inservice Inspection Deficiencies Result in Severely Degraded Steam Generator Tubes	12/23/94	All holders of OLs or CPs for pressurized water reactors.
94-87	Unanticipated Crack in a Particular Heat of Alloy 600 Used for Westinghouse Mechanical Plugs for Steam Generator Tubes	12/22/94	All holders of OLs or CPs for nuclear power reactors.
94-86	Legal Actions Against Thermal Science, Inc., Manufacturer of Thermo-Lag	12/22/94	All holders of OLs or CPs for nuclear power reactors.
94-85	Problems with the Latching Mechanism in Potter and Brumfield R10-E3286-2 Relays	12/21/94	All holders of OLs or CPs for nuclear power reactors.

OL = Operating License  
CP = Construction Permit



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
OFFICE OF NUCLEAR REACTOR REGULATION  
WASHINGTON, D.C. 20555-0001

March 25, 1996

NRC INFORMATION NOTICE 95-03, SUPPLEMENT 1: LOSS OF REACTOR COOLANT INVENTORY  
AND POTENTIAL LOSS OF EMERGENCY  
MITIGATION FUNCTIONS WHILE IN A  
SHUTDOWN CONDITION

Addressees

All holders of operating licenses or construction permits for PWR power plants.

Purpose

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice supplement to alert addressees to insights from additional analysis related to reactor coolant system drain-down events with the potential for adversely impacting accident-mitigation capability. It is expected that recipients will review the information in this supplement in conjunction with Information Notice 95-03 for applicability to their facilities and consider actions, as appropriate, to avoid similar problems. However, suggestions contained in this information notice supplement are not NRC requirements; therefore, no specific action or written response is required.

Background

Information Notice 95-03, "Loss of Reactor Coolant Inventory and Potential Loss of Emergency Mitigation Functions While in a Shutdown Condition," issued on January 18, 1995, discusses the Wolf Creek drain-down event of September 17, 1994. In that event, operators were attempting to reborate residual heat removal train B while at the same time, maintenance personnel were repacking a residual heat removal train A to train B crossover isolation valve. Train B is reborated by recirculating water through a loop that contains the residual heat removal system piping, the refueling water storage tank, a containment spray pump, a manual refueling water storage tank isolation valve, and a residual heat removal system crossover line.

When the storage tank isolation valve was opened for the reboration process and the train A to train B crossover isolation valve was opened for stroke testing, a drain-down path was inadvertently created from the reactor coolant system to the refueling water storage tank. As a result, an unintentional reactor coolant system flow path was created allowing approximately 35,000 liters (9200 gallons) of reactor coolant to transfer to the refueling water storage tank. If the drain-down had not been promptly terminated, the operability of the emergency core cooling system would have been compromised. Also, reactor coolant system water flashing to steam in the piping or in the refueling water storage tank would likely have created conditions conducive to water hammer.

9602050208



This information notice supplement discusses additional insights that have been gained from analyses of the Wolf Creek event.

### Discussion

Licensee and staff analyses of the event assumed failure to isolate the drain-down path. If this were to occur, within 5 minutes, reactor vessel water level could drain to the bottom of the hot leg and as a consequence the operating residual heat removal pump would lose suction, cavitate, and fail. Continued boil-off would result in uncovering of the core in less than one hour. If the event were to occur at the beginning of mode 4, at a higher reactor coolant temperature and pressure, the transient could evolve even faster.

Failure to quickly isolate the flow path could result in the refueling water storage tank suction header filling with steam which would continually discharge into the refueling water storage tank. This steam could lead to water hammer events with the potential for mechanical damage to pump components, piping, and tank structural components. Even if the drain-down path is isolated, if sufficient steam ingress has occurred, a potential continues to exist for water hammer and mechanical damage to components. In addition, there exists the potential for containment bypass through the refueling water storage tank.


Considering the size of the header and the geometrical arrangement of that pipe (i.e., no U or inverted U arrangements) it is estimated that, after drain-down isolation, water from the refueling water storage tank will flow back down into the header. However, adequate suction may or may not be available to all emergency core cooling system pumps because of steam or air pockets in the intakes of individual pumps. Therefore, even with isolation, the risk of pump damage could remain for some time.

Plants could be susceptible to events of this nature while operating the shutdown cooling system when the reactor coolant system is at more than 121 °C (250 °F). These conditions exist shortly after the plant is shut down for refueling, maintenance, or a forced outage.

A special NRC report dated March 1995 and titled "Reactor Coolant System Blowdown at Wolf Creek on September 17, 1994" (AEOD/S95-01), identified 19 loss-of-coolant events that have occurred at reactors during shutdown. Of these 19 events, only 2 have taken place at temperatures and pressures sufficient to result in voiding refueling water storage tank piping. Considering PWR operating experience, the staff estimated the initiating event frequency may be equal to or greater than 1E-3 per reactor year. The initiating event frequency and the heavy dependence upon short term operator action, highlight the importance of careful planning, accuracy of administrative procedures, and disciplined adherence to those procedures.



This information notice supplement requires no specific action or written response. If you have any questions about the information in this supplement, please contact the technical contact listed below or the Office of Nuclear Reactor Regulation project manager.

  
Dennis M. Crutchfield, Director  
Division of Reactor Program Management  
Office of Nuclear Reactor Regulation

Technical contact: Lambros Lois, NRP  
(301) 415-3233  
internet:lx11@nrc.gov

Attachment: List of Recently Issued NRC Information Notices



# Subsequent PRA Studies

- ❖ Although risks associated with shutdown and refueling conditions have not been studied as extensively as those for power operation, several limited PRAs have been completed for both PWRs and BWRs (e.g., Zion, Seabrook, Surry, Grand Gulf), as well as shutdown decay heat removal studies (Sequoyah, Brunswick); significant findings include:
  - ▶ Quantitative core damage frequency estimates for certain shutdown modes of operation are approximately equal to or greater than full power operation
    - ✓ Time spent in non-power modes usually much less than time at power



# Subsequent PRA Studies (Cont.)

- ▶ Most significant events identified from a shutdown risk perspective are
  - ✓ Failures that occur during midloop operation (PWRs)
  - ✓ Operator errors, especially
    - failure to determine proper actions to restore shutdown cooling
    - procedural deficiencies
  - ✓ Loss of RHR shutdown cooling, especially
    - operator induced
    - suction valve trips
    - cavitation due to overdraining of the RCS
  - ✓ Loss of offsite power



# Subsequent PRA Studies (Cont.)

- ▶ Most significant events:
  - ✓ LOCAs, especially
    - operator induced
    - stuck-open RHR relief valves
    - ruptured RHR pump seals
    - failure of temporary seals
- ❖ Actual events that have occurred and those identified in studies as risk-significant are in close agreement



# Low Power And Shutdown (LP&S)

## Modes Of Operation

- ❖ LP&S analyses include all plant operating states other than full power, i.e., low power (power < 15%); hot shutdown/standby; cold shutdown; and refueling
- ❖ During shutdown, Tech. Specs. are not as prescriptive as at full power
  - ▶ Due to need to perform maintenance and refueling, configuration of plant and availability of mitigation systems can vary significantly among operating modes
  - ▶ To accommodate this variability in PRA, Plant Operating States (POS) are defined as plant condition for which status of plant systems (operating, standby, unavailable) can be specified for modeling subsequent initiating events



# Low Power And Shutdown Modes Of Operation (Cont.)

- ❖ POS definitions based on plant modes or operating conditions as defined in the Tech. Specs., but not identical
- ❖ POS characteristics include
  - ▶ reactor power level
  - ▶ in-vessel temperature, pressure, and coolant level
  - ▶ equipment normally operating and required to maintain current operating parameter
  - ▶ changes in decay heat load or plant conditions that allow new success criteria
- ❖ Examples of POSs for PWRs and BWRs are taken from NUREG/CRs 6144 and 6143 (Surry and Grand Gulf LP&S PRAs)



# POS Definitions (BWR)

## Plant Operating State

- |               |  |
|---------------|--|
| <b>POS 1:</b> | <b>Vessel pressure from rated conditions to 500 psig and thermal power not greater than 15%; core coolant at any temperature</b> |
| <b>POS 2:</b> | <b>Vessel pressure from rated conditions to 500 psig</b>   |
| <b>POS 3:</b> | <b>Vessel pressure from 500 psig to above 100 psig</b>   |
| <b>POS 4:</b> | <b>Vessel pressure less than 100 psig and RHR/SDC on</b>   |
| <b>POS 5:</b> | <b>Until vessel head is detensioned</b>  |
| <b>POS 6:</b> | <b>Head off and coolant level raised to the steam lines</b>  |
| <b>POS 7:</b> | <b>Head off, upper pool filled, and refueling transfer tube open</b>   |



# POS Definitions (PWR)

## Plant Operating State

- |                |   |
|----------------|---|
| <b>POS 1:</b>  | <b>Initiation of low power operation (10-15% power level) proceeding to hot shutdown (average core temperature = 547°F, RCS pressure = 2235 psig)</b> |
| <b>POS 2:</b>  | <b>Cooldown with steam generators (S/Gs) to 345°F</b>   |
| <b>POS 3:</b>  | <b>Cooldown with RHR to 200°F</b>   |
| <b>POS 4:</b>  | <b>Cooldown to ambient temperatures using RHR</b>   |
| <b>POS 5:</b>  | <b>Draining RCS to mid-loop</b>   |
| <b>POS 6:</b>  | <b>Mid-loop operation</b>   |
| <b>POS 7:</b>  | <b>Fill for refueling</b>   |
| <b>POS 8:</b>  | <b>Refueling</b>  |
| <b>POS 9:</b>  | <b>Draining RCS to mid-loop after refueling</b>   |
| <b>POS 10:</b> | <b>Mid-loop operation after refueling</b>   |
| <b>POS 11:</b> | <b>Refill RCS completely after mid-loop operation</b>   |
| <b>POS 12:</b> | <b>RCS heatup solid and draw bubble</b>   |
| <b>POS 13:</b> | <b>RCS heatup to 350°F</b>  |
| <b>POS 14:</b> | <b>Startup with S/Gs</b>  |
| <b>POS 15:</b> | <b>Reactor startup and low power operation</b>  |



# Significant Plant POSs

- ❖ Although total risk from all POSs has not been examined, following POSs are believed to be most risk-significant:
  - ▶ For BWR, POS 5, which includes both cold shutdown and refueling modes, was analyzed in detail instead of POS 4 since
    - ✓ Plant is in POS 5 longer
    - ✓ Tech. Specs. allow more equipment to be inoperable in POS 5 during cold shutdown than in POS 4 during hot shutdown
  - ▶ For PWR, POSs 6 and 10, occurring during a refueling outage, and POS 6, occurring during a drained maintenance outage, define mid-loop operation and are considered the most risk-significant states due to the potential to lose RHR during operation with reduced inventory



# General Process for Detailed LP&S Risk Assessment

- ❖ Plant-specific information is required for amount of time spent in each POS
- ❖ Configuration of systems needed for continuous operation in each POS is determined
- ❖ Traditional engineering analyses and quantitative screening risk calculations needed to justify screening out POSs from detailed analysis



# General Process for Detailed LP&S Risk Assessment (Cont.)

- ❖ Plant models should be developed and quantified for each POS to be analyzed including consideration of
  - ▶ Initiating events that could occur during the POS timeframe
  - ▶ Modeling of alternate and diverse systems that may be successful for that POS configuration
  - ▶ Accounting for systems that may be undergoing maintenance or surveillance, or that may be isolated during that POS based on plant-specific records, outage procedures and schedules



# How Utilities are Addressing LP&S Risk

- ❖ Some utilities have performed limited PRA studies of selected modes of operation
- ❖ Most utilities have adopted non-PRA approach
  - ▶ Approach based on guidance in NUMARC 91-06
  - ▶ Approach based on maintaining barriers during shutdown
  - ▶ EPRI sponsored development of software to implement this approach (ORAM)



# MODULE N

## IMPORTANCE MEASURES

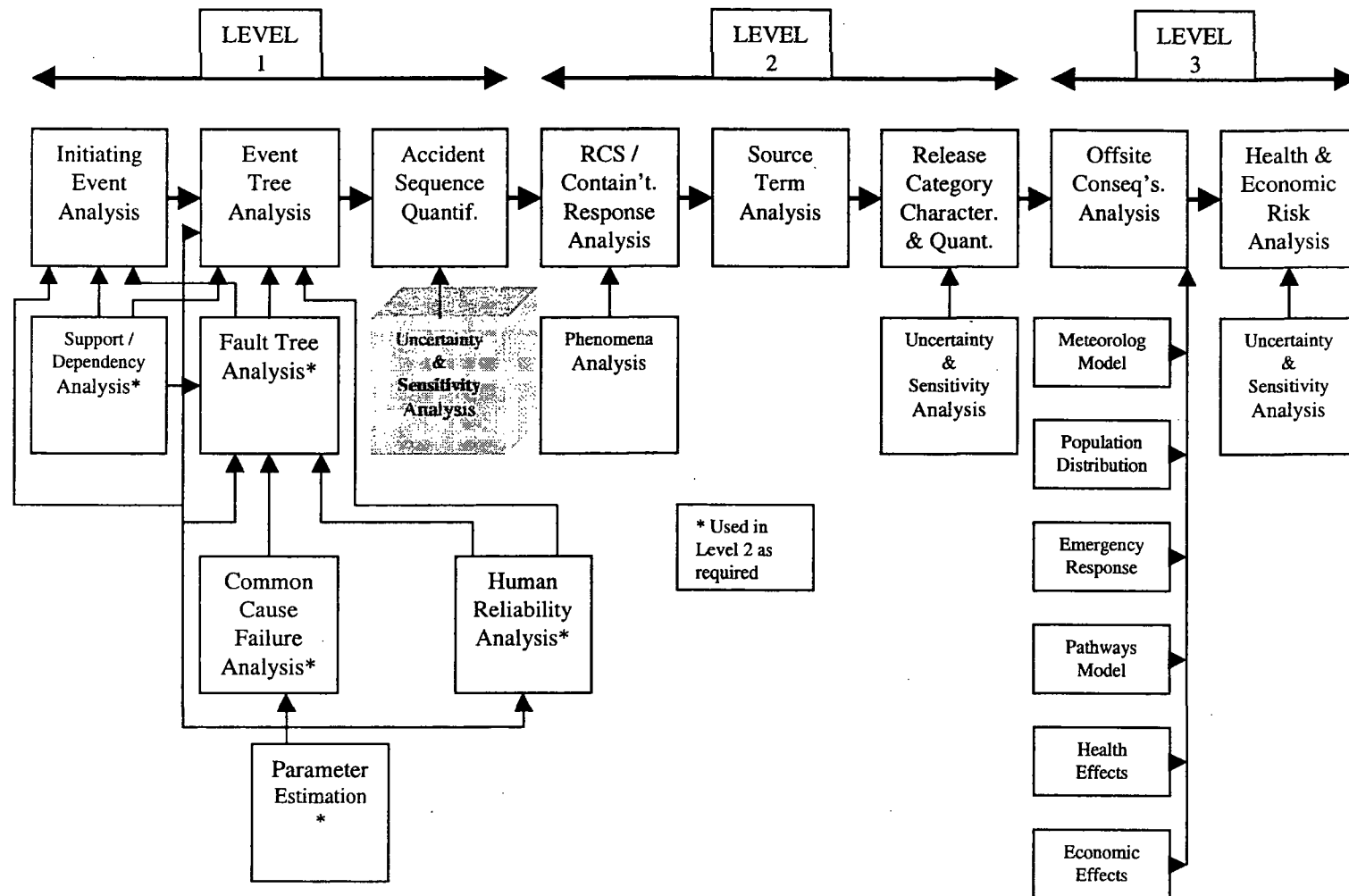


# Importance Measures

- Purpose: Students will be introduced to concepts of quantitative importance measures. Also includes a description of types of importance measures and their meanings in the context of Level 1 PRA results.
- Objectives:
  - \* Identify 3 types of quantitative importance measures
  - \* Calculate values for 3 types of importance measures given Level 1 PRA results
  - \* Understand implications of each importance measure for plant safety & inspection activities
- References:
  - \* NUREG-1489, App. C
  - \* NRC Inspection Manual Part 9900: Technical Guidance-Operations; Use of Probabilistic Risk Ranking Information
  - \* The Use of Risk Importances for Risk Based Applications and Regulation; W.E. Vesely, PSA-96
  - \* Some Perspectives on Risk Importance Measures, I. Wall, D. Worledge, PSA-96
  - \* Developing Useful Insights and Avoiding Misleading Conclusions from Risk Importance Measures in PSA Applications, K. Fleming, PSA-96



# Principal Steps in PRA





# What are Importance Measures

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



# Importance Measures

- Provide quantitative perspective on dominant contributors to risk and sensitivity of risk to changes in input values
- Usually calculated at core damage frequency level
- Three are encountered most commonly:
  - \* Fussell-Vesely
  - \* Risk reduction ratio
  - \* Risk achievement worth (RAW)



# Fussell-Vesely Importance

- Measures overall contribution of an event to risk (CDF)
- Calculated by adding up frequencies of cutsets containing event of interest and dividing by total CDF

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

or

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

where,

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

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

- Range is from 0 to 1
- Basic events with higher values of F-V importance contribute (are included in cut sets) a larger percentage of the total risk measure (e.g., core damage frequency)



# Fussell-Vesely Importance Measure

## Calculation Example

- Consider these minimal cut sets:

$$T * A = 1/\text{year} * 6 \times 10^{-4} = 6 \times 10^{-4}$$

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

$$T * C * D = 1/\text{year} * 3 \times 10^{-3} * 1 \times 10^{-3} = 3 \times 10^{-6}$$

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

where,

$$T = 1/\text{year}$$

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

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

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

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

- Fussell-Vesely Importance

$$FV_T = 6.0 \times 10^{-4} / 6.33 \times 10^{-4} = 1.0$$

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

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

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

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



# Risk Reduction

- Measures amount by which CDF would decrease if event's failure probability were set to 0 (never fails)
- Calculated as either ratio or difference between baseline CDF and CDF with event failure probability at 0
  - Ratio:  $RRR(x) = F(x)/F(0)$
  - Difference (or Interval):  $RRI(x) = F(x) - F(0)$
  - where,
    - $F(x)$  is risk with event  $x$  at nominal failure probability, and
    - $F(0)$  is risk when event  $x$  is never failed (failure probability = 0)
- Ratio - Range is from 1 to  $\infty$
- Basic event with largest risk-reduction value gives largest reduction in risk if failure is eliminated
- Gives same ranking as Fussell-Vesely
- For Maintenance Rule (10 CFR 50.65), NUMARC Guide 93-01 (endorsed by NRC) uses a RRR significance criterion of 1.005
  - \* Equivalent to Fussell-Vesely importance of 0.005



# Risk Reduction Importance Measure

## Calculation Example

- Consider these minimal cut sets:

$$T * A = 1/\text{year} * 6 \times 10^{-4} = 6 \times 10^{-4}$$

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

$$T * C * D = 1/\text{year} * 3 \times 10^{-3} * 1 \times 10^{-3} = 3 \times 10^{-6}$$

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

where,

$$T = 1/\text{year}$$

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

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

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

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

- Risk Reduction Ratio Importance

$$RRR_T = 6.33 \times 10^{-4} / 0.0 = \infty$$

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

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

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

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



# Risk Increase

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



# Risk Increase Importance Measure Calculation Example

- Consider these minimal cut sets:

$$T * A = 1/\text{year} * 6 \times 10^{-4} = 6 \times 10^{-4}$$

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

$$T * C * D = 1/\text{year} * 3 \times 10^{-3} * 1 \times 10^{-3} = 3 \times 10^{-6}$$

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

where,

$$T = 1/\text{year}$$

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

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

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

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

- Risk Achievement Worth Importance

$$RAW_T = 6.33 \times 10^{-4} / 6.33 \times 10^{-4} = 1.0 \text{ (caution interpreting IE RAW)}$$

$$RAW_A = 1.0 / 6.33 \times 10^{-4} = 1579.78$$

$$RAW_B = 3.603 \times 10^{-3} / 6.33 \times 10^{-4} = 5.69$$

$$RAW_C = 1.16 \times 10^{-2} / 6.33 \times 10^{-4} = 18.33$$

$$RAW_D = 3.63 \times 10^{-3} / 6.33 \times 10^{-4} = 5.73$$

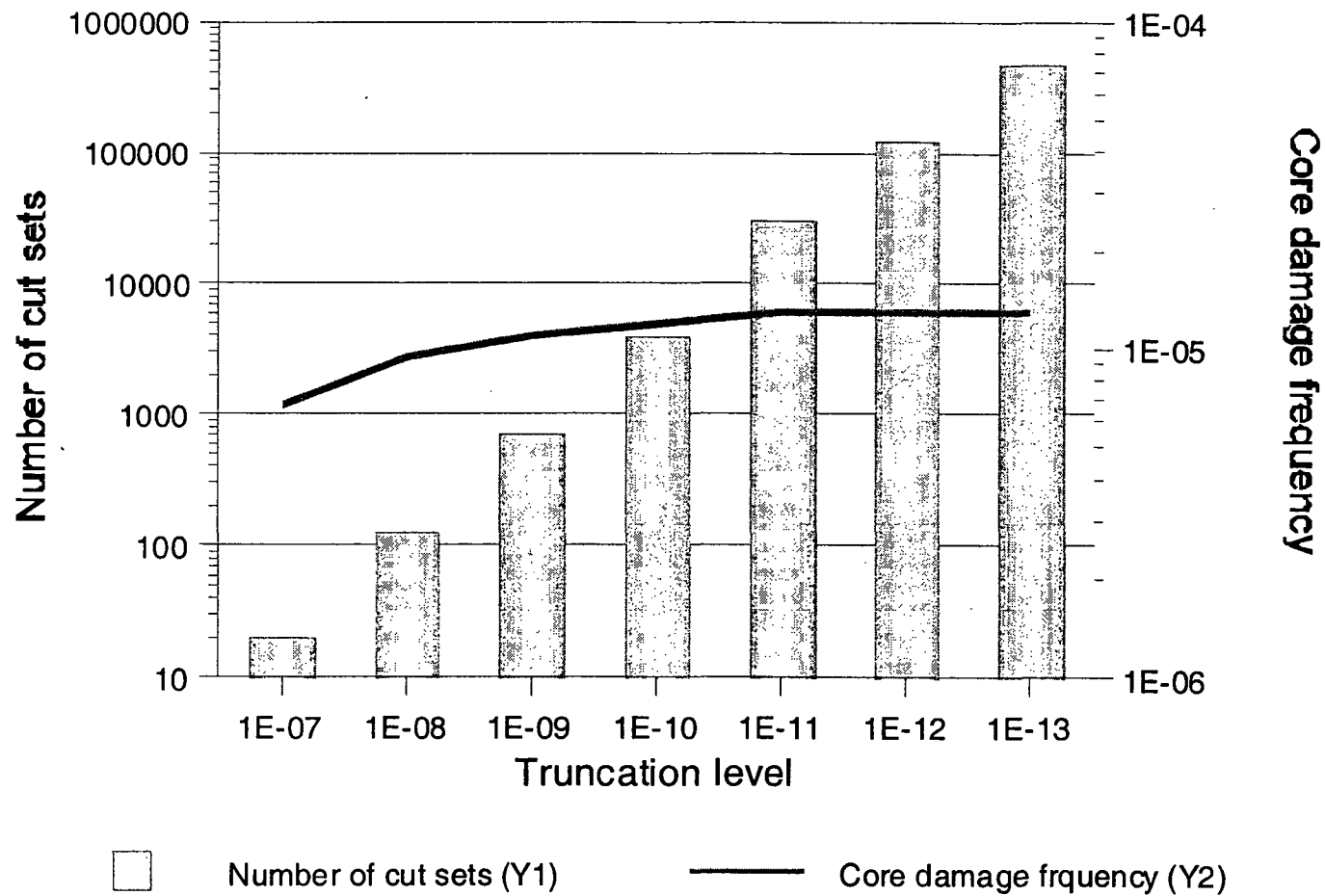


# Limitations of Risk Importance Measures

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

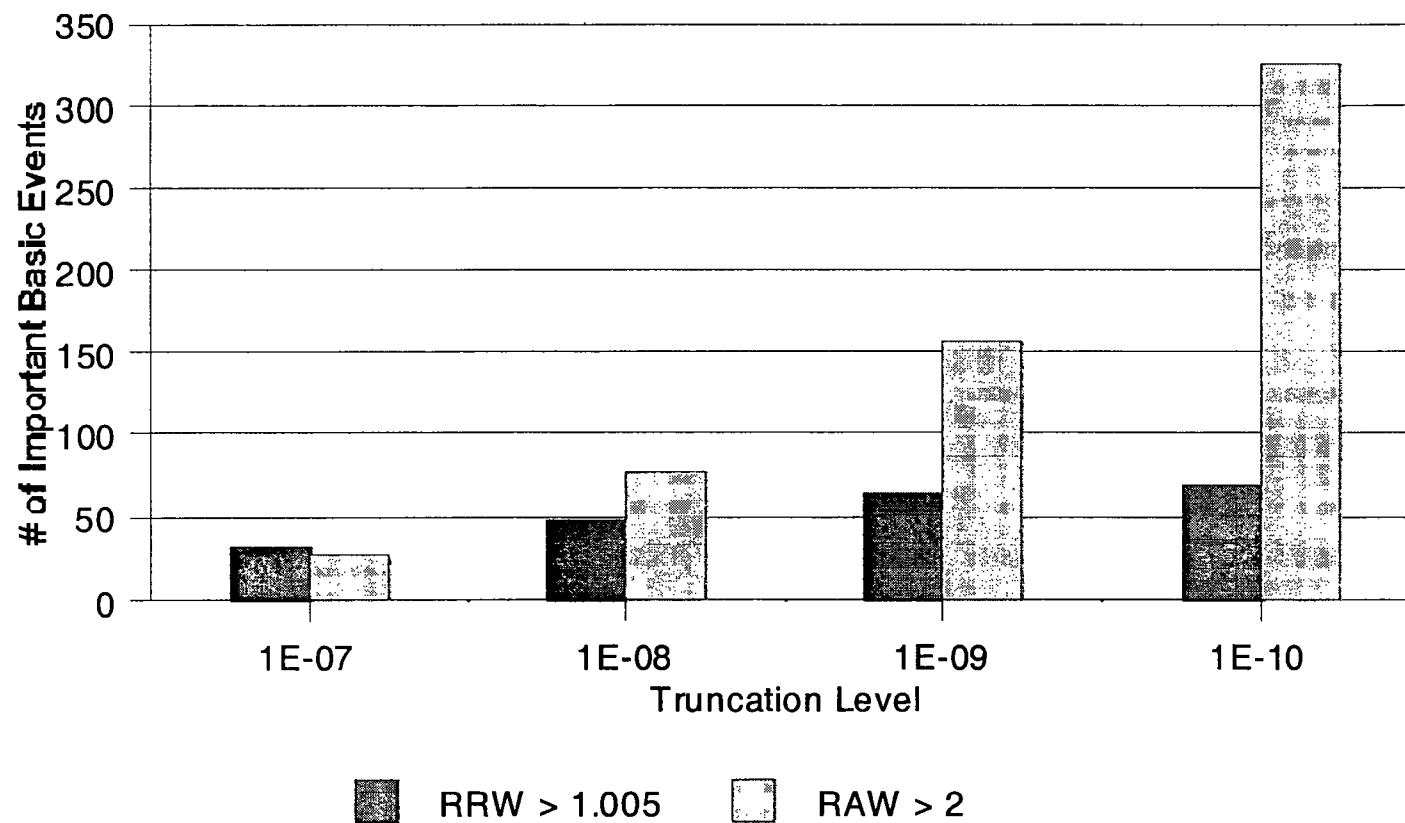


# Core Damage Frequency and Number of Cutsets Sensitive to Truncation Limits





# Truncation Limits Affect Importance Rankings





# Limitations of Risk Importance Measures (cont.)

- Risk rankings are not always well-understood in terms of their issues and engineering interpretations
  - \* That is, high importance does not necessarily mean dominant contributor to CDF
- RAW provides indication of risk impact of taking equipment out of service but full impact may not be captured
  - \* That is, taking component out of service for test and maintenance may increase likelihood of initiating event due to human error



# Other Considerations When Using Importance Measures

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



# NRC Technical Guidance for Inspection Programs

## ■ NRC Inspection Manual, Part 9900 provides technical guidance on use of Probabilistic Risk Ranking Information

### \* Some key points to consider:

- ✓ Use of PRA is effective in identifying and ranking risk-significant SSCs to prioritize inspection activities
- ✓ SSCs with highest rankings normally warrant greater concentration of inspection resources
- ✓ Risk reduction/F-V and risk increase measures convey fundamentally different information regarding a given SSC's importance to plant risk; therefore, no single importance measure should be used as the sole indicator
  - Risk reduction/F-V measures overall contribution of SSC to risk
  - RAW can be particularly informative in assessing risk impact of single out-of-service component



# NRC Technical Guidance for Inspection Programs (Cont.)

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



# NRC Technical Guidance for Inspection Programs (Cont.)

- ✓ Overall quality of the PRA must be adequate to support quantitative decisions, e.g., the PRA should be based on realistic, best estimate assumptions and data; conservative assumptions can elevate importance of certain SSCs and mask importance of others
- ✓ An appreciation of the uncertainty of PRA results provides a better understanding of the results including their precision and limitations



# Student Exercise

- From your IPE;
  - \* What are the most risk significant items (approximately top five) to risk from a Fussell-Vesely/Risk Reduction point of view?
  - \* What are the most risk significant items (approximately top five) to risk from a Risk Increase/Risk Achievement Worth (RAW) point of view?
- If your IPE does not provide a ranking of importance measures, review the risk rankings in the North Anna IPE (provided in Volume 2 of course material);
  - \* What are the most risk significant items (approximately top five) to risk from a Fussell-Vesely/Risk Reduction point of view?
  - \* What are the most risk significant items (approximately top five) to risk from a Risk Increase/Risk Achievement Worth (RAW) point of view?



# MODULE 0

## UNCERTAINTY -- TRADITIONAL ENGINEERING AND PROBABILISTIC

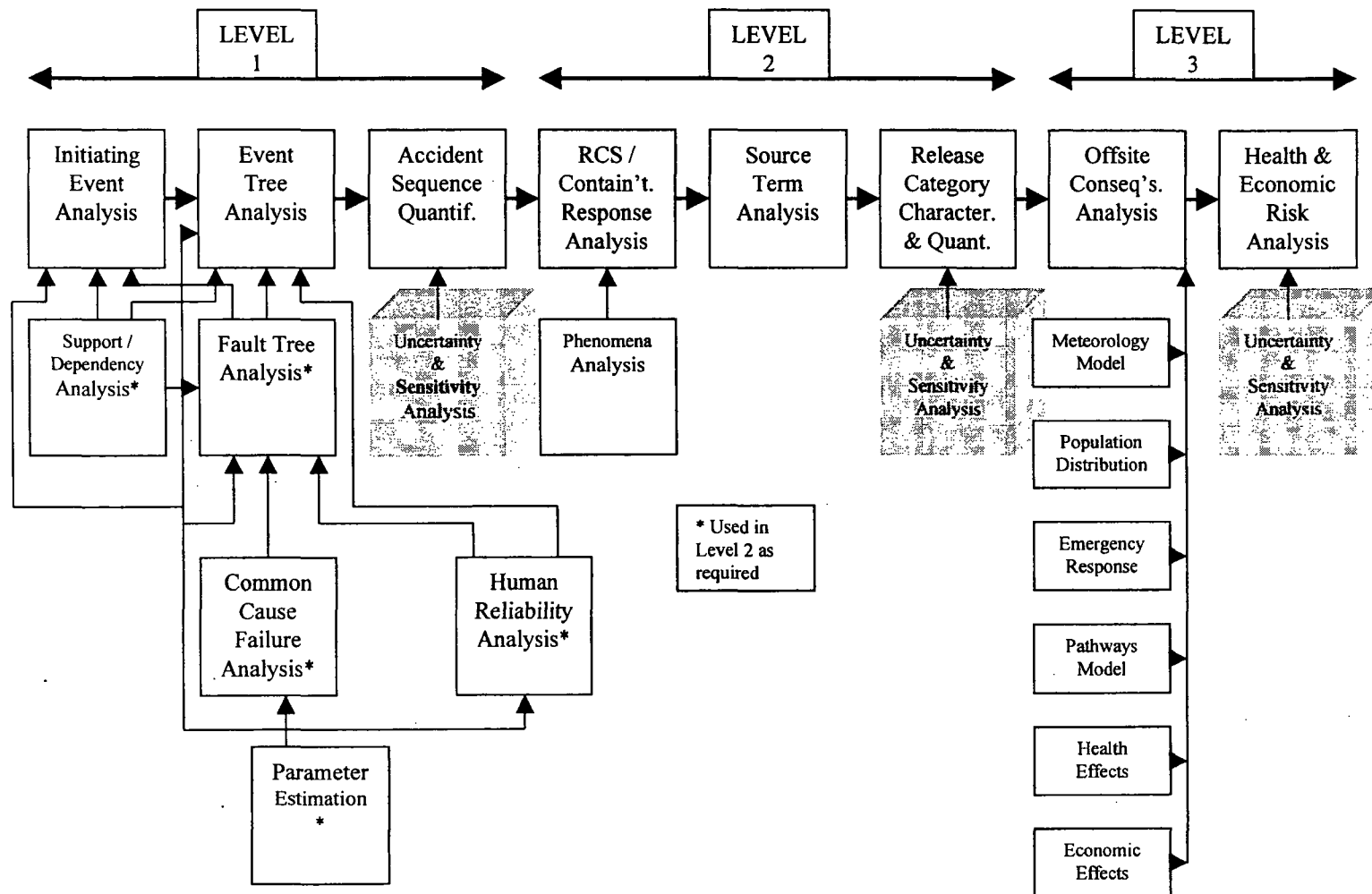


# Uncertainties in PRA

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



# Principal Steps in PRA





# Uncertainty

- Historically, the term “uncertainty” has been used to describe either of the following concepts:
  - random variability in some observable quantity
  - imprecision in state-of-knowledge regarding models, their parameters, their assumptions, and how well they reflect reality

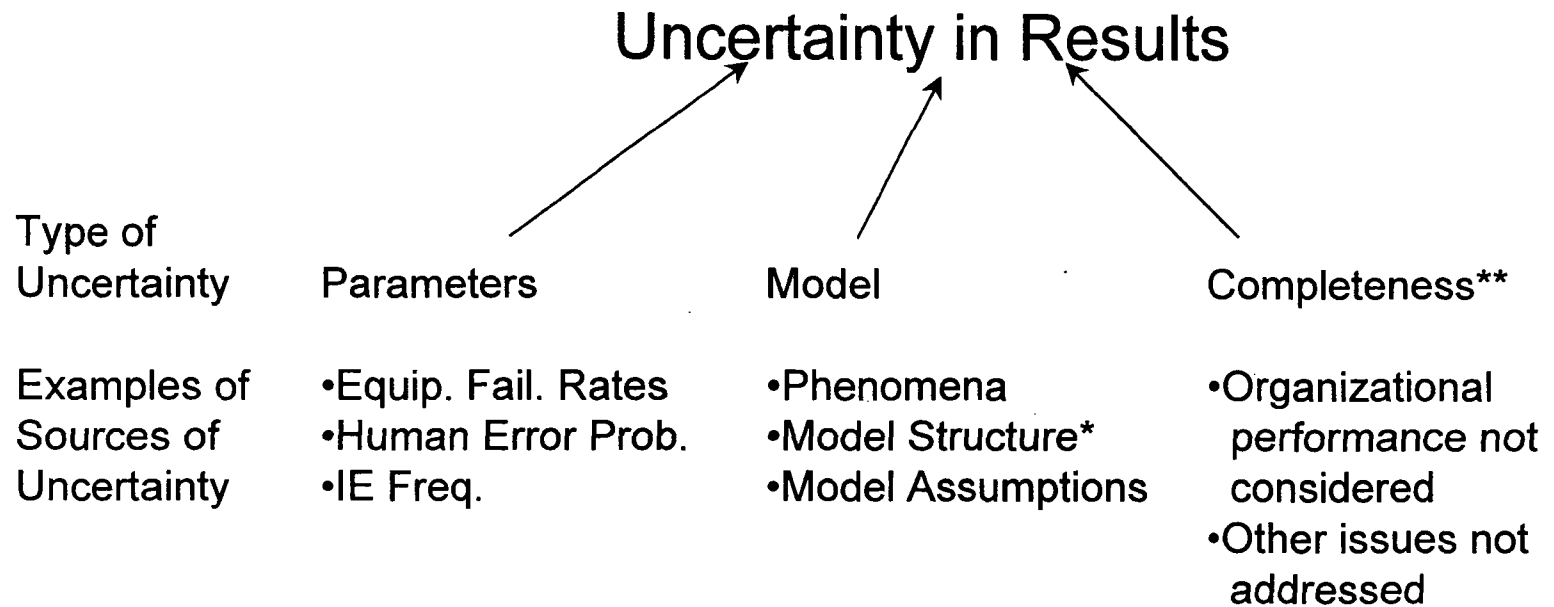


# Uncertainty arises from many sources

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



# Sources of Uncertainty



\* Model is approximation of reality; some model structures cause greater uncertainty in results than others

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



# Traditional Engineering Approaches to Uncertainty

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



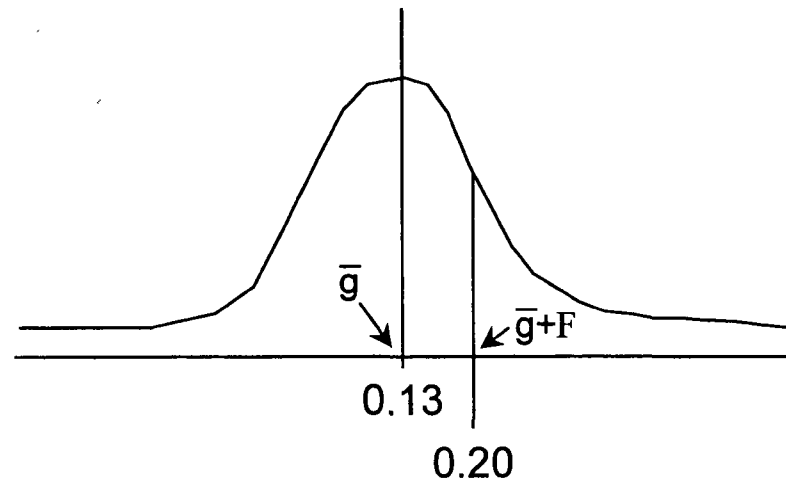
# SEISMIC EXAMPLE

## (Hope Creek FSAR Chapter 2)

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



# Seismic Example (cont.)



Acceleration (g)



# ANOTHER CHAPTER 2 (SITING) EXAMPLE

- ❖ Plume dispersion depends on time-varying parameters, limiting predictability of radionuclide concentration and position
- ❖ To overcome this limitation, empirically-based, conservative assumptions are made about how long fumigation and other atmospheric conditions exist (R.G.s 1.3 and 1.4).



# AIRCRAFT HAZARD EXAMPLE

## (Hope Creek FSAR Chapter 3)

- For general aviation small fixed-wing traffic near Hope Creek, following equation has been used (for crash density), because it is difficult to establish exact location--distance from plant and altitude of aircraft when the trouble leading to crash originated

$$\rho = 1/2 \gamma e^{-\gamma/|x|}$$

where:

x = lateral distance (flight path to plant)

$\gamma$  = crash decay rate = 2 mi<sup>-1</sup> for general aviation small fixed-wing aircraft.



# THERMAL-HYDRAULIC EXAMPLE (GESSAR II Chapter 4)

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



# DESCRIPTION OF UNCERTAINTIES

## (GESSAR II Chapter 4)

<u>Quantity</u>	<u>Standard Deviation (% of point)</u>	<u>Comment</u>
Feedwater Flow	1.76	This is the largest component of total reactor power uncertainty
Feedwater Temperature	0.76	These are the other significant parameters in core power distribution
Reactor Pressure	0.5	
Core Inlet Temperature	0.2	Affect quality and boiling length. Flow is not measured directly, but is calculated from jet pump $\Delta P$ . The listed uncertainty in flow corresponds to 11.2% standard deviation in each individual pump difference
Core Total Flow		



# Examples from GESSAR II Chapter 4 (Cont.)

<u>Quantity</u>	<u>Standard Deviation (% of point)</u>	<u>Comment</u>
Channel Flow Area	2.5	This accounts for manufacturing and service induced variations in the free flow area within the channel
Friction Factor Multiplier	10.0	Accounts for uncertainty in the correlation representing two-phase pressure losses



# PRAAs Identify Two Types of Uncertainty

- Random variability
- State-of-knowledge uncertainty



# Random Variability

- ☞ Variability in or lack of precise knowledge about underlying conditions makes events unpredictable. Such events are modeled as being probabilistic in nature (e.g., initiating events treated like radioactive decay). In PRAs, these include initiating events, component failures, and human errors.
- ☞ Models characterized by parameters values (e.g., initiating event frequency)



# State-of-Knowledge Uncertainty

Parameter values not known precisely

- ✱ Could model uncertainty in parameter values using statistical confidence intervals
  - ☹ Can't propagate confidence intervals through PRA models
  - ☹ Can't interpret confidence intervals as probability statements
- ✱ PRAs model lack of knowledge about parameter values by assigning (usually subjectively) a probability distribution to each parameter



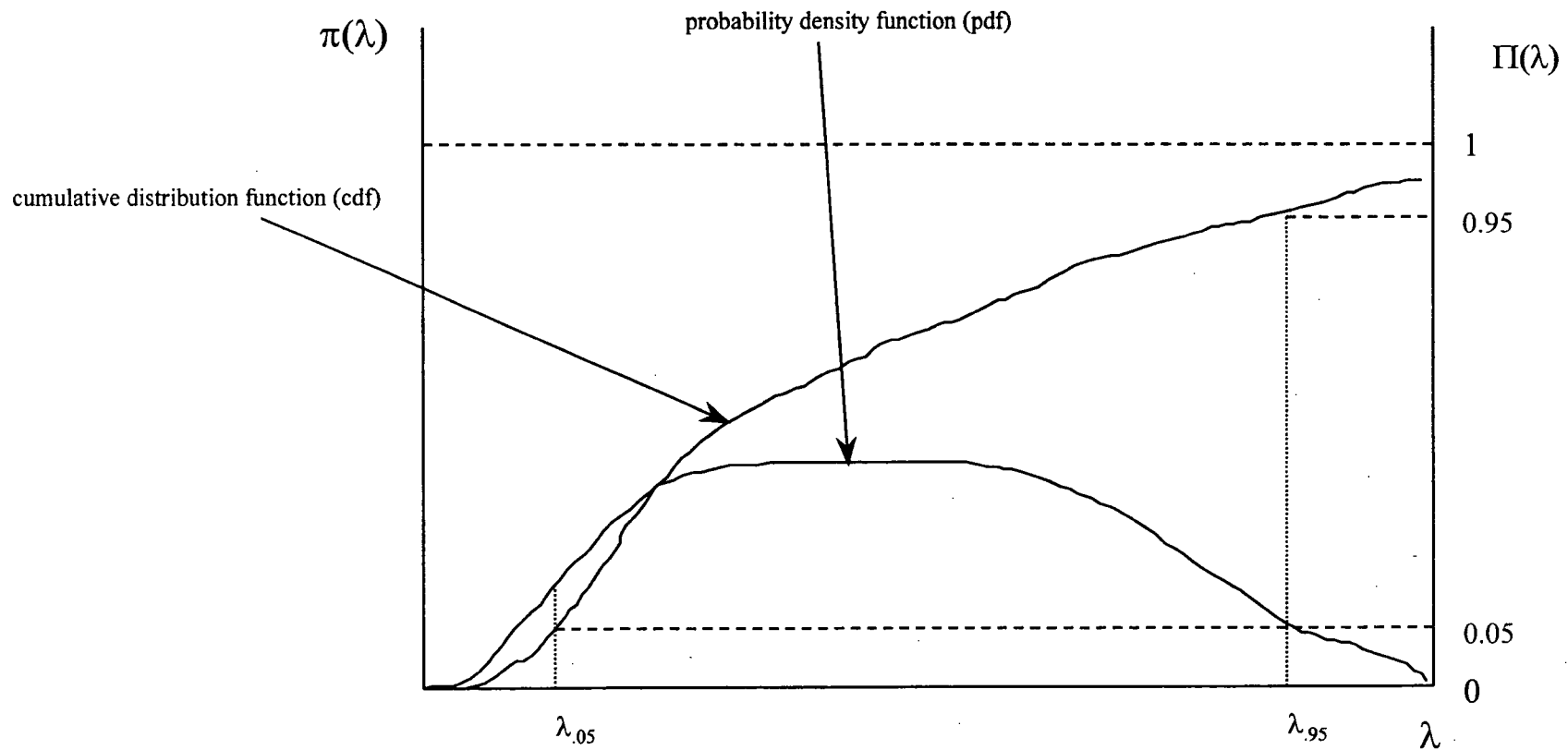
# State-of-Knowledge Uncertainty (cont.)

## Advantages to Bayesian Approach

- ☺ Allows uncertainties to be propagated easily through PRA models
- ☺ Allows probability statements to be made concerning parameter values and outputs that depend upon these values
- ☺ Provides unified, consistent framework for parameter estimation



# Uncertainty in $\lambda$ Expressed as Probability Distribution





# Uncertainty Propagation

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



# Nonparametric Uncertainties in PRA

## ■ Modeling uncertainty

- System success criteria
- Accident progression phenomenology
- Health effects models (linear vs. nonlinear, threshold vs. nonthreshold dose-response model)



# Nonparametric Uncertainties in PRA (cont.)

## ■ Completeness

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



# Nonparametric Uncertainties in PRA (cont.)

## ■ Errors in analysis

- Failure to model all trains of a system
- Data input errors
- Analysis errors



# Addressing Nonparametric PRA Uncertainties

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



# MODULE P

## Plant-Specific, Risk-Informed Applications



# Plant-Specific, Risk-Informed Applications

- ❖ **Purpose:** This section introduces students to the NRC Policy Statement on uses of PRA, the PRA Implementation Plan, the Risk-Informed Regulation Implementation Plan, the Regulatory Guides for PRA application, and the accompanying Standard Review Plans.
- ❖ **Objective:**
  - ▶ Describe the objectives of the PRA Policy Plan and the scope of the Implementation Plan for the various NRC offices affected.
  - ▶ List the major elements of the decision logic used to review submittals containing changes to the current licensing basis and the role of the new Regulatory Guides and SRPs in this process, including the numerical decision criteria related to CDF and LERF.



# Overview

- ◆ Background
- ◆ PRA Policy Statement
- ◆ PRA Implementation Plan/Risk-Informed Regulation  
Implementation Plan
- ◆ Risk-Informed Regulation
- ◆ Objectives of Risk-Informed Regulation
- ◆ Available Regulatory Guides and SRPs
- ◆ Change Processes
- ◆ Principles of Risk-Informed Regulation
- ◆ Expectations
- ◆ Acceptance Guidelines



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

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



# Background

## ❧ PRA Policy Statement

- ⊕ Agency-wide policy statement on the proposed uses of PRA
- ⊕ Broadest application to power reactors

## ❧ Risk-Informed Regulation Implementation Plan, formerly known as PRA Implementation Plan

- ⊕ Provides necessary interoffice management framework
- ⊕ Implementation ongoing - plan is a “living “ document
- ⊕ Approximately semi-annual progress reports to Commission



# *PRA Policy Statement*

## ❖ General Objectives

- ★ Improve regulatory decision-making and, therefore, safety
- ★ Make more efficient use of Staff resources
- ★ Reduce unnecessary regulatory burden on industry



# PRA Policy Statement (cont.)

- ✦ Use of PRA technology should be **increased in all Regulatory matters** to the extent supported by state-of-the-art in PRA methods and data and **in a manner that complements the NRC's deterministic approach** and **supports the NRC's traditional defense-in-depth philosophy**
- ✦ PRA and associated analyses should be used in Regulatory matters, where practical within the bounds of state-of-the-art, **to reduce unnecessary conservatism** associated with current Regulatory requirements, Regulatory guides, License commitments, and staff practices. Where appropriate, PRA should be used to **support the proposal for additional Regulatory requirements** in accordance with 10 CFR 50.109 (Backfit Rule). **The existing rules and regulations shall be complied with unless these rules and regulations are revised.**



# PRA Policy Statement (cont.)

- ❑ PRA evaluations in support of Regulatory decisions should be as **realistic as practicable** and appropriate supporting data should be publicly available for review.
- ❑ The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used **with appropriate consideration of uncertainties** in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.



# PRA Implementation Plan - Overall Objectives and Scope

- ❖ Agency-wide plan to implement PRA Policy Statement
- ❖ Included on-going and new PRA-related activities
  - ▶ e.g., maintenance rule, IPE program, generic safety issues
- ❖ Provided mechanisms for monitoring programs and management oversight
  - ▶ Defined, scheduled, and assigned responsibilities for staff activities needed to accomplish goals of PRA Policy Statement
- ❖ Encompassed activities in NRR, RES, former AEOD, and NMSS
- ❖ Informed Commission of staff progress via quarterly updates and briefings



# Risk-Informed Regulation Implementation Plan - Overall Objectives and Scope

- ❖ Organized to track three principal arenas in Agency's Strategic Plan: Nuclear Reactor Safety, Nuclear Materials Safety, and Nuclear Waste Safety.
- ❖ Provide clear objectives and linkages to PRA Policy Statement and to Agency's Strategic Plan.
- ❖ Identify criteria for the selection and prioritization of practices and policies to be risk-informed and guidelines for implementation
- ❖ Identify major pieces of work associated with these efforts and related major milestones, including plans for communicating information to stakeholders
- ❖ Informs Commission of staff progress via semi-annual updates and briefings



# Risk-Informed Regulation

- ❖ Insights derived from probabilistic risk assessments are used in combination with traditional engineering analyses to focus licensee and regulatory attention on issues commensurate with their importance to safety.
- ❖ Implementation can be by various means:
  - ▶ Prescriptive (e.g., design feature, program elements)
  - ▶ Performance-oriented (e.g., maintenance rule, Performance Indicators)
  - ▶ Risk-oriented (e.g., R.G. 1.174)

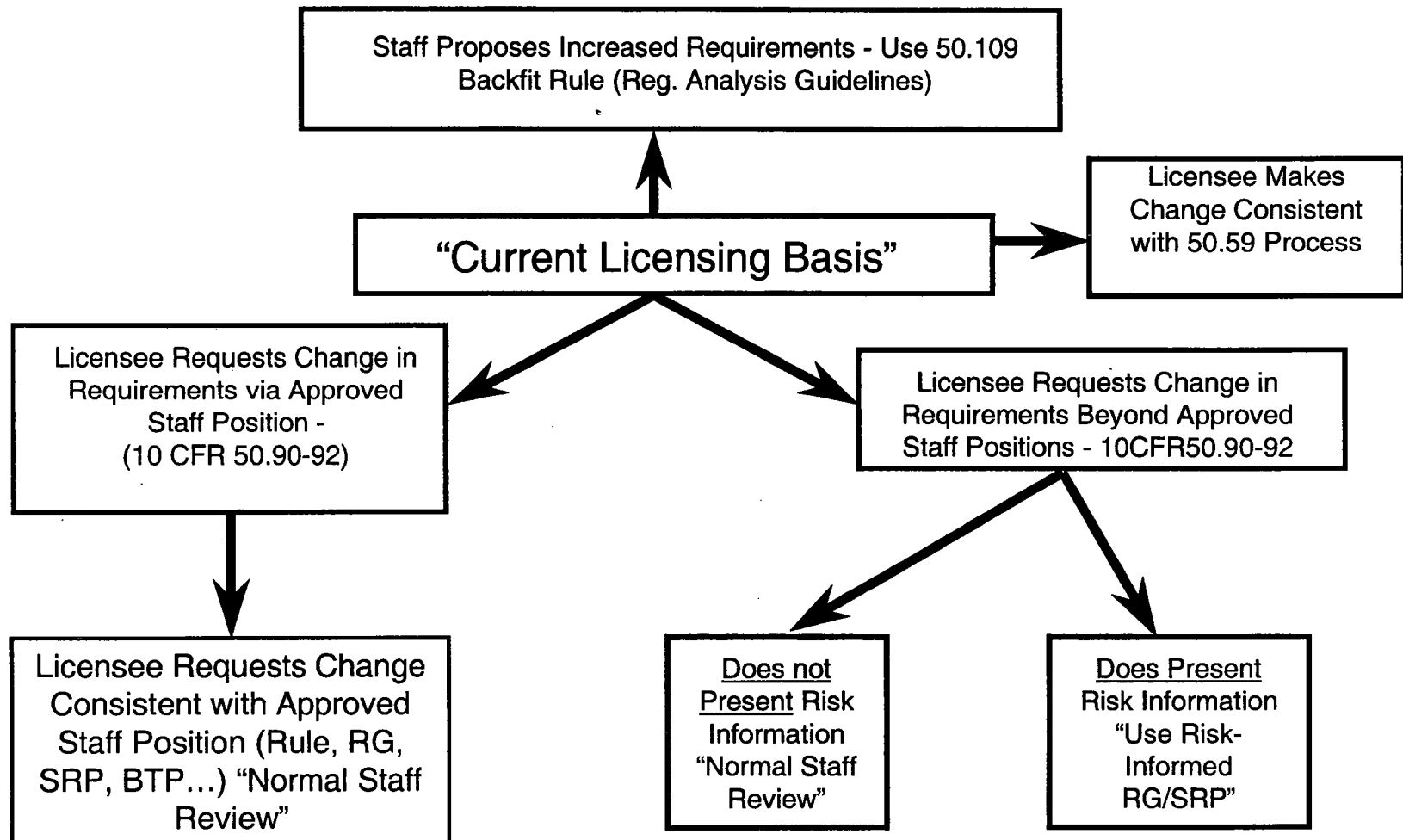


# Risk-Informed Regulatory Guides and SRPs

- ❖ R. G. 1.174 - General guidance to licensees
- ❖ R.G.-1.175 - Application-specific guidance on in-service testing
- ❖ R.G. – 1.176 - Application-specific guidance on graded quality assurance
- ❖ R.G. – 1.177 - Application-specific guidance on technical specifications
- ❖ R.G. – 1.178 - Application-specific guidance on in-service inspection
- ❖ SRP Chapter 19 - General guidance to staff
- ❖ SRP Section 3.9.7 - Application-specific guidance on IST
- ❖ Inspection guidance
- ❖ SRP Section 16.1 - Application-specific guidance on technical specifications
- ❖ SRP Section 3.9.8 - Application-specific guidance on ISI

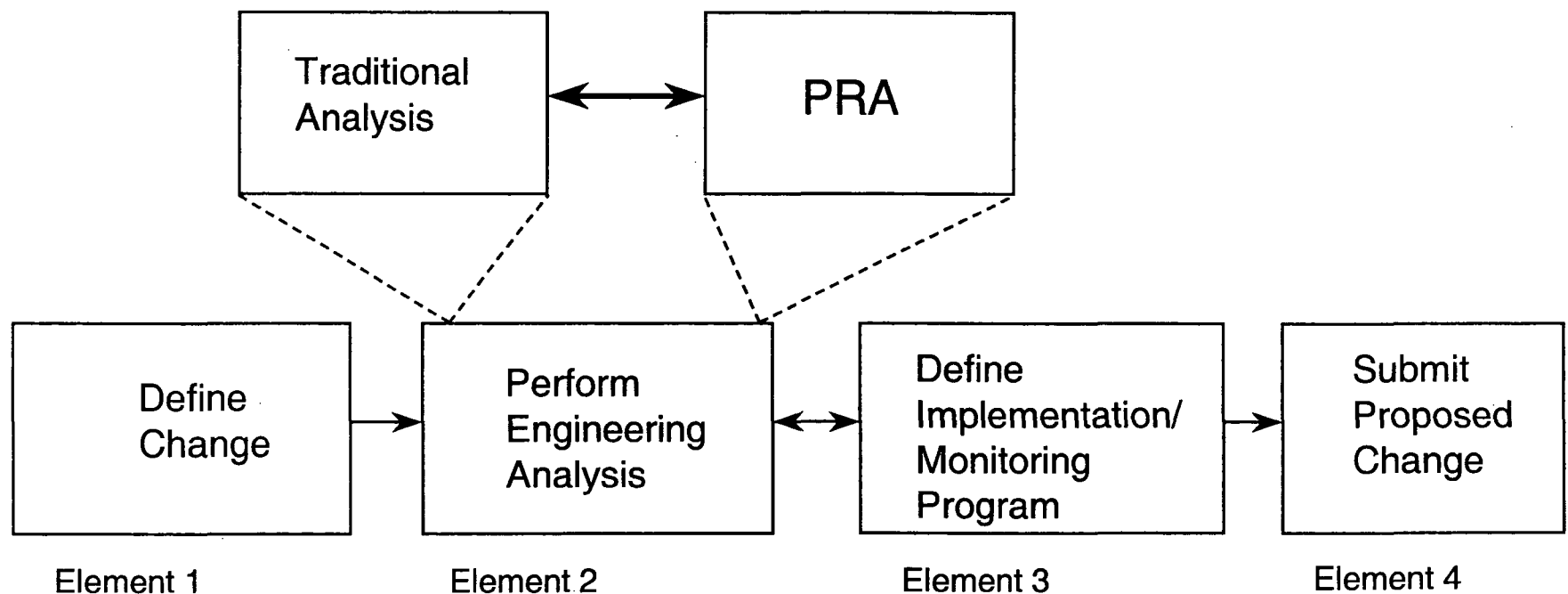


# Decision Logic for Submittal Reviews





# Principal Steps in Risk-Informed Plant-Specific Decision-Making





# Principles of Risk-Informed Regulation

- ❖ The proposed change meets current regulations unless it is explicitly related to a requested exemption or rule change
- ❖ The proposed change is consistent with the defense-in-depth philosophy
- ❖ The proposed change maintains sufficient safety margins
- ❖ Proposed increases in core damage frequency and risk are small and are consistent with the intent of the Commission's Safety Goal Policy Statement
- ❖ The impact of the proposed change should be monitored using performance measurement strategies



# Expectations from Risk-Informed Regulation (from RG-1.174)

- ❖ All safety impacts of the proposed change are evaluated in an integrated manner as part of an overall risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions broadly by identifying and taking advantage of opportunities for reducing risk, and not just to eliminate requirements the licensee sees as undesirable. For those cases where risk increases are proposed, the benefits should be described and should clearly outweigh the proposed risk increases. The approach used to identify changes in requirements should be used to identify areas where requirements should be increased, as well as where they could be reduced.



# Expectations from Risk-Informed Regulation (cont.)

- ❖ Acceptability of proposed changes should be evaluated by the licensee in an integrated fashion that ensures that all principles are met
- ❖ The use of core damage frequency (CDF) and large early release frequency (LERF) as bases for probabilistic risk assessment acceptance guidelines is an acceptable approach. Use of the Commission's Safety Goal Quantitative Health Objectives (QHOs) for this purpose is acceptable in principle and licensees may propose their use; however, in practice, implementing such an approach would require careful attention to the methods and assumptions used in the analysis, and treatment of uncertainties.



# Expectations from Risk-Informed Regulation (cont.)

- ❖ Increases in estimated CDF and LERF resulting from proposed changes will be limited to small increments and the cumulative effect of such changes should be tracked
- ❖ The scope and quality of the engineering analyses (including traditional and probabilistic analyses) conducted to justify the proposed change should be appropriate for the nature and scope of the change and should be based on the as-built and as-operated and maintained plant, including reflection of operating experience at the plant
- ❖ Appropriate consideration of uncertainty is given in analyses and interpretation of findings
- ❖ A program of monitoring, feedback, and corrective action should be used to address significant uncertainties



# Expectations from Risk-Informed Regulation (cont.)

- ❖ The plant-specific PRA supporting licensee proposals has been subjected to quality controls such as an independent peer review or certification
  - ▶ Note: Owner's groups have been conducting PRA reviews
- ❖ Data, methods, and assessment criteria used to support regulatory decision-making must be scrutable and available for public review



# Acceptance Guidelines

- ❖ Defense-in-depth is maintained
  - A reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved
  - Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided
  - System redundancy, independence, and diversity are preserved commensurate with the expected frequency and consequences of challenges to the system (e.g., no risk outliers)
  - Defenses against potential common-cause failures are preserved and the potential for introduction of new common-cause failure mechanisms is assessed



# Acceptance Guidelines (cont.)

- ❖ Defense-in-depth is maintained (cont.)
  - ▶ Independence of barriers is not degraded
  - ▶ Defenses against human errors are preserved
  - ▶ The intent of the General Design Criteria in 10 CFR 50, App. A, are maintained
- ❖ Sufficient safety margins are maintained
  - ▶ Codes and standards or alternatives approved for use by the NRC are met
  - ▶ Safety analysis acceptance criteria in the licensing basis (e.g., FSAR, supporting analyses) are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty

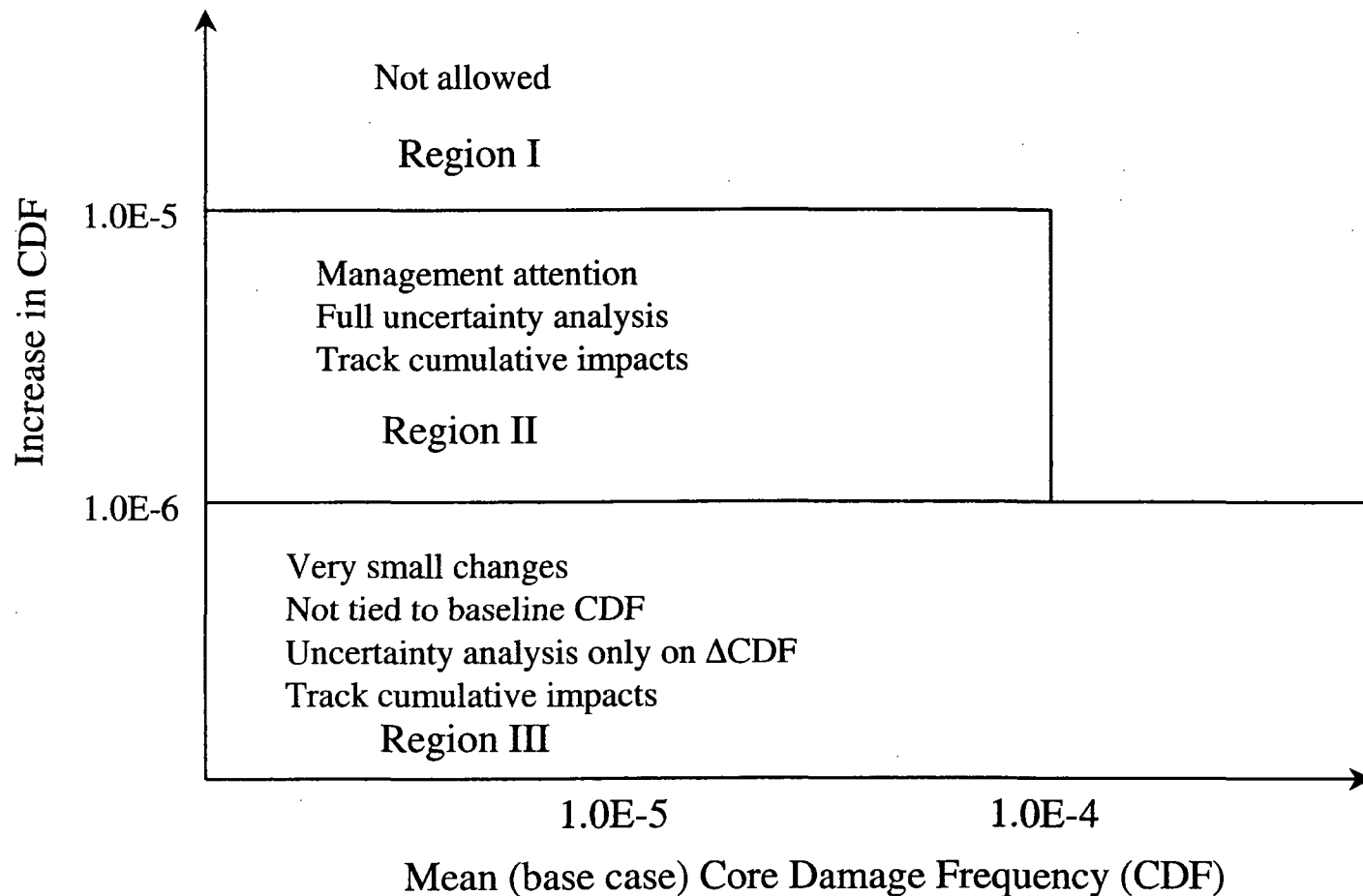


# Acceptance Guidelines (cont.)

- ❖ Risk guidelines on following slides are met
  - ▶ Risk guidelines are intended for comparison with full-scope PRA results
    - \* Internal events (full power, low-power/shutdown)
    - \* External events (seismic, fire, etc.)
    - \* Use of less than full scope PRA may be acceptable in certain circumstances

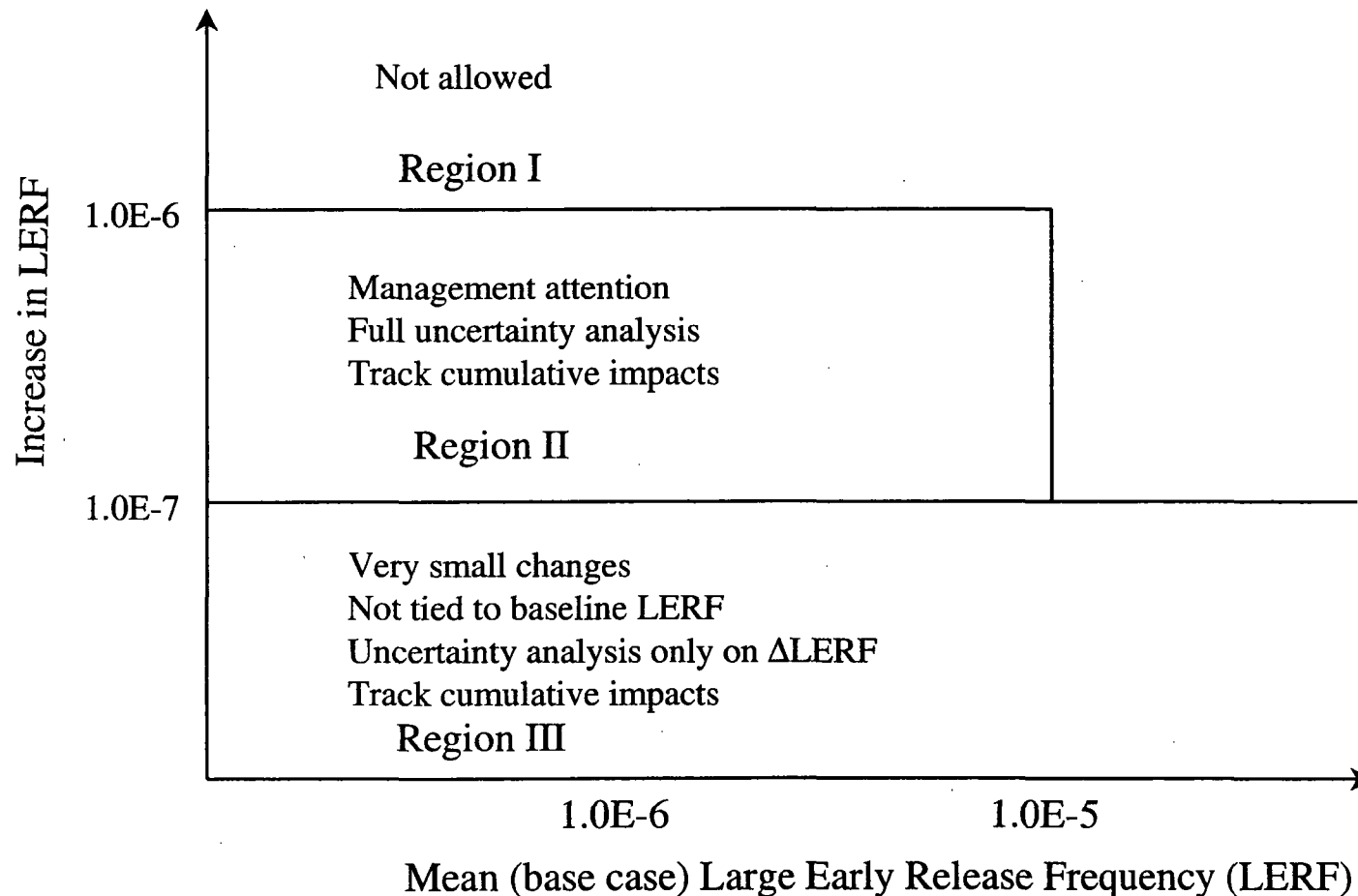


# Mean Core Damage Frequency Acceptance Guidelines (RG 1.174)





# Mean Large Early Release Frequency Acceptance Guidelines (RG 1.174)





# Increased Management Attention

- ❖ Application is given increased NRC management attention when the calculated values of the changes in the risk metrics, and their baseline values when appropriate, approach the guidelines. The issues addressed by management will include
  - ▶ Cumulative impact of previous changes and trend in CDF and LERF (licensee's risk management approach)
  - ▶ Impact of proposed change on operations complexity, burden on operating staff, and overall safety practices
  - ▶ Benefit of the change with respect to its risk increase
  - ▶ Level 3 PRA information, if available



# Consideration of Uncertainties

- ❖ Use mean values (not median) of CDF and LERF used for comparison with guidelines
- ❖ Identify important sources of uncertainty
  - ▶ Parameter
  - ▶ Modeling
  - ▶ Completeness
- ❖ Perform sensitivity calculations on parameter and modeling uncertainties
- ❖ Perform quantitative or qualitative analysis on completeness uncertainties
- ❖ Results of sensitivity studies should generally meet guidelines
- ❖ Region III - no need to calculate uncertainty on baseline CDF/LERF



# Combined Change Requests

- ❖ Several changes can be combined in one submittal
- ❖ Will be reviewed against acceptance guidelines
  - ▶ Individually with respect to defense in depth
  - ▶ Cumulatively
- ❖ Combined changes should be related. For example
  - ▶ Be associated with same system, function, or activity
  - ▶ Changes reviewed individually against risk criteria if not closely related
- ❖ Combined changes should not trade many small risk decreases for a large risk increase (i.e., create a new significant contributor to risk)



# Key Issues in PRA Quality

- ❖ Ensure that, within scope, PRA analysis is complete and has appropriate level of detail
  - ▶ Consideration of relevant initiating events, plant systems, and operator actions
  - ▶ Analysis reflects plant-specific operating experience, design features, and accident response
  - ▶ All calculations are documented
- ❖ PRA methodology and associated input
  - ▶ Influence of models, input data, and assumptions on results and conclusions
- ❖ Licensee review and QA process
  - ▶ Peer review
  - ▶ Certification
  - ▶ Standards (e.g., new ASME and ANS standards)



# NRC Staff and Management Responsibilities

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



# Module Q

## Configuration Risk Management



# Configuration Risk Management

- Purpose: To acquaint students with the basic concepts of using PRA models to control configuration risk by planning maintenance.
- Objectives:
  - ❖ Explain why base case or nominal PRA results cannot be used for maintenance planning
  - ❖ Explain what is meant by “configuration risk management” and how it related to risk-informed regulation
  - ❖ Evaluate “risk” profiles quantitatively
- Reference: NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications



# Configuration Risk Management

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



# Configuration Risk Management

## Why an Issue?

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



# Configuration Risk Management

## Why an Issue?

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

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



# Observed Preventive Maintenance Practices of Concern

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



# Configuration Risk Management

## Traditional Approaches

- Technical Specifications and Limiting Conditions for Operation
  - ❖ Identifies systems/components important to safety based on traditional engineering approach
  - ❖ Limit component out-of-service times for individual and combinations of component outages (not based on formal risk analysis)
- Maintenance planning guidelines such as 12-week rolling schedule, etc.
  - ❖ Based on train protection concept and Technical Specifications
  - ❖ Provide guidance to work week planners on allowable maintenance/testing
- Operator judgment



# Configuration Risk Management

## Traditional Approaches

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



# Configuration Risk Management

- Configuration risk management: one element of risk-informed regulation
- Can be forward-looking or retrospective
  - ❖ Forward-looking to plan maintenance activities & outage schedules
  - ❖ Retrospective to evaluate risk significance of past plant configurations (e.g., Accident Sequence Precursor analyses)

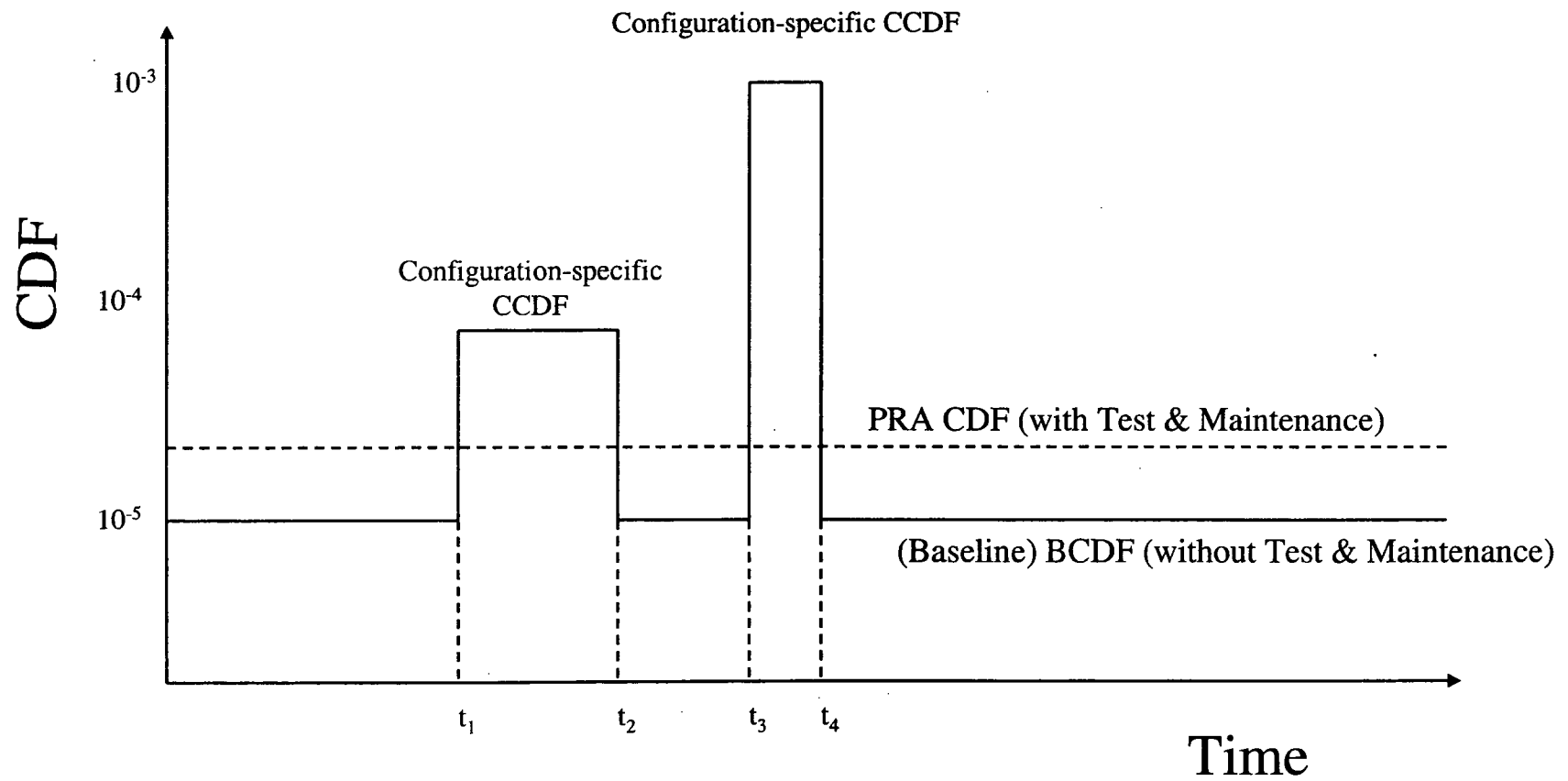


# Configuration Risk Management

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

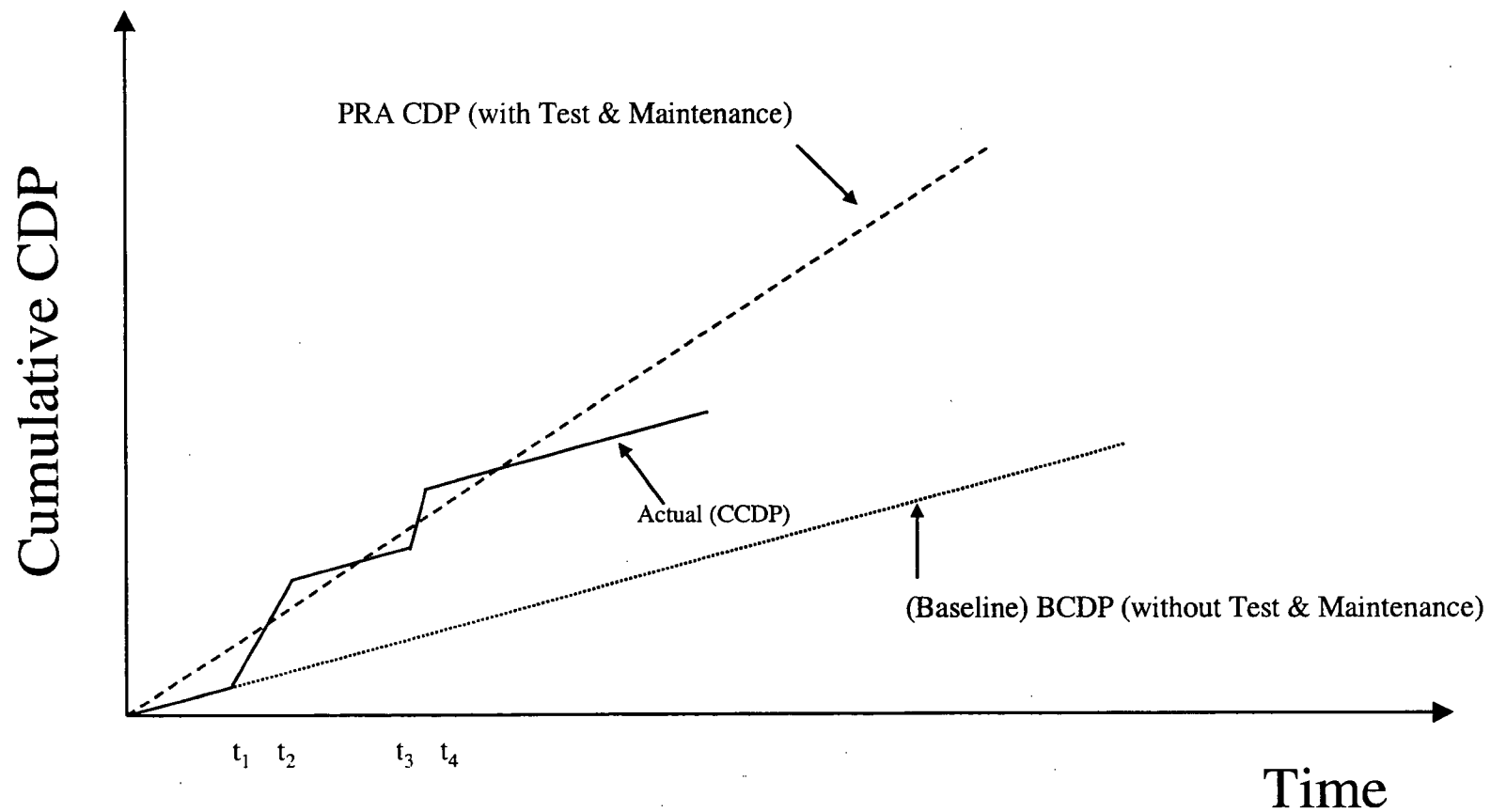


# CDF Profile





# Cumulative CDP Profile





# Configuration Risk Management

## ■ Includes management of:

- ❖ OOS components
  - instantaneous CCDF (configuration-specific CDF)
- ❖ Outage time of components & systems
  - configuration duration
  - CCDF
  - ICDP
- ❖ Backup components
  - instantaneous CCDF
- ❖ Frequency of specific configuration
  - cumulative CCDF over time

*(each of these discussed on the following slides)*



# Managing OOS Components

- Involves scheduling maintenance and tests to avoid having critical combinations of components or systems out of service concurrently
  - ❖ For Maintenance Rule, 10 CFR 50.65, NUMARC 93-01 suggest a ceiling configuration-specific CCDF value of 1E-3/year
    - Subject of such a ceiling value being studied by the NRC
    - NRC endorses the Feb. 22, 2000 revision of section 11 of NUMARC 93-01, but neither endorses nor disapproves the numerical value of 1E-3/year



# Managing Outage Time

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



# Managing Backup Components

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



# Controlling Frequency

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



# Why Configuration Risk Management is Needed...

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



# Preventive Maintenance Risk Calculations

- Risk impact of PM on single component
- Risk impact of maintenance schedule
- Risk impact of scheduling maintenance (power operations versus shutdown)



# Risk Monitors

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



# Current Risk Monitor Software Packages

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



# Requisite Features

- Risk monitor software requires (at a minimum) the following features:
  - ❖ PRA solution engine for analysis of the plant logic model
    - Can be ET/FT, single FT, or cutset equation
  - ❖ Database to manage the various potential plant configurations
    - That is, a library of results for configurations of interest
  - ❖ Plotting program to display results



# Risk Monitor Capabilities

- As a tool for plant operators to evaluate risk based on real-time plant configuration:
  - ❖ Calculates measure of risk for current or planned configurations
  - ❖ Displays maximum time that can be spent in that particular configuration without exceeding pre-defined risk threshold
  - ❖ Provides status of plant systems affected by various test and maintenance activities
  - ❖ Operators can do quick sensitivity studies to evaluate the risk impacts of proposed plant modifications



# Risk Monitor Capabilities (cont.)

- As a tool for plant scheduling for maintenance and outage planning:
  - ❖ Generates time-line that shows graphically the status of plant systems and safety functions
  - ❖ Generates risk profile as plant configuration varies over time
  - ❖ Identifies which components have strongest influence on risk



# Risk Monitor Strengths and Weaknesses

## ■ Risk Monitor Strengths

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



# Risk Monitor Strengths and Weaknesses (cont.)

## ■ Risk Monitor Limitations

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



# Risk Monitor Strengths and Weaknesses (cont.)

## ■ Risk Monitor Limitations

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



# Student Exercise

- Review your IPE and identify component out-of-service modeling
  - ❖ What type of outages are modeled?
    - testing
    - preventive maintenance
    - corrective maintenance
  - ❖ Any “special” events that cover multiple, simultaneous component outages?
  - ❖ What are the basis for the component outage probabilities?
    - generic
    - plant-specific
    - time period covered
    - sources for data collection
    - definition of outage duration



# Module R

## Maintenance Rule Implementation



# Maintenance Rule Implementation

- Purpose: To acquaint students with ways in which PRA typically supports licensee implementation of the Maintenance Rule.
- Objectives:
  - ❖ Explain the purposes of the Maintenance Rule and identify areas in which PRA can support the rule's implementation
  - ❖ Explain how performance goals/criteria are established using the "EPRI Method"
- References:
  - ❖ 10CFR50.65, Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
  - ❖ Regulatory Guide 1.160, Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
  - ❖ NUMARC 93-01, Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
  - ❖ EPRI Technical Bulletin 96-11-01, "Monitoring Reliability for the Maintenance Rule"
  - ❖ EPRI Technical Bulletin 97-3-01



# Maintenance Rule Description

- Performance -Based Rule
- Effective July 10, 1996
- “To monitor the effectiveness of maintenance activities...  
For safety-significant plant equipment...  
In order to minimize the likelihood...  
Of failures and events...  
Caused by the lack of effective maintenance.”

(Maintenance Rule Training Handouts)



# Maintenance Rule Description

## ■ Paragraph (a)(1)

- ❖ Monitor performance of “problem” structures, systems, and components (SSCs)
- ❖ Compare performance against goals
- ❖ (a)(1) SSCs

## ■ Paragraph (a)(2)

- ❖ Reduced monitoring for SCCs meeting performance criteria
- ❖ (a)(2) SSCs



# Maintenance Rule Description

## ■ Paragraph (a)(3)

- ❖ Periodically evaluate program
- ❖ Incorporate industry-wide experience
- ❖ Balance SSC unavailability and failures

## ■ Paragraph (a)(4)

- ❖ Assess and manage increase in risk from maintenance activities

## ■ Paragraph (b)

- ❖ Scope of program

Safety-related SSCs

Non-safety-related SSCs

Mitigate accidents or in plant Emergency Operating Procedures (EOPs)

Required for safety-related SSCs to work properly

Can cause a scram or actuation of safety-related SSC



# Maintenance Rule History

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



# Typical Maintenance Rule Implementation

- Combination of traditional engineering analysis and PRA approaches
  - ❖ Reliance on expert panel to make final decisions
- Overall structure is performance-based approach
- Heavy reliance by most utilities on PRA support/information



# PRA Support for Maintenance Rule Implementation

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



# Safety Significance of SSCs

- NUMARC 93-01 recommends use of 3 importance measures
  - ❖ Core damage frequency (CDF) contribution (in top 90% of CDF cut sets)
  - ❖ Risk reduction worth (RRW) ( $\geq 1.005$ )
  - ❖ Risk achievement worth (RAW) ( $\geq 2.0$ )
- SSCs above cut-off levels for each importance measure are candidates for high safety significance
- Expert panel's role is also to consider and compensate for SSCs not in the PRA as well as PRA uncertainties...



# Factors to be Considered in Use of PRA Importance Measures

- ❖ SSC importance vs PRA basic event importance
- ❖ Sequence truncation level used in PRA
- ❖ Core damage frequency importance vs large early release frequency importance
- ❖ Avoid reliance on just one measure of importance



## Some Relevant Statistics - Brunswick IPE

Truncation limit:  $1\text{E-}10/\text{yr}$

CDF:  $6.34\text{E-}6/\text{yr}$

No. basic events: 1543

No. events after truncation: 291

No. events w/ $F-V > 0.001$ : 150

No. events w/ $F-V > 0.005$ : 74

No. events w/ $\text{RAW} > 2$ : 147

### CDF Contribution

No. events in top cutsets

Highest  $F-V$  not included

Highest RAW not included

No. events w/ $F-V > 0.005$  not included

No. events w/ $\text{RAW} > 2$  not included

### Top 90% Cutsets

184

0.00194

33.3

0

36

### Top 99% Cutsets

281

0.000133

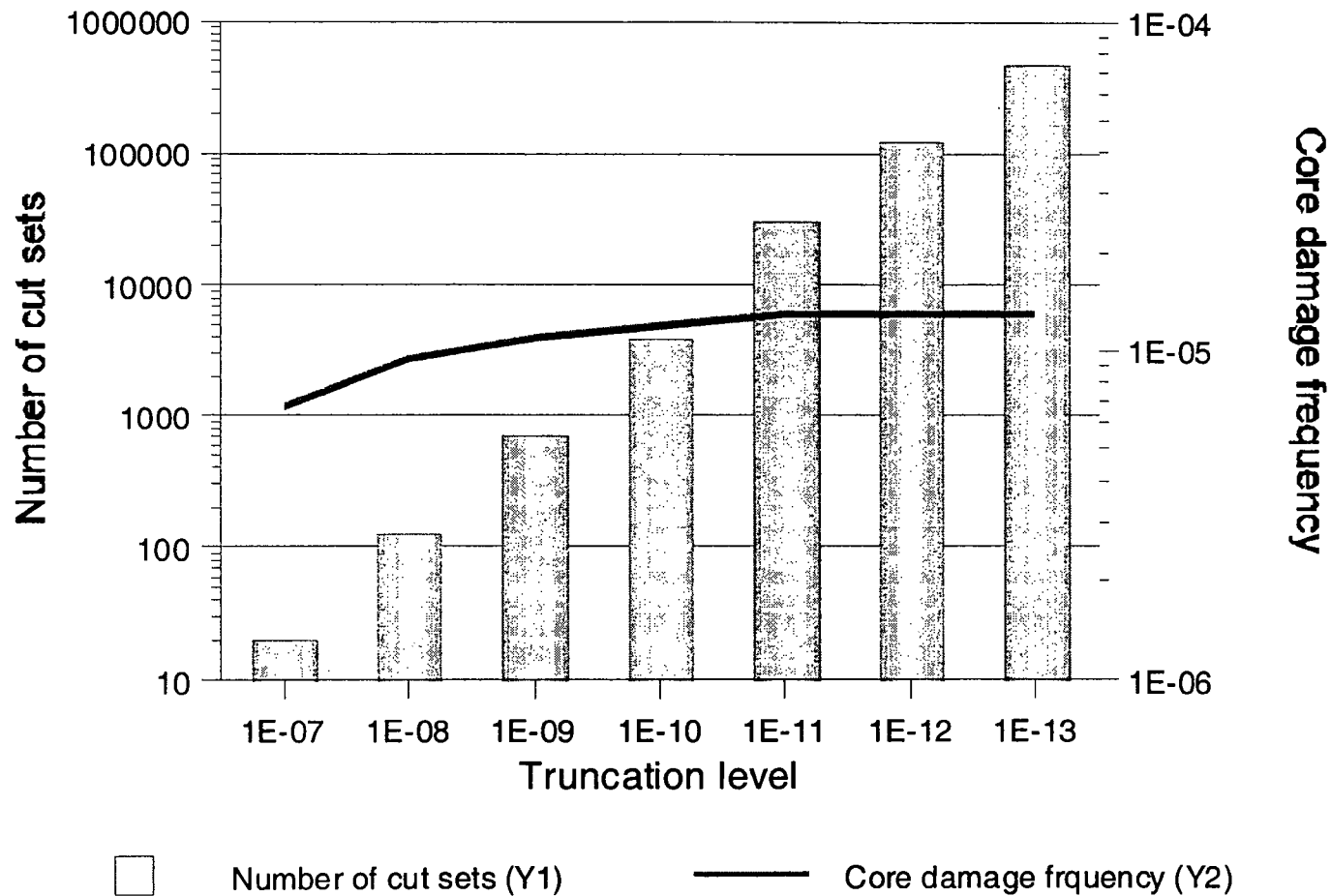
3.67

0

3

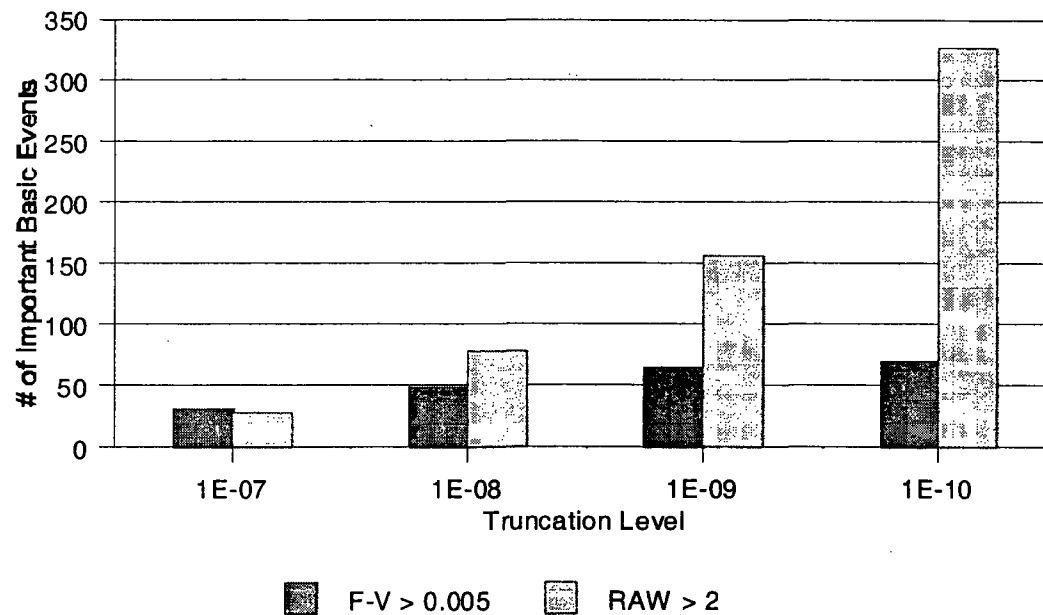


# Core Damage Frequency and Number of Cutsets Sensitive to Truncation Limits





# Truncation Limits Affect Importance Rankings





# SSC Performance Criteria

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



# Unavailability Performance Criteria

## ■ PRA information

- ❖ Plant-specific historical data

Time period covered

- ❖ Generic estimate

## ■ Other information

- ❖ System engineer's experience/judgement

- ❖ Industry-wide experience

## ■ Final choice

- ❖ Plant-specific data

- ❖ 95% of plant-specific data

- ❖ Other



# Unreliability Performance Criteria

## ✓ PRA information

- ❖ Plant-specific historical data

  - Time period covered

- ❖ Generic estimates often used

## ✓ Other information

## ✓ Final Choice

- ❖ Generally 0, 1 or 2 failures over 2- to 3-year period

- ❖ Relation to PRA values

  - Estimated or actual demands over 2- to 3-year period used to evaluate against value in PRA



# Performance Criteria Expected to be Commensurate with Safety

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



# Methods for Establishing Reliability Goals/Criteria

## ■ EPRI method for reliability on demand (EPRI Technical Bulletin 96-11-01)

- ❖ Assume failure probability in PRA/IPE is correct
- ❖ Estimate number of demands over next evaluation period
- ❖ Calculate number of failures, using binomial distribution, such that, if PRA value is correct, there is approximately a 5% chance of seeing more than that number of failures

Example 1: Probability of failure ( $p$ ) = 0.05, 24 demands

$$\Pr(X \leq 2, \text{ given } p = 0.05, n = 24) = 0.88$$

$$\Pr(X \leq 3, \text{ given } p = 0.05, n = 24) = 0.97$$

Therefore, set performance criterion at 2 or fewer failures over next evaluation period



# Methods for Establishing Reliability Goals/Criteria (cont.)

Example 2:  $p = 0.01$ ,  $n = 36$

$$\Pr(X \leq 1, \text{ given } p = 0.01, n = 36) = 0.95$$

Therefore, set performance criterion at 1 or fewer failures over next evaluation period



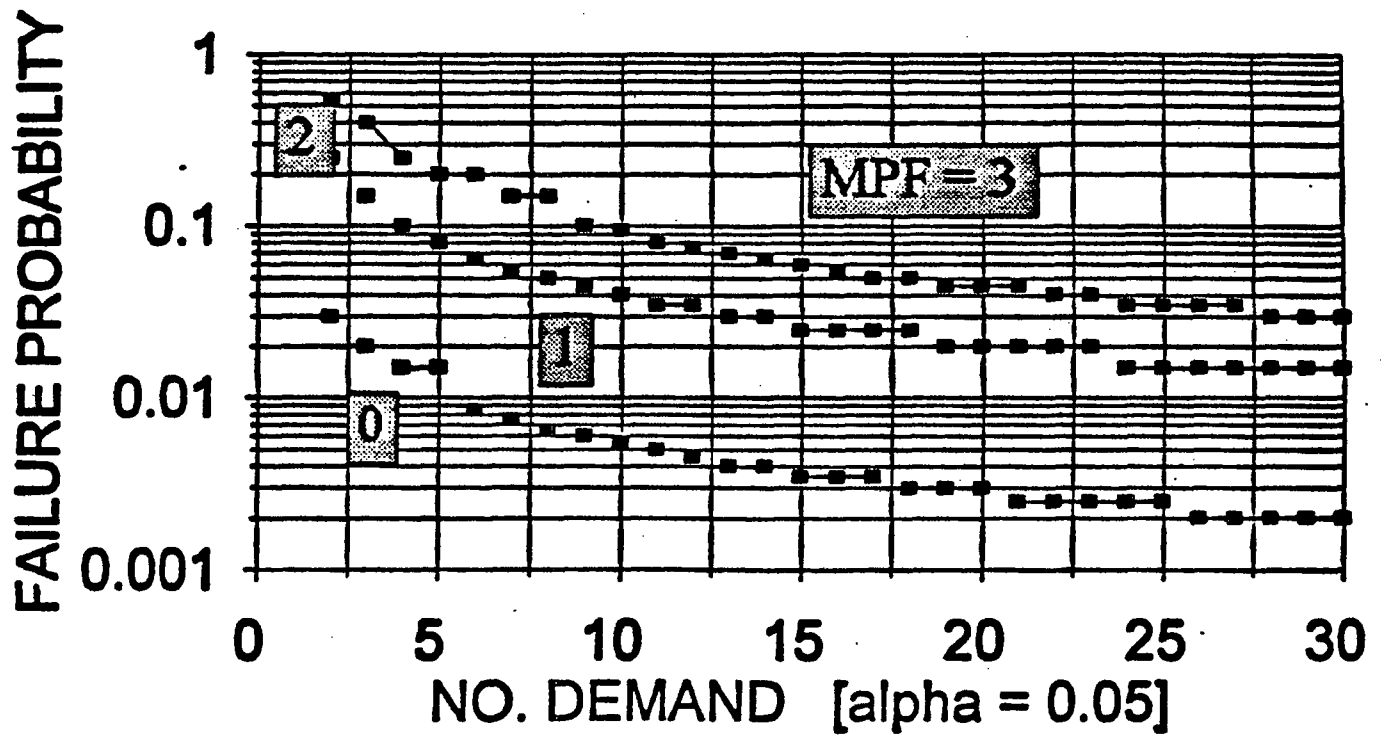




FIGURE 2

# FAILURE-ON-DEMAND

Maintenance Preventable Failure (MPF)



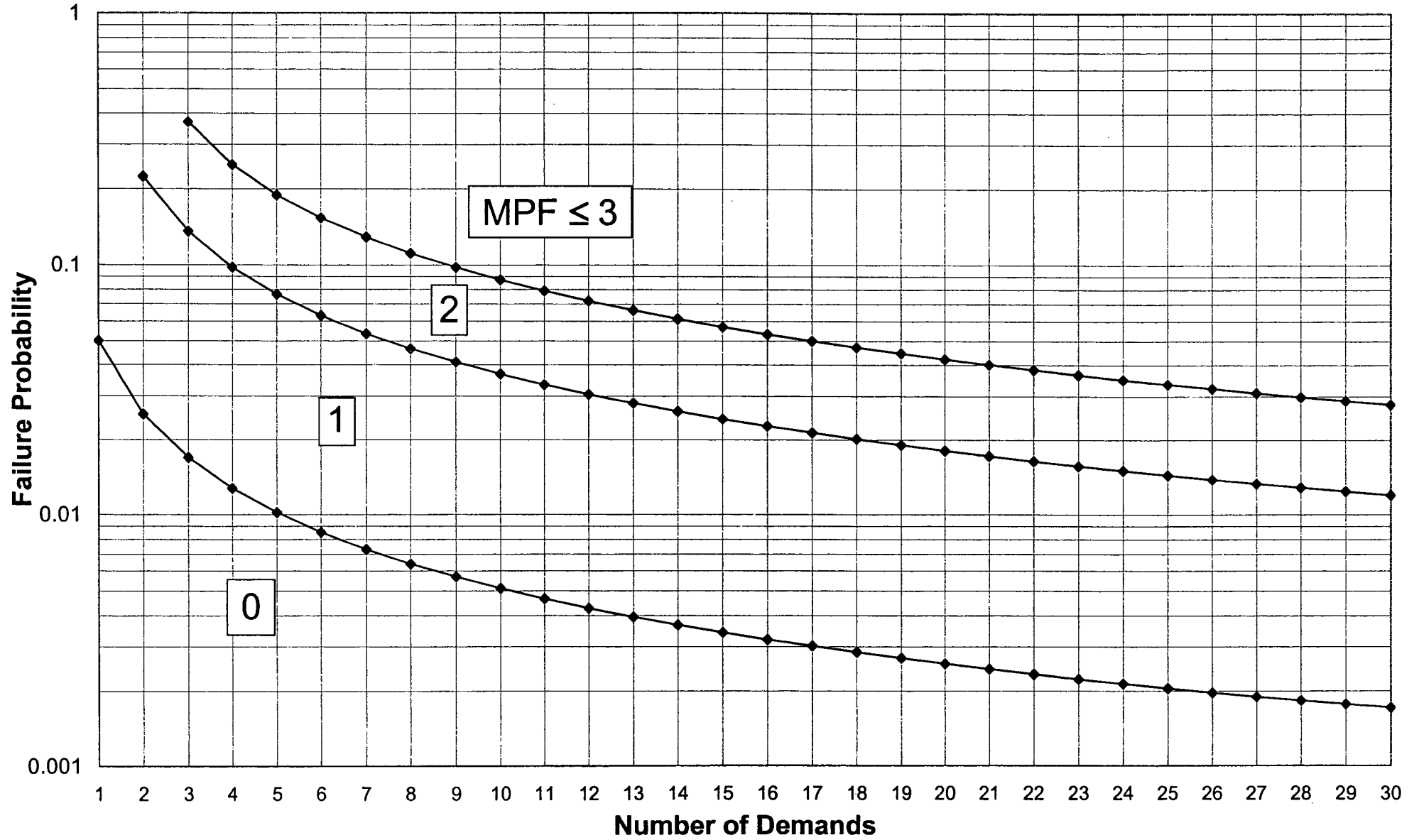






# Failure-on-Demand Curves

## Maintenance-preventable Failures (MPFs)









# Methods for Establishing Reliability Goals/Criteria (cont.)

## ■ EPRI method for reliability of normally running SSCs (EPRI Technical Bulletin 97-3-01)

- ❖ Assume failure rate in PRA/IPE is correct
- ❖ Estimate total running time over next evaluation period
- ❖ Calculate number of failures, using Poisson distribution, such that, if PRA value is correct, there is approximately a 5% chance of seeing more than that number of failures

Example 3: Failure rate ( $\lambda$ ) =  $5 \times 10^{-5}$ /hr,  $t = 10,000$  hrs

$\Pr(X \leq 1, \text{ given } \lambda = 5 \times 10^{-5}/\text{hr}, t = 10,000 \text{ hrs}) = 0.91$

$\Pr(X \leq 2, \text{ given } \lambda = 5 \times 10^{-5}/\text{hr}, t = 10,000 \text{ hrs}) = 0.99$

Conservative approach would be to set criterion at 1 or fewer failures

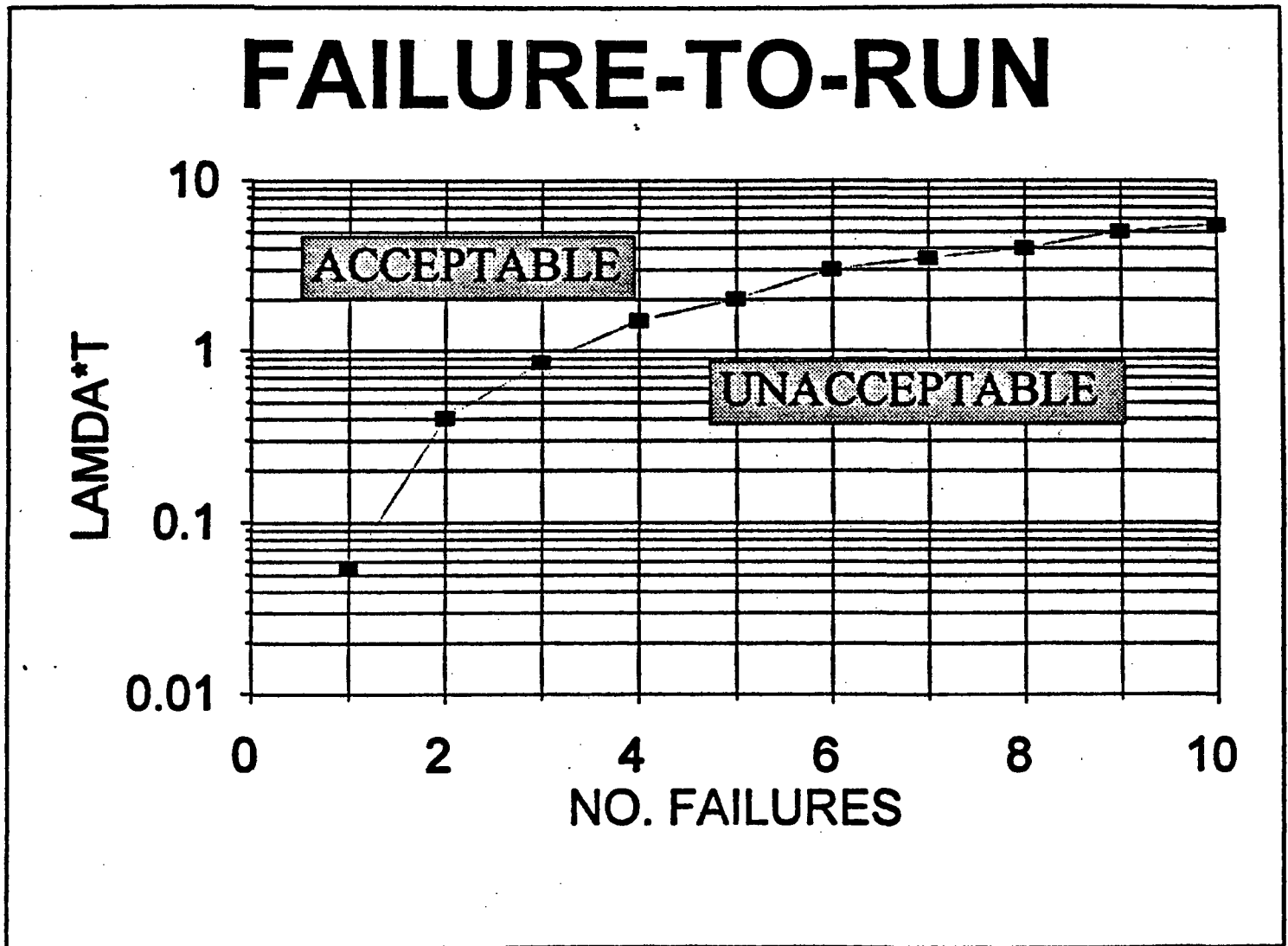
Less conservative, but still probably acceptable criterion would be 2 or fewer failures







FIGURE 3

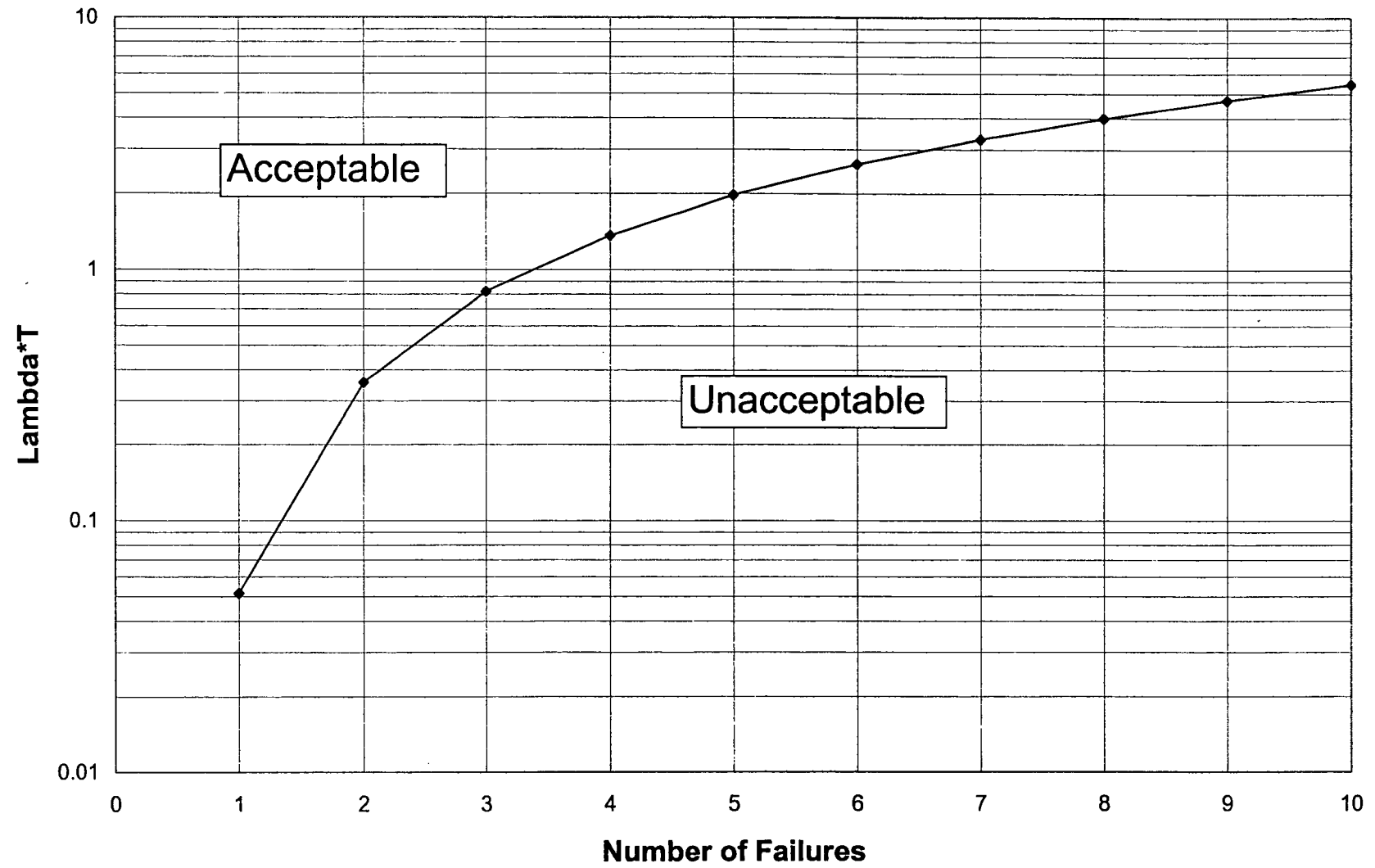








**Failure-to-Run Curve**









# Balancing of Unavailability and Unreliability

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



# Assessing Plant Risk From Maintenance

## ✖ Configuration management

### ❖ Work week schedule guidance

- 12-week rolling schedule

- Days of week schedule for SSCs

- Plant risk matrix or plant status monitor required by Maintenance Rule

- Operator experience/judgment



# Plant Risk Matrix

- Goal-Assess plant risk given all planned/unplanned SSC maintenance outages
- Typically a 2-dimensional matrix covering high safety significance SSC maintenance outages
  - ❖ PRA based
  - ❖ Yes or no for planned outages of 2 SSCs, based on PRA estimate of plant risk
  - ❖ Guidance for 3 or more planned SSC outages
- Consideration of emergent failures



# Plant Risk Matrix

Diesel Generator 1	Diesel Generator 2	HPCI	RCIC	Control Rod Drive Hydraulic
DG1	No	Yes*	Yes*	Yes
	DG2	Yes*	Yes*	Yes
		HPCI	No	No
			RCIC	No

No - High plant risk

Yes - Low plant risk

\* Time limitation applies



# For Additional Information

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



# Module S

## Reactor Safety SDP Principles



# Reactor Safety SDP Principles

- Purpose
  - Describe the purpose of the SDP
  - Describe the tables that are used to perform an SDP
  - Describe how the SDP principles are consistent with PRA principles and practices



# Reactor Safety SDP Principles

- Objectives - Upon completion of this module, students should be able to
  - Describe the PRA basis behind the SDP Tables 1 through 5 in IMC 0609, App. A, Att. 1
  - Describe how these tables are used in the SDP
  - Describe how SDP is consistent with PRA principles and practices
  - Describe basis for shutdown risk checklist in IMC 0609, Appendix G
  - Describe difference between Type A and Type B findings related to containment integrity in IMC 0609, Appendix H



# Significance Determination Process (SDP) Purpose and Objectives

- SDP Purpose
  - Use risk insights, where appropriate, to help NRC inspectors and staff determine the safety significance of findings.
  - SDP determinations for inspection findings and the Performance Indicator (PI) information are combined for use in assessing licensee performance in accordance with guidance provided in IMC 0305, “Operating Reactor Assessment Program.”
- SDP Objectives
  - Characterize significance of inspection findings for the Reactor Oversight Process (ROP), using risk insights as appropriate.
  - Provide all stakeholders an objective and common framework for communicating the potential safety significance of inspection findings.
  - Provide a basis for timely assessment and/or enforcement actions associated with an inspection finding.
  - Provide inspectors with plant-specific risk information for use in risk-informing the inspection program.



# Selection of Initiating Event(s) to Evaluate

- Site specific risk-informed inspection notebook
  - Table 2 - Initiators and System Dependency
    - Affected Systems
    - Major Components
    - Support Systems
    - Initiating Event Scenarios
  - For affected system(s), identify which initiating events need to be evaluated



# Estimating Initiating Event Likelihood During Degraded Period

- PRA uses constant (time-independent) frequencies for various initiating events
- Each core damage sequence starts with initiating event
- CDF for sequence is frequency of initiating event multiplied by probability of failure of mitigating systems and/or operator responses, given initiating event
- Probability of initiating event occurring between  $t_1$  and  $t_2$  is approximately

$$\Pr(IE \text{ between } t_1 \text{ and } t_2) \approx \lambda_{IE} (t_2 - t_1)$$



# Estimating Initiating Event Likelihood During Degraded Period (cont.)

- Site specific risk-informed inspection notebook
  - Table 1 - Categories for Initiating Events
    - Rows in Table 1 correspond to different frequency ranges for different IEs
      - Most frequent IEs at top, least frequent at bottom
      - Row I > 0.1 per year
      - Row II 0.1 – 0.01 per year
      - Row III 0.01 – 0.001 per year, etc.
    - Right hand columns in Table 1 correspond to duration of degraded condition
      - > 30 days (upper bound duration of 1 year)
      - 3 - 30 days (upper bound duration of 0.1 year)
      - < 3 days (upper bound duration of 0.01 year)
    - Estimated initiating event likelihood is product of IE frequency (lower bound) and duration (upper bound) of degraded condition
      - Initiating Event Likelihood =  $-\log_{10}[\text{IE Frequency (lower bound)} * \text{duration}]$
      - Example: An IE with frequency in Row I with an exposure duration of >30 days
        - 0.1 per year (lower bound) \* 1 year (upper bound) = 0.1
        - Initiating Event Likelihood =  $-\log_{10}[0.1] = 1$
      - Note: Each initiating event to be assessed for a finding will use the same duration column, but each assessed IE will have frequency corresponding to its respective row.



# Summary of Estimated Initiating Event Likelihood

- Result from Table 1 represents probability of having IE occur during degraded condition
- $X = -\log_{10}[\text{IE Frequency (lower bound)} * \text{duration (upper bound)}]$ 
  - $1 \leftrightarrow 10^0 \text{ to } 10^{-1}$
  - $2 \leftrightarrow 10^{-1} \text{ to } 10^{-2}$
  - $3 \leftrightarrow 10^{-2} \text{ to } 10^{-3}$
  - $4 \leftrightarrow 10^{-3} \text{ to } 10^{-4}$
  - $5 \leftrightarrow 10^{-4} \text{ to } 10^{-5}$
  - $6 \leftrightarrow 10^{-5} \text{ to } 10^{-6}$
  - $7 \leftrightarrow 10^{-6} \text{ to } 10^{-7}$
  - $8 \leftrightarrow \leq 10^{-7}$



# Summary of Estimated Initiating Event Likelihood (cont.)

- Note the uncertainty in IE frequencies shown in Table 1 (order of magnitude in each row)
- IE frequency will impact final risk significance, can adjust upward (subjectively) if degraded condition can increase IE frequency
  - Examples provided in IMC 0609, App. A, Att. 2



# SDP Worksheets for Initiating Event(s) Evaluation and Remaining Mitigation Capability

- Table 3 site specific risk-informed inspection notebook
  - For IE Scenarios identified in Table 2 – Initiators and System Dependency, complete just the affected Table 3 SDP Worksheet and just the row with the affected function
    - Circle the affected functions in each row
      - Number in parenthesis in each row indicate corresponding sequences with at least those systems indicated (minimal cut set at sequence logic level)
        - » Example: Table 3.XX row 1 TRAN – PCS – CHR – CV (5, 9); on the Transient event tree sequence 5 and 9 represent failures of the indicated systems, with sequence 9 have the indicated systems plus one or more other system failures. Only need to assess contribution from the highest contributing sequence
    - From Table 1 – Categories of Initiating Events, assign the identified initiating event likelihood (IEL) for that IE
    - Assign remaining mitigation capability rating for all other functions in each row that had a circled affected function
    - Assess and assign remaining mitigation capability rating for the circled affected function
      - Example: If LPI function affected in Table 3.XX, IMC 0609, App A, Att 1, but only LPCI mode affected; then the full mitigation capability (LPCI of 3 + LPCS of 3 = 6) for the evaluation would be LPCI of 0 + LPCS of 3 = 3.
    - Assign recovery of affected (failed) train if applicable (see Table 4).
    - Add all assigned values for each circle affected row in Table 3 and enter the result in the Results column (right most column of Table 3)



# Remaining Mitigation Capability

- Table 4 is not site specific.
- Table 4 assigns probabilities of failure to different means of mitigation (systems, operator actions, and recovery of failed systems), based on past PRA experience
  - Recovery of failed train: 0.1
  - One automatic steam-driven (ASD) train: 0.1
  - One train: 0.01
  - One multi-train system: 0.001 (system of two or more trains that are considered susceptible to common cause failures)
  - Two diverse trains: 0.0001 (system of two trains that are not considered susceptible to common cause failures; one train \* one train =  $0.01 * 0.01 = 0.0001$ )
  - Operator action credit:
    - 0.1 (failure probability between 0.5 and 0.05)
    - 0.01 (failure probability between 0.05 and 0.005)
    - 0.001 (failure probability between 0.005 and 0.0005)
- Remaining Mitigation Capability Credit =  $X = -\log_{10}[\text{failure probability}]$ , thus
  - Recovery of failed train: 1
  - One automatic steam-driven (ASD) train: 1
  - One train: 2
  - One multi-train system: 3
  - Two diverse trains: 4
  - Operator action credit: 1, 2, or 3



# Estimation of Risk Significance of Inspection Finding

- Determine final risk significance by completing Table 5 – Counting Rule Worksheet
- For each affected row for each Table 3 SDP Worksheet completed (IE assessed), count the total number of rows with a specific risk significance level equal to;
  - Number of rows with 9 =
  - Number of rows with 8 =
  - Number of rows with 7 =
  - etc. for each significance level to a 4
- Complete Table 5 - Counting Rule Worksheet
  - A “Step” in Table 5 that divides a risk significance level by 3 and rounds down is producing a higher risk significance from contributing lower risk significance; Three sequences of less risk significance are equal to one sequence of greater risk significance
    - Example: Three sequences with risk significance 9 equals one risk significance 8 sequence
- Result of Table 5 – Counting Rule Worksheet indicates risk significance of inspection finding
  - Red – highest safety significance – at least one sequence with a 4 =  $1\text{E-}4$
  - Yellow – at least substantial safety significance – at least one sequence with a 5 =  $1\text{E-}5$
  - White – at least low to moderate safety significance – at least one sequence with a 6 =  $1\text{E-}6$
  - Green – very low safety significance – at least one sequence with a 7 =  $1\text{E-}7$



# Final Risk Significance of Inspection Finding

- Note:
  - Cannot assess impact of degraded equipment reliability
  - SDP set up to analyze conditions that exist for a period of time, not set up for initiating event assessments (IE has occurred)
    - Initiating event assessment results in CCDP “spike,” which is different type of assessment than the SDP assessment
- Note that result of SDP is a probability: the probability of core damage, given a degraded condition of specified duration and probability of an IE during that condition
  - Called conditional core damage probability (CCDP)
- Problems with using CCDP as risk metric
  - PI program uses  $\Delta$ CDF, as does R.G. 1.174
  - NRC has no criteria for using CCDP

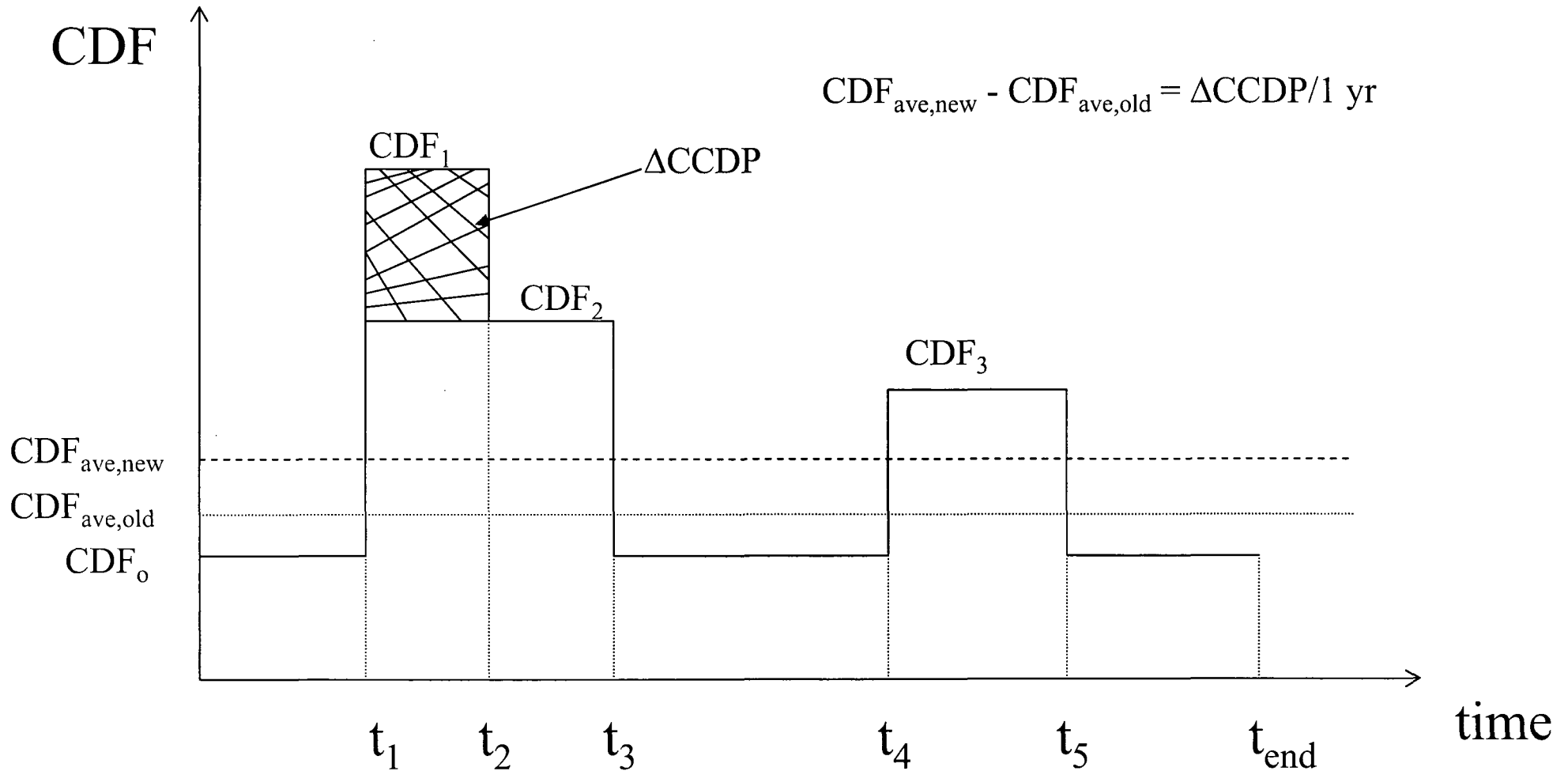


# Final Risk Significance of Inspection Finding (cont.)

- SDP estimates risk significance of licensee performance problems
  - Does not include equipment out of service for test or maintenance, unless related specifically to performance problem
  - Therefore, final result is increase in CCDP, or incremental CCDP, caused by the performance problem (see following graph for illustration)
  - It turns out (see algebra following graph) that, numerically, the incremental CCDP is equal to the increase in the time-weighted average CDF, if the averaging is done for a period of one year
    - So result from SDP can be compared to color criteria for PIs
- What the colors in Table 5 mean in terms of increase in annual time-averaged CDF
  - Red: increase is  $\geq 10^{-4}/\text{yr}$
  - Yellow: increase is between  $10^{-5}/\text{yr}$  and  $10^{-4}/\text{yr}$
  - White: increase is between  $10^{-6}/\text{yr}$  and  $10^{-5}/\text{yr}$
  - Green: increase is  $< 10^{-6}/\text{yr}$



# Illustrative CDF Profile





# Algebra for CDF Profile (optional)

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

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



# Algebra for CDF Profile (cont.)

$$\begin{aligned}
 CDF_{ave,new} - CDF_{ave,old} &= \frac{CDF_1 t_2 - CDF_1 t_1 + CDF_2 t_3 - CDF_2 t_2 - CDF_2 t_3 + CDF_2 t_1}{t_{end}} \\
 &= \frac{CDF_1(t_2 - t_1) - CDF_2(t_2 - t_1)}{t_{end}} = \frac{(CDF_1 - CDF_2)(t_2 - t_1)}{t_{end}} = \frac{\Delta C C D P}{t_{end}}
 \end{aligned}$$

**If  $t_{end} = 1$  yr, then numerically  $\Delta CDF_{ave} = \Delta C C D P$ , as claimed**



# SDP for External Initiators

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



# SDP for External Initiators (cont.)

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



# SDP for Containment Integrity

- IMC 0609, App. H contains Containment Integrity SDP
- Significance criteria for  $\Delta\text{LERF}$  are order of magnitude less than for  $\Delta\text{CDF}$ 
  - Red: increase  $\geq 10^{-5}/\text{yr}$
  - Yellow: increase  $\geq 10^{-6}/\text{yr}$  and  $< 10^{-5}/\text{yr}$
  - White: increase  $\geq 10^{-7}/\text{yr}$  and  $< 10^{-6}/\text{yr}$
  - Green: increase  $< 10^{-7}/\text{yr}$
- Finding that is “Green” for  $\Delta\text{CDF}$  could be “White” for  $\Delta\text{LERF}$



# SDP for Containment Integrity (cont.)

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



# SDP for Containment Integrity (cont.)

- SDP considers two types of findings, Type A and Type B
- Type A findings
  - Findings that affect CDF; CDF SDP performed
  - LERF considerations may adjust final risk significance
  - Use Appendix H
- Type B findings
  - Findings that do not affect CDF; CDF SDP not performed
  - Appendix H, Section 6, Phase 1 and 2 for findings at full power and at shutdown



# Combustion Engineering Owners Group

## Probabilistic Safety Assessment Working Group AOT Pilot Program



# MODULE B

## TRADITIONAL ENGINEERING ANALYSIS AND PRA APPROACHES TO SAFETY ANALYSIS



**Combustion Engineering Owners Group  
Probabilistic Safety Assessment Working Group  
AOT Pilot Program**



## **AOT Pilot Program is a Group Submittal**

- CEOG is the pilot for the 3 proposed AOT changes
- Pilot includes AOT changes to SIT, LPSI, & EDGs
- Utilizes a blended approach:
  - Statement of Need
  - Deterministic Issues
  - Specific plant PRA evaluations (these are compared for consistency/differences & differences are understood as part of the PRA validation process)
  - Where appropriate, contingency/compensatory measures identified
- One single joint application; however individual plant results are evident
- First submitted May 1995; has had multiple reviews and presentations to NRC and ACRS.



# **Safety Injection Tank (SIT)**

## **Technical Specification Change Requested**

- Extend AOT for a single Inoperable SIT from 1 hour (typically) to 24 hours
- NEED:
  - Number of entries into action statements by CE plants
  - Concern over 1 hour AOT has led to unnecessary doses to correct potential malfunctions
  - Change will allow time to diagnose and correct problems at power
  - Should avert unnecessary plant shutdowns (safety and economical impact)
- DETERMINISTIC CONSIDERATIONS:
  - Design Basis calculations are quite conservative; best estimate calcs show do not need 1 LPSI train & 1 HPSI train & all SITs
  - 10CFR100 results also very conservative for a Large LOCA, even without design basis number of SITs



# **Low Pressure Safety Injection (LPSI)**

## **Technical Specification Change Requested**

- Extend AOT for a single Inoperable LPSI train from its present value (24 or 72 hrs depending on the plant) to 7 days (168 hours) [a LPSI train is defined as 1 pump, 2 flow paths including MOVs on a common AC power source]
- NEED:
  - Reduce simultaneous PMs and avoid stress of being near AOT
  - Will allow time for maint./repair/testing of LPSI while at power
  - Avert unnecessary shutdowns with an impaired SDC (LPSI)
- DETERMINISTIC CONSIDERATIONS:
  - LOCA Design Basis calcs are quite conservative; best estimate calcs show do not need 1 LPSI train & 1 HPSI train & all SITs (can be successful without LPSI at all)
  - 10CFR100 results also very conservative for a Large LOCA, no core melt expected even without LPSI using best estimate calcs
  - Can mitigate SGTR w/o SDC by steaming SG, refill CST/use AFW, use cont't. spray for SDC-no release expected if SG isolated



# **Emergency Diesel Generator (EDG) Technical Specification Change Requested**

- Extend AOT for a single Inoperable EDG from 72 hours to 10 days (for most plants)
- NEED:
  - Reduce number of entries into action statements to perform activities to meet SBO Rule (perform more in a single tagout)
  - Reduce simultaneous PMs and avoid stress of being near AOT
  - Will allow time for maint./repair/testing of EDGs while at power
  - Avert unnecessary shutdowns
  - Better EDG reliability “at power” and in early stages of shutdown
- DETERMINISTIC CONSIDERATIONS:
  - EDGs provide emergency power following events involving loss of offsite power -  
- applies to both power and lower mode operations. Would be better to have improved reliability for power & lower modes of operation.



## **Any Proposed Technical Specification Change Should Either:**

- Be risk neutral, or
- Result in a decrease in plant risk, or
- Result in a small increase in plant risk

And

- Be needed to more efficiently and/or more safely manage plant operations



## **Multiple Analyses Performed & Compared**

- Performed for each CE plant
- The most up-to-date PRA used at each plant
- In cases where plant design or other information yield non-symmetric results (i.e., it matters which SIT or LPSI train or EDG is affected), the most pessimistic results (for allowing the tech spec change) were always used
- While the calculation manipulations were actually made using the already solved complete model cut sets, this course material will demonstrate the effects on the individual parts of the PRA for instructional purposes.



## **We Will Go Over in Class...**

- Initiating Events and Event Tree considerations for the SIT and LPSI cases
- The complete SIT case analysis
- Touch upon the additional complexities of the LPSI and EDG cases



# MODULE D

## ACCIDENT SEQUENCE INITIATING EVENTS



**Based on the Example Information Provided  
for 1 Plant in the Following Slides,  
For Which Initiating Events in the PRA Does  
Each AOT Case Have to be Analyzed?**

- ▲ SITs AOT Extension?
- ▲ LPSI AOT Extension?



## **Design Basis Requirements for the Plant (in accordance with Appendix K to 10CFR50)**

- ▲ Injection by all but one of the SITs (one is assumed ineffective due to break location) in Large Break LOCAs.
- ▲ Injection by LPSI during a Large Break LOCA in combination with the SITs (mentioned above) & HPSI, and in combination with a loss of offsite power and the “worst” single equipment failure.
- ▲ Use of LPSI to provide shutdown cooling (SDC) in a steam generator tube rupture (SGTR) event with/without offsite power.



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

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

\* Large LOCA success criteria based on calculations performed for a (<3 ft<sup>2</sup> equivalent area) credible pipe break, and realistic post-accident thermal hydraulic system performance.

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

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



Table 3.1.1: Initiating Event Summary

Initiator	Description	Classification
$T_1$	Reactor Trip - results from a system disturbance that causes the RPS to insert control rods to terminate the nuclear chain reaction.	Transient
$T_2$	Loss of Condenser Vacuum - results in a loss of MFW, and a loss of SDBC system for secondary pressure relief and heat removal. A loss of condenser vacuum causes depletion of hotwell inventory failing MFW. It also prevents steam dump to the condenser.	Transient
$T_3$	Turbine Trip - includes events that generate a turbine trip signal and a consequent reactor trip signal.	Transient
$T_4$	Loss of Main Feedwater - results in a failure of all Main Feedwater flow to the steam generator. This loss of flow may result in a pressurization of the primary system if SDBC fails. This class of events includes total loss of MFW flow, full closure of feedwater isolation valves, and feedline breaks upstream of the feedwater check valves.	Transient
$T_{SA}$	Loss of 345 KV with 161 KV Unavailable (Plant-Centered) - can lead to a reactor trip and a requirement for emergency diesel generators to prevent station blackout. $T_{SA}$ results in a loss of power to all 4KV buses.	Transient
$T_{SB}$	Loss of 161 KV with Failure to Fast Transfer (Plant-Centered) - can lead to a reactor trip and a requirement for emergency diesel generators to prevent station blackout. $T_{SB}$ results in a loss of power to all 4KV buses.	Transient
$T_{SC}$	Loss of Off-Site Power (Grid-Related) - can lead to a reactor trip and a requirement for emergency diesel generators to prevent station blackout. $T_{SC}$ results in a loss of offsite power to all the 4160 V buses due to events related to the reliability of the grid.	Transient



Initiator	Description	Classification
T <sub>5D</sub>	Loss of Off-Site Power (Weather-Induced) - can lead to a reactor trip and a requirement for emergency diesel generators to prevent station blackout. T <sub>5D</sub> results in a loss of offsite power to all the 4160 V buses due to events related to severe weather conditions.	Transient
T <sub>6</sub>	Steamline/Feedline Break on SG2 Upstream of MSIVs and Downstream of FWCVs - assumed to cause a blowdown of SG2 and a rapid depressurization of the primary system, causing a Pressurizer Pressure Low Signal (PPLS), main steam isolation, main feedwater isolation, and isolation of AFW to SG2. The steam supply to the turbine-driven AFW pump from SG2 will also be unavailable.	Transient
T <sub>7</sub>	Steamline Break on SG2 Downstream - assumed to cause an initial blowdown of both SGs and a rapid depressurization of the primary system, causing a PPLS and Steam Generator Isolation Signal (SGIS).	Transient
T <sub>8</sub>	Loss of 4 KV Bus 1A1 - represents a loss of power on 4 KV Bus 1A1 due to an electrical fault that causes bus failure. A loss of power to 4 KV Bus 1A1 will result in a loss of Reactor Coolant Pump RC-3A and subsequent reactor trip on low RCS flow. (special initiator)	Transient
T <sub>9</sub>	Loss of 4 KV Bus 1A3 - represents a loss of power on 4 KV Bus 1A3 due to an electrical fault that causes bus failure. A loss of power to 4 KV Bus 1A3 will result in a loss of Reactor Coolant Pump RC-3C and subsequent reactor trip on low RCS flow. (special initiator)	Transient
T <sub>10</sub>	Loss of 4 KV Bus 1A4 - represents a loss of power on 4 KV Bus 1A4 due to an electrical fault that causes bus failure. A loss of power to 4 KV Bus 1A4 will result in a loss of Reactor Coolant Pump RC-3D and subsequent reactor trip on low RCS flow. (special initiator)	Transient
T <sub>11</sub>	Loss of 4 KV Bus 1A2 - represents a loss of power on 4 KV Bus 1A2 due to an electrical fault that causes bus failure. A loss of power to 4 KV Bus 1A2 will result in a loss of Reactor Coolant Pump RC-3B and subsequent reactor trip on low RCS flow. (special initiator)	Transient



Initiator	Description	Classification
T <sub>12</sub>	Loss of 125 VDC Bus # 1 - represents a loss of power on 125 VDC Bus #1 due to an electrical fault that causes bus failure. (special initiator)	Transient
T <sub>13</sub>	Loss of 125 VDC Bus # 2 - represents a loss of power on 125 VDC Bus #2 due to an electrical fault that causes bus failure. This event is expected to cause a challenge to the primary PORVs. (special initiator)	Transient
T <sub>14A</sub>	Loss of 125 VDC Panel AI-41A - represents a loss of power on 125 VDC Panel AI-41A due to an electrical fault that causes panel failure or by a loss of power to the panel because the power supply breaker to the panel transfers open. (special initiator)	Transient
T <sub>14B</sub>	Loss of 125 VDC Panel AI-41B - represents a loss of power on 125 VDC Panel AI-41B due to an electrical fault that causes panel failure or by a loss of power to the panel because the power supply breaker to the panel transfers open. This event is expected to cause a challenge to the primary PORVs. (special initiator)	Transient
T <sub>15</sub>	Loss of CCW System - represents a failure of CCW flow due to system initiated failures. (special initiator)	Transient
T <sub>16</sub>	Loss of Raw Water System - represents failure of Raw Water flow due to system initiated failures. (special initiator)	Transient
T <sub>17</sub>	Loss of Instrument Air - represents a failure of instrument air due to system induced failure. Automatic or manual trip is assumed to occur. (special initiator)	Transient
T <sub>18</sub>	Loss of HVAC to Room 56 - T <sub>18</sub> represents a loss of cooling to electrical equipment in Room 56. Specifically, a loss of cooling to Inverters A and C (without human intervention) is assumed to result in a loss of power to Instrument Buses AI-40A and AI-40C respectively. (special initiator)	Transient
T <sub>19</sub>	Loss of HVAC to Room 56A - represents a loss of cooling to electrical equipment in Room 56A. Specifically, a loss of cooling to Inverters B and D (without human intervention) is assumed to result in a loss of power to Instrument Buses AI-40B and AI-40D respectively. (special initiator)	Transient



Initiator	Description	Classification
T <sub>20</sub>	Loss of HVAC to Control Room (Rm. 77) - represents a loss of cooling to electrical equipment in Room 77. Specifically, loss of cooling to normally energized ESCS relays (without human intervention) is assumed to cause the relays to fail in the de-energized state. (special initiator)	Transient
T <sub>21</sub>	Closure of MSIV (1 SG Loop) - results in a reactor trip on loss of load or asymmetric SG transient. This event causes secondary side pressurization of the affected SG loop resulting in a challenge to the MSSVs. RCS pressurization to the PORV setpoint is precluded if the SDBC valves or MSSVs of the affected SG provide adequate steam flow. If a MSSV fails to reclose, secondary depressurization causes a SGIS signal which isolates MFW and Main Steam to both SGs.	Transient
T <sub>22</sub>	Closure of both MSIVs - results in a reactor trip on loss of load and causes secondary side pressurization resulting in a challenge to the MSSVs in both SG loops. RCS pressurization to the PORV setpoint is precluded if the MSSVs on both SG loops provide adequate steam flow. If a MSSV fails to reclose, secondary depressurization will cause a SGIS signal which isolates MFW and Main Steam to both SGs.	Transient
T <sub>23</sub>	Partial Load Rejection - represents a partial reduction of external load on the main generator that precludes a turbine/generator reactor trip. RCS pressure increases above 2350 psia causing reactor trip on high pressurizer pressure and a challenge to the PORVs.	Transient
T <sub>24</sub>	Spurious SGIS Signal - represents a spurious SGIS Signal that isolates MFW and MSIV to both SGs. The reactor trips on loss of load.	Transient
T <sub>25</sub>	Reactor Trip With PORV Opening - represents a transient initiator that causes direct opening of a PORV.	Transient
S	Small LOCA - is a break in the RCS pressure boundary in some location other than the steam generator that exceeds normal charging flow. For these break sizes, the normal charging system cannot maintain level in the pressurizer. Break sizes less than 0.0005 ft <sup>2</sup> in area are considered leaks rather than small LOCAs.	Small LOCA



Initiator	Description	Classification
M	Medium LOCA - will depressurize the RCS without secondary heat removal to a point where HPSI flow will be sufficient to prevent core damage by removing decay heat, but is not large enough to require the safety injection tanks (SITs) or LPSI. The minimum size for a medium LOCA is 0.00225 ft <sup>2</sup> in area.	Medium LOCA
A	Large LOCA - represents a wide range of requirements on the ECCS. HPSI or LPSI supplemented by the SITs will have sufficient capacity to cover the entire large LOCA range.	Large LOCA
R	Steam Generator Tube Rupture - credible tube failures range in severity from leak rates of a few gallons to several hundred gallons per minute for the guillotine rupture of several tubes. The event chosen as representative of this range is the complete severance of a single tube.	SGTR
I <sub>1</sub>	Failure of LPSI due to RCS/LPSI Injection Interface (M17) ISL - a LOCA from the primary system through an interfacing system of lower design pressure.	ISL
I <sub>2</sub>	Failure of LPSI due to RCS/LPSI DHR Return Interface (M16) ISL - a LOCA from the primary system through an interfacing system of lower design pressure.	ISL
I <sub>3</sub>	Failure of CCW due to RCS/CCW Interface (M18, M19) ISL - a LOCA from the primary system through an interfacing system of lower design pressure.	ISL
I <sub>4</sub>	Failure of CVCS due to RCS/Letdown Interface (M2) ISL - a LOCA from the primary system through an interfacing system of lower design pressure.	ISL
F	Reactor Vessel Failure - failure of the FCS reactor vessel boundary that results in a small or medium LOCA is assumed to be covered by the S and M LOCA categories, since penetrations for in-core instrumentation are located near the top of the vessel. Therefore, the reactor vessel failure event is assumed to result in an unmitigatable large LOCA that occurs at the bottom of the vessel. This initiator was not modeled due to low expected likelihood of occurrence. ( $\leq 1.0E-08$ )	Not Modeled



# MODULE F

## SYSTEMS ANALYSIS USING FAULT TREES



**Based on the Example Information  
Which Follows for 1 Plant,  
Which Event Trees/Sequences in the PRA  
Need to be Used to Examine Each AOT Case?**

- SITs AOT Extension?
- LPSI AOT Extension?



11



**A:METHEEFIO31.THE**

**3.1-49**



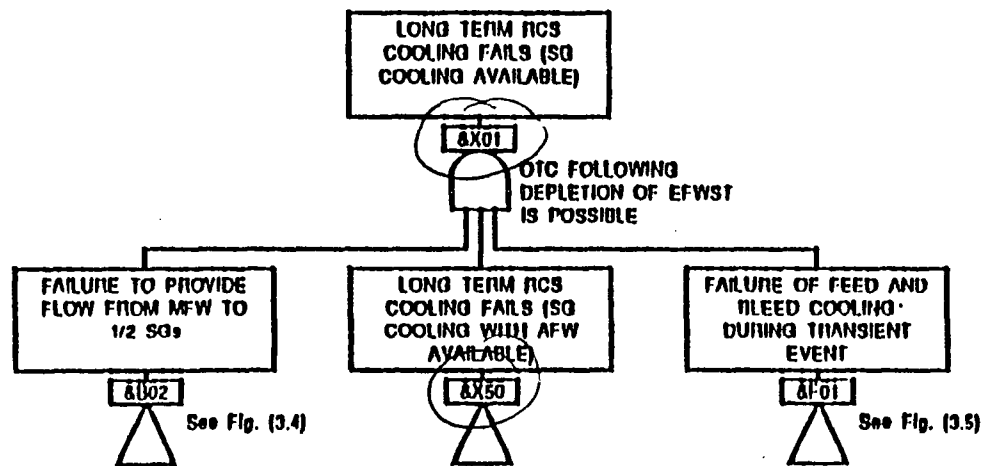


Fig. (3.6): TOP LOGIC MODEL - &X01

A:\TREE\FIG36.CAF

9-01-93



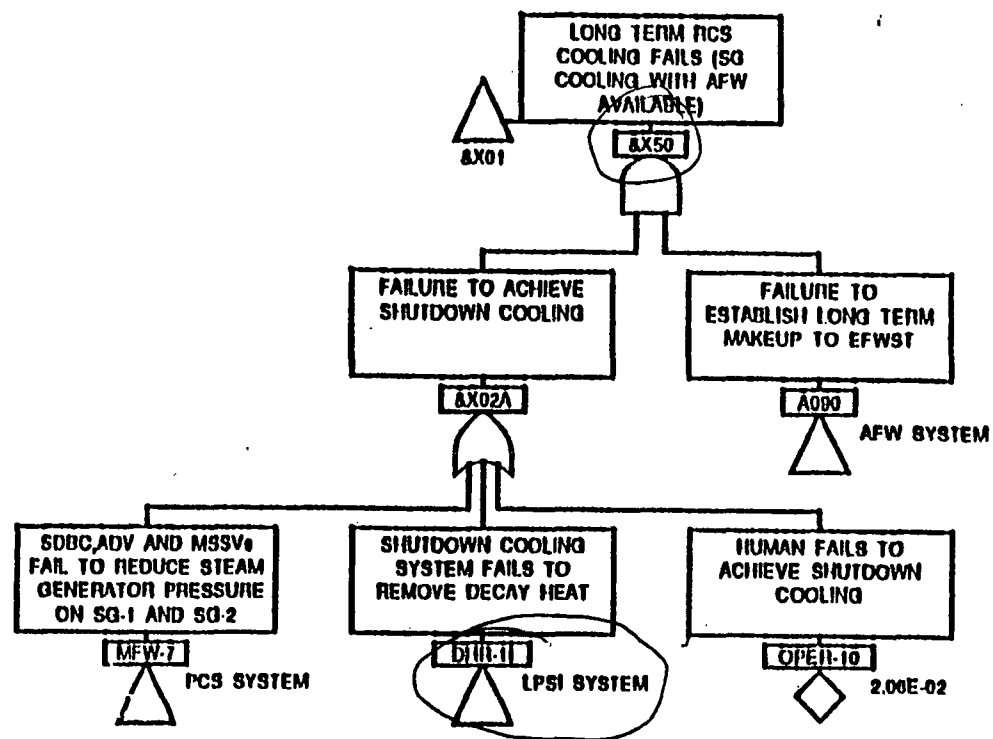


Fig. (3.6): TOP LOGIC MODEL - &X01

A:\TREE\FIG36.CAF

9-01-93



(3.8): FCS SMALL LOCA EVENT TREE

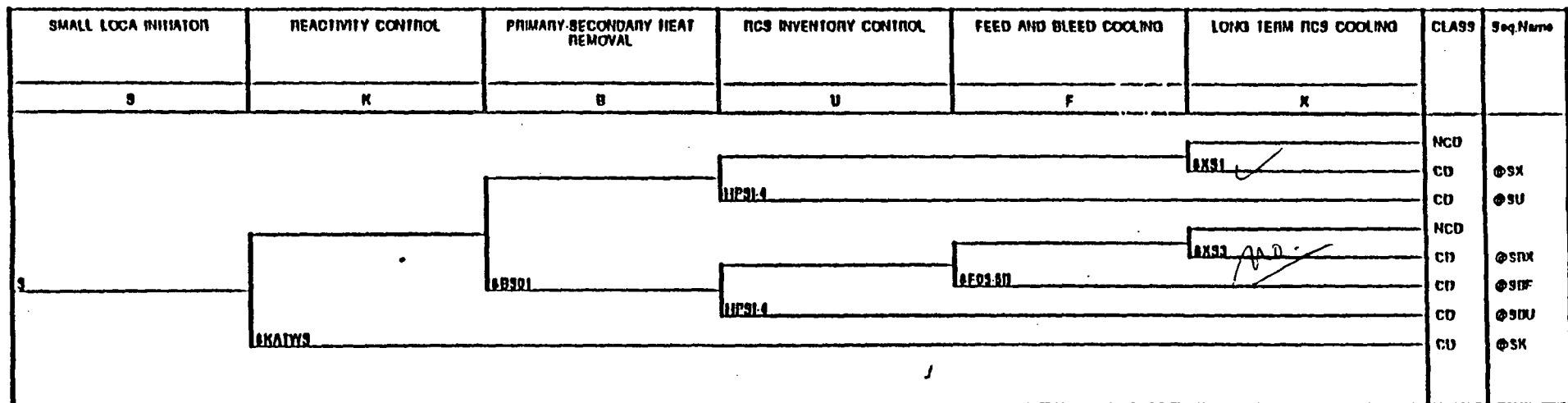


FIG. (3.8): FCS SMALL LOCA EVENT TREE ASEPNEEFK030.1NE 0-27-03



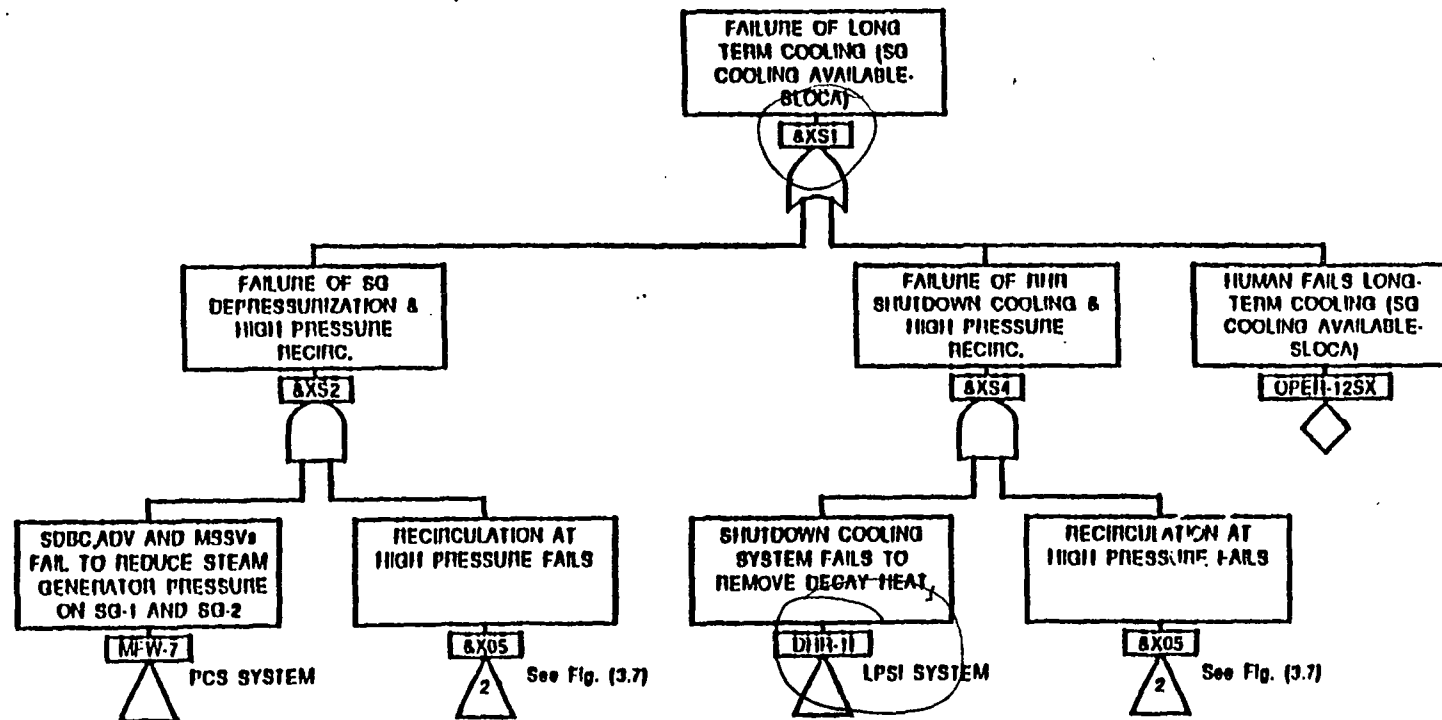
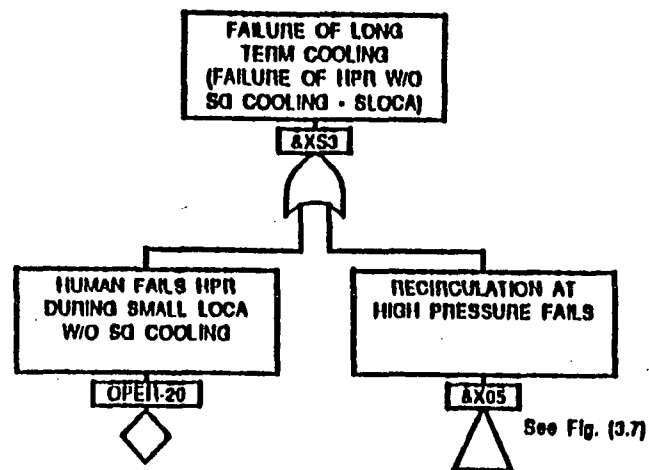


Fig. (3.11): TOP LOGIC MODEL - &amp;XS1

A:\TREE\FIG311.CAF

9-01-93







(3.15): FCS LARGE LOCA EVENT TREE

LARGE LOCA INITIATOR	RCS INVENTORY CONTROL	RECIRCULATION & INVENTORY CONTROL	CLASS	Seq.Name
A	UA	XA		
A			NCD	@AXA  @AUA
	&XA01 ✓		CD	
	&UA01 ✓		CD	

FIG. (3.15): FCS LARGE LOCA EVENT TREE

A:\ETREE\FIG315.TRE

8-27-93



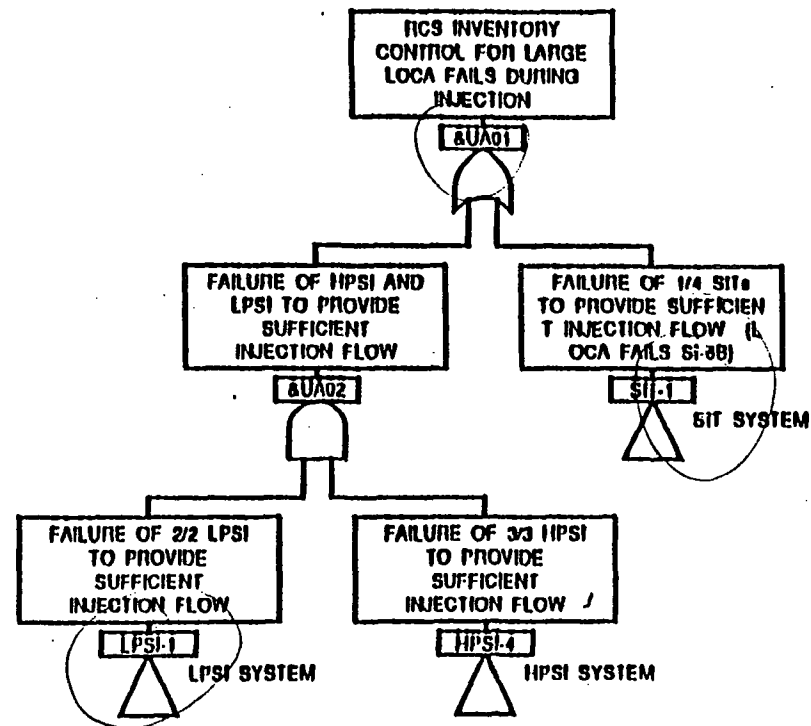


Fig. (3.16): TOP LOGIC MODEL - &amp;UA01

A:\TREE\FIG316.CAF

9-01-93



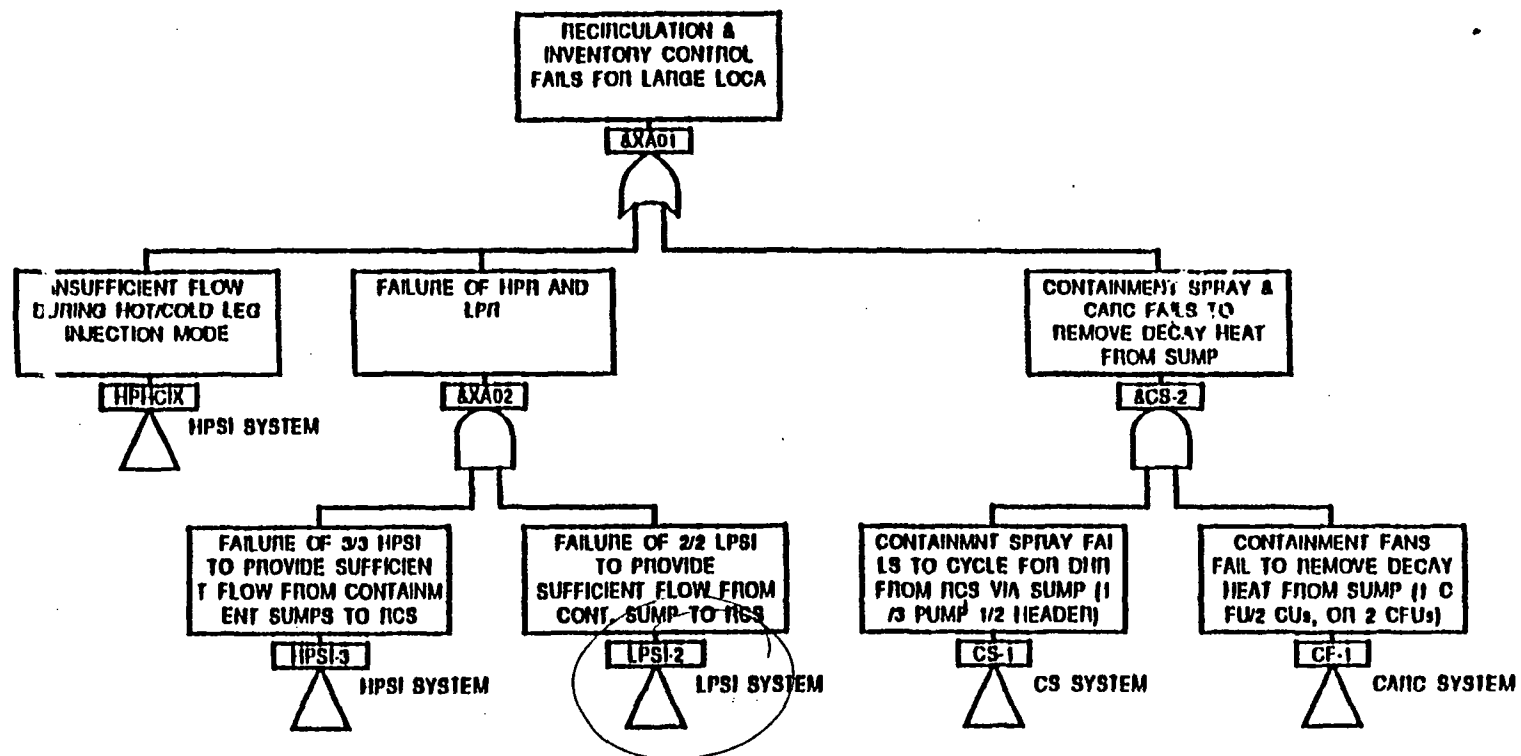


Fig. (3.17): TOP LOGIC MODEL - &XA01

A:\TREE\FIG317.CAF

9-01-93



(3.18): FCS SGTR EVENT TREE MODEL

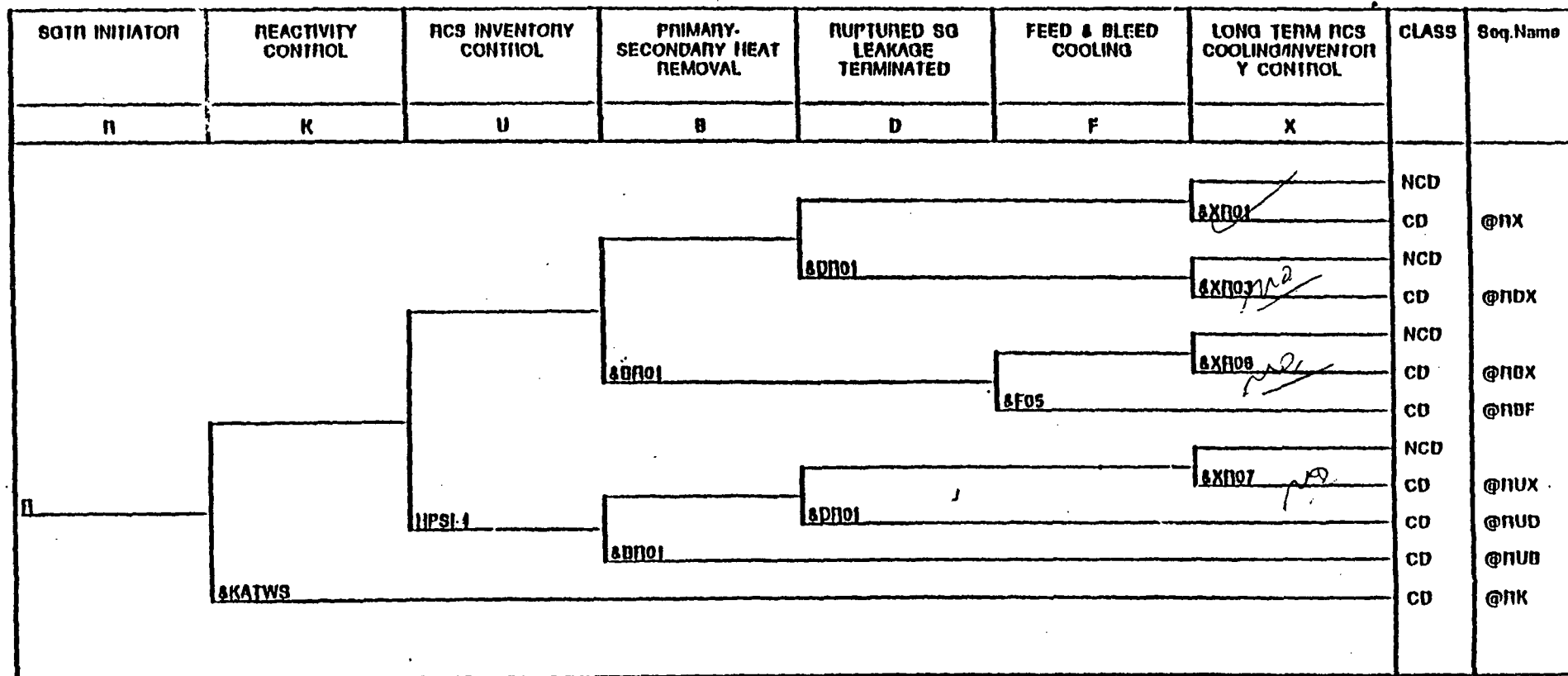


FIG. (3.18): FCS SGTR EVENT TREE MODEL

A:\ETREE\FIG318.TRE

8-27-93



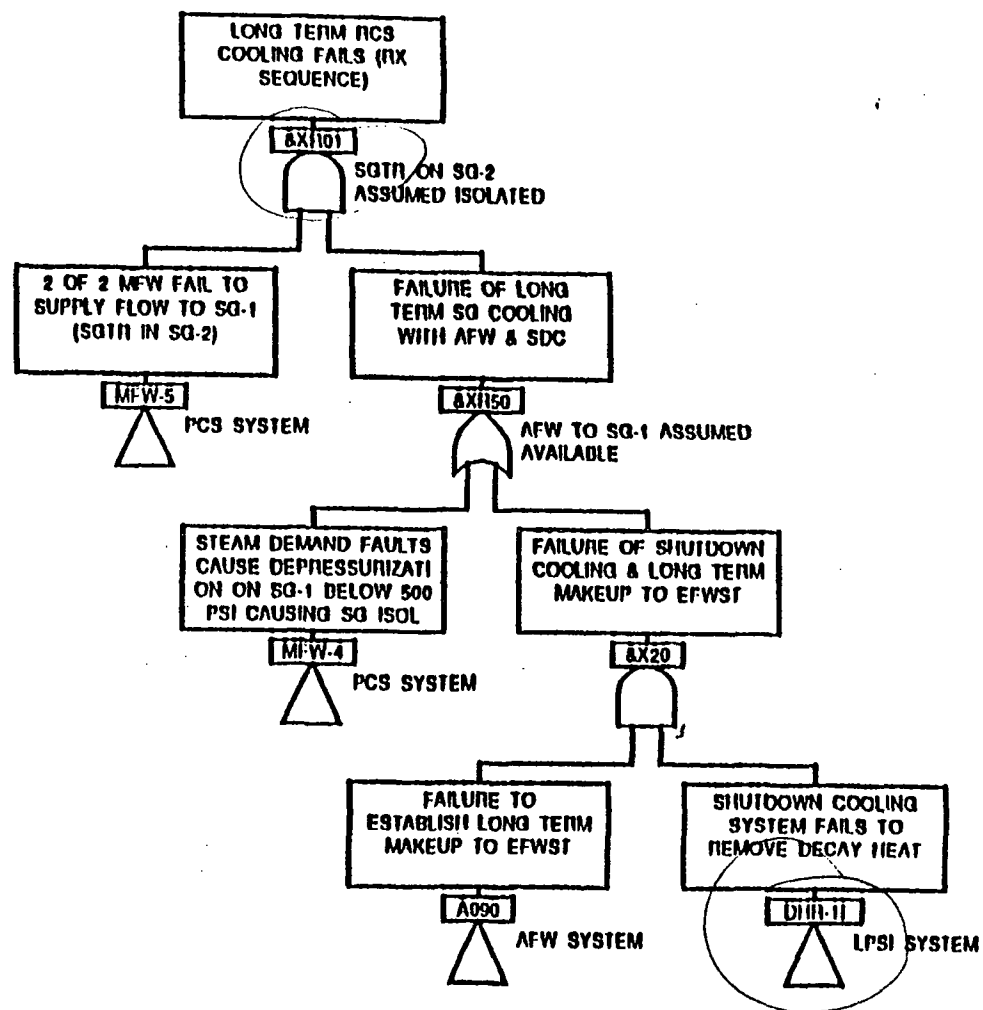


Fig. (3.22): TOP LOGIC MODEL - &XR01

A:\TREE\FIG322.CAF

9-01-93



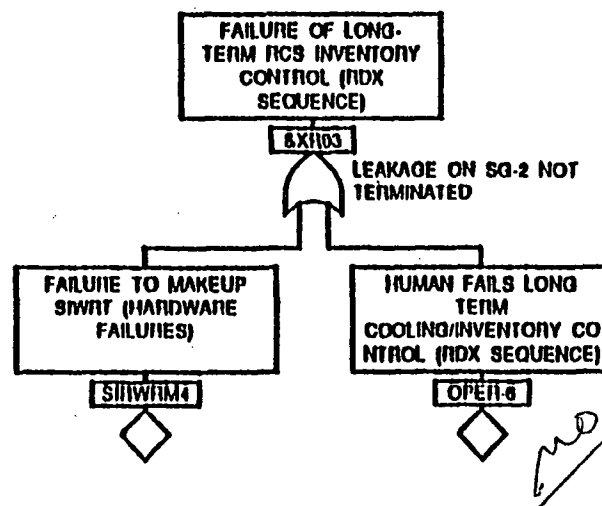
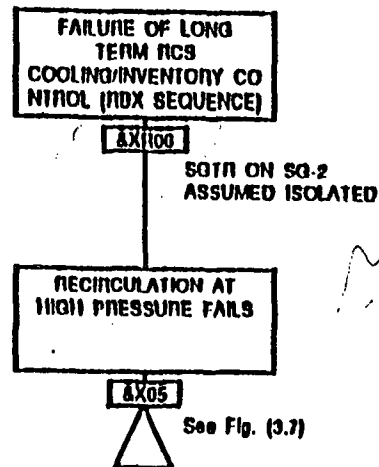


Fig. (3.23): TOP LOGIC MODEL - XR03

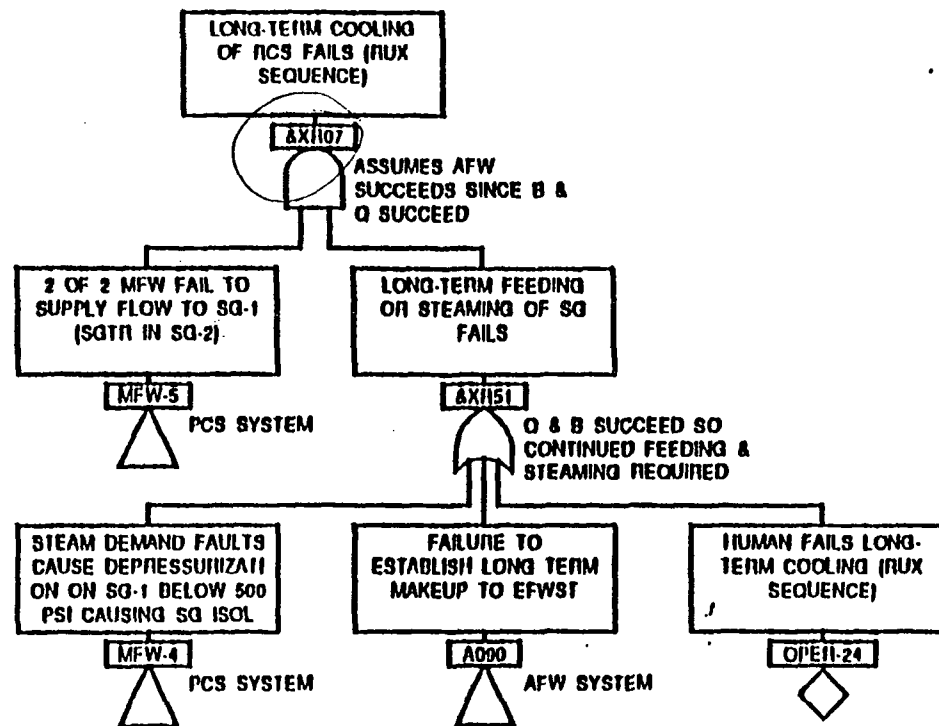
A:\TREE\FIG323.CAF

9-01-93









*mo.*

Fig. (3.25): TOP LOGIC MODEL - &XR07

A:\TREE\FIG325.CAF

9-01-93



(3.34): FCS ISL 13 EVENT TREE MODEL

INITIAL CONDITION	REACTIVITY CONTROL	INITIAL PHENOMENON	PRIMARY-SECONDARY HEAT REMOVAL	TERMINATION OF EX-CONTAINMENT LEAKAGE	LONG TERM FCS COOLING	CLASS	ECO NAME
ISO	R	U	B	D	X		
INIT	IKALWS	IKSL 4	BDSOI	BDSOI	BXOI	NCD	
						CD	Q110X
						CD	Q110DX
						CD	Q110N
						CD	Q110U
						CD	Q110K

FIG (3.34) ISL 13 EVENT TREE MODEL

ANALYSIS OF THE

8-27-93



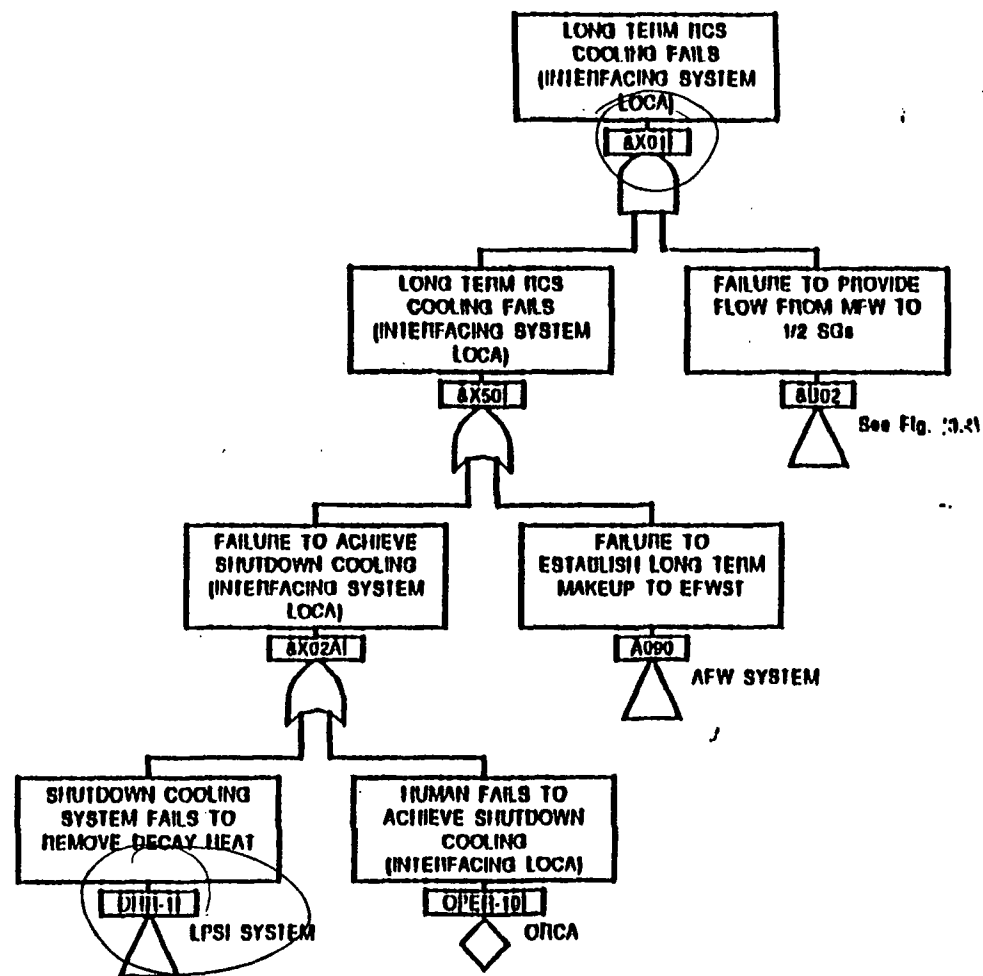


Fig. (3.41): Top Logic Model - &amp;X011

A:\TREE\FIG341.CAF

9-01-93



# **Overall Results of AOT Extension Analyses from Core Damage (Level 1 PRA) Perspective**



# SIT AOT Extension Case

<b>Plant</b>	<b>At-Power Single AOT (assuming full 24 hrs)</b>	<b>Transition Risk CDP</b>
ANO-2	2.30E-8	6.92E-7
CC-1/2	9.37E-7	4.45E-6
Ft Calhoun	2.74E-8	2.49E-7
Maine Yankee	negligible	1.56E-6



## SIT AOT Extension Case (continued)

Plant	At-Power Single AOT (assuming full 24 hrs)	Transition Risk CDP
Millstone-2	negligible	7.19E-7
Palisades	8.77E-9	1.09E-6
Palo Verde 1,2,3	3.84E-9	1.00E-6
San Onofre 2/3	1.03E-6	5.78E-7

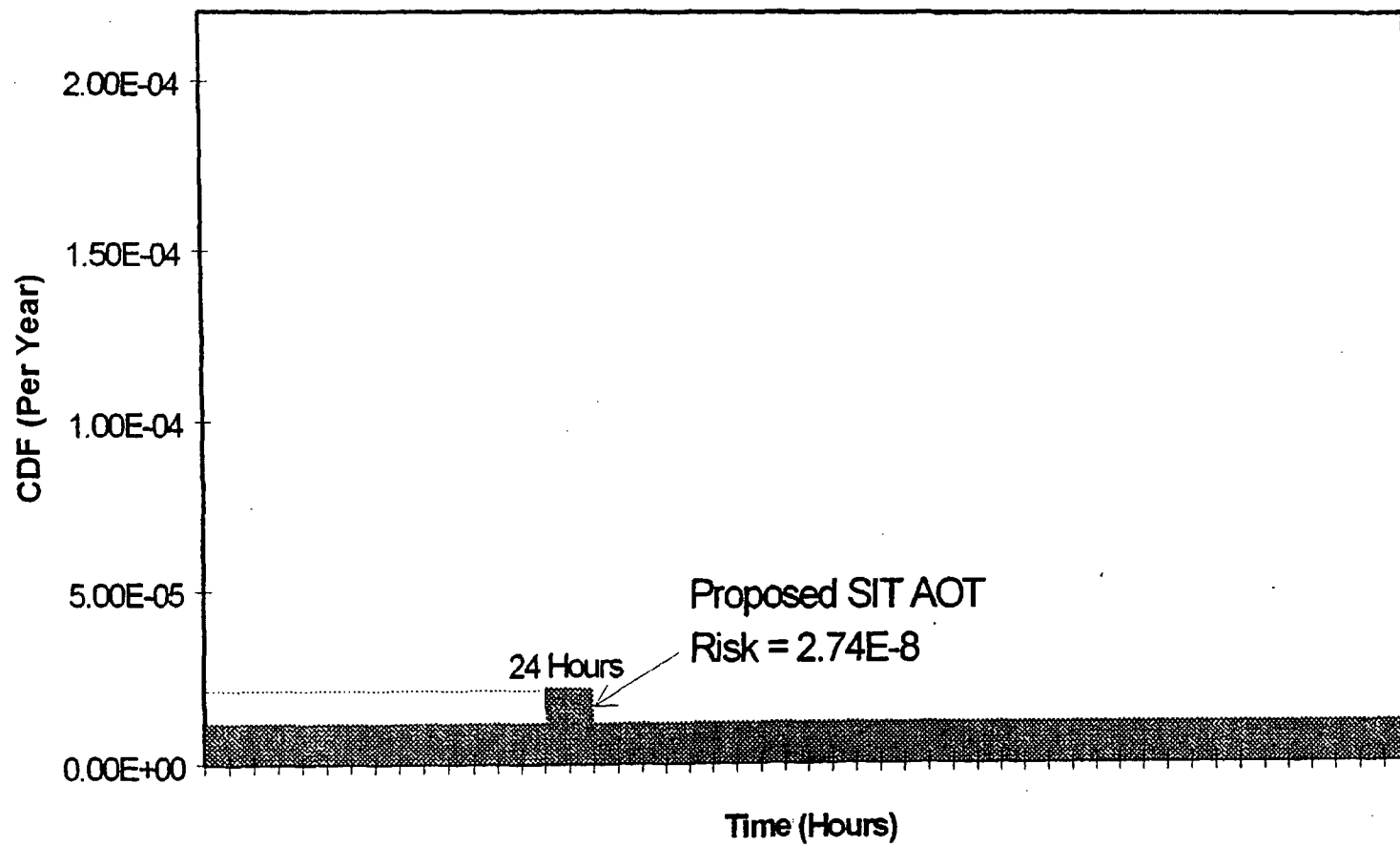


## SIT AOT Extension Case (continued)

Plant	At-Power Single AOT (assuming full 24 hrs)	Transition Risk CDP
St Lucie 1	5.5E-7	4.51E-7
St Lucie 2	5.5E-7	4.96E-7
Waterford 3	1.37E-7	3.25E-7



# Ft. Calhoun SIT AOT Case





# SIT AOT Extension Case (continued)

## Observations

- ✱ Performing SIT maintenance at power (per the extension request) versus during shutdown generally results in a decrease in overall risk
  - ⇒ CDP for continued operation of the plant with one SIT inoperable is generally less than the CDP associated with transitioning the plant to shutdown
  - ⇒ Even for those plants where there is a slightly greater CDP for at-power, when one considers the bias of the analysis (optimistic toward shutting down) and the fact that not *all* the transition risk was accounted for (e.g., did not include lower mode operation and return to power risks), SIT maintenance during power would be beneficial
- ✱ Expected yearly risk by performing at-power SIT maintenance is small
- ✱ Average CDFs are virtually unchanged
- ✱ Do not need design basis number of SITs to prevent core damage
- ✱ Should avert shutdowns (unnecessary safety risk & economic impact)



# SIT AOT Extension Case (continued)

Additionally, plants noted:

- ✧ No extraordinary compensatory actions need to be performed when 1 SIT is out of service
- ✧ Operability of other SITs should be verified before taking SIT out of service
- ✧ This should not coincide with scheduled removal of additional ECCS plant components from service
- ✧ The process of considering both the deterministic bases for the SITs, including conservatism in the Design Basis, and the different risk results from the PRA calculations, allowed for a better appreciation for the risk importance of the SITs and a feeling for how changes in the AOT can affect this importance.



## LPSI AOT Extension Case

Plant	At-Power Single AOT (assumes full 7 days)		Transition Risk CDP
	CM	PM	
ANO-2	2.92E-7	8.06E-8	6.92E-7
CC-1/2	1.92E-7	1.34E-7	4.45E-6
Ft Calhoun	negligible	negligible	2.49E-7
Maine Yankee	1.50E-6	1.04E-7	1.56E-6



# LPSI AOT Extension Case (continued)

Plant	At-Power Single AOT (assumes full 7 days)		Transition Risk CDP
	CM	PM	
Millstone-2	2.40E-6	1.80E-7	7.19E-7
Palisades	negligible	negligible	1.09E-6
Palo Verde 1,2,3	4.33E-7	1.15E-8	1.00E-6
San Onofre 2/3	1.55E-6	1.09E-7	5.78E-7

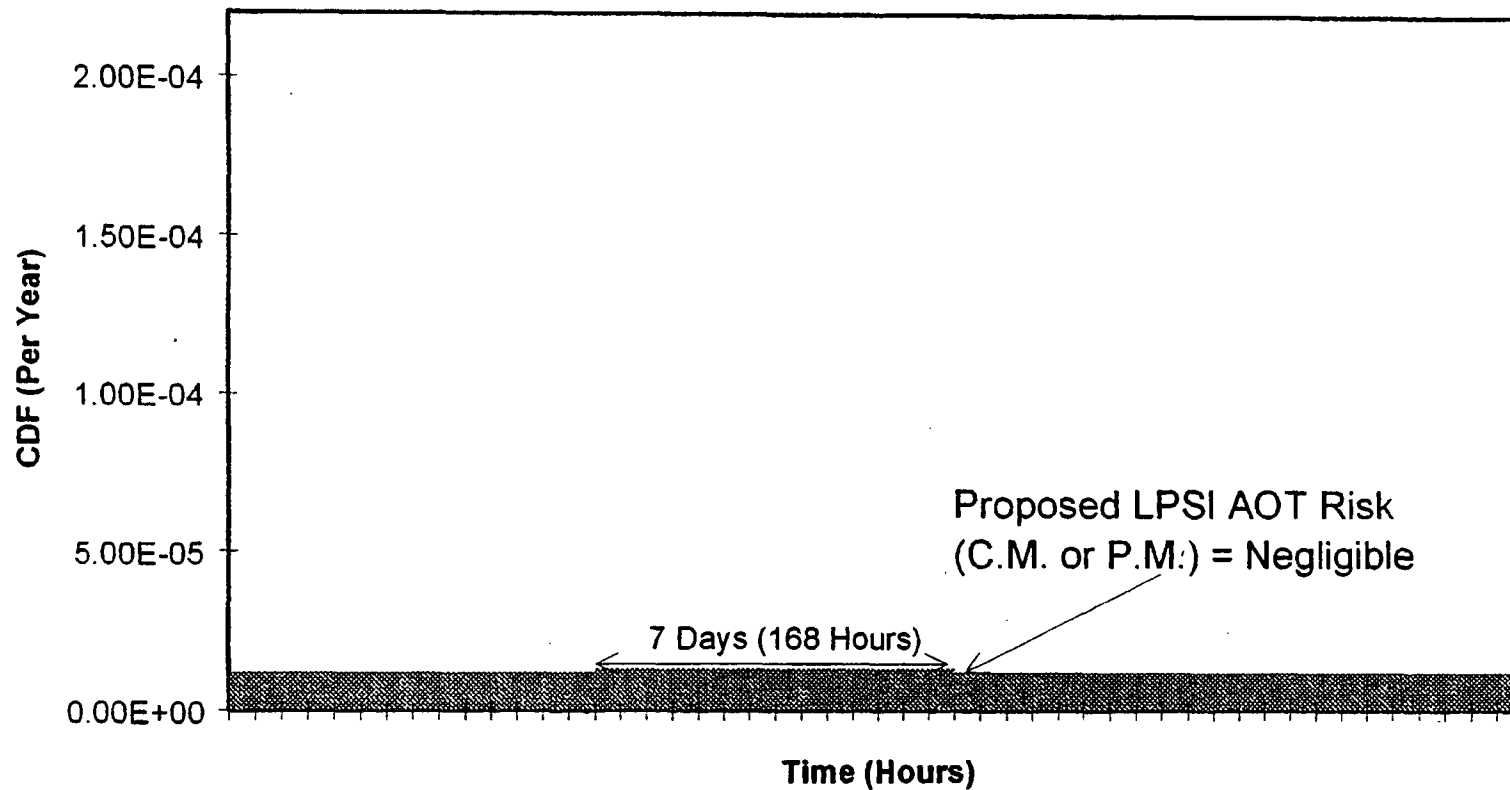


## LPSI AOT Extension Case (continued)

Plant	At-Power Single AOT (assumes full 7 days)		Transition Risk CDP
	CM	PM	
St Lucie 1	1.3E-6	2.1E-7	4.51E-7
St Lucie 2	1.3E-6	1.6E-7	4.96E-7
Waterford 3	4.14E-7	1.34E-8	3.25E-7



# Ft. Calhoun LPSI AOT Case





# Increased Management Attention

- ❖ Application is given increased NRC management attention when the calculated values of the changes in the risk metrics, and their baseline values when appropriate, approach the guidelines. The issues addressed by management will include
  - ▶ Cumulative impact of previous changes and trend in CDF and LERF (licensee's risk management approach)
  - ▶ Impact of proposed change on operations complexity, burden on operating staff, and overall safety practices
  - ▶ Benefit of the change with respect to its risk increase
  - ▶ Level 3 PRA information, if available



# Consideration of Uncertainties

- ❖ Use mean values (not median) of CDF and LERF used for comparison with guidelines
- ❖ Identify important sources of uncertainty
  - ▶ Parameter
  - ▶ Modeling
  - ▶ Completeness
- ❖ Perform sensitivity calculations on parameter and modeling uncertainties
- ❖ Perform quantitative or qualitative analysis on completeness uncertainties
- ❖ Results of sensitivity studies should generally meet guidelines
- ❖ Region III - no need to calculate uncertainty on baseline CDF/LERF



# Combined Change Requests

- ❖ Several changes can be combined in one submittal
- ❖ Will be reviewed against acceptance guidelines
  - ▶ Individually with respect to defense in depth
  - ▶ Cumulatively
- ❖ Combined changes should be related. For example
  - ▶ Be associated with same system, function, or activity
  - ▶ Changes reviewed individually against risk criteria if not closely related
- ❖ Combined changes should not trade many small risk decreases for a large risk increase (i.e., create a new significant contributor to risk)



# Key Issues in PRA Quality

- ❖ Ensure that, within scope, PRA analysis is complete and has appropriate level of detail
  - ▶ Consideration of relevant initiating events, plant systems, and operator actions
  - ▶ Analysis reflects plant-specific operating experience, design features, and accident response
  - ▶ All calculations are documented
- ❖ PRA methodology and associated input
  - ▶ Influence of models, input data, and assumptions on results and conclusions
- ❖ Licensee review and QA process
  - ▶ Peer review
  - ▶ Certification
  - ▶ Standards (e.g., new ASME and ANS standards)



# NRC Staff and Management Responsibilities

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



# Module Q

## Configuration Risk Management



# Configuration Risk Management

- Purpose: To acquaint students with the basic concepts of using PRA models to control configuration risk by planning maintenance.
- Objectives:
  - ❖ Explain why base case or nominal PRA results cannot be used for maintenance planning
  - ❖ Explain what is meant by “configuration risk management” and how it related to risk-informed regulation
  - ❖ Evaluate “risk” profiles quantitatively
- Reference: NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications



# Configuration Risk Management

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



# Configuration Risk Management

## Why an Issue?

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



# Configuration Risk Management

## Why an Issue?

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

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



# Observed Preventive Maintenance Practices of Concern

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



# Configuration Risk Management

## Traditional Approaches

- Technical Specifications and Limiting Conditions for Operation
  - ❖ Identifies systems/components important to safety based on traditional engineering approach
  - ❖ Limit component out-of-service times for individual and combinations of component outages (not based on formal risk analysis)
- Maintenance planning guidelines such as 12-week rolling schedule, etc.
  - ❖ Based on train protection concept and Technical Specifications
  - ❖ Provide guidance to work week planners on allowable maintenance/testing
- Operator judgment



# Configuration Risk Management

## Traditional Approaches

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



# Configuration Risk Management

- Configuration risk management: one element of risk-informed regulation
- Can be forward-looking or retrospective
  - ❖ Forward-looking to plan maintenance activities & outage schedules
  - ❖ Retrospective to evaluate risk significance of past plant configurations (e.g., Accident Sequence Precursor analyses)

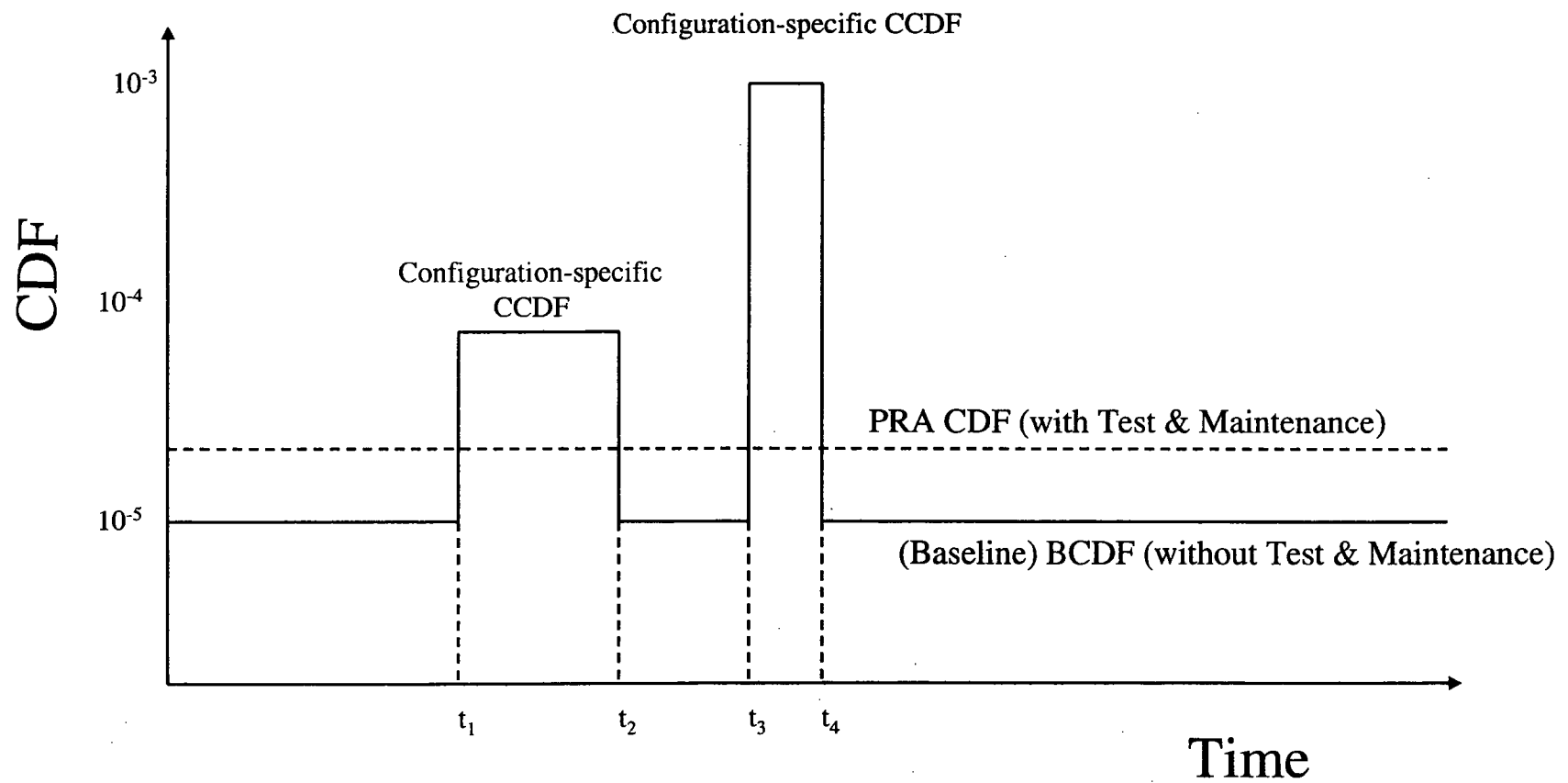


# Configuration Risk Management

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

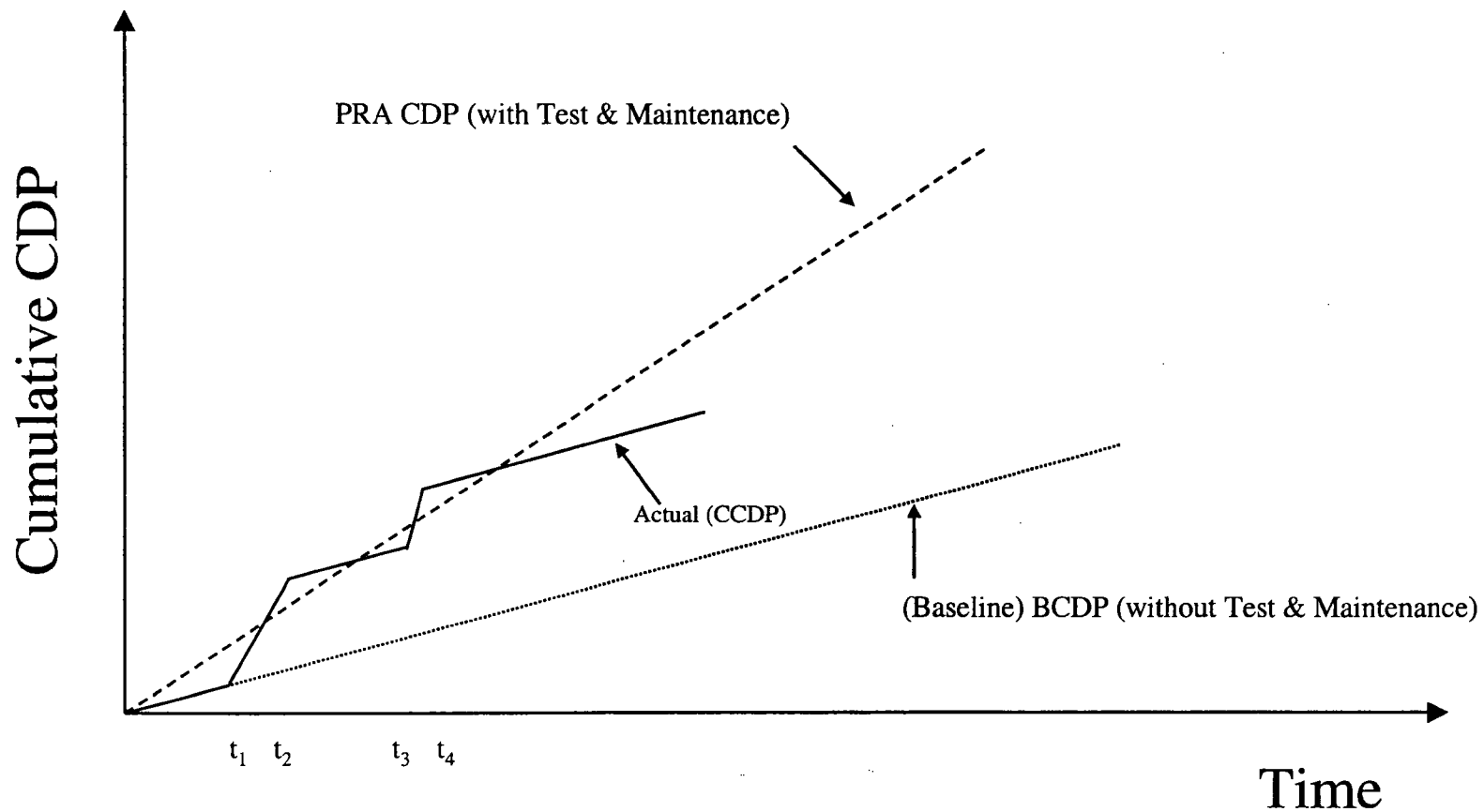


# CDF Profile





# Cumulative CDP Profile





# Configuration Risk Management

## ■ Includes management of:

- ❖ OOS components
  - instantaneous CCDF (configuration-specific CDF)
- ❖ Outage time of components & systems
  - configuration duration
  - CCDF
  - ICDP
- ❖ Backup components
  - instantaneous CCDF
- ❖ Frequency of specific configuration
  - cumulative CCDF over time

*(each of these discussed on the following slides)*



# Managing OOS Components

- Involves scheduling maintenance and tests to avoid having critical combinations of components or systems out of service concurrently
  - ❖ For Maintenance Rule, 10 CFR 50.65, NUMARC 93-01 suggest a ceiling configuration-specific CCDF value of 1E-3/year
    - Subject of such a ceiling value being studied by the NRC
    - NRC endorses the Feb. 22, 2000 revision of section 11 of NUMARC 93-01, but neither endorses nor disapproves the numerical value of 1E-3/year



# Managing Outage Time

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



# Managing Backup Components

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



# Controlling Frequency

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



# Why Configuration Risk Management is Needed...

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



# Preventive Maintenance Risk Calculations

- Risk impact of PM on single component
- Risk impact of maintenance schedule
- Risk impact of scheduling maintenance (power operations versus shutdown)



# Risk Monitors

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



# Current Risk Monitor Software Packages

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



# Requisite Features

- Risk monitor software requires (at a minimum) the following features:
  - ❖ PRA solution engine for analysis of the plant logic model
    - Can be ET/FT, single FT, or cutset equation
  - ❖ Database to manage the various potential plant configurations
    - That is, a library of results for configurations of interest
  - ❖ Plotting program to display results



# Risk Monitor Capabilities

- As a tool for plant operators to evaluate risk based on real-time plant configuration:
  - ❖ Calculates measure of risk for current or planned configurations
  - ❖ Displays maximum time that can be spent in that particular configuration without exceeding pre-defined risk threshold
  - ❖ Provides status of plant systems affected by various test and maintenance activities
  - ❖ Operators can do quick sensitivity studies to evaluate the risk impacts of proposed plant modifications



# Risk Monitor Capabilities (cont.)

- As a tool for plant scheduling for maintenance and outage planning:
  - ❖ Generates time-line that shows graphically the status of plant systems and safety functions
  - ❖ Generates risk profile as plant configuration varies over time
  - ❖ Identifies which components have strongest influence on risk



# Risk Monitor Strengths and Weaknesses

## ■ Risk Monitor Strengths

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



# Risk Monitor Strengths and Weaknesses (cont.)

## ■ Risk Monitor Limitations

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



# Risk Monitor Strengths and Weaknesses (cont.)

## ■ Risk Monitor Limitations

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



# Student Exercise

- Review your IPE and identify component out-of-service modeling
  - ❖ What type of outages are modeled?
    - testing
    - preventive maintenance
    - corrective maintenance
  - ❖ Any “special” events that cover multiple, simultaneous component outages?
  - ❖ What are the basis for the component outage probabilities?
    - generic
    - plant-specific
    - time period covered
    - sources for data collection
    - definition of outage duration



# Module R

## Maintenance Rule Implementation



# Maintenance Rule Implementation

- Purpose: To acquaint students with ways in which PRA typically supports licensee implementation of the Maintenance Rule.
- Objectives:
  - ❖ Explain the purposes of the Maintenance Rule and identify areas in which PRA can support the rule's implementation
  - ❖ Explain how performance goals/criteria are established using the "EPRI Method"
- References:
  - ❖ 10CFR50.65, Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
  - ❖ Regulatory Guide 1.160, Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
  - ❖ NUMARC 93-01, Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants
  - ❖ EPRI Technical Bulletin 96-11-01, "Monitoring Reliability for the Maintenance Rule"
  - ❖ EPRI Technical Bulletin 97-3-01



# Maintenance Rule Description

- Performance -Based Rule
- Effective July 10, 1996
- “To monitor the effectiveness of maintenance activities...  
For safety-significant plant equipment...  
In order to minimize the likelihood...  
Of failures and events...  
Caused by the lack of effective maintenance.”

(Maintenance Rule Training Handouts)



# Maintenance Rule Description

## ■ Paragraph (a)(1)

- ❖ Monitor performance of “problem” structures, systems, and components (SSCs)
- ❖ Compare performance against goals
- ❖ (a)(1) SSCs

## ■ Paragraph (a)(2)

- ❖ Reduced monitoring for SCCs meeting performance criteria
- ❖ (a)(2) SSCs



# Maintenance Rule Description

## ■ Paragraph (a)(3)

- ❖ Periodically evaluate program
- ❖ Incorporate industry-wide experience
- ❖ Balance SSC unavailability and failures

## ■ Paragraph (a)(4)

- ❖ Assess and manage increase in risk from maintenance activities

## ■ Paragraph (b)

- ❖ Scope of program

Safety-related SSCs

Non-safety-related SSCs

Mitigate accidents or in plant Emergency Operating Procedures (EOPs)

Required for safety-related SSCs to work properly

Can cause a scram or actuation of safety-related SSC



# Maintenance Rule History

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



# Typical Maintenance Rule Implementation

- Combination of traditional engineering analysis and PRA approaches
  - ❖ Reliance on expert panel to make final decisions
- Overall structure is performance-based approach
- Heavy reliance by most utilities on PRA support/information



# PRA Support for Maintenance Rule Implementation

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



# Safety Significance of SSCs

- NUMARC 93-01 recommends use of 3 importance measures
  - ❖ Core damage frequency (CDF) contribution (in top 90% of CDF cut sets)
  - ❖ Risk reduction worth (RRW) ( $\geq 1.005$ )
  - ❖ Risk achievement worth (RAW) ( $\geq 2.0$ )
- SSCs above cut-off levels for each importance measure are candidates for high safety significance
- Expert panel's role is also to consider and compensate for SSCs not in the PRA as well as PRA uncertainties...



# Factors to be Considered in Use of PRA Importance Measures

- ❖ SSC importance vs PRA basic event importance
- ❖ Sequence truncation level used in PRA
- ❖ Core damage frequency importance vs large early release frequency importance
- ❖ Avoid reliance on just one measure of importance



## Some Relevant Statistics - Brunswick IPE

Truncation limit: 1E-10/yr

CDF: 6.34E-6/yr

No. basic events: 1543

No. events after truncation: 291

No. events w/F-V > 0.001: 150

No. events w/F-V > 0.005: 74

No. events w/RAW > 2: 147

### CDF Contribution

No. events in top cutsets

Highest F-V not included

Highest RAW not included

No. events w/F-V > 0.005 not included

No. events w/RAW > 2 not included

### Top 90% Cutsets

184

0.00194

33.3

0

36

### Top 99% Cutsets

281

0.000133

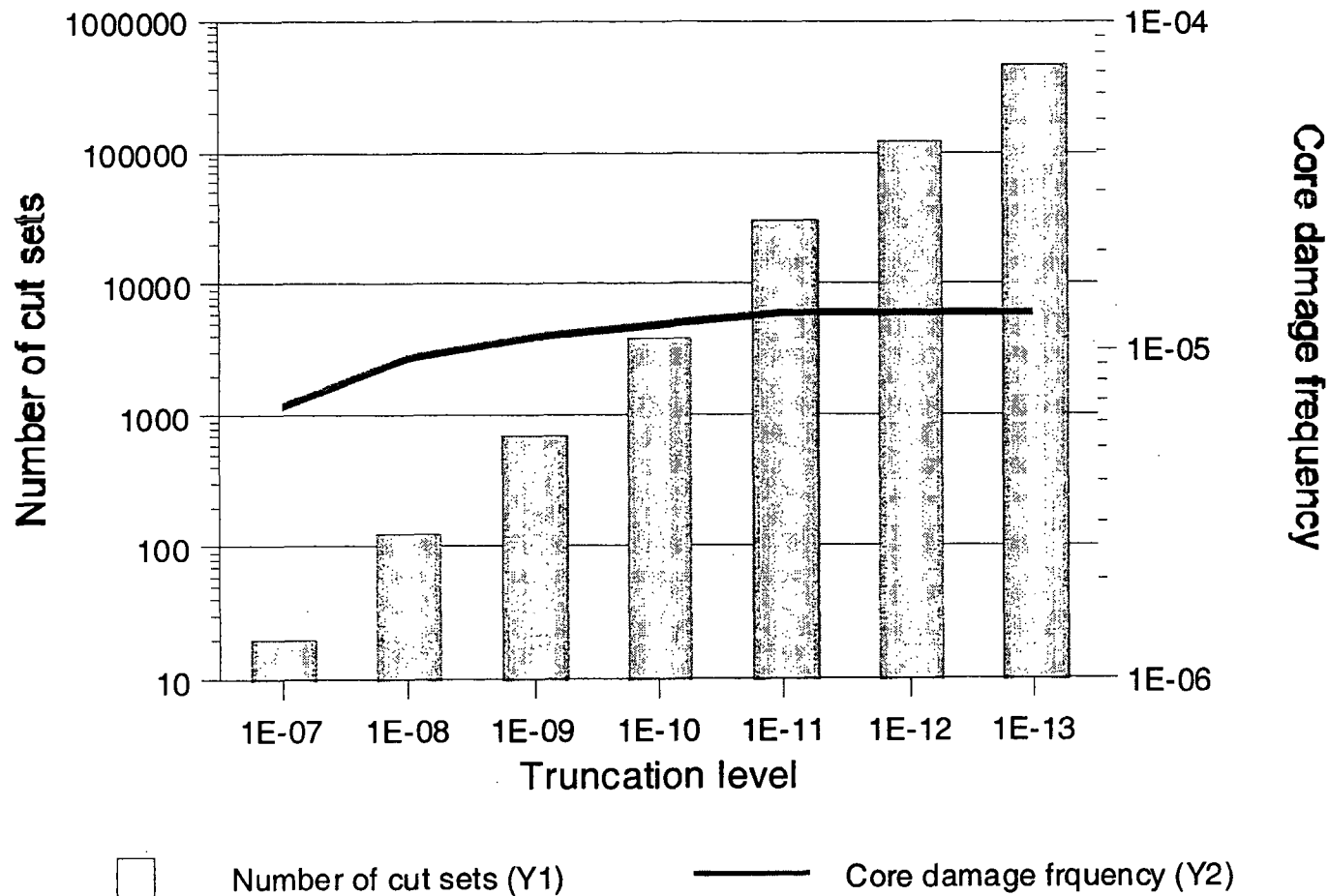
3.67

0

3

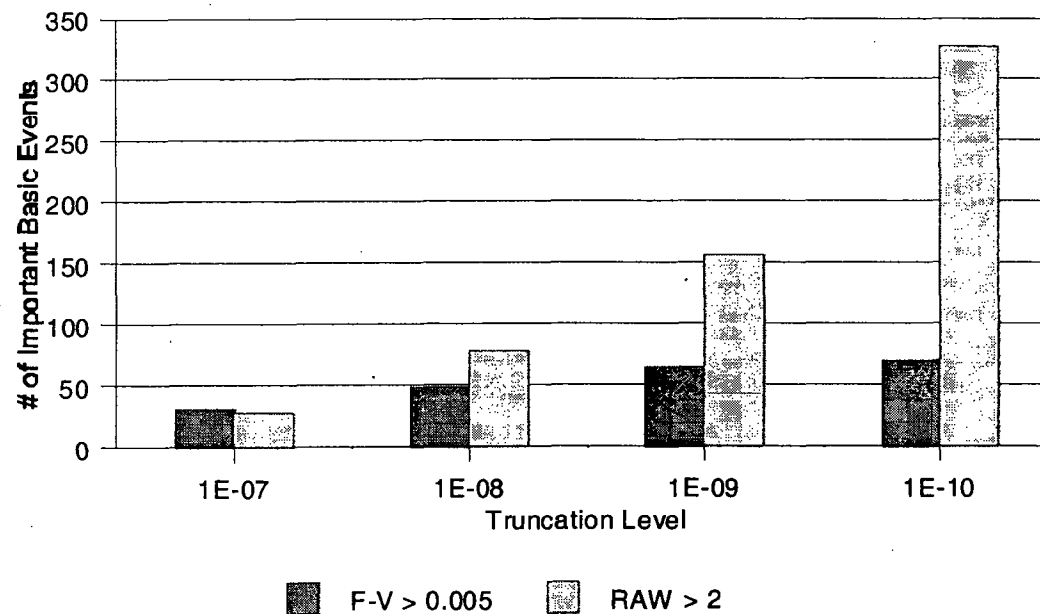


# Core Damage Frequency and Number of Cutsets Sensitive to Truncation Limits





# Truncation Limits Affect Importance Rankings





# SSC Performance Criteria

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



# Unavailability Performance Criteria

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



# Unreliability Performance Criteria

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



# Performance Criteria Expected to be Commensurate with Safety

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



# Methods for Establishing Reliability Goals/Criteria

## ■ EPRI method for reliability on demand (EPRI Technical Bulletin 96-11-01)

- ❖ Assume failure probability in PRA/IPE is correct
- ❖ Estimate number of demands over next evaluation period
- ❖ Calculate number of failures, using binomial distribution, such that, if PRA value is correct, there is approximately a 5% chance of seeing more than that number of failures

Example 1: Probability of failure ( $p$ ) = 0.05, 24 demands

$\Pr(X \leq 2, \text{ given } p = 0.05, n = 24) = 0.88$

$\Pr(X \leq 3, \text{ given } p = 0.05, n = 24) = 0.97$

Therefore, set performance criterion at 2 or fewer failures over next evaluation period



# Methods for Establishing Reliability Goals/Criteria (cont.)

Example 2:  $p = 0.01$ ,  $n = 36$

$$\Pr(X \leq 1, \text{ given } p = 0.01, n = 36) = 0.95$$

Therefore, set performance criterion at 1 or fewer failures over next evaluation period



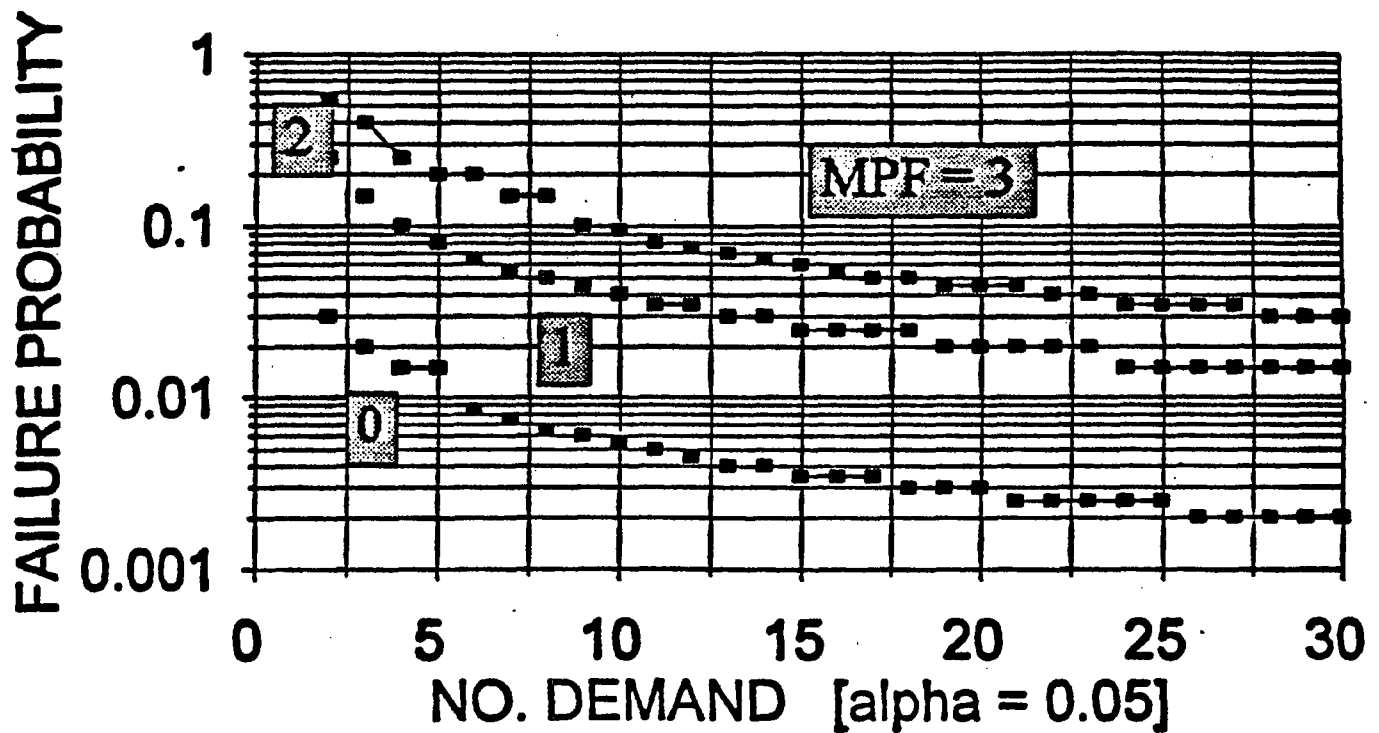




FIGURE 2

# FAILURE-ON-DEMAND

Maintenance Preventable Failure (MPF)



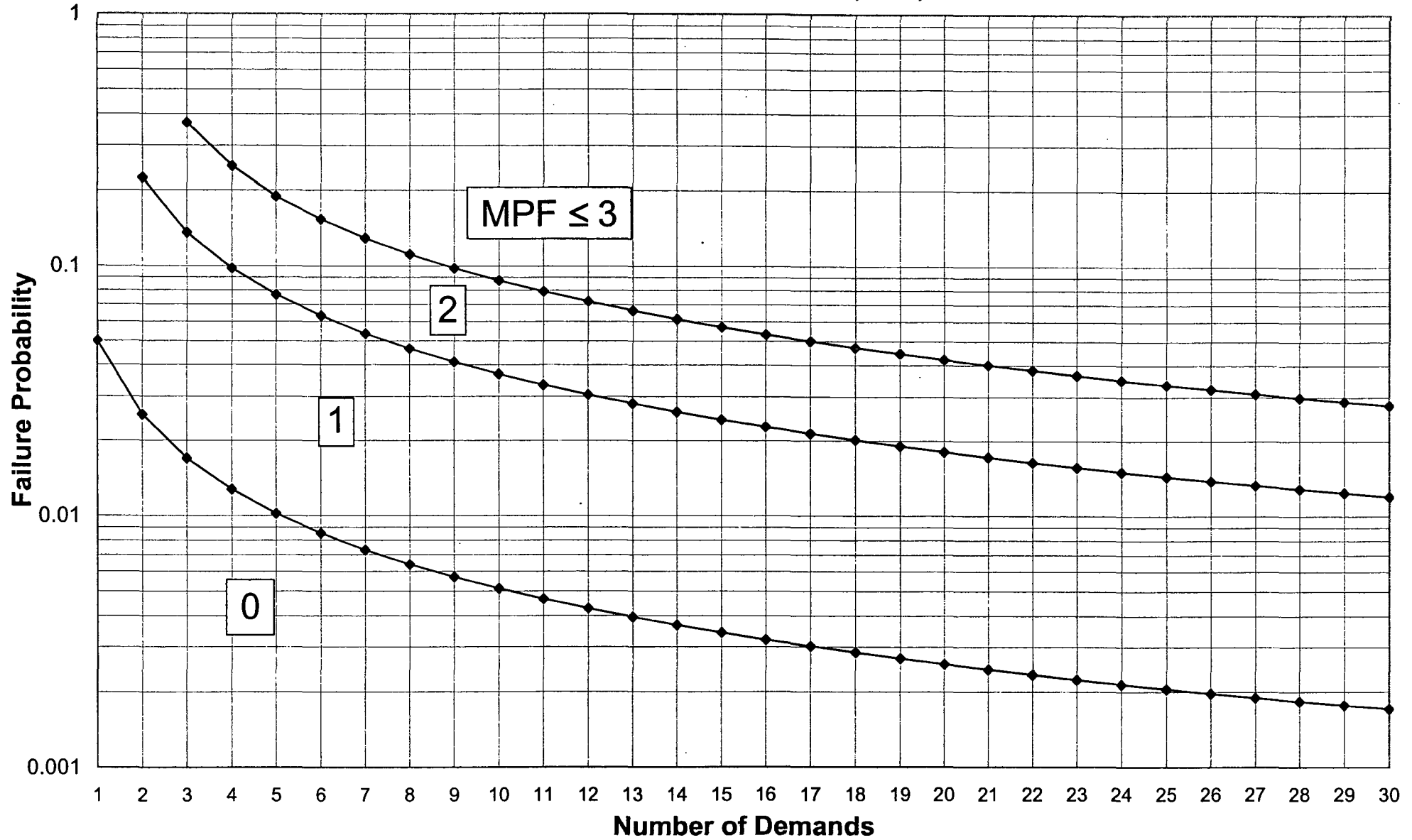






# Failure-on-Demand Curves

## Maintenance-preventable Failures (MPFs)









# Methods for Establishing Reliability Goals/Criteria (cont.)

## ■ EPRI method for reliability of normally running SSCs (EPRI Technical Bulletin 97-3-01)

- ❖ Assume failure rate in PRA/IPE is correct
- ❖ Estimate total running time over next evaluation period
- ❖ Calculate number of failures, using Poisson distribution, such that, if PRA value is correct, there is approximately a 5% chance of seeing more than that number of failures

Example 3: Failure rate ( $\lambda$ ) =  $5 \times 10^{-5}$ /hr,  $t = 10,000$  hrs

$\Pr(X \leq 1, \text{ given } \lambda = 5 \times 10^{-5}/\text{hr}, t = 10,000 \text{ hrs}) = 0.91$

$\Pr(X \leq 2, \text{ given } \lambda = 5 \times 10^{-5}/\text{hr}, t = 10,000 \text{ hrs}) = 0.99$

Conservative approach would be to set criterion at 1 or fewer failures

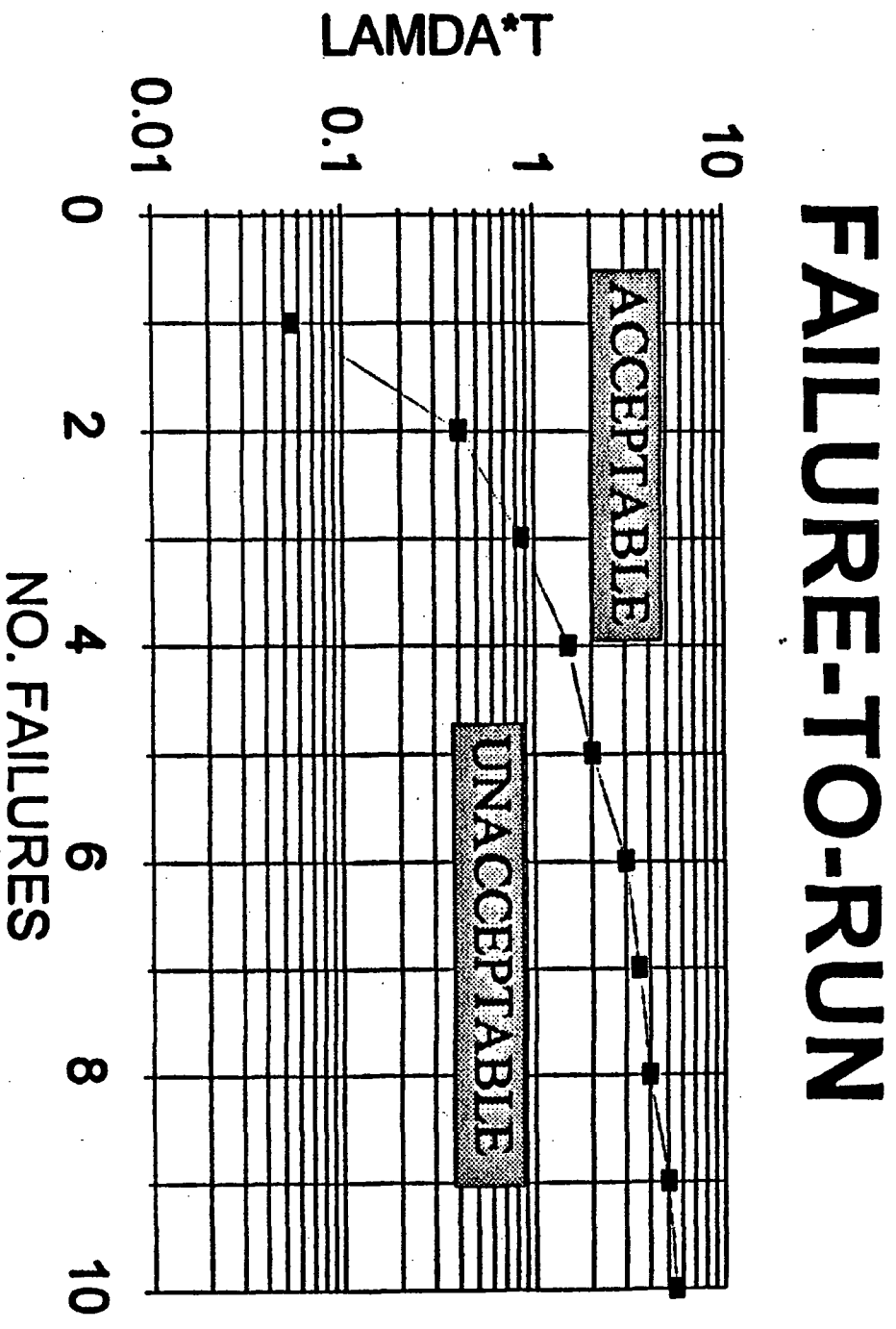
Less conservative, but still probably acceptable criterion would be 2 or fewer failures







FIGURE 3

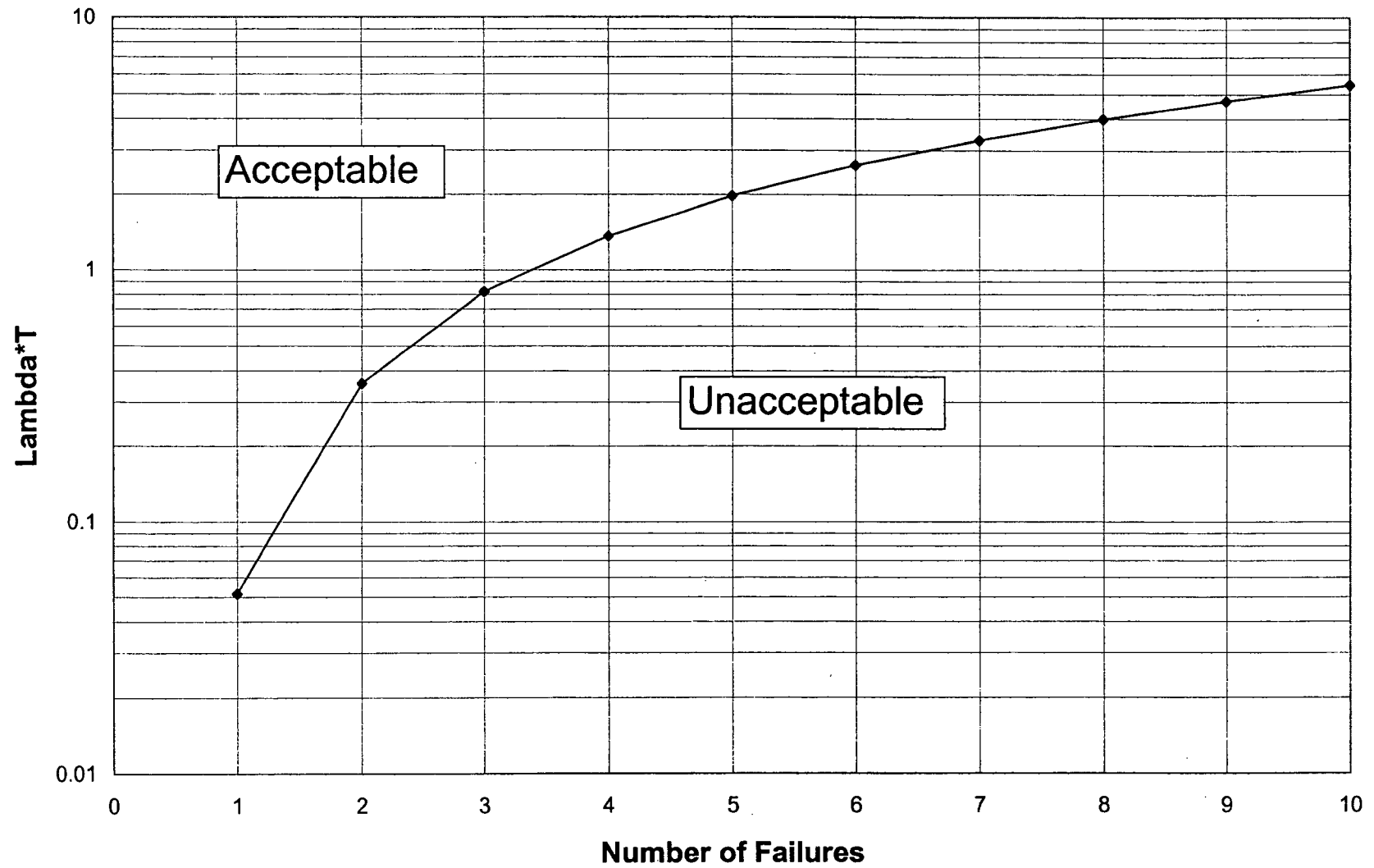








**Failure-to-Run Curve**









# Balancing of Unavailability and Unreliability

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



# Assessing Plant Risk From Maintenance

## ✖ Configuration management

### ❖ Work week schedule guidance

12-week rolling schedule

Days of week schedule for SSCs

Plant risk matrix or plant status monitor required by Maintenance Rule

Operator experience/judgment



# Plant Risk Matrix

- Goal-Assess plant risk given all planned/unplanned SSC maintenance outages
- Typically a 2-dimensional matrix covering high safety significance SSC maintenance outages
  - ❖ PRA based
  - ❖ Yes or no for planned outages of 2 SSCs, based on PRA estimate of plant risk
  - ❖ Guidance for 3 or more planned SSC outages
- Consideration of emergent failures



# Plant Risk Matrix

Diesel Generator 1	Diesel Generator 2	HPCI	RCIC	Control Rod Drive Hydraulic
DG1	No	Yes*	Yes*	Yes
	DG2	Yes*	Yes*	Yes
		HPCI	No	No
			RCIC	No

No - High plant risk

Yes - Low plant risk

\* Time limitation applies



# For Additional Information

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



# Module S

## Reactor Safety SDP Principles



# Reactor Safety SDP Principles

- Purpose
  - Describe the purpose of the SDP
  - Describe the tables that are used to perform an SDP
  - Describe how the SDP principles are consistent with PRA principles and practices



# Reactor Safety SDP Principles

- Objectives - Upon completion of this module, students should be able to
  - Describe the PRA basis behind the SDP Tables 1 through 5 in IMC 0609, App. A, Att. 1
  - Describe how these tables are used in the SDP
  - Describe how SDP is consistent with PRA principles and practices
  - Describe basis for shutdown risk checklist in IMC 0609, Appendix G
  - Describe difference between Type A and Type B findings related to containment integrity in IMC 0609, Appendix H



# Significance Determination Process (SDP) Purpose and Objectives

- SDP Purpose
  - Use risk insights, where appropriate, to help NRC inspectors and staff determine the safety significance of findings.
  - SDP determinations for inspection findings and the Performance Indicator (PI) information are combined for use in assessing licensee performance in accordance with guidance provided in IMC 0305, “Operating Reactor Assessment Program.”
- SDP Objectives
  - Characterize significance of inspection findings for the Reactor Oversight Process (ROP), using risk insights as appropriate.
  - Provide all stakeholders an objective and common framework for communicating the potential safety significance of inspection findings.
  - Provide a basis for timely assessment and/or enforcement actions associated with an inspection finding.
  - Provide inspectors with plant-specific risk information for use in risk-informing the inspection program.



# Selection of Initiating Event(s) to Evaluate

- Site specific risk-informed inspection notebook
  - Table 2 - Initiators and System Dependency
    - Affected Systems
    - Major Components
    - Support Systems
    - Initiating Event Scenarios
  - For affected system(s), identify which initiating events need to be evaluated



# Estimating Initiating Event Likelihood During Degraded Period

- PRA uses constant (time-independent) frequencies for various initiating events
- Each core damage sequence starts with initiating event
- CDF for sequence is frequency of initiating event multiplied by probability of failure of mitigating systems and/or operator responses, given initiating event
- Probability of initiating event occurring between  $t_1$  and  $t_2$  is approximately

$$\Pr(IE \text{ between } t_1 \text{ and } t_2) \approx \lambda_{IE}(t_2 - t_1)$$



# Estimating Initiating Event Likelihood During Degraded Period (cont.)

- Site specific risk-informed inspection notebook
  - Table 1 - Categories for Initiating Events
    - Rows in Table 1 correspond to different frequency ranges for different IEs
      - Most frequent IEs at top, least frequent at bottom
      - Row I > 0.1 per year
      - Row II 0.1 – 0.01 per year
      - Row III 0.01 – 0.001 per year, etc.
    - Right hand columns in Table 1 correspond to duration of degraded condition
      - > 30 days (upper bound duration of 1 year)
      - 3 - 30 days (upper bound duration of 0.1 year)
      - < 3 days (upper bound duration of 0.01 year)
    - Estimated initiating event likelihood is product of IE frequency (lower bound) and duration (upper bound) of degraded condition
      - Initiating Event Likelihood =  $-\log_{10}[\text{IE Frequency (lower bound)} * \text{duration}]$
      - Example: An IE with frequency in Row I with an exposure duration of >30 days
        - 0.1 per year (lower bound) \* 1 year (upper bound) = 0.1
        - Initiating Event Likelihood =  $-\log_{10}[0.1] = 1$
- Note: Each initiating event to be assessed for a finding will use the same duration column, but each assessed IE will have frequency corresponding to its respective row.



# Summary of Estimated Initiating Event Likelihood

- Result from Table 1 represents probability of having IE occur during degraded condition
- $X = -\log_{10}[\text{IE Frequency (lower bound)} * \text{duration (upper bound)}]$ 
  - $1 \leftrightarrow 10^0 \text{ to } 10^{-1}$
  - $2 \leftrightarrow 10^{-1} \text{ to } 10^{-2}$
  - $3 \leftrightarrow 10^{-2} \text{ to } 10^{-3}$
  - $4 \leftrightarrow 10^{-3} \text{ to } 10^{-4}$
  - $5 \leftrightarrow 10^{-4} \text{ to } 10^{-5}$
  - $6 \leftrightarrow 10^{-5} \text{ to } 10^{-6}$
  - $7 \leftrightarrow 10^{-6} \text{ to } 10^{-7}$
  - $8 \leftrightarrow \leq 10^{-7}$



# Summary of Estimated Initiating Event Likelihood (cont.)

- Note the uncertainty in IE frequencies shown in Table 1 (order of magnitude in each row)
- IE frequency will impact final risk significance, can adjust upward (subjectively) if degraded condition can increase IE frequency
  - Examples provided in IMC 0609, App. A, Att. 2



# SDP Worksheets for Initiating Event(s) Evaluation and Remaining Mitigation Capability

- Table 3 site specific risk-informed inspection notebook
  - For IE Scenarios identified in Table 2 – Initiators and System Dependency, complete just the affected Table 3 SDP Worksheet and just the row with the affected function
    - Circle the affected functions in each row
      - Number in parenthesis in each row indicate corresponding sequences with at least those systems indicated (minimal cut set at sequence logic level)
        - » Example: Table 3.XX row 1 TRAN – PCS – CHR – CV (5, 9); on the Transient event tree sequence 5 and 9 represent failures of the indicated systems, with sequence 9 have the indicated systems plus one or more other system failures. Only need to assess contribution from the highest contributing sequence
    - From Table 1 – Categories of Initiating Events, assign the identified initiating event likelihood (IEL) for that IE
    - Assign remaining mitigation capability rating for all other functions in each row that had a circled affected function
    - Assess and assign remaining mitigation capability rating for the circled affected function
      - Example: If LPI function affected in Table 3.XX, IMC 0609, App A, Att 1, but only LPCI mode affected; then the full mitigation capability (LPCI of 3 + LPCS of 3 = 6) for the evaluation would be LPCI of 0 + LPCS of 3 = 3.
    - Assign recovery of affected (failed) train if applicable (see Table 4).
    - Add all assigned values for each circle affected row in Table 3 and enter the result in the Results column (right most column of Table 3)



# Remaining Mitigation Capability

- Table 4 is not site specific.
- Table 4 assigns probabilities of failure to different means of mitigation (systems, operator actions, and recovery of failed systems), based on past PRA experience
  - Recovery of failed train: 0.1
  - One automatic steam-driven (ASD) train: 0.1
  - One train: 0.01
  - One multi-train system: 0.001 (system of two or more trains that are considered susceptible to common cause failures)
  - Two diverse trains: 0.0001 (system of two trains that are not considered susceptible to common cause failures; one train \* one train =  $0.01 * 0.01 = 0.0001$ )
  - Operator action credit:
    - 0.1 (failure probability between 0.5 and 0.05)
    - 0.01 (failure probability between 0.05 and 0.005)
    - 0.001 (failure probability between 0.005 and 0.0005)
- Remaining Mitigation Capability Credit =  $X = -\log_{10}[\text{failure probability}]$ , thus
  - Recovery of failed train: 1
  - One automatic steam-driven (ASD) train: 1
  - One train: 2
  - One multi-train system: 3
  - Two diverse trains: 4
  - Operator action credit: 1, 2, or 3



# Estimation of Risk Significance of Inspection Finding

- Determine final risk significance by completing Table 5 – Counting Rule Worksheet
- For each affected row for each Table 3 SDP Worksheet completed (IE assessed), count the total number of rows with a specific risk significance level equal to;
  - Number of rows with 9 =
  - Number of rows with 8 =
  - Number of rows with 7 =
  - etc. for each significance level to a 4
- Complete Table 5 - Counting Rule Worksheet
  - A “Step” in Table 5 that divides a risk significance level by 3 and rounds down is producing a higher risk significance from contributing lower risk significance; Three sequences of less risk significance are equal to one sequence of greater risk significance
    - Example: Three sequences with risk significance 9 equals one risk significance 8 sequence
- Result of Table 5 – Counting Rule Worksheet indicates risk significance of inspection finding
  - Red – highest safety significance – at least one sequence with a 4 =  $1\text{E}-4$
  - Yellow – at least substantial safety significance – at least one sequence with a 5 =  $1\text{E}-5$
  - White – at least low to moderate safety significance – at least one sequence with a 6 =  $1\text{E}-6$
  - Green – very low safety significance – at least one sequence with a 7 =  $1\text{E}-7$



# Final Risk Significance of Inspection Finding

- Note:
  - Cannot assess impact of degraded equipment reliability
  - SDP set up to analyze conditions that exist for a period of time, not set up for initiating event assessments (IE has occurred)
    - Initiating event assessment results in CCDP “spike,” which is different type of assessment than the SDP assessment
- Note that result of SDP is a probability: the probability of core damage, given a degraded condition of specified duration and probability of an IE during that condition
  - Called conditional core damage probability (CCDP)
- Problems with using CCDP as risk metric
  - PI program uses  $\Delta$ CDF, as does R.G. 1.174
  - NRC has no criteria for using CCDP

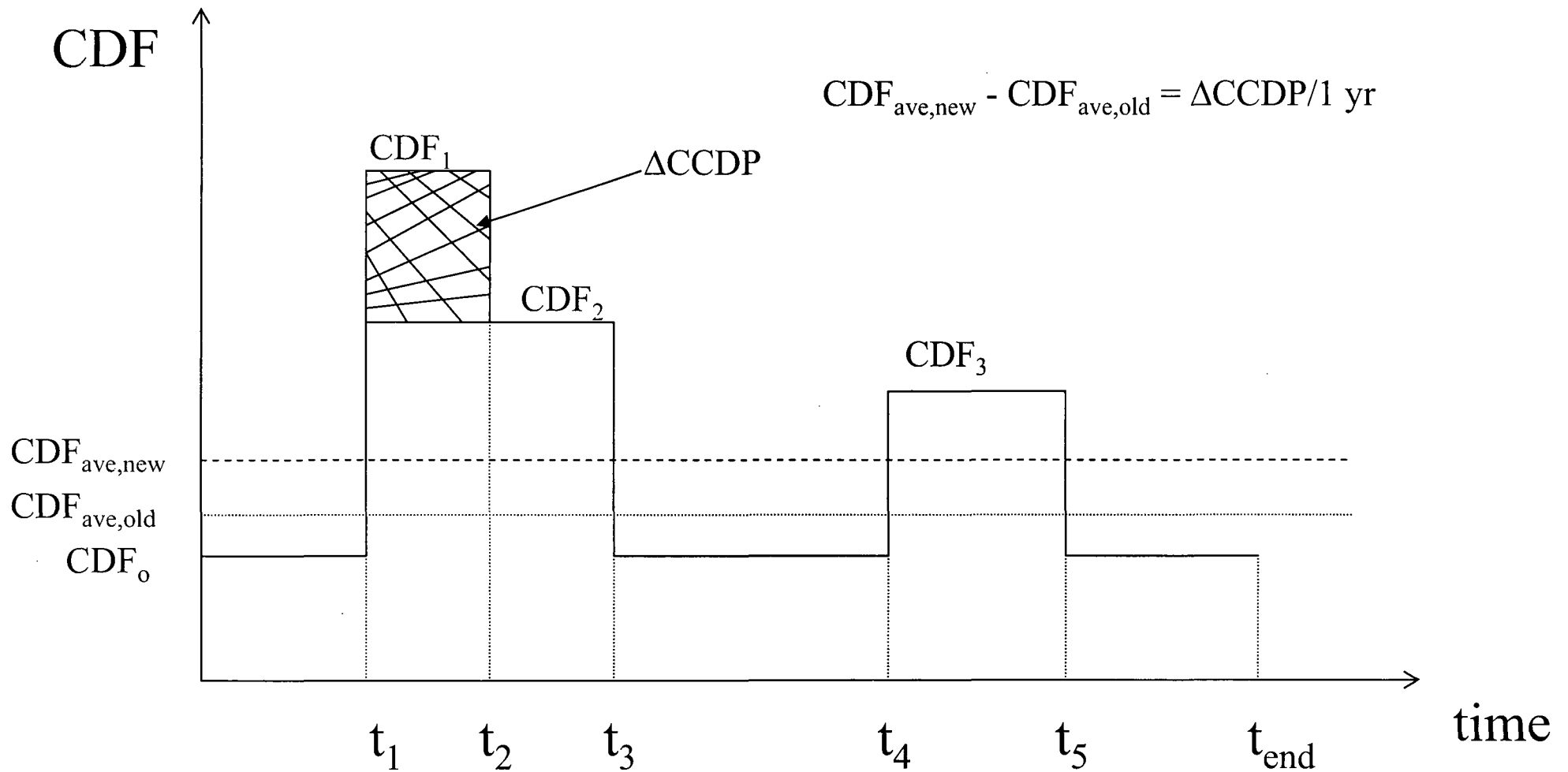


# Final Risk Significance of Inspection Finding (cont.)

- SDP estimates risk significance of licensee performance problems
  - Does not include equipment out of service for test or maintenance, unless related specifically to performance problem
  - Therefore, final result is increase in CCDP, or incremental CCDP, caused by the performance problem (see following graph for illustration)
  - It turns out (see algebra following graph) that, numerically, the incremental CCDP is equal to the increase in the time-weighted average CDF, if the averaging is done for a period of one year
    - So result from SDP can be compared to color criteria for PIs
- What the colors in Table 5 mean in terms of increase in annual time-averaged CDF
  - Red: increase is  $\geq 10^{-4}/\text{yr}$
  - Yellow: increase is between  $10^{-5}/\text{yr}$  and  $10^{-4}/\text{yr}$
  - White: increase is between  $10^{-6}/\text{yr}$  and  $10^{-5}/\text{yr}$
  - Green: increase is  $< 10^{-6}/\text{yr}$



# Illustrative CDF Profile





# Algebra for CDF Profile (optional)

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

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



# Algebra for CDF Profile (cont.)

$$\begin{aligned}
 CDF_{ave,new} - CDF_{ave,old} &= \frac{CDF_1 t_2 - CDF_1 t_1 + CDF_2 t_3 - CDF_2 t_2 - CDF_2 t_3 + CDF_2 t_1}{t_{end}} \\
 &= \frac{CDF_1(t_2 - t_1) - CDF_2(t_2 - t_1)}{t_{end}} = \frac{(CDF_1 - CDF_2)(t_2 - t_1)}{t_{end}} = \frac{\Delta C C D P}{t_{end}}
 \end{aligned}$$

**If  $t_{end} = 1$  yr, then numerically  $\Delta CDF_{ave} = \Delta C C D P$ , as claimed**



# SDP for External Initiators

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



# SDP for External Initiators (cont.)

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



# SDP for Containment Integrity

- IMC 0609, App. H contains Containment Integrity SDP
- Significance criteria for  $\Delta\text{LERF}$  are order of magnitude less than for  $\Delta\text{CDF}$ 
  - Red: increase  $\geq 10^{-5}/\text{yr}$
  - Yellow: increase  $\geq 10^{-6}/\text{yr}$  and  $< 10^{-5}/\text{yr}$
  - White: increase  $\geq 10^{-7}/\text{yr}$  and  $< 10^{-6}/\text{yr}$
  - Green: increase  $< 10^{-7}/\text{yr}$
- Finding that is “Green” for  $\Delta\text{CDF}$  could be “White” for  $\Delta\text{LERF}$



# SDP for Containment Integrity (cont.)

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



# SDP for Containment Integrity (cont.)

- SDP considers two types of findings, Type A and Type B
- Type A findings
  - Findings that affect CDF; CDF SDP performed
  - LERF considerations may adjust final risk significance
  - Use Appendix H
- Type B findings
  - Findings that do not affect CDF; CDF SDP not performed
  - Appendix H, Section 6, Phase 1 and 2 for findings at full power and at shutdown



# Combustion Engineering Owners Group

## Probabilistic Safety Assessment Working Group AOT Pilot Program



# MODULE B

## TRADITIONAL ENGINEERING ANALYSIS AND PRA APPROACHES TO SAFETY ANALYSIS



**Combustion Engineering Owners Group  
Probabilistic Safety Assessment Working Group  
AOT Pilot Program**



## **AOT Pilot Program is a Group Submittal**

- CEOG is the pilot for the 3 proposed AOT changes
- Pilot includes AOT changes to SIT, LPSI, & EDGs
- Utilizes a blended approach:
  - Statement of Need
  - Deterministic Issues
  - Specific plant PRA evaluations (these are compared for consistency/differences & differences are understood as part of the PRA validation process)
  - Where appropriate, contingency/compensatory measures identified
- One single joint application; however individual plant results are evident
- First submitted May 1995; has had multiple reviews and presentations to NRC and ACRS.



# **Safety Injection Tank (SIT)**

## **Technical Specification Change Requested**

- Extend AOT for a single Inoperable SIT from 1 hour (typically) to 24 hours

- NEED:

- Number of entries into action statements by CE plants
- Concern over 1 hour AOT has led to unnecessary doses to correct potential malfunctions
- Change will allow time to diagnose and correct problems at power
- Should avert unnecessary plant shutdowns (safety and economical impact)

- DETERMINISTIC CONSIDERATIONS:

- Design Basis calculations are quite conservative; best estimate calcs show do not need 1 LPSI train & 1 HPSI train & all SITs
- 10CFR100 results also very conservative for a Large LOCA, even without design basis number of SITs



## **Low Pressure Safety Injection (LPSI) Technical Specification Change Requested**

- Extend AOT for a single Inoperable LPSI train from its present value (24 or 72 hrs depending on the plant) to 7 days (168 hours) [a LPSI train is defined as 1 pump, 2 flow paths including MOVs on a common AC power source]
- NEED:
  - Reduce simultaneous PMs and avoid stress of being near AOT
  - Will allow time for maint./repair/testing of LPSI while at power
  - Avert unnecessary shutdowns with an impaired SDC (LPSI)
- DETERMINISTIC CONSIDERATIONS:
  - LOCA Design Basis calcs are quite conservative; best estimate calcs show do not need 1 LPSI train & 1 HPSI train & all SITs (can be successful without LPSI at all)
  - 10CFR100 results also very conservative for a Large LOCA, no core melt expected even without LPSI using best estimate calcs
  - Can mitigate SGTR w/o SDC by steaming SG, refill CST/use AFW, use cont't. spray for SDC-no release expected if SG isolated



# **Emergency Diesel Generator (EDG)**

## **Technical Specification Change Requested**

- Extend AOT for a single Inoperable EDG from 72 hours to 10 days (for most plants)
- NEED:
  - Reduce number of entries into action statements to perform activities to meet SBO Rule (perform more in a single tagout)
  - Reduce simultaneous PMs and avoid stress of being near AOT
  - Will allow time for maint./repair/testing of EDGs while at power
  - Avert unnecessary shutdowns
  - Better EDG reliability “at power” and in early stages of shutdown
- DETERMINISTIC CONSIDERATIONS:
  - EDGs provide emergency power following events involving loss of offsite power -
    - applies to both power and lower mode operations. Would be better to have improved reliability for power & lower modes of operation.



## **Any Proposed Technical Specification Change Should Either:**

- Be risk neutral, or
- Result in a decrease in plant risk, or
- Result in a small increase in plant risk

And

- Be needed to more efficiently and/or more safely manage plant operations



## **Multiple Analyses Performed & Compared**

- Performed for each CE plant
- The most up-to-date PRA used at each plant
- In cases where plant design or other information yield non-symmetric results (i.e., it matters which SIT or LPSI train or EDG is affected), the most pessimistic results (for allowing the tech spec change) were always used
- While the calculation manipulations were actually made using the already solved complete model cut sets, this course material will demonstrate the effects on the individual parts of the PRA for instructional purposes.



## **We Will Go Over in Class...**

- Initiating Events and Event Tree considerations for the SIT and LPSI cases
- The complete SIT case analysis
- Touch upon the additional complexities of the LPSI and EDG cases



# MODULE D

## ACCIDENT SEQUENCE INITIATING EVENTS



**Based on the Example Information Provided  
for 1 Plant in the Following Slides,  
For Which Initiating Events in the PRA Does  
Each AOT Case Have to be Analyzed?**

- ▲ SITs AOT Extension?
- ▲ LPSI AOT Extension?



## **Design Basis Requirements for the Plant (in accordance with Appendix K to 10CFR50)**

- ▲ Injection by all but one of the SITs (one is assumed ineffective due to break location) in Large Break LOCAs.
- ▲ Injection by LPSI during a Large Break LOCA in combination with the SITs (mentioned above) & HPSI, and in combination with a loss of offsite power and the “worst” single equipment failure.
- ▲ Use of LPSI to provide shutdown cooling (SDC) in a steam generator tube rupture (SGTR) event with/without offsite power.



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

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

\* Large LOCA success criteria based on calculations performed for a (<3 ft<sup>2</sup> equivalent area) credible pipe break, and realistic post-accident thermal hydraulic system performance.

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

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



Table 3.1.1: Initiating Event Summary

Initiator	Description	Classification
$T_1$	Reactor Trip - results from a system disturbance that causes the RPS to insert control rods to terminate the nuclear chain reaction.	Transient
$T_2$	Loss of Condenser Vacuum - results in a loss of MFW, and a loss of SDBC system for secondary pressure relief and heat removal. A loss of condenser vacuum causes depletion of hotwell inventory failing MFW. It also prevents steam dump to the condenser.	Transient
$T_3$	Turbine Trip - includes events that generate a turbine trip signal and a consequent reactor trip signal.	Transient
$T_4$	Loss of Main Feedwater - results in a failure of all Main Feedwater flow to the steam generator. This loss of flow may result in a pressurization of the primary system if SDBC fails. This class of events includes total loss of MFW flow, full closure of feedwater isolation valves, and feedline breaks upstream of the feedwater check valves.	Transient
$T_{SA}$	Loss of 345 KV with 161 KV Unavailable (Plant-Centered) - can lead to a reactor trip and a requirement for emergency diesel generators to prevent station blackout. $T_{SA}$ results in a loss of power to all 4KV buses.	Transient
$T_{SB}$	Loss of 161 KV with Failure to Fast Transfer (Plant-Centered) - can lead to a reactor trip and a requirement for emergency diesel generators to prevent station blackout. $T_{SB}$ results in a loss of power to all 4KV buses.	Transient
$T_{SC}$	Loss of Off-Site Power (Grid-Related) - can lead to a reactor trip and a requirement for emergency diesel generators to prevent station blackout. $T_{SC}$ results in a loss of offsite power to all the 4160 V buses due to events related to the reliability of the grid.	Transient



Initiator	Description	Classification
$T_{SD}$	Loss of Off-Site Power (Weather-Induced) - can lead to a reactor trip and a requirement for emergency diesel generators to prevent station blackout. $T_{SD}$ results in a loss of offsite power to all the 4160 V buses due to events related to severe weather conditions.	Transient
$T_6$	Steamline/Feedline Break on SG2 Upstream of MSIVs and Downstream of FWCVs - assumed to cause a blowdown of SG2 and a rapid depressurization of the primary system, causing a Pressurizer Pressure Low Signal (PPLS), main steam isolation, main feedwater isolation, and isolation of AFW to SG2. The steam supply to the turbine-driven AFW pump from SG2 will also be unavailable.	Transient
$T_7$	Steamline Break on SG2 Downstream - assumed to cause an initial blowdown of both SGs and a rapid depressurization of the primary system, causing a PPLS and Steam Generator Isolation Signal (SGIS).	Transient
$T_8$	Loss of 4 KV Bus 1A1 - represents a loss of power on 4 KV Bus 1A1 due to an electrical fault that causes bus failure. A loss of power to 4 KV Bus 1A1 will result in a loss of Reactor Coolant Pump RC-3A and subsequent reactor trip on low RCS flow. (special initiator)	Transient
$T_9$	Loss of 4 KV Bus 1A3 - represents a loss of power on 4 KV Bus 1A3 due to an electrical fault that causes bus failure. A loss of power to 4 KV Bus 1A3 will result in a loss of Reactor Coolant Pump RC-3C and subsequent reactor trip on low RCS flow. (special initiator)	Transient
$T_{10}$	Loss of 4 KV Bus 1A4 - represents a loss of power on 4 KV Bus 1A4 due to an electrical fault that causes bus failure. A loss of power to 4 KV Bus 1A4 will result in a loss of Reactor Coolant Pump RC-3D and subsequent reactor trip on low RCS flow. (special initiator)	Transient
$T_{11}$	Loss of 4 KV Bus 1A2 - represents a loss of power on 4 KV Bus 1A2 due to an electrical fault that causes bus failure. A loss of power to 4 KV Bus 1A2 will result in a loss of Reactor Coolant Pump RC-3B and subsequent reactor trip on low RCS flow. (special initiator)	Transient



Initiator	Description	Classification
T <sub>12</sub>	Loss of 125 VDC Bus # 1 - represents a loss of power on 125 VDC Bus #1 due to an electrical fault that causes bus failure. (special initiator)	Transient
T <sub>13</sub>	Loss of 125 VDC Bus # 2 - represents a loss of power on 125 VDC Bus #2 due to an electrical fault that causes bus failure. This event is expected to cause a challenge to the primary PORVs. (special initiator)	Transient
T <sub>14A</sub>	Loss of 125 VDC Panel AI-41A - represents a loss of power on 125 VDC Panel AI-41A due to an electrical fault that causes panel failure or by a loss of power to the panel because the power supply breaker to the panel transfers open. (special initiator)	Transient
T <sub>14B</sub>	Loss of 125 VDC Panel AI-41B - represents a loss of power on 125 VDC Panel AI-41B due to an electrical fault that causes panel failure or by a loss of power to the panel because the power supply breaker to the panel transfers open. This event is expected to cause a challenge to the primary PORVs. (special initiator)	Transient
T <sub>15</sub>	Loss of CCW System - represents a failure of CCW flow due to system initiated failures. (special initiator)	Transient
T <sub>16</sub>	Loss of Raw Water System - represents failure of Raw Water flow due to system initiated failures. (special initiator)	Transient
T <sub>17</sub>	Loss of Instrument Air - represents a failure of instrument air due to system induced failure. Automatic or manual trip is assumed to occur. (special initiator)	Transient
T <sub>18</sub>	Loss of HVAC to Room 56 - T <sub>18</sub> represents a loss of cooling to electrical equipment in Room 56. Specifically, a loss of cooling to Inverters A and C (without human intervention) is assumed to result in a loss of power to Instrument Buses AI-40A and AI-40C respectively. (special initiator)	Transient
T <sub>19</sub>	Loss of HVAC to Room 56A - represents a loss of cooling to electrical equipment in Room 56A. Specifically, a loss of cooling to Inverters B and D (without human intervention) is assumed to result in a loss of power to Instrument Buses AI-40B and AI-40D respectively. (special initiator)	Transient



Initiator	Description	Classification
T <sub>20</sub>	Loss of HVAC to Control Room (Rm. 77) - represents a loss of cooling to electrical equipment in Room 77. Specifically, loss of cooling to normally energized ESCS relays (without human intervention) is assumed to cause the relays to fail in the de-energized state. (special initiator)	Transient
T <sub>21</sub>	Closure of MSIV (1 SG Loop) - results in a reactor trip on loss of load or asymmetric SG transient. This event causes secondary side pressurization of the affected SG loop resulting in a challenge to the MSSVs. RCS pressurization to the PORV setpoint is precluded if the SDBC valves or MSSVs of the affected SG provide adequate steam flow. If a MSSV fails to reclose, secondary depressurization causes a SGIS signal which isolates MFW and Main Steam to both SGs.	Transient
T <sub>22</sub>	Closure of both MSIVs - results in a reactor trip on loss of load and causes secondary side pressurization resulting in a challenge to the MSSVs in both SG loops. RCS pressurization to the PORV setpoint is precluded if the MSSVs on both SG loops provide adequate steam flow. If a MSSV fails to reclose, secondary depressurization will cause a SGIS signal which isolates MFW and Main Steam to both SGs.	Transient
T <sub>23</sub>	Partial Load Rejection - represents a partial reduction of external load on the main generator that precludes a turbine/generator reactor trip. RCS pressure increases above 2350 psia causing reactor trip on high pressurizer pressure and a challenge to the PORVs.	Transient
T <sub>24</sub>	Spurious SGIS Signal - represents a spurious SGIS Signal that isolates MFW and MSIV to both SGs. The reactor trips on loss of load.	Transient
T <sub>25</sub>	Reactor Trip With PORV Opening - represents a transient initiator that causes direct opening of a PORV.	Transient
S	Small LOCA - is a break in the RCS pressure boundary in some location other than the steam generator that exceeds normal charging flow. For these break sizes, the normal charging system cannot maintain level in the pressurizer. Break sizes less than 0.0005 ft <sup>2</sup> in area are considered leaks rather than small LOCAs.	Small LOCA



Initiator	Description	Classification
M	Medium LOCA - will depressurize the RCS without secondary heat removal to a point where HPSI flow will be sufficient to prevent core damage by removing decay heat, but is not large enough to require the safety injection tanks (SITs) or LPSI. The minimum size for a medium LOCA is 0.00225 ft <sup>2</sup> in area.	Medium LOCA
A	Large LOCA - represents a wide range of requirements on the ECCS. HPSI or LPSI supplemented by the SITs will have sufficient capacity to cover the entire large LOCA range.	Large LOCA
R	Steam Generator Tube Rupture - credible tube failures range in severity from leak rates of a few gallons to several hundred gallons per minute for the guillotine rupture of several tubes. The event chosen as representative of this range is the complete severance of a single tube.	SGTR
I <sub>1</sub>	Failure of LPSI due to RCS/LPSI Injection Interface (M17) ISL - a LOCA from the primary system through an interfacing system of lower design pressure.	ISL
I <sub>2</sub>	Failure of LPSI due to RCS/LPSI DHR Return Interface (M16) ISL - a LOCA from the primary system through an interfacing system of lower design pressure.	ISL
I <sub>3</sub>	Failure of CCW due to RCS/CCW Interface (M18, M19) ISL - a LOCA from the primary system through an interfacing system of lower design pressure.	ISL
I <sub>4</sub>	Failure of CVCS due to RCS/Letdown Interface (M2) ISL - a LOCA from the primary system through an interfacing system of lower design pressure.	ISL
F	Reactor Vessel Failure - failure of the FCS reactor vessel boundary that results in a small or medium LOCA is assumed to be covered by the S and M LOCA categories, since penetrations for in-core instrumentation are located near the top of the vessel. Therefore, the reactor vessel failure event is assumed to result in an unmitigatable large LOCA that occurs at the bottom of the vessel. This initiator was not modeled due to low expected likelihood of occurrence. ( $\leq 1.0E-08$ )	Not Modeled



# MODULE F

## SYSTEMS ANALYSIS USING FAULT TREES



**Based on the Example Information  
Which Follows for 1 Plant,  
Which Event Trees/Sequences in the PRA  
Need to be Used to Examine Each AOT Case?**

- SITs AOT Extension?
- LPSI AOT Extension?



# (3.1): FCS TRANSIENT EVENT TREE

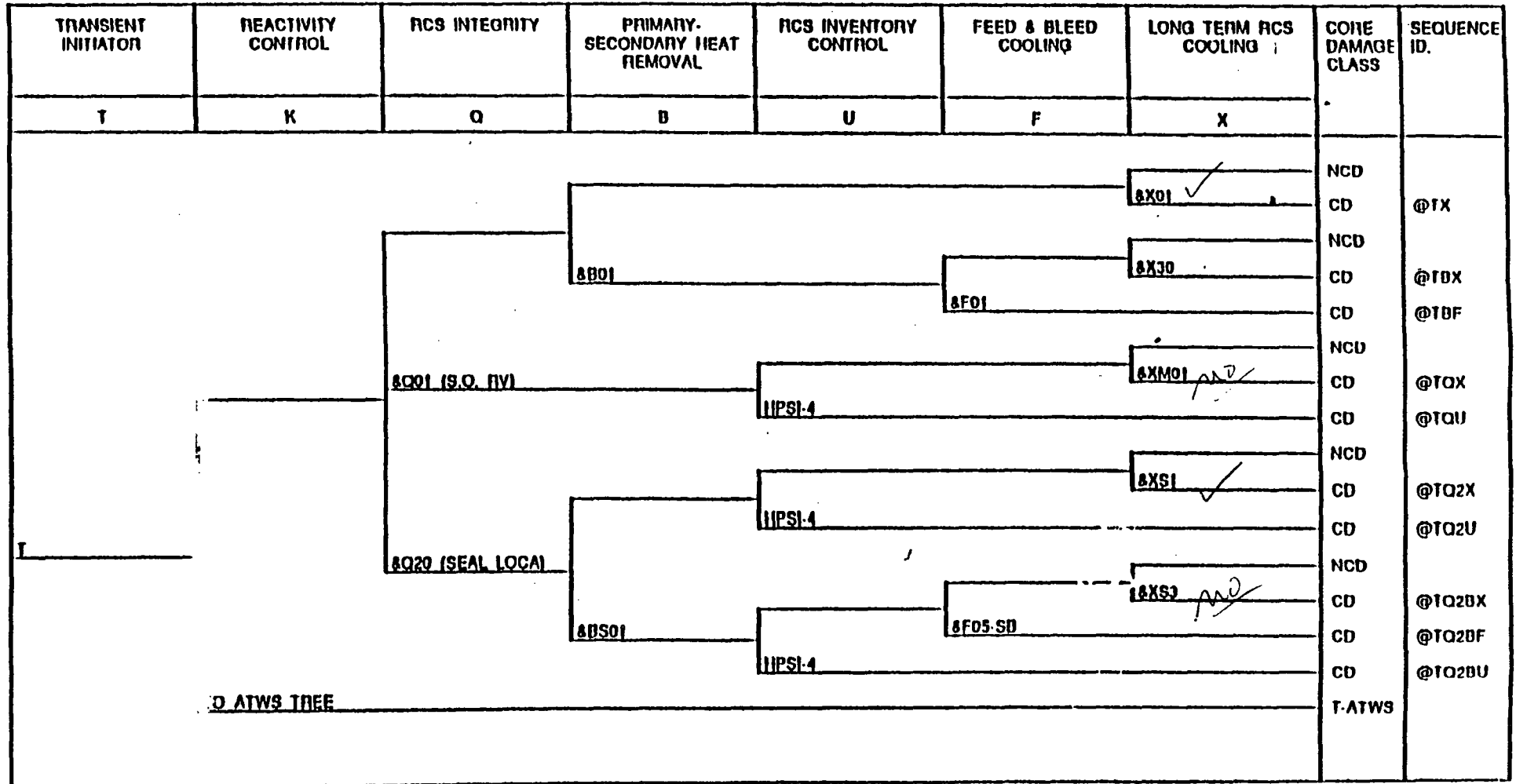


FIG. (3.1): FCS TRANSIENT EVENT TREE

ATWS TREE FIG. 3.1

8-27-93



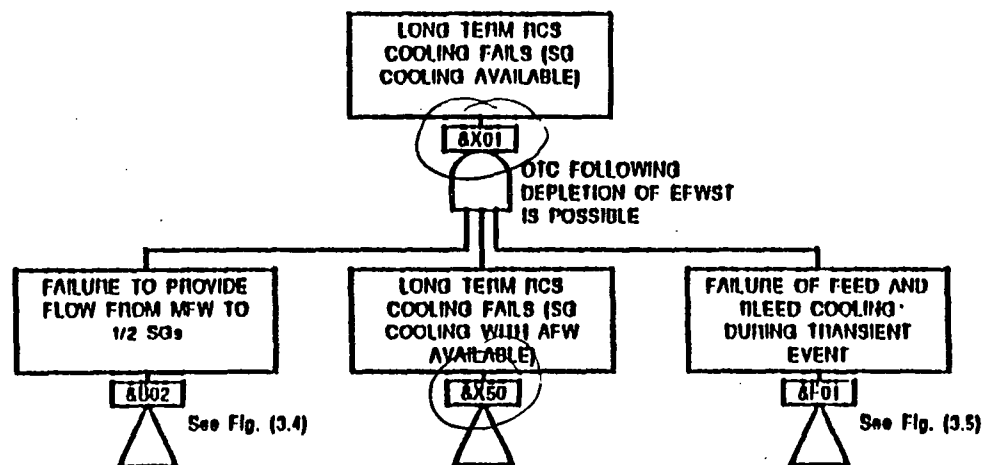


Fig. (3.6): TOP LOGIC MODEL - &X01

A:\TREE\FIG36.CAF

9-01-93



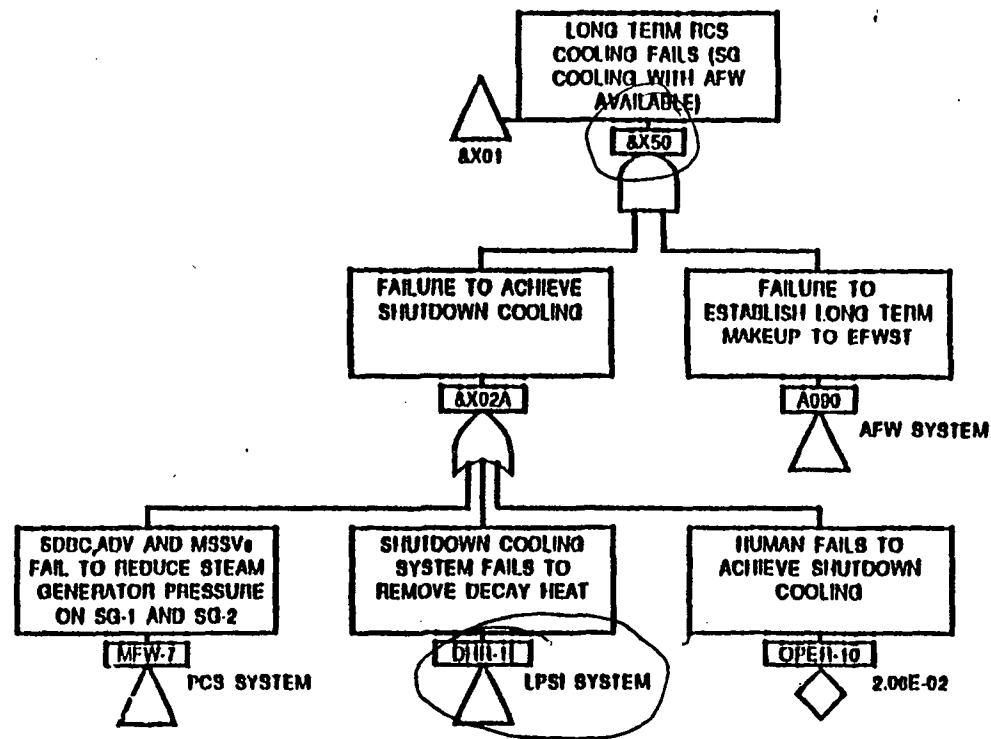


Fig. (3.6): TOP LOGIC MODEL - &X01

A:\TREE\FIG36.CAF

9-01-93



# (3.8): FCS SMALL LOCA EVENT TREE

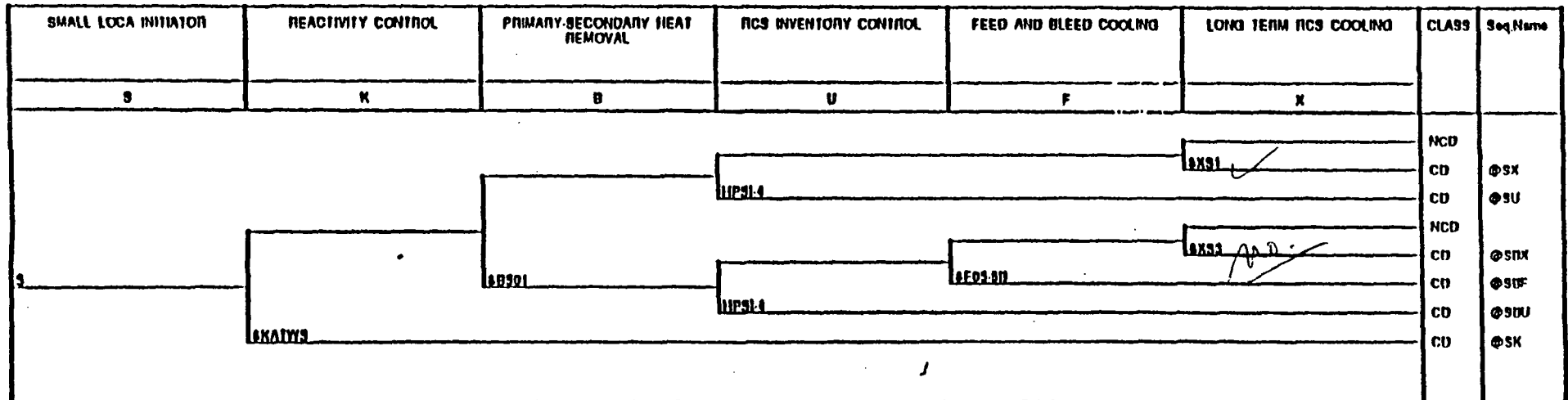


FIG. (3.8): FCS SMALL LOCA EVENT TREE

ANETREEV1030.THE

8-27-03



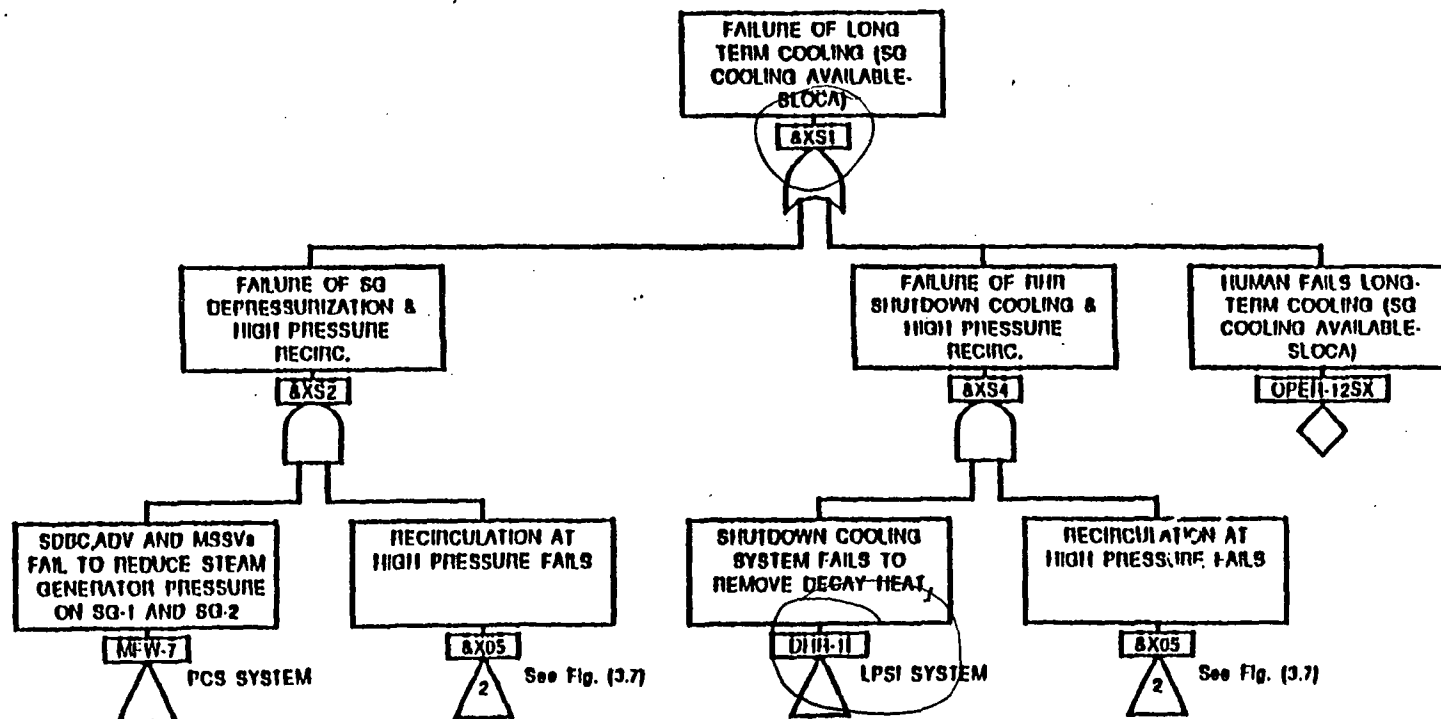
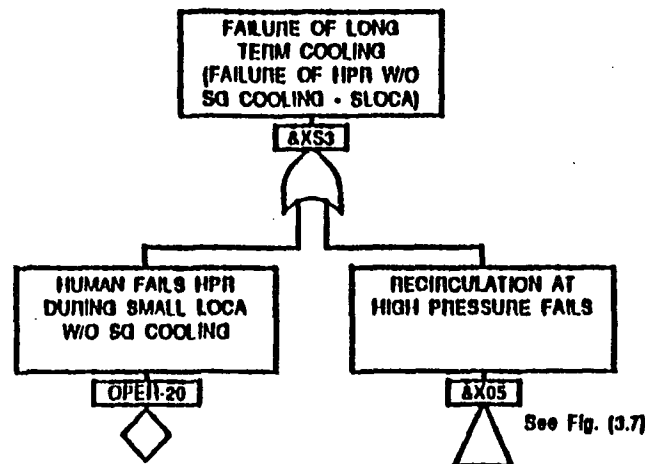


Fig. (3.11): TOP LOGIC MODEL - &amp;XS1

A:\TREE\FIG311.CAF

9-01-93





See Fig. (3.7)

*no*



(3.15): FCS LARGE LOCA EVENT TREE

LARGE LOCA INITIATOR	FCS INVENTORY CONTROL	RECIRCULATION & INVENTORY CONTROL	CLASS	Seq.Name
A	UA	XA		
A			NCD	
	&XA01 ✓		CD	@AXA
	&UA01 ✓		CD	@AUA

FIG. (3.15): FCS LARGE LOCA EVENT TREE

A:\ETREE\FIG315.TRE

8-27-93



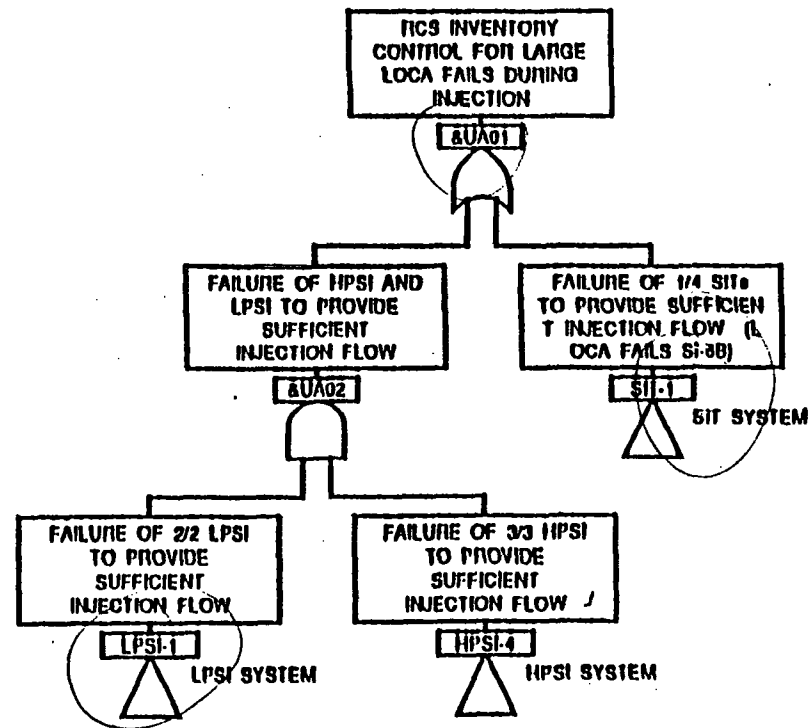


Fig. (3.16): TOP LOGIC MODEL - &amp;UA01

A:\TREE\FIG316.CAF

9-01-93



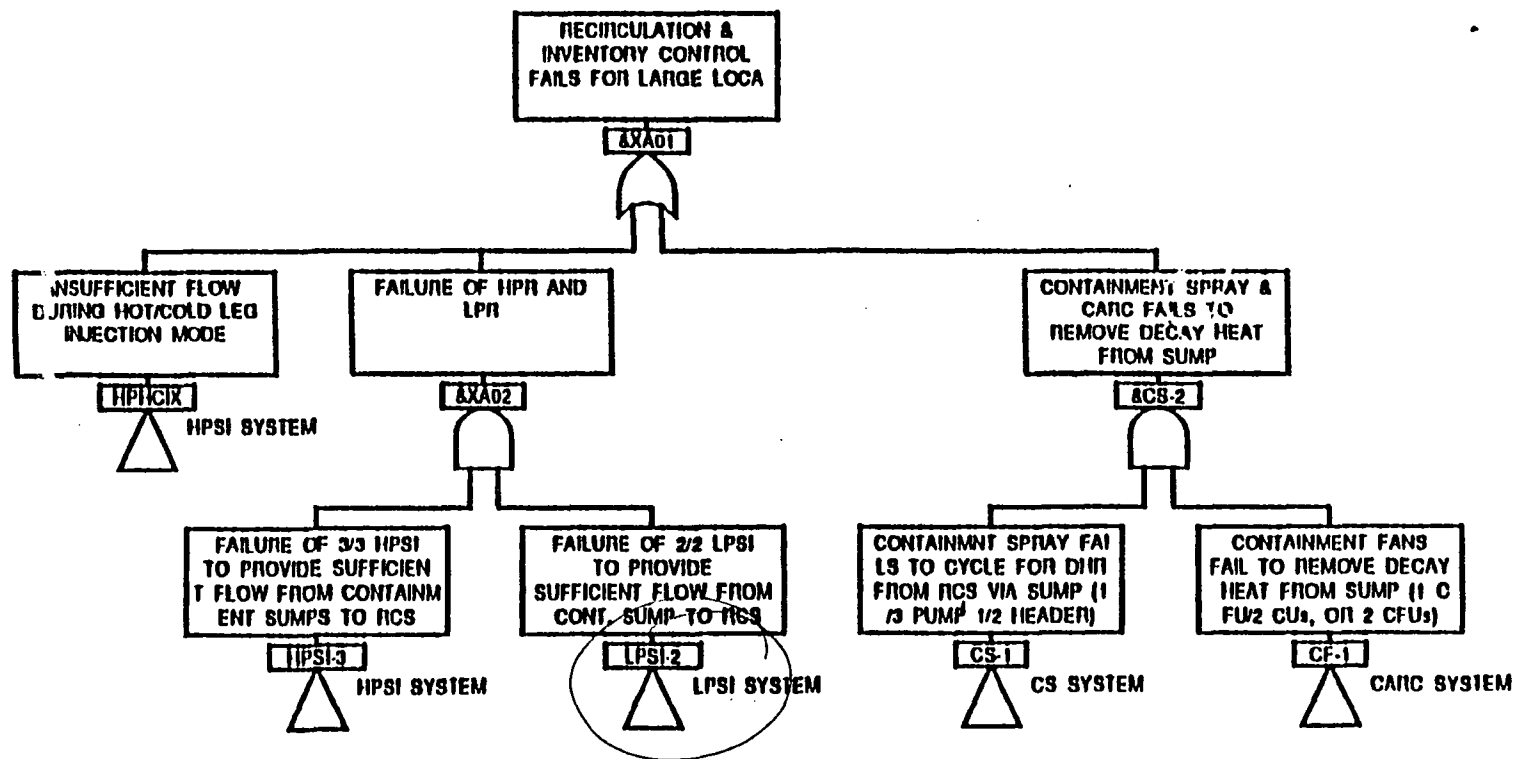


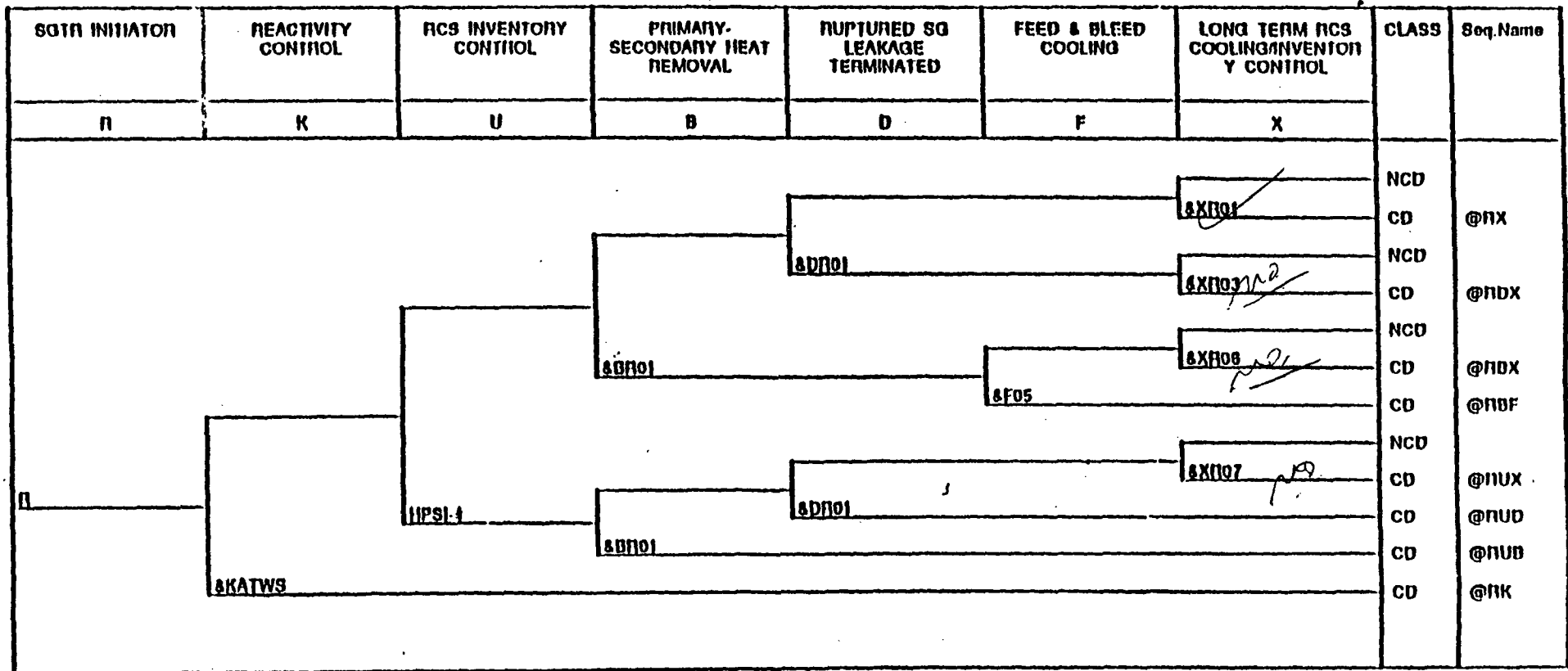
Fig. (3.17): TOP LOGIC MODEL - &XA01

A:\TREE\FIG317.CAF

9-01-93



(3.18): FCS SGTR.EVENT TREE MODEL



**FIG. (3.18): FCS SGTN EVENT TREE MODEL**

## A: A TREE FIGURE THE

**8-27-83**



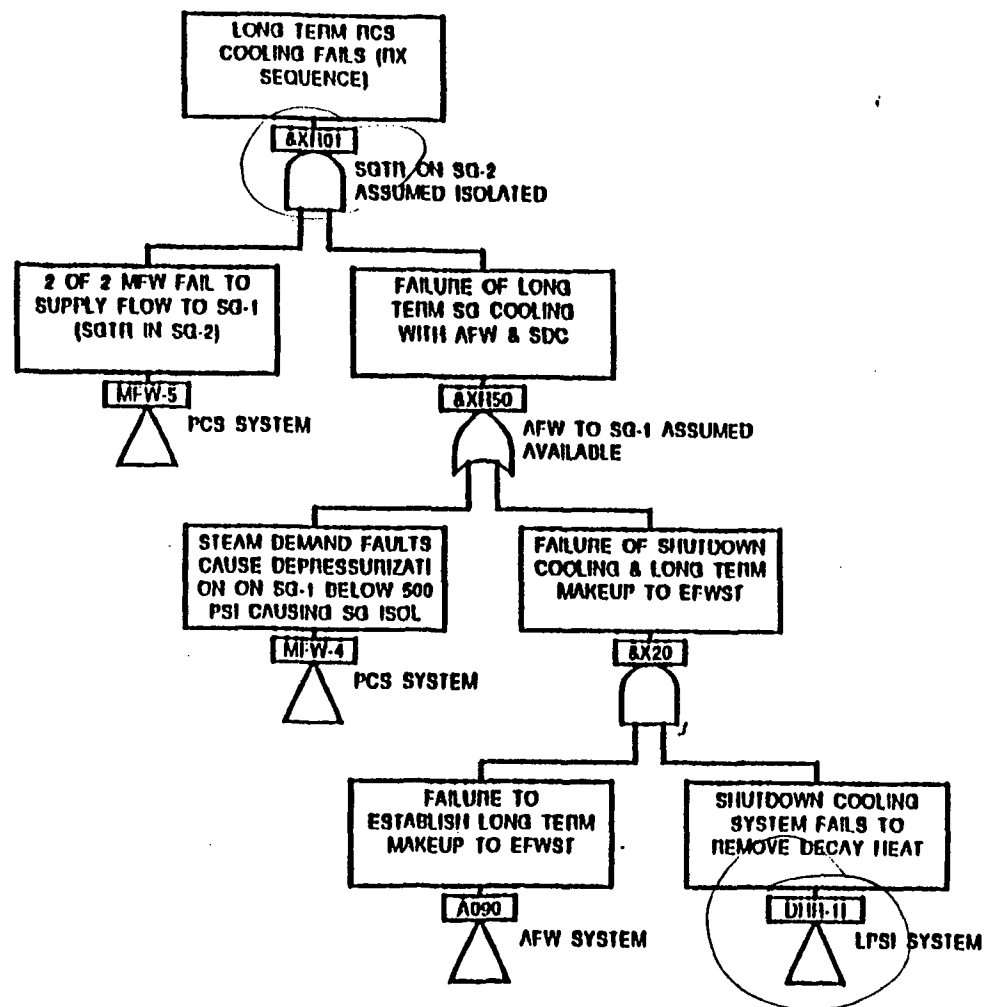


Fig. (3.22): TOP LOGIC MODEL - &XR01

A:\TREE\FIG322.CAF

9-01-93



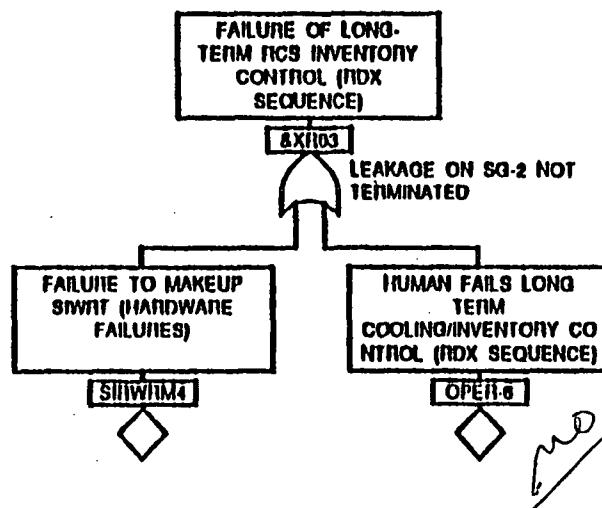


Fig. (3.23): TOP LOGIC MODEL - XR03

A:\TREE\FIG323.CAF

9-01-93



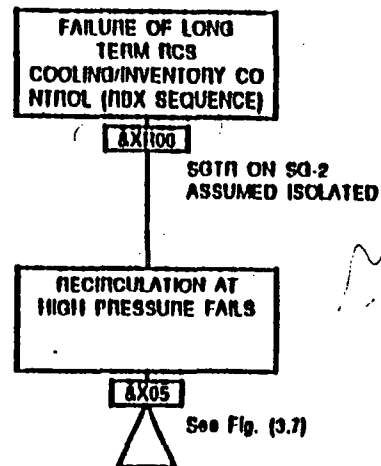
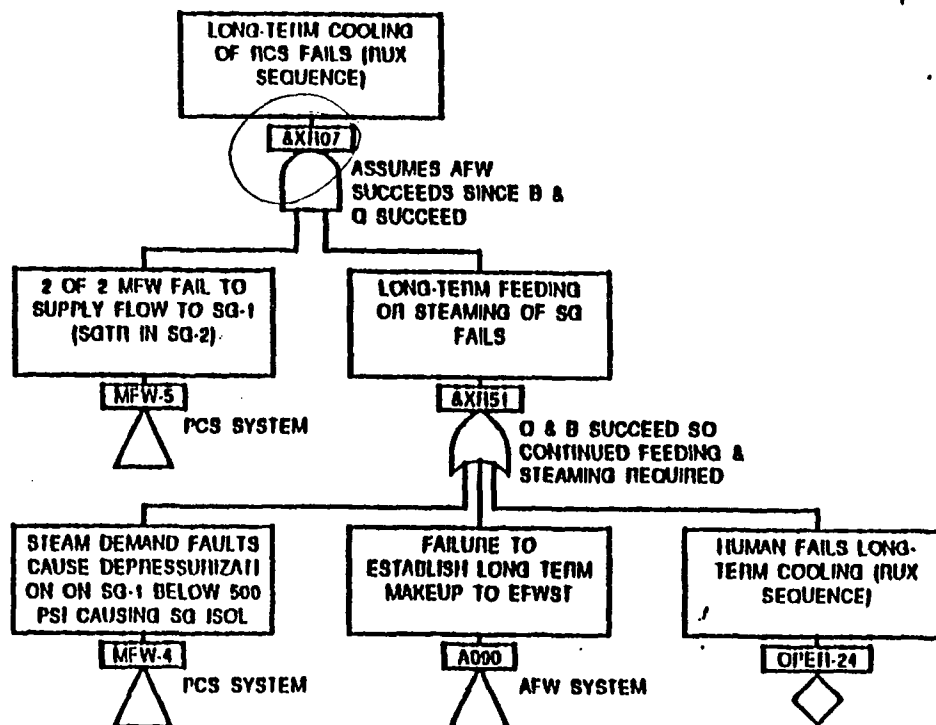


Fig. (3.24): TOP LOGIC MODEL - &XR06

A:\TREE\FIG324.CAF

9-01-93





*no.*

Fig. (3.25): TOP LOGIC MODEL - &XR07

A:\TREE\FIG325.CAF

9-01-93



(3.34): FCS ISL 13 EVENT TREE MODEL

INITIAL CONDITION	REACTIVITY CONTROL	INIT PRESSURE REACTION	PRIMARY/SECONDARY HEAT REMOVAL	TERMINATION OF EX-CONTAINMENT LEAKAGE	LONG TERM RCS COOLING	CLASS	REQ NAME
ISO	R	U	B	D	X		
INIT	REACTORS	ISLSA	BD581	BD581	BD581 ✓	NCD	Q10X
						CD	Q100X
						CD	Q100X
						CD	Q100U
						CD	Q100U
						CD	Q100X

FIN (334) ISL IS EV'NT TREE MODEL. A/EINTERVIEW TIME 0 27:03

FCS (3.34) ISL 13 EVENT TREE MODEL. AVEINER10334 TIE 0 27-93



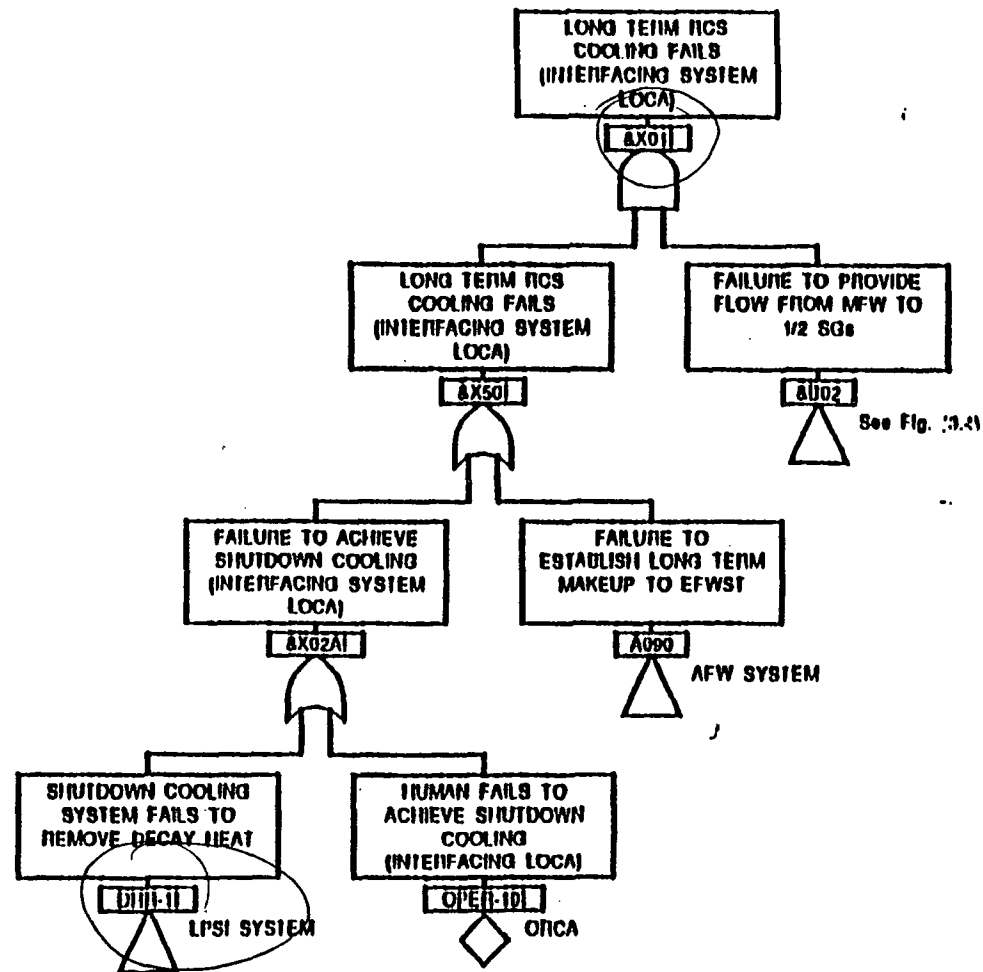


Fig. (3.41): Top Logic Model - &amp;X011

A:\TREE\FIG341.CAF

9-01-93



# **Overall Results of AOT Extension Analyses from Core Damage (Level 1 PRA) Perspective**



## SIT AOT Extension Case

<b>Plant</b>	<b>At-Power Single AOT (assuming full 24 hrs)</b>	<b>Transition Risk CDP</b>
ANO-2	2.30E-8	6.92E-7
CC-1/2	9.37E-7	4.45E-6
Ft Calhoun	2.74E-8	2.49E-7
Maine Yankee	negligible	1.56E-6



## SIT AOT Extension Case (continued)

Plant	At-Power Single AOT (assuming full 24 hrs)	Transition Risk CDP
Millstone-2	negligible	7.19E-7
Palisades	8.77E-9	1.09E-6
Palo Verde 1,2,3	3.84E-9	1.00E-6
San Onofre 2/3	1.03E-6	5.78E-7

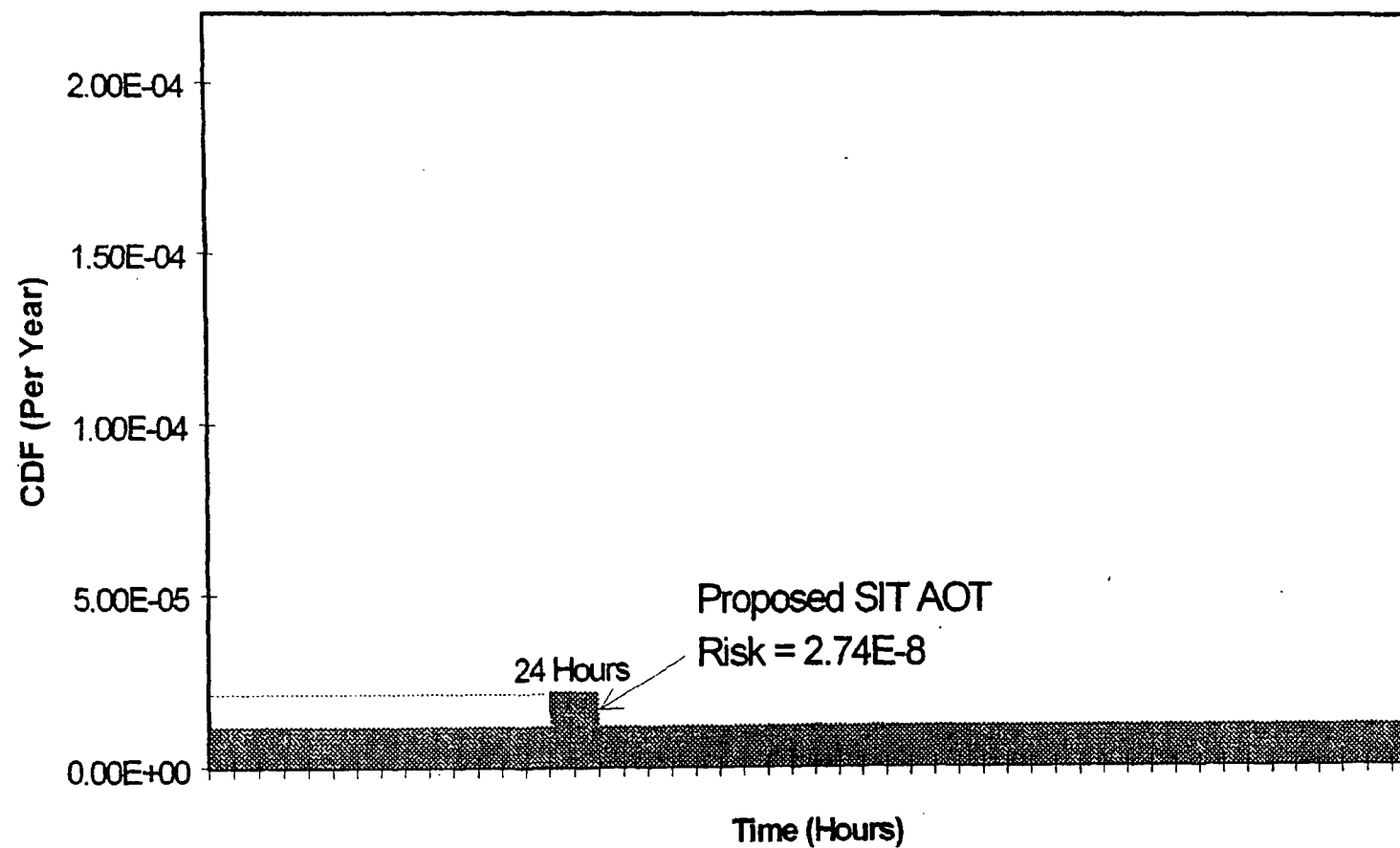


## SIT AOT Extension Case (continued)

Plant	At-Power Single AOT (assuming full 24 hrs)	Transition Risk CDP
St Lucie 1	5.5E-7	4.51E-7
St Lucie 2	5.5E-7	4.96E-7
Waterford 3	1.37E-7	3.25E-7



# Ft. Calhoun SIT AOT Case





# SIT AOT Extension Case (continued)

## Observations

- ※ Performing SIT maintenance at power (per the extension request) versus during shutdown generally results in a decrease in overall risk
  - ⇒ CDP for continued operation of the plant with one SIT inoperable is generally less than the CDP associated with transitioning the plant to shutdown
  - ⇒ Even for those plants where there is a slightly greater CDP for at-power, when one considers the bias of the analysis (optimistic toward shutting down) and the fact that not *all* the transition risk was accounted for (e.g., did not include lower mode operation and return to power risks), SIT maintenance during power would be beneficial
- ※ Expected yearly risk by performing at-power SIT maintenance is small
- ※ Average CDFs are virtually unchanged
- ※ Do not need design basis number of SITs to prevent core damage
- ※ Should avert shutdowns (unnecessary safety risk & economic impact)



# SIT AOT Extension Case (continued)

Additionally, plants noted:

- ✱ No extraordinary compensatory actions need to be performed when 1 SIT is out of service
- ✱ Operability of other SITs should be verified before taking SIT out of service
- ✱ This should not coincide with scheduled removal of additional ECCS plant components from service
- ✱ The process of considering both the deterministic bases for the SITs, including conservatism in the Design Basis, and the different risk results from the PRA calculations, allowed for a better appreciation for the risk importance of the SITs and a feeling for how changes in the AOT can affect this importance.



## LPSI AOT Extension Case

Plant	At-Power Single AOT (assumes full 7 days)		Transition Risk CDP
	CM	PM	
ANO-2	2.92E-7	8.06E-8	6.92E-7
CC-1/2	1.92E-7	1.34E-7	4.45E-6
Ft Calhoun	negligible	negligible	2.49E-7
Maine Yankee	1.50E-6	1.04E-7	1.56E-6



# LPSI AOT Extension Case (continued)

Plant	At-Power Single AOT (assumes full 7 days)		Transition Risk CDP
	CM	PM	
Millstone-2	2.40E-6	1.80E-7	7.19E-7
Palisades	negligible	negligible	1.09E-6
Palo Verde 1,2,3	4.33E-7	1.15E-8	1.00E-6
San Onofre 2/3	1.55E-6	1.09E-7	5.78E-7

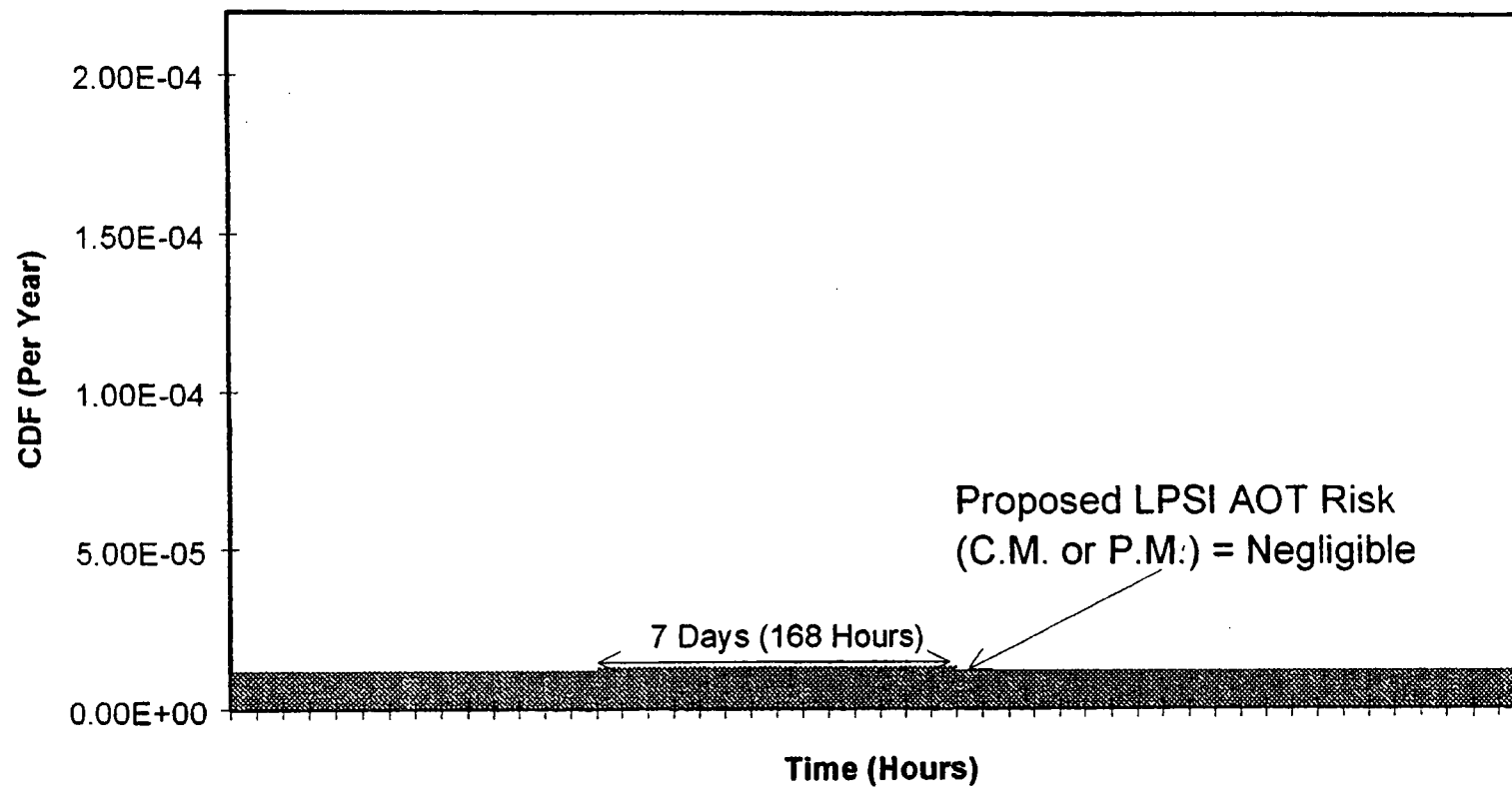


# LPSI AOT Extension Case (continued)

Plant	At-Power Single AOT (assumes full 7 days)		Transition Risk CDP
	CM	PM	
St Lucie 1	1.3E-6	2.1E-7	4.51E-7
St Lucie 2	1.3E-6	1.6E-7	4.96E-7
Waterford 3	4.14E-7	1.34E-8	3.25E-7



# Ft. Calhoun LPSI AOT Case





# LPSI AOT Extension Case (continued)

## Observations

- ✱ Performing LPSI maintenance at power (per the full extension request) versus during shutdown generally results in a decrease in overall risk
  - ⇒ CDP for continued operation of the plant with one LPSI inoperable is generally less than the CDP associated with transitioning the plant to shutdown (in some cases a small increase for CM)
  - ⇒ Even for those plants where there is a slightly greater CM-CDP for at-power, when one considers the bias of the analysis (optimistic toward shutting down) and the fact that shutdown risk can be lessened by small improvements made to LPSI rel'y while at-power, LPSI maintenance during power would be beneficial
- ✱ Expected yearly risk by performing at-power LPSI maint. is small
- ✱ Average CDFs are virtually unchanged
- ✱ Gained an appreciation that do not need LPSI to prevent core damage
- ✱ Averting shutdowns important, *especially* with a potentially degraded LPSI needed for SDC (unnecessary safety risk & economic impact)



# **LPSI AOT Extension Case (continued)**

Additionally, plants noted:

- ✱ No extraordinary compensatory actions need to be performed when 1 LPSI train is out of service
- ✱ Operability of other LPSI train should be verified before taking 1 LPSI out of service
- ✱ This should not coincide with scheduled removal of any single SIT from service (since LPSI & SITs used in Large LOCA), nor with the scheduled removal of any AFW components from service (since AFW and LPSI for SDC backup each other for long term heat removal)
- ✱ Should attempt to minimize maintenance risks (plans for re-establishing train to service if required, align for emergency use to extent possible...)



# EDG AOT Extension Case

- ✱ Still under review by NRC staff and potentially subject to modification.



# MODULE L

## LEVEL 2 & 3 ANALYSIS



# **Overall Results of AOT Extension Analyses from Large Early Release (Level 2 PRA) Perspective**



# Large Early Releases Are Dominated By...

- ☞ Containment Bypass Events
  - ❖ ISLOCAs
  - ❖ SGTRs with concomitant loss of SG isolation
- ☞ Severe Accidents Accompanied by Loss of Containment Isolation
- ☞ Containment Failure Associated With Energetic Events in Containment (high pressure melt phenomena including direct containment heating and hydrogen burns)



Detailed Level 2 Analyses Were Not Performed  
But The Following Impacts Were Noted



# The Inoperability of 1 SIT...

- ☞ Would not impact containment bypass events as SITs do not significantly alter the event progression.
- ☞ Would cause a small increase in containment isolation failure events based on a slight increase in severe accidents involving SIT failure but note that in most cases, containment sprays would be operable thereby scrubbing any release. Also, containment isolation failure is low probability.
- ☞ Would not impact energetic events which are dominated by transients under high pressure; SITs come into play in low pressure events.



# The Inoperability of 1 LPSI Train...

- ☞ Would not impact containment bypass events since even though the LPSI lines could be a source of an ISLOCA, testing of applicable valves are governed by other tech specs which would not change under the arguments presented in this request.
- ☞ Would cause a small increase in containment isolation failure events based on a slight increase in severe accidents involving LPSI failure but note that in most cases, containment sprays would be operable thereby scrubbing any release. Also, containment isolation failure is low probability.
- ☞ Would not impact energetic events which are dominated by transients under high pressure; LPSI comes into play in low pressure events.



# The Inoperability of 1 EDG...

- ☞ Still being reviewed by NRC and is potentially subject to modification



# MODULE M

## SHUTDOWN RISK



# **Evaluation of AOT Extension on Avoiding Shutdown (Transition Risk)**



# Calculated on the Basis of One Plant & Then Modified for Other Plants

- ❖ Used base PRA results for simple manual shutdown (risk tends to be dominated by subsequent loss of MFW and reliance on AFW)
- ❖ Added the fact that 1 SIT or 1 LPSI train or 1 EDG is out-of-service
- ❖ Generally optimistic analysis (tended to lower core damage probability during transition)
- ❖ Did not account for risk during low power mode with impaired equipment nor risk of return to power
- ❖ Transition time assumed as 12 hrs (6 to hot standby and 6 to hot shutdown)
- ❖ Core Damage Probability (CDP) during transition found to be about  $1 \text{ E-}06$  regardless of whether SIT, LPSI, EDG out of service
- ❖ Assumed transition risks for plants is based on the ratio (assumed constant) between the CDP for Transition Risk and the base average CDF since analysis showed CDP more a function of loss of MFW than equipment out-of-service

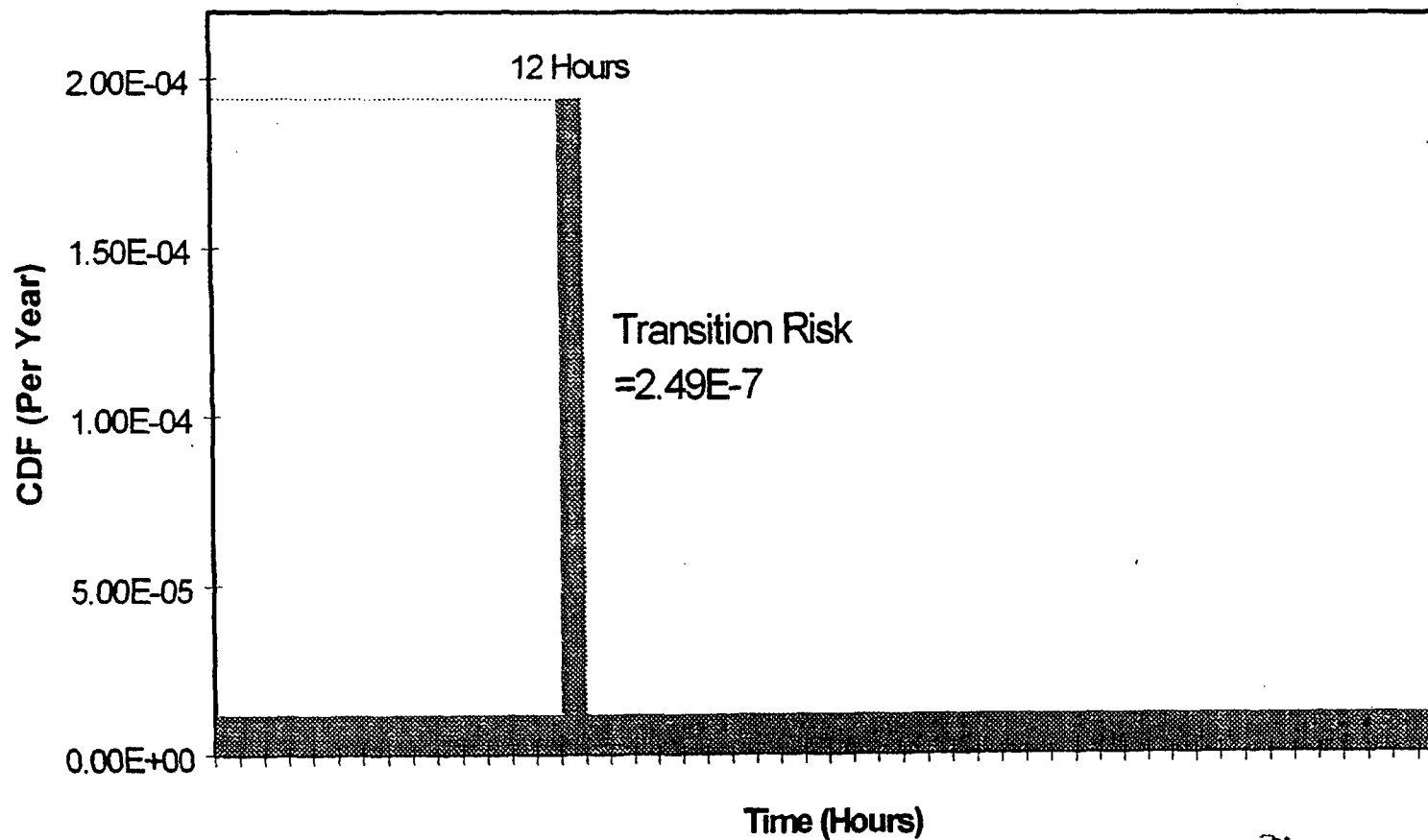


# Resulting Individual Plant Transition Core Damage Probabilities

Plant	CDP	Plant	CDP	Plant	CDP
ANO-2	6.92E-7	Millstone 2	7.19E-7	St Lucie 1	4.51E-7
CC-1/2	4.45E-6	Palisades	1.09E-6	St Lucie 2	4.96E-7
Ft Calhoun	2.49E-7	Palo Verde	1.00E-6	Waterfd 3	3.25E-7
Maine Y.	1.56E-6	San On 2/3	5.78E-7		



# Ft. Calhoun Transition Risk





## **Additional Complication Particularly for the LPSI Case**

- ❖ LPSI needed during shutdown to perform shutdown cooling (SDC)
- ❖ Risk of shutting down with 1 LPSI train out-of-service not insignificant
- ❖ Found that if doing test/preventive maintenance at power increases LPSI reliability for later SDC use by only 1%, this more than offsets the single incremental AOT risk of doing LPSI preventive maintenance “at-power”



# MODULE P

## Plant-Specific, Risk-Informed Applications



# **NRC Staff's Safety Evaluation**

**(For SIT & LPSI AOT Extensions)**



## **SECY-97-095 Addresses NRC Staff's Safety Evaluation**

- ❖ For CEOG AOT extensions lead plant
- ❖ “Model” review for the other CE plants-will issue separate safety evaluations for other plants with comparable results
- ❖ NRC Staff:
  - Approved SIT & LPSI AOT extensions, as requested
  - Reviewed CEOG-provided mark-up to NUREG-1432 (Std Tech Specs-CE Plants) for adoption of revised SIT/LPSI AOTs
- ❖ License Amendment to be issued



## **NRC's Review**

- ❖ Review and submittals consistent with drafts of:
  - RG DG-1061 (PRA for changes to current licensing basis)
  - SRP 19 (General guidance for use of PRA)
  - RG DG-1065 (Risk-informed decision-making - Tech Specs)
  - SRP 16.1 (Risk-informed decision making - Tech Specs)
- ❖ Considered:
  - Need to maintain reliable safety systems
  - Design basis requirements for SITs and LPSI
  - Insights from PRA quantitative evaluations
  - Use of a three-tiered implementation strategy
  - Use of performance monitoring thru Maint. Rule to provide feedback as to effectiveness of AOT extensions



## **NRC's Review (continued)**

### **❖ Traditional analysis considerations**

- Previous AOTs based on judgment; not quantitative risk
- Best estimate analyses show current design basis conservative relative to averting core melt in large LOCA
- Allowing AOT extensions provide sufficient defense-in-depth and safety margin
- For LPSI case (for SGTR), shutdown cooling can also be achieved using combination of steaming SGs and eventual alignment of containment spray pumps to perform SDC
- Safer to perform maintenance of LPSI at power than at shutdown when demand for the system (for SDC) is at its highest



## **NRC's Review (continued)**

- ❖ Review of PRA evaluations (Tier 1)
  - PRA modeling, data, assumptions, quantification, results consistent with Staff expectations and found to be acceptable considering additional sensitivity (e.g., success criteria and operator failure estimates such as failure to isolate SGTR) & uncertainty analysis insights and involvement of lead plant personnel
  - Risk effects of AOT extensions found to be low and within normal operating risk fluctuations of the plant
  - Agreement as to negligible large early release impact (Level 2)



## **NRC's Review (continued)**

- ❖ Review of avoidance of risk-significant plant configurations (Tier 2)
  - CE plants will use risk matrix to make sure unacceptable risk configurations are not achieved with a SIT or LPSI unavailable
  - Agreement that no additional constraints or compensatory measures needed just because a SIT or LPSI train is in maintenance



## NRC's Review (continued)

- ❖ Review of licensee's Configuration Risk Management Program - CRMP (Tier 3)
  - An acceptable risk matrix as long as additional procedures in place to determine risk impact of performing maintenance activities in safety functions *before* the removal of equipment from service for PM, and *before* (as a pre-evaluation) or as soon *after* as possible for a CM.



## **Staff Expectations**

- ❖ CE plants will implement these Tech Spec changes in accordance with three-tiered approach
- ❖ Maintenance Rule will be used to monitor effectiveness of AOT changes
- ❖ Because of Staff's reliance on licensee's risk-informed configuration control program, Staff will ensure that commitment to use this program is incorporated into operating licenses



Mr. Harold B. Ray  
Executive Vice President  
Southern California Edison Company  
San Onofre Nuclear Generating Station  
P.O. Box 128  
San Clemente, California 92674-0128

SUBJECT: ISSUANCE OF AMENDMENT FOR SAN ONOFRE NUCLEAR GENERATING  
STATION, UNIT NO. 2 (TAC NOS. M94934 AND M94936) AND UNIT NO. 3  
(TAC NOS. M94935 AND M94937)

Dear Mr. Ray:

The Commission has issued the enclosed Amendment No. \_\_\_\_\_ to Facility Operating License No. NPF-10 and Amendment No. \_\_\_\_\_ to Facility Operating License No. NPF-15 for San Onofre Nuclear Generating Station, Unit Nos. 2 and 3. The amendments consist of changes to the Technical Specifications (TS) in response to your applications dated November 6, 1995, as supplemented by letters dated January 9, 1998, and February 3, 1998, for the safety injection tanks (SITs), and November 8, 1995, as supplemented by letters dated January 9, 1998, and February 3, 1998, for the low pressure safety injection (LPSI).

These amendments modify the technical specifications (TSs) to extend the allowed outage times (AOTs) for a single inoperable SIT from one hour to 24 hours, and for a single inoperable SIT specifically due to malfunctioning SIT water level or nitrogen cover pressure instrumentation inoperability from one hour to 72 hours. In addition, the amendments extend the AOT for a single inoperable LPSI train from 72 hours to 7 days. The amendments also add a Configuration Risk Management Program to the TSs that puts a proceduralized probabilistic risk assessment-informed process in place that ensures the licensee assesses the overall impact of plant maintenance on plant risk.

A copy of our related Safety Evaluation is also enclosed. The Notice of Issuance will be included in the Commission's next biweekly Federal Register notice.

Sincerely,

James W. Clifford, Senior Project Manager  
Project Directorate IV-2  
Division of Reactor Projects III/IV  
Office of Nuclear Reactor Regulation

Docket Nos. 50-361  
and 50-362

Enclosures: 1. Amendment No. \_\_\_\_\_ to NPF-10  
2. Amendment No. \_\_\_\_\_ to NPF-15  
3. Safety Evaluation

cc w/encls: See next page



Mr. Harold B. Ray  
Executive Vice President  
Southern California Edison Company  
San Onofre Nuclear Generating Station  
P.O. Box 128  
San Clemente, California 92674-0128

SUBJECT: ISSUANCE OF AMENDMENT FOR SAN ONOFRE NUCLEAR GENERATING  
STATION, UNIT NO. 2 (TAC NOS. M94934 AND M94936) AND UNIT NO. 3  
(TAC NOS. M94935 AND M94937)

Dear Mr. Ray:

The Commission has issued the enclosed Amendment No. \_\_\_\_\_ to Facility Operating License No. NPF-10 and Amendment No. \_\_\_\_\_ to Facility Operating License No. NPF-15 for San Onofre Nuclear Generating Station, Unit Nos. 2 and 3. The amendments consist of changes to the Technical Specifications (TS) in response to your applications dated November 6, 1995, as supplemented by letters dated January 9, 1998, and February 3, 1998, for the safety injection tanks (SITs), and November 8, 1995, as supplemented by letters dated January 9, 1998, and February 3, 1998, for the low pressure safety injection (LPSI).

These amendments modify the technical specifications (TSs) to extend the allowed outage times (AOTs) for a single inoperable SIT from one hour to 24 hours, and for a single inoperable SIT specifically due to malfunctioning SIT water level or nitrogen cover pressure instrumentation inoperability from one hour to 72 hours. In addition, the amendments extend the AOT for a single inoperable LPSI train from 72 hours to 7 days. The amendments also add a Configuration Risk Management Program to the TSs that puts a proceduralized probabilistic risk assessment-informed process in place that ensures the licensee assesses the overall impact of plant maintenance on plant risk.

A copy of our related Safety Evaluation is also enclosed. The Notice of Issuance will be included in the Commission's next biweekly Federal Register notice.

Sincerely,

James W. Clifford, Senior Project Manager  
Project Directorate IV-2  
Division of Reactor Projects III/IV  
Office of Nuclear Reactor Regulation

Docket Nos. 50-361  
and 50-362

Enclosures: 1. Amendment No. to NPF-10  
2. Amendment No. to NPF-15  
3. Safety Evaluation

cc w/encls: See next page

DISTRIBUTION:

Docket File	EPeyton
PUBLIC	EAdensam
PDIV-2 Reading	GHill, (4) T5C3
ACRS, T2E26	JKilcrease, RIV
WBateman	JBianchi, WCFO (2)
JClifford	OGC, O15B18
WBeckner, O13H14	TLH1 (SE)
LHurley, RIV	KPerkins, WCFO
RHuey, WCFO	PGwynn, RIV
TCollins	JFlack

DOCUMENT NAME: SO94934.AMD

OFC	PDIV-2/PM	PDIV-2/LA	BC/SRXB	BC/SPSB(A)	BC/TSB	OGC
NAME	JClifford	EPeyton	TCollins	JFlack	WBeckner	
DATE	/ /98	/ /98	/ /98	/ /98	/ /98	/ /98

OFFICIAL RECORD COPY



SOUTHERN CALIFORNIA EDISON COMPANY

SAN DIEGO GAS AND ELECTRIC COMPANY

THE CITY OF RIVERSIDE, CALIFORNIA

THE CITY OF ANAHEIM, CALIFORNIA

DOCKET NO. 50-361

SAN ONOFRE NUCLEAR GENERATING STATION, UNIT NO. 2

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No.  
License No. NPF-10

1. The Nuclear Regulatory Commission (the Commission) has found that:
  - A. The applications for amendment by Southern California Edison Company, et al. (SCE or the licensee) dated November 6, 1995 and November 8, 1995, as supplemented by letters dated January 9, 1998, and February 3, 1998, comply with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's regulations set forth in 10 CFR Chapter I;
  - B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;
  - C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;
  - D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and
  - E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.



2. Accordingly, the license is amended by changes to the Technical Specifications as indicated in the attachment to this license amendment, and paragraph 2.C(2) of Facility Operating License No. NPF-10 is hereby amended to read as follows:

(2) Technical Specifications

The Technical Specifications contained in Appendix A and the Environmental Protection Plan contained in Appendix B, as revised through Amendment No. , are hereby incorporated in the license. Southern California Edison Company shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

3. This license amendment is effective as of the date of its issuance and is to be implemented within 30 days from the date of its issuance.

FOR THE NUCLEAR REGULATORY COMMISSION

James W. Clifford, Senior Project Manager  
Project Directorate IV-2  
Division of Reactor Projects III/IV  
Office of Nuclear Reactor Regulation

Attachment: Changes to the Technical  
Specifications

Date of Issuance:



ATTACHMENT TO LICENSE AMENDMENT

AMENDMENT NO. \_\_\_\_\_ TO FACILITY OPERATING LICENSE NO. NPF-10

DOCKET NO. 50-361

Revise Appendix A Technical Specifications by removing the pages identified below and inserting the enclosed pages. The revised pages are identified by Amendment number and contain marginal lines indicating the areas of change.

REMOVE

3.5-1  
3.5-4  
5.0-20  
---

INSERT

3.5-1  
3.5-4  
5.0-20  
5.0-20a



SOUTHERN CALIFORNIA EDISON COMPANY

SAN DIEGO GAS AND ELECTRIC COMPANY

THE CITY OF RIVERSIDE, CALIFORNIA

THE CITY OF ANAHEIM, CALIFORNIA

DOCKET NO. 50-362

SAN ONOFRE NUCLEAR GENERATING STATION, UNIT NO. 3

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No.  
License No. NPF-15

1. The Nuclear Regulatory Commission (the Commission) has found that:
  - A. The applications for amendment by Southern California Edison Company, et al. (SCE or the licensee) dated November 6, 1995 and November 8, 1995, as supplemented by letters dated January 9, 1998, and February 3, 1998, comply with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's regulations set forth in 10 CFR Chapter I;
  - B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;
  - C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;
  - D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and
  - E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.



2. Accordingly, the license is amended by changes to the Technical Specifications as indicated in the attachment to this license amendment, and paragraph 2.C(2) of Facility Operating License No. NPF-15 is hereby amended to read as follows:

(2) Technical Specifications

The Technical Specifications contained in Appendix A and the Environmental Protection Plan contained in Appendix B, as revised through Amendment No. \_\_\_\_\_, are hereby incorporated in the license. Southern California Edison Company shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

3. This license amendment is effective as of the date of its issuance and is to be implemented within 30 days from the date of its issuance.

FOR THE NUCLEAR REGULATORY COMMISSION

James W. Clifford, Senior Project Manager  
Project Directorate IV-2  
Division of Reactor Projects III/IV  
Office of Nuclear Reactor Regulation

Attachment: Changes to the Technical  
Specifications

Date of Issuance:



ATTACHMENT TO LICENSE AMENDMENT

AMENDMENT NO. \_\_\_\_\_ TO FACILITY OPERATING LICENSE NO. NPF-15

DOCKET NO. 50-362

Revise Appendix A Technical Specifications by removing the pages identified below and inserting the enclosed pages. The revised pages are identified by Amendment number and contain marginal lines indicating the areas of change.

REMOVE

3.5-1  
3.5-4  
5.0-20  
---

INSERT

3.5-1  
3.5-4  
5.0-20  
5.0-20a



SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION  
RELATED TO AMENDMENT NO. \_\_\_\_\_ TO FACILITY OPERATING LICENSE NO. NPF-10  
AND AMENDMENT NO. \_\_\_\_\_ TO FACILITY OPERATING LICENSE NO. NPF-15  
SOUTHERN CALIFORNIA EDISON COMPANY  
SAN DIEGO GAS AND ELECTRIC COMPANY  
THE CITY OF RIVERSIDE, CALIFORNIA  
THE CITY OF ANAHEIM, CALIFORNIA  
SAN ONOFRE NUCLEAR GENERATING STATION, UNITS 2 AND 3  
DOCKET NOS. 50-361 AND 50-362

## 1.0 INTRODUCTION

By applications dated November 6, 1995, for the safety injection tanks (SITs), and November 8, 1995, for the low pressure safety injection (LPSI) system, with additional information submitted by the licensee through the Combustion Engineering Owners Group (CEOG), on June 14, 1996, Southern California Edison Company, et al. (SCE or the licensee) requested changes to the Technical Specifications (Appendix A to Facility Operating License Nos. NPF-10 and NPF-15) for San Onofre Nuclear Generating Station, Unit Nos. 2 and 3. Both applications were subsequently supplemented by letters dated January 9, 1998, and February 3, 1998.

The proposed changes would modify the technical specifications (TSs) to extend the allowed outage times (AOTs) for a single inoperable SIT from one hour to 24 hours, and for a single SIT inoperable specifically due to malfunctioning SIT water level or nitrogen cover pressure instrumentation inoperability from one hour to 72 hours. In addition, the amendments extend the AOT for a single LPSI train from 72 hours to 7 days. The amendments also add a Configuration Risk Management Program (CRMP) to the TSs that puts a proceduralized probabilistic risk assessment-informed process in place that ensures the licensee assesses the overall impact of plant maintenance on plant risk.

## 2.0 BACKGROUND

Since the mid-1980s, the NRC has been reviewing and granting improvements to TS that are based, at least in part, on probabilistic risk assessment (PRA) insights. In its final policy statement on TS improvements of July 22, 1993, the NRC stated that it:



"expects that licensees, in preparing their Technical Specification related submittals, will utilize any plant-specific PSA [probabilistic safety assessment]<sup>1</sup> or risk survey and any available literature on risk insights and PSAs. . . . Similarly, the NRC staff will also employ risk insights and PSAs in evaluating Technical Specifications related submittals. Further, as a part of the Commission's ongoing program of improving Technical Specifications, it will continue to consider methods to make better use of risk and reliability information for defining future generic Technical Specification requirements."

The NRC reiterated this point when it issued the revision to 10 CFR 50.36, "Technical Specifications," in July 1995 (60 FR 36953). In August 1995, the NRC adopted a final policy statement on the use of PRA methods in nuclear regulatory activities that encouraged greater use of PRA to improve safety decisionmaking and regulatory efficiency (60 FR 42622). The PRA policy statement included the following points:

1. The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
2. PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state of the art, to reduce unnecessary conservatism associated with current regulatory requirements.
3. PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.

In August 1995, the Combustion Engineering Owners Group (CEOG) submitted several Joint Application Reports for the staff's review. Two of the CEOG Joint Application Reports provided justifications for extensions of the TS AOTs for SITs and for the LPSI system<sup>2</sup>. The justifications for these extensions are based on a balance of probabilistic considerations, traditional engineering considerations, including defense-in-depth, and operating experience. Risk assessments for all of the Combustion Engineering (CE) plants are contained in the reports. The staff first reviewed the Joint Application Reports and then reviewed the licensee's plant-specific amendment request which incorporated the Joint Application Reports by reference.

Arkansas Nuclear One, Unit 2 (ANO-2) had been the lead CE plant for the SIT and LPSI system TS changes. The staff performed an in-depth review of the ANO-2 PRA methodology relating to these changes, as the lead plant for all of the CEOG. Therefore, a portion of the review of the

---

<sup>1</sup> PSA and PRA are used interchangeably herein.

<sup>2</sup> CE NPSD-994, "Joint Application Report for Safety Injection Tank AOT/STI Extension," May 1995, and CE NPSD-995, "Joint Application Report for Low Pressure Safety Injection System AOT Extension," May 1995.



SONGS amendment request was based on a comparison of the SONGS PRA results with those from ANO-2.

In addition, one of the proposed changes would revise TS 3.5.1, "Safety Injection Tanks (SITs)" to incorporate recommendations and suggestions from Generic Letter (GL) 93-05, "Line-Item Technical Specifications Improvements to Reduce Surveillance Requirements for Testing During Power Operations."

### **3.0 PROPOSED CHANGES**

#### **3.1 TS 3.5.1 - Safety Injection Tanks**

The licensee proposes extending the TS completion time for one SIT that is inoperable for the inability to verify level or pressure from 1 to 72 hours. The licensee also proposes extending the TS completion time for one SIT that is inoperable for reasons other than boron concentration being outside of limits or the inability to verify level or pressure from 1 to 24 hours.

#### **3.2 TS 3.5.2 - ECCS - Operating**

The licensee proposes extending the TS completion time for one inoperable LPSI train from 72 hours to 7 days.

#### **3.3 TS 5.5.2.14 - Configuration Risk Management Program**

The licensee proposes adding TS 5.5.2.14, "Configuration Risk Management Program (CRMP)," to Section 5.5, "Procedures, Programs, and Manuals," of the Administrative Controls Chapter. The purpose of the CRMP is to ensure that a proceduralized PRA-informed process is in place that assesses the overall impact of plant maintenance on plant risk.

### **4.0 EVALUATION**

The staff evaluated the licensee's proposed amendment to the TS using a combination of traditional engineering analysis, PRA methods, and a review of operating experience. The staff's traditional analysis evaluated the capabilities of the plant to mitigate design basis events with one SIT or one LPSI train inoperable. The staff then used insights derived from the use of PRA methods to determine the risk significance of the proposed changes. The results of these evaluations were used in combination by the staff to determine the safety impact of extending the AOTs for one inoperable SIT and for one inoperable LPSI train.



#### **4.1 Justification for Proposed Changes**

##### **4.1.a Justification for Proposed Change to SIT Completion Time from 1 to 72 Hours when SIT is Inoperable Due to Inability to Verify Level or Pressure**

The NRC issued GL 93-05 on September 27, 1993, and recommended that licensees add a condition to the SIT TS for the case where one SIT is inoperable due to the inoperability of water level and pressure channels in which the completion time to restore the SIT to operable status would be 72 hours. GL 93-05 stated that the NRC staff and industry efforts to develop new STS recognized that SIT instrumentation operability was not directly related to the capability of the SITs to perform their safety function. Therefore, surveillance requirements for SIT pressure and level instrumentation were relocated from the new STS and the only surveillance that was retained was that surveillance required to confirm that the parameters defining SIT operability are within their specified limits. At the time of the development of the STS, the staff did not include a separate condition in the SIT TS for a SIT inoperable due to the inability to verify level or pressure, as was recommended in GL 93-05. However, the staff believes this is appropriate based on the analysis done during the development of NUREG-1366, "Improvements to Technical Specifications Surveillance Requirements," which formed the basis for the issuance of GL 93-05.

##### **4.1.b Justification for Proposed Change to SIT Completion Time from 1 to 24 Hours when SIT is Inoperable for Other Reasons**

Industry operating experience has demonstrated that many of the causes of SIT inoperability have been diagnosed and corrected within a relatively short period, but one that is often longer than the existing 1-hour completion time. In several cases, the diagnosis of an inoperable SIT has resulted in plant shutdowns.

If a single SIT were to be diagnosed as inoperable for reasons other than boron concentration being outside of limits (which is already addressed under a separate Action with a 72-hour completion time), TS 3.5.1, Action B, would allow 1 hour for operators to restore the SIT to operability. If the action were not completed within 1 hour, the plant would have to be placed in Mode 3 within the next 6 hours and brought to less than 715 psia within the next 12 hours, in accordance with Action C. The extension of the existing SIT completion time from 1 to 24 hours should provide the licensee with sufficient time in which to diagnose and possibly repair minor SIT system malfunctions at power, thereby averting an unplanned plant shutdown. Since risk analyses demonstrate that the increased risk of operating with a single SIT out of service is negligible, increasing the completion time can be beneficial by possibly avoiding unplanned shutdowns associated with an inoperable SIT. Unnecessary plant shutdowns associated with the outage of non-risk-significant equipment are undesirable because mode changes have the potential to increase the risk above that of steady state operation.



#### 4.1.c Justification for Proposed Change to LPSI Train Completion Time from 72 Hours to 7 Days

The current SONGS TS address the LPSI system as a portion of the emergency core cooling system (ECCS). TS 3.5.2 requires two ECCS trains to be operable. With one ECCS train inoperable, on the basis of any component inoperability but at least 100 percent of the ECCS flow equivalent to a single operable ECCS train available, the train must be returned to operable status within 72 hours or a plant shutdown is required. The proposed change will allow up to 7 days for the licensee to restore operability to an inoperable LPSI train that is the cause of ECCS train inoperability.

The primary role of LPSI trains during power operation is to contribute to the mitigation of a large loss-of-coolant accident (LOCA). The postulated frequency of a large LOCA event is on the order of  $10^{-4}$  per year. In contrast, during Modes 5 and 6, the operability of at least one LPSI train operating in the shutdown cooling mode is required at all times for reactor coolant system (RCS) heat removal. Thus, in the broad view, performing preventive and corrective maintenance at power on LPSI trains can contribute to an overall enhancement of plant safety by increasing the availability of the LPSI train for shutdown cooling (SDC) during Modes 5 and 6, when it is most needed.

In some instances, corrective maintenance of the LPSI pump and valves and testing of valves may require taking one train of LPSI out of service for more than several days. Thus, repair within the existing completion time cannot be ensured and may result in an unscheduled shutdown or a request for temporary relief to allow continued plant operation while repairs are completed. To avoid these situations, the licensee is requesting a longer completion time. On the basis of the review of maintenance requirements of the LPSI train for CE pressurized water reactors (PWRs), the licensee determined that a 7-day completion time would provide sufficient margin to effect most anticipated preventive and corrective maintenance activities and LPSI train valve surveillance tests at power.

## 4.2 Traditional Engineering Evaluation

### 4.2.a Current Traditional Analysis

The performance of all of the ECCS, including SITs and the LPSI system, is calculated in accordance with 10 CFR Part 50, Appendix K, such that the ECCS ensures that the acceptance criteria of 10 CFR 50.46 are satisfied. These criteria were established in order to define deterministic acceptance criteria that could be used to judge the acceptability of a given ECCS design. The methodology defined in Appendix K conservatively represents LOCA thermohydraulic and hydrodynamic phenomenology to calculate fuel peak clad temperature. As a result, the methodology may well overstate the minimum equipment requirements for adequate response to an event.



#### 4.2.b SIT Evaluation

The SITs are passive pressure vessels partially filled with borated water and pressurized with a cover gas (nitrogen) to facilitate injection into the reactor vessel during the blowdown phase of a large break LOCA. This action provides inventory to assist in accomplishing the refill stage following blowdown. The SITs also provide reactor coolant system (RCS) makeup for a small break LOCA.

Each SIT is piped into an associated RCS cold leg via an ECCS line also utilized by HPSI and LPSI. Each SIT is isolated from the RCS during full pressure operations by two series check valves. Each SIT also has a normally deenergized open motor-operated isolation valve utilized to isolate the SIT from the RCS during normal cooldown and depressurization evolutions. Each of these valves receive a safety injection actuation signal to open. The SIT gas pressure and volume, water volume, and outlet pipe size are designed to allow three of the four SITs to inject the inventory necessary to keep clad melt and zirconium-water reaction within design assumptions following a design basis LOCA. The design assumes the loss of inventory from one SIT through the LOCA break.

LCO 3.5.1 requires that all SITs be operable whenever the plant is in Modes 1, 2, or 3, with pressurizer pressure greater than or equal to 715 psia. The LCO is based on the assumption that when the plant is in any of these modes of operation, the SITs must have the same functionality that would be required for a LOCA at full rated thermal power. When the plant is in any of the applicable modes, a SIT is considered operable when the following conditions exist:

- The associated isolation valve is fully open.
- Electric power has been interrupted to the motor for the associated isolation valve.
- Water inventory in the tank is within the assumed band.
- The boric acid concentration of the water inventory of the tank is within the assumed band.
- The nitrogen cover pressure within the tank is within the assumed band.

In the past, a justification for the short completion time for one inoperable SIT has been that the perceived severity of the consequences of not having all SITs available to provide passive injection during a design basis LOCA warranted the severity of the requirement to return the SIT to operable status within 1 hour or shut down the unit. However, the current SIT completion time was based solely on engineering judgment and did not take into consideration a quantitative assessment of risk.

The SIT operational parameters are set by the design basis licensing large break LOCA analysis. Since the SIT is a passive device and provides a limited function, operability has been restricted to mean that the equipment's initial conditions are within a band supported by 10 CFR Part 50, Appendix K, design basis analysis. Analytical models of Appendix K to 10 CFR Part 50.



are devised so as to overestimate the amount of liquid lost from the break and to underestimate the residual inventory in the reactor vessel lower plenum. Consequently, inventory discharge requirements are conservatively set at a high level. Extending the completion time from 1 to 24 hours for one SIT that is inoperable for reasons other than boron concentration being outside of limits or the inability to verify level or pressure will allow time for the licensee to correct minor problems with a SIT. Considering the short time frame that a SIT is allowed to be out of service, the low likelihood of a large break LOCA during this short time frame, and the potential risk associated with plant shutdowns, extending the SIT completion time will allow defense in depth to be maintained while not significantly affecting overall safety margins assumed in the design basis analysis.

The current SONGS TS do not differentiate between a SIT that is inoperable due to tank inventory or nitrogen gas pressure discrepancies and a SIT whose inventory or gas pressure cannot be verified due solely to malfunctioning water level instrumentation or pressure instrumentation. Because these instruments provide no safety actuation, it is reasonable to extend the completion time to 72 hours under these conditions since the SIT is available to perform its safety function during this time. This change is consistent with the staff's recommendations in GL 93-05.

#### 4.2.c LPSI System Evaluation

The two trains of the LPSI system, in combination with the two trains of the high pressure safety injection (HPSI) system, form two redundant ECCS trains. The two LPSI pumps are high volume, low head centrifugal pumps designed to supplement the SIT inventory in reflooding the reactor vessel to ensure core cooling during the early stages of a large break LOCA. The LPSI pumps take suction from the refueling water storage tank (RWST), during the injection phase of a LOCA event, and pump the water through a common discharge header. Once inside containment, the LPSI headers combine with HPSI and SIT discharge piping, and flow is directed through independent injection headers into each of the four RCS cold legs and into the reactor vessel. The LPSI system pumps start and valves open upon receipt of a safety injection actuation signal. When the RWST level is drawn down by inventory transfer during the injection phase, a low RWST level actuates a recirculation actuation signal which stops the LPSI pumps. This step is necessary to ensure adequate net positive suction head remains available for the HPSI pumps and the containment spray pumps. By design, post-LOCA long term core cooling is supplied by the HPSI pumps and containment spray pumps taking suction from the containment emergency sump.

Another role of the LPSI system is defining the end state for a design basis steam generator tube rupture (SGTR) event. In this design basis event, the HPSI functions to keep the core covered at all times, and the LPSI system is required to effect SDC and thereby terminate the event. SDC is initiated after the break has been isolated and the radioactive releases have been controlled.

In the event that one LPSI train is out of service and the second LPSI train fails, the operator can continue to control the plant during a SGTR event by drawing steam off of the unaffected steam generator. Even though loss of both LPSI trains is beyond the design basis accident



assumptions, this cooling mechanism can be maintained indefinitely, provided condensate is available to the unaffected steam generator. Without considering condensate storage tank refill, SONGS has sufficient inventory to steam the unaffected steam generator for greater than 24 hours. SONGS also has the ability to realign the containment spray pumps to provide RCS SDC capability. Therefore, having one LPSI train out of service should not affect the licensee's ability to mitigate a SGTR event, including conditions beyond design basis.

In addition to responding to accidents, the most common use of the LPSI system is during normal shutdown operations (Modes 4, 5, and 6), when the LPSI system is used for decay heat removal in the SDC alignment.

The fact that the LPSI system is required for decay heat removal every time the plant is placed in cold shutdown indicates that it would be prudent to perform maintenance on the LPSI system during power operations rather than during shutdown when the demand for the system is at its highest.

Based on the above, the staff concludes that extending the completion time for one inoperable LPSI train from 72 hours to 7 days should continue to ensure defense-in-depth is maintained and sufficient safety margin exists to meet the design basis analysis for the SONGS ECCS.

#### **4.3 Evaluation of the PRA Used to Support the Proposed TS Changes**

The staff used a three-tiered approach to evaluate the risk associated with the proposed TS changes. The first tier evaluated the PRA model and the impact of the completion time extensions for the LPSI system and SITs on plant operational risk. The second tier addressed the need to preclude potentially high risk configurations, should additional equipment outages occur during the time when one SIT or one LPSI train is out of service. The third tier evaluated the licensee's configuration risk management program to ensure that the applicable plant configuration will be appropriately assessed from a risk perspective before entering into or during the proposed AOTs. Each tier and the associated findings are discussed below.

##### **4.3.a Cross Comparison Approach**

After completing a detailed evaluation for the tentative approval of SIT and LPSI TS AOT extensions for Arkansas Nuclear One, Unit 2 (ANO-2), the original CEOG lead plant for the risk-informed TS pilot project, the staff used a cross comparison approach to consider the viability of similar AOT relaxations for other participating CEOG plants, including SONGS. The pilot technical evaluation report<sup>3</sup> used in support of the staff's draft safety evaluation for ANO-2 focused on:

---

<sup>3</sup>SCIE-NRC-318-97, "Technical Evaluation of Combustion Engineering Owners Group (CEOG) Joint Application for Safety Injection Tanks and Low Pressure Safety Injection System Allowed Outage Time (AOT) Extension," July 21, 1997.

<sup>4</sup>SECY-97-095, "Probabilistic Risk Assessment Implementation Plan Pilot Application for Risk-Informed Technical Specifications," April 30, 1997.



- the process adopted by the CEOG to assess single AOT risk,
- the identification of ANO-2 accident sequences in which credit was taken for SITs and LPSI,
- independent verification of the single AOT risk [essentially equivalent to incremental conditional core damage probability (ICCDP)<sup>5</sup>], and
- determination of the significance of single AOT risk relative to an acceptance guideline value.

The objective of this cross comparison evaluation is to use insights derived from the ANO-2 technical evaluation to examine the validity of the conclusions drawn in the joint submittals. Because a common methodology was employed by the CEOG to quantify AOT risk and because CE plants generally have similar design characteristics, the staff believes that the findings of the lead pilot plant evaluation will be generally applicable to other CE plants. The staff confirmed that differences in the underlying PRA models are chiefly attributed to:

- minor design differences,
- operational differences,
- success criteria assumptions, and
- common cause failure  $\beta$ -factor assumptions.

The cross comparison draws on information contained in the CEOG Joint Application Reports, the licensees' responses to the staff's requests for additional information, the licensees' individual plant examinations (IPEs) performed in response to Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities," and the corresponding IPE evaluations performed by the staff.

#### 4.3.b Impact of SITs on Tier 1, 2, and 3 Requirements (Risk Measures)

The following factors are chiefly responsible for the differences in SIT AOT risks among the CE plants:

- modeling for success criteria for SITs,
- initiating event (IE) frequency assumed for the initiators challenging the SITs, and
- credit for SITs in mitigating medium LOCAs.

The SIT single AOT risk (or essentially equivalently, ICCDP) for SONGS is 1.03E-06 and is slightly in excess of the acceptance guideline value of 5.0E-07 published in DG-1065, "An Approach for Plant-Specific Risk-Informed Decisionmaking: Technical Specifications," (62 FR 34321, June 25, 1997), due largely to the use of conservative 3-out-of-4 success criteria (ANO-2 used 2-out-of-4). In addition, the change in the SONGS updated baseline core damage frequency (CDF) (as reported in the CEOG Joint Application Report) due to the SIT AOT change is about 3%, i.e., from 2.74E-05 per year to 2.85E-05 per year. The change in CDF of 1.1E-06 is within the acceptance guidelines published in DG-1061, "An Approach for Using Probabilistic

---

<sup>5</sup>ICCDP = [(conditional CDF with the subject equipment out of service) - (baseline CDF with nominal expected equipment unavailabilities)] X (duration of single AOT under consideration).



Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis" (62 FR 34321, June 25, 1997).

In the context of integrated decisionmaking, the acceptance guidelines should not be interpreted as being overly prescriptive. They are intended to provide an indication, in numerical terms, of what is considered acceptable. As such, the numerical acceptance guideline is an approximate value that provides an indication of the changes that are generally acceptable. Furthermore, the state of knowledge, or epistemic, uncertainties associated with PRA calculations preclude a definitive decision with respect to the acceptance of the proposed change based purely on the numerical results. The intent in making the comparison of the PRA results with the acceptance guidelines is to demonstrate with reasonable assurance that the increase in risk is small and consistent with the intent of the Commission's Safety Goal Policy Statement. Given the licensee's use of conservative 3-out-of-4 success criteria, the staff believes that the proposed change to the SONGS SIT TS meets this principle.

The Tier 2 evaluation did not identify the need for any additional constraints or compensatory actions that, if implemented, would avoid or reduce the probability of a risk-significant configuration. Because the SIT sequence modeling is relatively independent of that for other systems, the staff concludes that application of Tier 3 to the proposed SIT AOT is not necessary.

#### 4.3.c Impact of LPSI on Tier 1, 2, and 3 Requirements

The following factors are chiefly responsible for the differences in LPSI AOT risks among the CE plants:

- use of LPSI to mitigate multiple initiating events,
- HPSI redundancies, and
- LPSI common cause  $\beta$ -factor assumptions.

The LPSI preventive and corrective maintenance weighted average single AOT risk for SONGS is  $2.53\text{E-}07$  and is less than the acceptance guideline value  $5.0\text{E-}07$  from DG-1065. In addition, the change in the SONGS updated baseline core damage frequency (CDF) (as reported in the CEOG Joint Application Report) due to the LPSI AOT change is about 1%, i.e., from  $2.74\text{E-}05$  per year to  $2.78\text{E-}05$  per year. The change in CDF of  $4.0\text{E-}07$  per year is within the acceptance guidelines published in DG-1061.

The Tier 2 evaluation did not identify the need for any additional constraints or compensatory actions that, if implemented, would avoid or reduce the probability of a risk-significant configuration.

The Tier 3 requirements for configuration risk management are considered to be adequately satisfied, since the licensee has an on-line PRA-based monitor, called the Safety Monitor, to analyze the risk impact of outage configurations in a timely manner. Procedures related to use of the Safety Monitor are SONGS Work Process Procedure, "SONGS Work Scheduling and Coordination Process" and MPG-SO123-G-31, "Utilization of the Safety Monitor in Support of Work Control." The licensee has proposed adding TS 5.5.2.14, "Configuration Risk



Management Program (CRMP),” to provide a means of implementing and controlling their Tier 3 process. The licensee and the staff have agreed to implementation of the CRMP as described below.

### **Purpose of CRMP**

The purpose of the CRMP is to ensure that a proceduralized PRA-informed process is in place that assesses the overall impact of plant maintenance on plant risk. Implementation of the CRMP will enable appropriate actions to be taken or decisions to be made to minimize and control risk when performing on-line maintenance for systems, structures, and components (SSCs) with a risk-informed completion time.

### **Scope of CRMP**

The scope of the SSCs included in the CRMP are those SSCs modeled in the licensee’s plant PRA in addition to those SSCs considered of high safety significance per Regulatory Guide 1.160, Revision 2, “Monitoring the Effectiveness of Maintenance at Nuclear Power Plants,” that are not modeled in the PRA.

The Configuration Risk Management Program (CRMP) includes the following components and key elements:

### **Components**

- a. Risk Assessment Tool
- b. Tier 2 Restrictions
- c. Level 2 and External Events
- d. Decision Making Process
- e. Associated Procedures

### **Key Element 1. Implementation of CRMP**

The intent of the CRMP is to implement Maintenance Rule, Section 10 CFR 50.65a(3) with respect to on-line maintenance for risk-informed technical specifications, with the following additions and clarifications:

- a. The scope of the SSCs to be included in the CRMP will be those SSCs modeled in the licensee’s plant PRA in addition to those SSCs considered to be of high safety significance per Regulatory Guide 1.160, Revision 2, that are not modeled in the PRA.
- b. The CRMP assessment tool is PRA informed, and may be in the form of either a risk matrix, an on-line assessment, or a direct PRA assessment.
- c. CRMP will be invoked as follows for:



**Risk-Informed Inoperability:** A risk assessment will be performed prior to entering the LCO condition for preplanned activities. For unplanned entry into the LCO condition, a risk assessment will be performed in a time frame consistent with the plant's Corrective Action Program.

**Additional SSC Inoperability and/or Loss of Functionality:** When in the risk-informed completion time, if an additional SSC within the scope of the CRMP becomes inoperable/non-functional, a risk assessment shall be performed in a time frame consistent with the plant's Corrective Action Program.

- d. Tier 2 commitments apply for planned maintenance only, but will be evaluated as part of the Tier 3 assessment for unplanned occurrences.

### **Key Element 2. Control & Use of the CRMP Assessment Tool**

- a. Plant modifications and procedure changes will be monitored, assessed, and dispositioned.
  - Evaluation of changes in plant configuration or PRA model features can be dispositioned by implementing PRA model changes or by the qualitative assessment of the impact of the changes on the CRMP assessment tool. This qualitative assessment recognizes that changes to the PRA take time to implement and that changes can be effectively compensated for without compromising the ability to make sound engineering judgments.
  - Limitations of the CRMP assessment tool are identified and understood for each specific completion time extension.
- b. Procedures exist for the control and application of CRMP assessment tools, including description of the process when outside the scope of the CRMP assessment tool.

### **Key Element 3. Level 1 Risk-Informed Assessment**

The CRMP assessment tool is based on a Level 1, at power, internal events PRA model. The CRMP assessment may use any combination of quantitative and qualitative input. Quantitative assessments can include reference to a risk matrix, pre-existing calculations, or new PRA analyses.

- a. Quantitative assessments should be performed whenever necessary for sound decision making.
- b. When quantitative assessments are not necessary for sound decision making, qualitative assessments will be performed. Qualitative assessments will consider applicable, existing insights from quantitative assessments previously performed.



#### **Key Element 4. Level 2 Issues/External Events**

External events and Level 2 issues are treated qualitatively and/or quantitatively.

Guidance for implementing the CRMP is provided by plant procedures.

##### **4.3.d Conclusions Regarding the Licensee's LPSI and SIT Design Similarities to ANO-2 and PRA Used to Support the Proposed Amendment**

SONGS, Units 2 and 3 have strong LPSI and SIT design similarities to ANO-2, the original CEOG lead pilot plant for this project. Therefore, the staff believes that, on the basis of the three-tiered approach, cross comparative results provide sufficient validation for the following conclusions:

- The proposed TS AOT modifications have only a minimal quantitative impact on plant risk. The calculated ICCDPs are small, primarily because of the association of SITs and LPSI with low probability initiating events and limited impact on the success criteria of other mitigation systems (Tier 1).
- The review did not identify the need for any additional constraints or compensatory actions that, if implemented, would avoid or reduce the probability of a risk-significant configuration (Tier 2).
- The licensee has implemented a risk-informed Configuration Risk Management Program to assess the risk associated with the removal of equipment from service during the proposed LPSI AOT. The program provides the necessary assurances that appropriate assessments of plant risk configurations using the Safety Monitor, augmented by additional analysis, when appropriate, are sufficient to support the present AOT extension requests for the LPSI system (Tier 3). Because the SIT sequence modeling is relatively independent of that for other systems, the staff concludes that application of Tier 3 to the proposed SIT AOT is not necessary.

##### **4.4 Implementation and Monitoring**

The staff expects the licensee to implement these TS changes in accordance with the three-tiered approach described above. In addition, the licensee has stated through endorsement of the CEOG Joint Application Reports that the maintenance rule (10 CFR 50.65) will be the vehicle that controls the actual equipment maintenance cycle by defining unavailability performance criteria for the SITs and the LPSI systems. The AOT extensions will allow efficient scheduling of maintenance within the boundaries established by implementing the maintenance rule. The effect of the AOT extensions should be considered if any adverse trends in meeting established performance criteria are identified for the SITs and the LPSI systems. The maintenance rule will thereby be the vehicle that monitors the effectiveness of the AOT extensions. Application of these implementation and monitoring strategies will help to ensure that extension of TS AOTs for SITs and the LPSI system does not degrade operational safety



over time and that the risk incurred when a SIT or a LPSI system is taken out of service is minimized.

## 5.0 Summary

The staff has evaluated the licensee's proposed changes for compliance with regulatory requirements as documented in this evaluation and has determined that they are acceptable. This determination is based on the following:

1. The need to maintain reliable safety systems.
2. Consideration of the design basis requirements for the SITs and the LPSI systems.
3. Staff recommendations contained in GL 93-05 regarding SIT TS requirements.
4. Insights gained from the quantitative evaluation of the risk associated with having one LPSI train out of service.
5. A three-tiered implementation strategy that ensures that the risk incurred when a SIT or LPSI system is taken out of service is minimized.
6. Performance monitoring through the maintenance rule to ensure that extension of TS AOTs for SITs and the LPSI system does not degrade operational safety over time.

The staff therefore finds that the AOT for one SIT that is inoperable for the inability to verify level or pressure may be extended to 72 hours, the AOT for one SIT that is inoperable for reasons other than boron concentration not within limits or inability to verify level or pressure may be extended to 24 hours, and that the AOT for one inoperable LPSI system may be extended to 7 days, with a negligible impact on risk.

## 6.0 STATE CONSULTATION

In accordance with the Commission's regulations, the California State official was notified of the proposed issuance of the amendments. The State official had no comments.

## 7.0 ENVIRONMENTAL CONSIDERATION

The amendments change a requirement with respect to the installation or use of a facility component located within the restricted area as defined in 10 CFR Part 20. The NRC staff has determined that the amendments involve no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite, and that there is no significant increase in individual or cumulative occupational radiation exposure. The Commission has previously issued a proposed finding that the amendments involve no significant hazards consideration, and there has been no public comment on such finding (61 FR 15995 and 63 FR 6991). Accordingly, the amendments meet the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9). The amendments also involve changes in



recordkeeping, reporting or administrative procedures or requirements. Accordingly, with respect to these items, the amendments meet the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(10). Pursuant to 10 CFR 51.22(b) no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendments.

## 8.0 CONCLUSION

The Commission has concluded, based on the considerations discussed above, that (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendments will not be inimical to the common defense and security or to the health and safety of the public.

Principal Contributor: N. Gilles

Date:



# Module Q

## Configuration Risk Management



# **Evaluation of AOT Extension on At-Power Risk**



# **Examination of AOT Extensions First Required Calculation of At-Power Conditional CDFs to Assess the Increased Risk of Continued Operation With The Equipment Out of Service**

## **■ For SITs:**

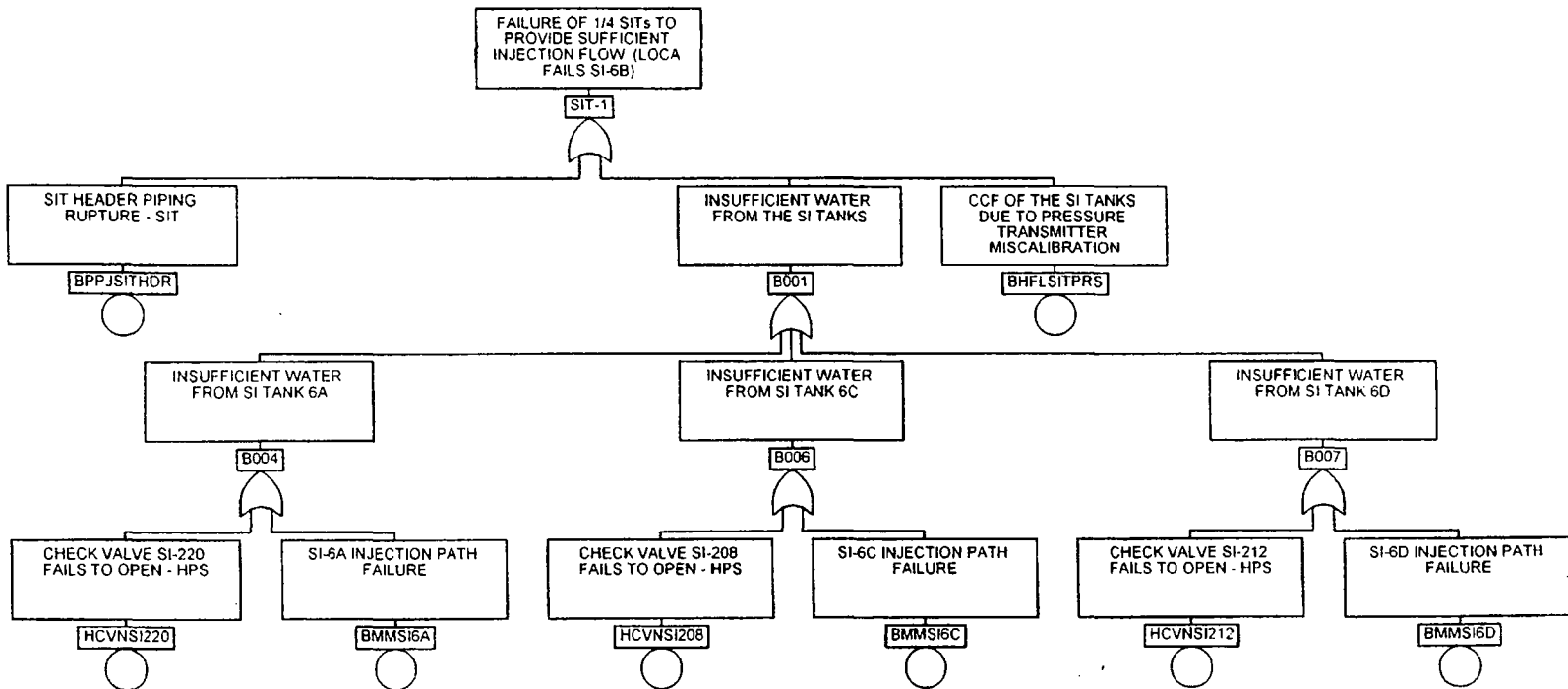
$$\begin{aligned} &\text{❖ Change in CDF} = \\ &\quad \text{Conditional CDF (1 SIT unavailable)} - \\ &\quad \text{Conditional CDF (1 SIT not out for T/M)} \end{aligned}$$



## For the SIT Case...

- Cond CDF (1 SIT unavailable):
  - ❖ Set basic event probability for a component that will make a SIT train unavailable = 1.0
  - ❖ Set basic event probabilities for other failure modes for that train = 0
- Cond CDF (1 SIT not out for T/M):
  - ❖ Set basic event T/M probability (if modeled) for 1 SIT = 0
- Change in CDF = difference in Cond CDFs (per year)
- Then, Single AOT risk contribution (increment in risk due to the SIT being unavailable over the full AOT) = Change in CDF x T where T=full AOT
- Then, Yearly AOT = Single AOT x F where F=avg no. of entries into LCO action statement per year = 0.35 based on experience







**Table 6.3.2-1**  
**CEOG AOT CONDITIONAL CDF CONTRIBUTIONS FOR SITs - Corrective Maintenance**

PARAMETER	ANO-2	Calvert Cliffs 1 & 2	Port Calhoun	Maine Yankee*	Millstone 2	Palisades	Palo Verde 1, 2 & 3	San Onofre 2 & 3	St. Lucie 1	St. Lucie 2	Waterford 3
SIT Success Criteria	3 of 4	3 of 4**	3 of 3 to unbroken legs	1 of 2 to unbroken legs	2 of 3 to unbroken legs	3 of 3 to unbroken legs**	2 of 3 to unbroken legs	3 of 4 to unbroken legs	3 of 4	3 of 4	3 of 3 to unbroken legs
Present AOT hrs	1	1	1	1***	1	1	1	1	1	1	1
Proposed AOT, hrs	24	24	24	24	24	24	24	24	24	24	24
Conditional CDF, per yr (1 SIT unavailable)	4.12E-05	5.53E-04	2.18E-05	7.40E-05	3.41E-05	5.47E-05	4.88E-05	4.02E-04	2.2E-04	2.2E-04	6.53E-05
Conditional CDF, per yr (1 SIT not out for maintenance)	3.28E-05	2.11E-04	1.18E-05	7.40E-05	3.41E-05	5.15E-05	4.74E-05	2.74E-05	2.14E-05	2.35E-05	1.54E-05
Increase in CDF, per yr	8.38E-06	3.42E-04	1.00E-05	negligible	negligible	3.20E-06	1.40E-06	3.75E-04	2.2E-04	2.2E-04	4.99E-05
Single AOT Risk (based on Current full AOT)	9.57E-10	3.90E-08	1.14E-09	negligible	negligible	3.65E-10	1.60E-10	4.28E-08	2.3E-08	2.3E-08	5.70E-09
Single AOT Risk (based on Proposed full AOT)	2.30E-08	9.37E-07	2.74E-08	negligible	negligible	8.77E-09	3.84E-09	1.03E-06	5.5E-07	5.5E-07	1.37E-07
Downtime Frequency, per yr	0.35****	0.35****	0.35****	0.35****	0.35****	0.35****	0.35****	0.35****	0.35****	0.35****	0.35****
Yearly AOT Risk, per yr (based on Current full AOT)	3.35E-10	1.37E-08	4.00E-10	negligible	negligible	1.28E-10	5.59E-11	1.50E-08	8E-09	8E-09	1.99E-09
Yearly AOT Risk, per yr (based on Proposed full AOT)	8.04E-09	3.28E-07	9.59E-09	negligible	negligible	3.07E-09	1.34E-09	3.59E-07	1.9E-07	1.9E-07	4.78E-08

\* SITs were not modeled in PSA, impact judged negligible due to success criteria

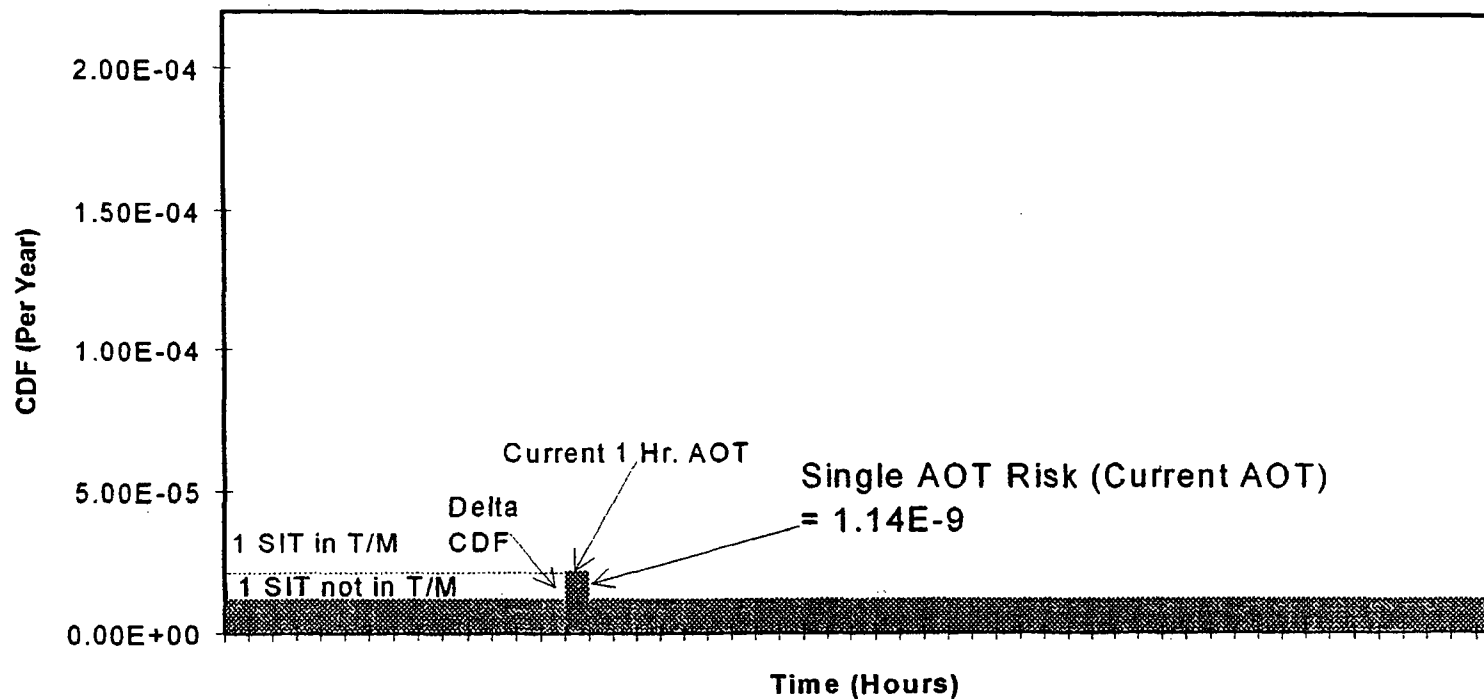
\*\* Success criteria varies based on details of scenario

\*\*\* 4 hours for SIT out of spec

\*\*\*\* Based on actual data for representative CE plant

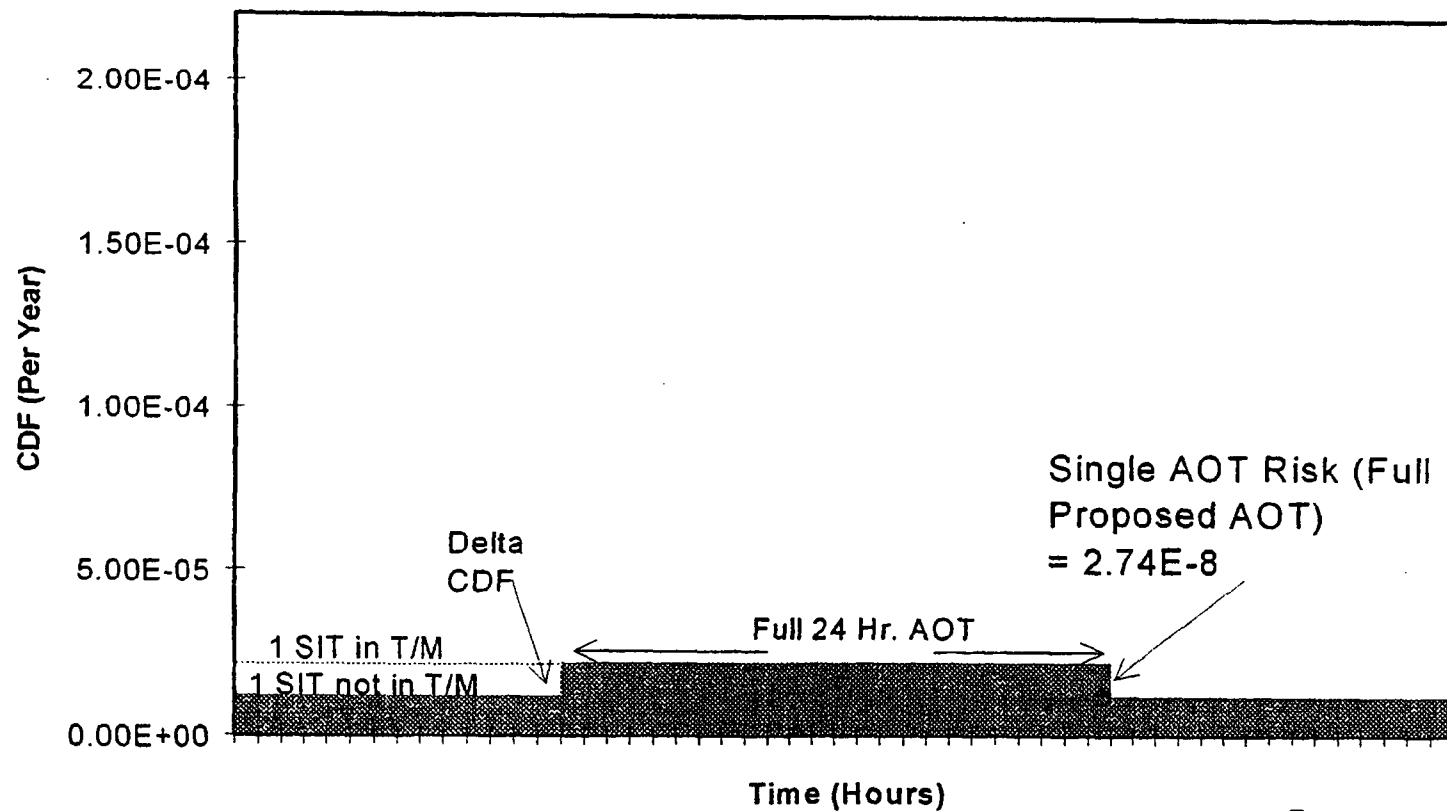


# Ft. Calhoun Example





# Ft. Calhoun Example





**Table 6.3.2-2  
CEOG PROPOSED AVERAGE CDFs**

PARAMETER	ANO-2	Calvert Cliffs 1 & 2	Fort Calhoun	Maine Yankee*	Millstone 2	Palisades	Palo Verde 1, 2 & 3	San Onofre 2 & 3	St. Lucie 1	St. Lucie 2	Waterford 3
SIT Success Criteria	3 of 4	3 of 4**	3 of 3 to unbroken legs	1 of 2 to unbroken legs	2 of 3 to unbroken legs	3 of 3 to unbroken legs**	2 of 3 to unbroken legs	3 of 4 to unbroken legs	3 of 4	3 of 4	3 of 3 to unbroken legs
Present AOT hrs	1	1	1	1***	1	1	1	1	1	1	1
Proposed AOT, hrs	24	24	24	24	24	24	24	24	24	24	24
Proposed Downtime, hrs/yr	Assume 24	Assume 24	Assume 24	Assume 24	Assume 24	Assume 24	Assume 24	Assume 24	Assume 24	Assume 24	Assume 24
Average CDF, per yr (PSA case)	3.28E-05	2.11E-04	1.18E-05	7.40E-05	3.41E-05	5.15E-05	4.74E-05	2.74E-05	2.14E-05	2.35E-05	1.54E-05
Average CDF, per yr (Proposed)	3.28E-05	2.11E-04	1.18E-05	7.40E-05	3.41E-05	5.16E-05	4.74E-05	2.85E-05	2.4E-05	2.6E-05	1.56E-05

\* SITs were not modeled in PSA, impact judged negligible due to success criteria

\*\* Success criteria varies based on details of scenario

\*\*\* 4 hours for SIT out of spec



## **For the SIT Case...(continued)**

- Then, as another measure, a new average CDF (per year) was calculated by putting in a new value for SIT unavailability due to T/M assuming the full AOT duration for the SITs (i.e., 24 hrs).
- This new average CDF was then compared to the base case average CDF in the original PRA.



## For the LPSI & EDG Cases...

- Additional complications had to be treated
  - ❖ Consider both Corrective Maintenance (expected frequency and duration) and Preventive Maintenance (scheduled frequency and expected duration)
  - ❖ Account for common cause potential
    - Treat other train(s) as potentially having a failure probability = CCF-Beta Factor for Corrective Maintenance



# DAILY REQUIRED READING ASSIGNMENTS FOR P-111

## Day 1

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

Module B - Traditional Engineering Analysis and PRA

Module C - Overview of PRA Process

## **Required Reading:**

1. Review PRA Final Policy Statement  
Section III - Deterministic and Probabilistic Approaches to Regulation (pp. 18-21)
2. ACRS Letter dated April 11, 1997 "Risk-Based Regulatory Acceptance Criteria for Plant-Specific Application of Safety Goals"
3. IMC 0609, App. A, pp. A1-1 through A1-4.
4. Part 9900 Inspection Guidance  
Operability - Section 6.9  
Resolution of Degraded and Non-conforming Conditions - Section 4.5.3

## **Optional (Background) Reading:**

1. PRA Final Policy Statement, all sections
2. NUREG 1560 pp. 14-4 to 14-5

## **Look up Questions:**

- 1) As discussed in the Final Policy Statement on PRA, how does the deterministic approach to safety requirements consider probabilistic risk?
- 2) The Final Policy Statement on PRA says that the safety goals should not be used for plant-specific applications. Given that the intent of the Safety Goal Policy was to set a risk standard for nuclear power plants which could be compared to other risks which were acceptable to society at large, what is the concern here? Why does the ACRS, in its letter dated April 11, 1997, recommend differently?
- 3) The Final Policy Statement on PRA cites two knowledge areas as specific examples of where current PRA methods are not fully developed and contribute to the uncertainty in estimated risks. What are these examples?



# DAILY REQUIRED READING ASSIGNMENTS FOR P-111

## Day 2

Module D - Accident Sequence Initiating Events

Module E - Accident Sequence Analysis Using Event Trees

Module F - System Analysis Using Fault Trees

## **Required Reading:**

1. IMC 0609 App. A, pp. A1-5 through A1-14
2. NUREG 1560 - Chapter 2 Tables (e.g., 2.1, 2.2, 2.3) applicable to the student's chosen plant

## **Optional (Background) Reading:**

NUREG 1560 - Sections 14.3.1, 14.3.2, 14.3.3 (pp. 14-6 to 14-22)

## **Look up Questions:**

- 1) In an IPE of your own choosing, identify whether the licensee used large or small event tree methodology and locate any descriptions or diagrams of the dominant accident sequences. Also, locate any description of plant improvements implemented, intended, or under consideration. Compare these to other plants of the same type by looking at NUREG-1560 Chapter 2 Tables 2.1-2.3. Note if these other plants have identified vulnerabilities that your chosen plant did not. Based on your knowledge of your chosen plant, could these additional vulnerabilities exist at your chosen plant? If you don't immediately know, take note of these and keep them in mind as you explore your chosen IPE during this course.
- 2) Should hypothetical failures (e.g., assumption of one single, active failure) be included in the inspection finding for evaluation by the SDP?



# DAILY REQUIRED READING ASSIGNMENTS FOR P-111

## Day 3

Module G - Estimation of Equipment Reliability and Unavailability

Module H - Estimation of Common-Cause Failure Probabilities

Module I - Human Reliability Analysis

Module J - Accident Sequence Quantification

Module K - External Events

## **Required Reading:**

1. ACRS Letter dated July 19, 1991 (D910719) "The Consistent Use of PRA"
2. IMC 0609, App. A, pp. A1-15 through A1-23
3. NUREG 1560 - Chapter 5 Tables (e.g., 5.1, 5.2, 5.3, 5.4) applicable to the student's chosen plant

## **Optional (Background) Reading:**

NUREG 1560 Sections 14.3.4, 14.3.5 (pp. 14-23 to 14-31)

## **Look up Questions:**

- 1) The ACRS letter states that conservatism should not be added to the PRA itself. If conservatism is taken to mean the choice of inputs and assumptions which tend to increase the estimated frequency of core damage, and if such conservative inputs are made to a PRA, then how can this contribute to the "self-deception" stated in the ACRS letter?
- 2) Traditional engineering methods established a plant's design which included safety margins determined to be adequate by (engineering) judgment. A probabilistic analysis attempts to model a plant's design and account for these engineered safety margins realistically. A PRA may use either a realistic or a design (licensing) basis engineering analysis to make important choices about probabilistic success criteria (e.g., what is the minimum cooling flow needed for core cooling), which can have dramatic effects on which accident sequences dominate PRA results. Question: A reactor plant is designed with three dual-train injection systems. The design basis engineering analysis assumes one train is available in each of the three systems to mitigate the effect (protect the core) of the maximum credible LOCA. This analysis assumes worst-case flow from each train. A realistic engineering analysis shows that, for this maximum credible LOCA, any two of the six trains operating with realistic flow rates will provide adequate cooling. Two PRAs are done for this plant, one assuming success criteria based on the design basis (one train in each system is needed for success) and the other based on realistic analysis. If all other aspects of the PRA are equal, which will have the greater core damage frequency? Which will show injection pumps as being more risk-significant (i.e., more likely to appear in dominant accident sequences)?
- 3) In an IPE of your own choosing, note any human/operator actions identified by the licensee as important. Compare these to other plants of the same type by looking at NUREG-1560 Chapter 5 Tables 5.1-5.4. Note if these other plants have identified important human/operator actions that your chosen plant did not. Based on your knowledge of your chosen plant, could these actions exist at your chosen plant? If you don't immediately know, take note of these and keep them in mind as you explore your chosen IPE during this course. Also, note if your licensee considered pre-initiator human errors such as miscalibrations or improper test restoration. Finally, note the extent to which operator recovery actions were modeled. Do they appear to be modeled consistently (i.e., modeled for all potentially recoverable equipment using similar methods for estimating non-recovery probabilities)?



# DAILY REQUIRED READING ASSIGNMENTS FOR P-111

## Day 4

Module L - Level 2 and 3 PRA

Module M - Shutdown Risk

Module N - Importance Measures

Module O - Uncertainty

## **Required Reading:**

1. IMC 0609, App. A, pp. A1-24 through A1-27
2. NUREG 1560 Chapter 3 and 4 Tables applicable to the student's chosen plant

## **Optional (Background) Reading:**

NUREG 1560 Sections 14.3.6 (pp. 14-32 to 14-35)

## **Look up Questions:**

- 1) If the licensee disagrees with your assessment of the risk-significance of an issue, what should you do?
- 2) IMC 0609 states that understanding the applicable risk analysis may help the inspector do a better job of developing the facts surrounding an issue. How could this guidance be applied given the following scenario:

During an electrical storm, a capacitor becomes shorted in a safety-related inverter causing a high frequency electrical signal to be fed back onto the associated safety-related DC bus. This signal effectively disables the emergency diesel generator electronic starting circuit, which receives power from the affected DC bus. The risk analysis for this plant indicates that one of the more likely core damage accident sequences involves a loss of offsite power, common-cause failure of both emergency diesel generators, and non-recovery of emergency power. Alternate emergency power (for SBO) is only available after a sequence of switchyard manipulations estimated to take 1 hour to complete.

- 3) In an IPE of your own choosing, note core damage or containment performance perspectives identified by the licensee as important. Compare these to other plants of the same type by looking at NUREG-1560 Chapters 3 and 4. Note if these other plants have identified important perspectives that your chosen plant did not. Based on your knowledge of your chosen plant, could these issues exist at your chosen plant? If you don't immediately know, take note of these and keep them in mind as you explore your chosen IPE during this course.



# **DAILY REQUIRED READING ASSIGNMENTS FOR P-111**

## Day 5

Module P - Plant-Specific, Risk-Informed Applications

Module Q - Configuration Risk Management

Module R - Maintenance Rule Implementation

Module S - Reactor Safety Significance Determination Process

## **Required Reading:**

1. Reread NRC Final PRA Policy Statement, Section III.B. "Uncertainties and Limitations of Deterministic and Probabilistic Approaches"
2. ACRS Letter dated Dec 16, 1997 "Treatment of Uncertainties versus Point Values in the PRA-related Decision-making Process"
3. IMC 0609, Apps. F, G, and H

## **Optional (Background) Reading:**

None

## **Look up Questions:**

- 1) According to the ACRS letter dated December 16, 1997, where did WASH-1400 underestimate the risk of nuclear power plant operation?
- 2) The ACRS letter discusses "parameter uncertainty" and "model uncertainty". How does the ACRS define these?
- 3) How does the ACRS recommend that uncertainties be addressed by a PRA?



## **DAILY REQUIRED READING ASSIGNMENTS FOR P-111**

### Day 6

Closed-Book Exam (Time Limit: 2 hours)

#### Integrated Workshop #1 - Inspection Planning

Reading: None - students are encouraged to use IPEs, NUREG 1560, and the Maintenance Rule Guidebook to formulate a list of questions for discussion with licensee PRA analysts for a plant of their choosing. Students may begin drafting a risk-informed inspection plan (optional).

### Day 7

#### Integrated Workshop #2 - Assessing the Significance of Inspection Findings

Reading: None - students are encouraged to use IPEs, NUREG 1560, and the Maintenance Rule Guidebook to formulate a list of questions for discussion with licensee PRA analysts for a plant of their choosing. Students may begin drafting a risk-informed inspection plan (optional).

### Day 8

#### Integrated Workshop #3 - Inspecting the Maintenance Rule (PRA applications)

Review for open-book exam

### Day 9

Open-Book Exam (Time Limit: 2.5 hours)



[7590-01]

NUCLEAR REGULATORY COMMISSION

Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory  
Activities; Final Policy Statement

AGENCY: Nuclear Regulatory Commission.

ACTION: Final policy statement.

SUMMARY: This statement presents the policy that the Nuclear Regulatory Commission (NRC) will follow in the use of probabilistic risk assessment (PRA) methods in nuclear regulatory matters. The Commission believes that an overall policy on the use of PRA methods in nuclear regulatory activities should be established so that the many potential applications of PRA can be implemented in a consistent and predictable manner that would promote regulatory stability and efficiency. In addition, the Commission believes that the use of PRA technology in NRC regulatory activities should be increased to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach. The pertinent comments received from the published draft policy statement are reflected in this final policy statement. This policy statement will be implemented through the execution of the NRC's PRA Implementation Plan.

EFFECTIVE DATE: August 16, 1995

ADDRESSES: The proposed policy statement and the comments received may be examined at: NRC Public Document Room, 2120 L Street, NW. (Lower Level), Washington, D.C.

FOR FURTHER INFORMATION CONTACT: Anthony Hsia, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, Washington, DC 20555.  
Telephone (301) 415-1075



SUPPLEMENTARY INFORMATION:

- I. Background
- II. Summary of Public Comments and NRC Responses
- III. Deterministic and Probabilistic Approaches to Regulation
- IV. The Commission Policy
- V. Availability of Documents

I. Background

The NRC has generally regulated the use of nuclear material based on deterministic approaches. Deterministic approaches to regulation consider a set of challenges to safety and determine how those challenges should be mitigated. A probabilistic approach to regulation enhances and extends this traditional, deterministic approach, by (1) allowing consideration of a broader set of potential challenges to safety, (2) providing a logical means for prioritizing these challenges based on risk significance, and (3) allowing consideration of a broader set of resources to defend against these challenges.

Until the accident at Three Mile Island (TMI) in 1979, the Atomic Energy Commission (now the NRC), only used probabilistic criteria in certain specialized areas of licensing reviews. For example, human-made hazards (e.g., nearby hazardous materials and aircraft) and natural hazards (e.g., tornadoes, floods, and earthquakes) were typically addressed in terms of probabilistic arguments and initiating frequencies to assess site suitability. The Standard Review Plan (NUREG-0800) for licensing reactors and some of the Regulatory Guides supporting NUREG-0800 provided review and evaluation guidance with respect to these probabilistic considerations.

The TMI accident substantially changed the character of the analysis of severe accidents worldwide. It led to a substantial research program on



severe accident phenomenology. In addition, both major investigations of the accident (the Kemeny and Rogovin studies) recommended that PRA techniques be used more widely to augment the traditional nonprobabilistic methods of analyzing nuclear plant safety. In 1984, the NRC completed a study (NUREG-1050) that addressed the state-of-the-art in risk analysis techniques.

In early 1991, the NRC published NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants." In NUREG-1150, the NRC used improved PRA techniques to assess the risk associated with five nuclear power plants. This study was a significant turning point in the use of risk-based concepts in the regulatory process and enabled the Commission to greatly improve its methods for assessing containment performance after core damage and accident progression. The methods developed for and results from these studies provided a valuable foundation in quantitative risk techniques.

PRA methods have been applied successfully in several regulatory activities and have proved to be a valuable complement to deterministic engineering approaches. This application of PRA represents an extension and enhancement of traditional regulation rather than a separate and different technology. Several recent Commission policies or regulations have been based, in part, on PRA methods and insights. These include the Backfit Rule (§50.109, "Backfitting"), the Policy Statement on "Safety Goals for the Operation of Nuclear Power Plants," (51 FR 30028; August 21, 1986), the Commission's "Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants" (50 FR 32138; August 8, 1985), and the Commission's "Final Policy Statement on Technical Specifications Improvement for Nuclear Power Reactors" (58 FR 39132; July 22, 1993). PRA methods also were used effectively during the anticipated transient without scram (ATWS) and station blackout (SBO) rulemaking, and supported the generic issue prioritization and resolution process. Additional benefits have been found in the use of risk-based inspection



guides to focus NRC inspector efforts and make more efficient use of NRC inspection resources. Probabilistic analyses were extensively used in the development of the recently proposed rule change to reactor siting criteria in 10 CFR Part 100 (59 FR 52255; October 17, 1994). The proposed rule change invoked the use of a probabilistic approach to estimate the Safe Shutdown Earthquake Ground Motion for a nuclear reactor site, instead of the purely deterministic method currently specified in Appendix A to 10 CFR Part 100.

Currently, the NRC is using PRA techniques to assess the safety importance of operating reactor events and is using these techniques as an integral part of the design certification review process for advanced reactor designs. In addition, the Individual Plant Examination (IPE) program and the Individual Plant Examination - External Events (IPEEE) program (an effort resulting from the implementation of the Commission's "Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants") have resulted in commercial reactor licensees using risk-assessment methods to identify any vulnerabilities needing attention.

The Commission has been developing performance assessment methods for low-level and high-level waste since the mid-1970s and these activities intensified using performance assessments techniques in the late 1980s and early 1990s. This has involved the development of conceptual models and computer codes to model the disposal of waste. Because waste-disposal systems are passive, certain analysis methods used for active systems in PRA studies for power reactors had to be adapted to provide scenario analysis for the performance assessment of the potential geologic repository at Yucca Mountain, Nevada. In regard to high-level waste, the NRC staff participates in a variety of international activities (e.g., the Performance Assessment Advisory Group of the Organization for Economic Cooperation and Development, Nuclear Energy Agency) to ensure that consistent performance assessment methods are used to the degree appropriate.



The Commission believes that an overall policy on the use of PRA in nuclear regulatory activities should be established so that the many potential applications of PRA methodology can be implemented in a consistent and predictable manner that promotes regulatory stability and efficiency and enhances safety. In May 1994, the NRC staff forwarded a draft PRA policy statement to the Advisory Committee on Reactor Safeguards (ACRS) for review and briefed ACRS on the same subject. On August 18, 1994, the NRC staff proposed a PRA policy statement to the Commission in SECY-94-218, "Proposed Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities." In that Commission paper, the staff proposed that an overall policy on the use of probabilistic risk assessment (PRA) methods in nuclear regulatory activities should be established and that the use of PRA technology in NRC regulatory activities should be increased. Comments from the ACRS regarding the policy statement as documented in a letter dated May 11, 1994, were incorporated. On August 19, 1994, the staff forwarded SECY-94-219, "Proposed Agency-Wide Implementation Plan for Probabilistic Risk Assessment (PRA)," to the Commission. On August 30, 1994, the staff discussed the PRA policy statement and the PRA implementation plan in a public meeting with the Commission. On September 13 and October 4, 1994, the Secretary issued two staff requirements memoranda (SRMs) providing Commission guidance regarding the draft policy statement. In these SRMs, the Commission directed the staff to revise the proposed PRA policy statement, publish the policy statement for public comment in the Federal Register, and conduct a public workshop on the PRA implementation plan.

As directed by the Commission, the staff conducted a public workshop on December 2, 1994, to discuss the PRA implementation plan. The purpose of the workshop was to inform the public of NRC activities related to increasing the use of PRA methods and techniques in regulatory applications and to receive public comments on these activities. After the staff



incorporated the comments from the SRMs, the proposed policy statement "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities" was published in the Federal Register on December 8, 1994 (59 FR 63389). The public comment period expired on February 7, 1995.

## II. Summary of Public Comments and NRC Responses

In January and February 1995, the NRC received 17 letters commenting on the proposed policy statement on "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities". These comments were from the following organizations: six utilities - PECO Energy Company, Detroit Edison, Washington Public Power Supply System, Carolina Power and Light Company, Virginia Power Company, and Centerior Energy; three State regulatory agencies - State of Illinois Department of Nuclear Safety, State of New Jersey Department of Environmental Protection, State of Nevada Agency for Nuclear Projects; two industry groups - Nuclear Energy Institute and Westinghouse Owners Group; two engineering firms - PLG, Inc. and ICF Kaiser Engineers, Inc.; University of California at Los Angeles; Ohio Citizens For Responsible Energy; Winston and Strawn, Counsel to the Nuclear Utility Backfitting and Reform Group; and the Department of Energy. Copies of the letters may be examined at the NRC Public Document Room at 2120 L Street., NW. (Lower Level), Washington, DC.

### General Comments

Twelve commenters explicitly supported the basic tenet of the policy to increase the use of PRA technology in NRC's regulatory activities. The other commenters did not object to the policy statement but provided recommendations for the NRC to modify and improve the policy statement and/or the PRA implementation plan. Five commenters indicated that they agreed with the NEI comments on the proposed PRA policy statement. The NRC staff has reviewed the comments and summarized them in the following areas.



The staff response to the comments are also included in this final policy statement.

#### Use of PRA in Regulatory Decisions

*Several comments dealt with the scope of the PRA applications (where can PRA be used) and the implementation of the policy statement (how can PRA be used).*

*One commenter felt that neither the policy statement nor the PRA implementation plan provided consistent decision criteria for accepting PRA results as part of the justification for licensing decisions. The commenter was concerned that the short term effect of the policy statement would likely be an increased burden on the licensees. For the long term, the commenter recommended a systematic review of the rules and regulations to identify opportunities for elimination of unnecessary regulations. The proposed policy statement directed the staff to use PRA and associated analyses, where appropriate, as part of the justification for licensing decisions. The PRA implementation plan describes how the stated policy is to be implemented. Appropriate decision criteria will be developed and documented as part of the PRA implementation plan. The Commission has already performed a systematic review of the many current rules and regulations to identify opportunities for the elimination of unnecessary regulations. In 1993, the NRC established the Regulatory Review Group (RRG) to conduct a structured review of power reactor regulations with special attention on the opportunity to reduce unnecessary regulatory burdens. The RRG recommendations to reduce the regulatory burden included the suggestion to use more risk-based approaches in quality assurance, inservice inspection and testing, and the concept of a PRA plan. The RRG recommendations were documented in SECY-94-003. To better focus the NRC's effort on the PRA related activities recommended by the RRG, the PRA Working Group, and the Regulatory Analysis Steering Group, the PRA implementation plan was developed in 1994. The implementation plan*



included a task to develop guidelines for determining when it is practical to use PRA technology and results in regulatory activities. The NRC has had discussions with volunteer licensees regarding the pilot applications of risk-based regulatory initiatives. Results from the pilot applications will be incorporated in the NRC's guidance for PRA applications in regulatory activities. A number of current regulatory requirements are being considered as part of the PRA implementation plan to determine if alternative risk-based approaches are practical. Over time, the Commission would expect some streamlining and refocusing of its rules and regulations as part of this process. The Commission has implemented a continuing regulatory improvement program which is responsive to the commenter's recommendation of a systematic examination of marginal regulatory requirements.

*Another commenter recommended that the policy statement be amended to state that when backfitting analyses are performed, mean risk levels be the exclusive basis of regulatory decision-making when comparisons are made against the \$1000/person-rem criterion. The Commission does not feel this policy statement needs to address the issue regarding the use of mean risk level as the exclusive basis for applying the \$1000/person-rem criterion because the Commission's safety goal policy statement has already spoken to the use of mean values of risk in connection with the cost-benefit analyses. Furthermore, this issue is addressed in the proposed Revision 2 of NUREG/BR-0058, "Regulatory Analysis Guidelines of the U. S. Nuclear Regulatory Commission, Draft Report for Comment." This commenter also recommended that the policy statement should direct the staff to use the relevant plant specific PRA in assessing the need for any backfitting action at that plant. For generic backfits, this commenter recommended that the policy should allow licensees to take credit for plant specific information to justify relief from NRC imposed action. The Commission believes that the use of the plant specific PRA in the backfit analysis to evaluate whether there is a substantial increase in the overall protection*



or to justify relief from NRC imposed action is acceptable when combined with other relevant deterministic considerations, as appropriate.

*Regarding the use of safety goals, one commenter recommended retention of the language in SECY-94-218 to effect that safety goals could be used in granting relief from unnecessary requirements. Another commenter recommended that the safety goals should be used as a minimum goal, rather than the maximum level of safety. As stated in the proposed PRA policy statement published on December 8, 1994, the Commission's safety goals are "...intended to be generically applied by the NRC as opposed to plant specific applications," and "...to be used with appropriate consideration of uncertainties in making regulatory judgements in the context of backfitting new generic requirements on nuclear power plant licensees." In the Staff Requirement Memorandum (SRM) dated June 15, 1990, regarding the implementation of safety goals, the Commission directed that "Safety goals are to be used in a more generic sense and not to make specific licensing decisions." Therefore, at this time, the NRC would use the safety goals in making regulatory decisions regarding backfitting new generic requirements but not to make specific licensing decisions including granting relief from unnecessary requirements. Any changes to the safety goal policy are outside the scope of the PRA policy statement and would, therefore, need to be pursued independently.*

*Referring to paragraphs 1 and 2 of the proposed policy statement, a commenter suggested that it should include the application to NRC enforcement decisions, including the severity levels. As noted in NUREG-1525, "Assessment of the NRC Enforcement Program," the Commission does not support defining severity levels using PRA results. The NRC's basis for severity level categorization clearly is safety significance. In judging safety significance, the NRC considers (1) actual consequences, (2) potential consequences, and (3) regulatory significance. It is recognized that PRA results may be helpful to provide risk insights on the likelihood and significance of potential consequences. The NRC plans to*



continue to consider the use of PRA results where relevant as part of the integrated process considering all facets surrounding the violation in support of enforcement decisions.

*Several commenters discussed the role of PRA in reducing the unnecessary conservatisms in regulations and to support additional regulatory requirements. One commenter's concern was that the proposed policy statement appeared to be biased in the direction of using PRA to support deregulation. Another commenter was concerned with the implication that PRA could result in an additional layer of regulation. The policy statement addressed the need to remove unnecessary conservatism associated with regulatory requirements. It is not the Commission's intent to replace traditional defense-in-depth concepts with PRA, but rather to exploit the use of PRA insights to further understand the risk and improve risk-effective safety decision-making in regulatory matters. In doing so, the Commission is focusing its attention and resource allocation to areas of true safety significance. Where appropriate, PRA should be used to support additional regulatory requirements, according to 10 CFR 50.109 (Backfit Rule).*

*One commenter recommended that the policy statement should explicitly state that the use of PRA by licensees in regulatory matters is at the discretion of each licensee. The commenter also believed that the NRC should not prescribe how and when PRA methods should be used by licensees in regulatory matters, but should address the potential impact the expanded use of PRA may have on regulatory interactions with licensees. The Commission's PRA policy statement is intended only to encourage the NRC staff and industry to use probabilistic risk assessment methods in regulatory matters. It is not intended to prescribe or require any of the many potential PRA applications. Any requirements for licensees to perform PRA analyses would be expected to occur through formal rulemaking.*



*One commenter's concern was that there was a wide range of applications for which PRA was being applied without consistency and standards. This commenter urged the NRC to insist on quality PRAs commensurate with the intended applications and to develop standards which require rigorous and living PRAs by regulation for nuclear power plant applications. The commenter also questioned whether the PRA analyses for the IPE may be used for other applications because of a lack of PRA standards. Another commenter expressed the concern that strict conformance to detailed PRA standards would not be desirable, and recommended that flexibility in PRA models should be allowed.* The Commission issued Generic Letter (GL) 88-20 with the primary purpose of generating IPEs to identify severe accident vulnerabilities. The PRAs which supported the IPE efforts may be useful for other applications, however, this would have to be evaluated on a case-by-case basis under well-defined objectives. After the Commission briefing on the IPE program, the Commission recognized, as stated in the SRM dated April 28, 1995, that current industry IPE results do not provide a complete basis for supporting risk-based regulatory decision-making. The SRM suggested that "...the industry should, in coordination with the staff, initiate the actions necessary to develop PRAs that are acceptable for risk-based regulatory use (i.e., standardized methods, assumptions, level of detail)." The industry is encouraged to formulate a general approach for performing PRAs acceptable for regulatory use. This approach should include guidance on standardizing approaches for use of PRA techniques for specific applications, narrowing some of the variability in the IPE results, and strengthening its usefulness in the regulatory and safety decision-making process. The Commission is currently considering the quality level and scope of assessment necessary to justify use of specific PRAs for specific regulatory applications. The Commission will require PRA quality commensurate with the proposed application.



### PRA Methodology

*One commenter agreed with the NRC that the probabilistic approach should be used to complement the deterministic approach and that PRA numbers alone should not be used to make regulatory decisions. The commenter also believed that uncertainties should not prevent or delay the implementation of PRA in regulatory activities.* The Commission understands that uncertainties exist in any regulatory approach. These uncertainties are derived from knowledge limitations that are not created by PRA, but are often exposed by it. The PRA implementation plan has provided a framework to assess the significance of potential uncertainties and to develop a strategy to accommodate them in the regulatory process.

*One commenter stated that probabilistic analysis is simply an extension of deterministic analysis. They are not separate and distinctive concepts.* The Commission agrees with this concept as the proposed policy statement stated that "The probabilistic approach to regulation is, therefore, considered an extension and enhancement of traditional regulation by considering risk in a more coherent and complete manner." The Commission believes that the PRA method plays a complementary role in relationship to the deterministic method. This was reflected in the policy statement that "Deterministic-based regulations have been successful in protecting the public health and safety and PRA techniques are most valuable when they serve to focus the traditional, deterministic-based, regulations and support the defense-in-depth philosophy."

*One commenter recommended that the most efficient use of NRC resources should be to enhance or improve the existing methods, but not to develop new ones.* The Commission's principal focus will be on improving the existing methods, but some new methods development may also be useful.

*Another commenter recommended that the PRA policy statement should seek a uniform and standard application of PRA within the NRC, and begin*



*with a commitment to ensure that PRA is used consistently and is not ignored when required by those unfamiliar or reluctant to apply it. The Commission's PRA policy statement specifically emphasizes the need for consistent and predictable application of PRA within the Commission to promote regulatory stability and efficiency. The Commission believes that this goal can be achieved through the implementation plan which will ensure that the appropriate use of PRA is implemented by the staff.*

#### Schedule of PRA Activities

*Two letters commented that the activities discussed in the PRA implementation plan appeared to be on a protracted schedule and recommended that priority and urgency be stressed and reflected in the plan, including the use of PRA and PRA insights in the near term. The Commission's PRA implementation plan showed the target completion dates for all the tasks. The Commission fully realizes the need for near term PRA applications and has included them in the implementation plan wherever possible. These milestones include examples such as pilot applications for risk-based initiatives and transfer of IPE insights to NRC staff members for use in regulatory matters in the near term. The Commission plans to periodically review the progress of the "living" PRA implementation plan and, as appropriate, to adjust the priorities.*

*One letter commented that the NRC review and approval of licensing actions that are based on PRA insights should not be contingent upon the schedule for implementation of the plan. The plan should not be an impediment to moving forward toward the goals outlined in the policy statement. The Commission's implementation plan had been developed to effectively and expeditiously establish a framework for increasing the use of PRA technology inside the Commission. Since it is a "living" plan, new tasks could be added and existing tasks could be modified, as the plan progresses. The Commission agrees that the plan should not be an impediment to moving forward to achieve the goals stated in the policy.*



The Commission welcomes risk-based regulatory initiatives from the industry as the plan is being carried out and will adjust resources, as appropriate.

*One commenter asked how the NRC will propose to control the utilities' application of PRA and the timeframe to implement the consistent use of PRA within the NRC.* The Commission's PRA implementation plan describes the activities and schedule to effect a coherent and consistent PRA application within the agency. As the plan is implemented, the NRC expects to interact with licensees and publish guidelines for the application of PRA in their submittal to the NRC.

#### PRA Training

*Two commenters advocated PRA training for appropriate NRC and licensee staff as soon as possible to ensure proper application of PRA in regulatory matters.* A PRA training program has been in place for the NRC staff for a number of years. As part of the PRA implementation plan, the existing training program is being enhanced. The existing PRA training curriculum serves as the basis on which to build a more comprehensive staff PRA training program. Six new courses have been incorporated in the training program to address the short term needs from the increasing use of PRA in regulatory activities. As a result of the PRA implementation plan, the number of NRC staff participating in the training program has increased significantly during the first half of fiscal year 1995.

*One commenter recommended that NRC's PRA training should be extended to State agencies that can justify attendance.* Historically, attendance at NRC courses has been routinely available on a space-available, no-cost basis to State personnel as well as for other non-NRC personnel (such as foreign regulators, EPA, DOE, and other Federal personnel). This has included training in the PRA area for a limited number of State regulators. In courses that were under-subscribed by NRC personnel, many had sufficient available space to allow acceptance of outside personnel. Logistics for



these arrangements are handled by the NRC office responsible for interactions with the outside group (i.e., Office of State Programs for States or Office of International Programs for foreign personnel). NRC training currently is not available to NRC licensees. Because of recent budgetary constraints, as described in SECY-95-017 "Reinventing NRC Fee Policies," full cost reimbursements from States for NRC training is expected in future years. However, NRC will continue its space-available policy for all courses, including PRA courses.

#### Data Collection

*Several commenters expressed concerns about the potential data collection implications of the proposed PRA policy. They are summarized as follows:*

*One commenter stated that the desire to collect detailed data related to equipment and human reliability should not prohibit the use of PRA for applications or support for decision-making. The collection of plant-specific data must be commensurate with the benefit that specific information might have on the quality or insight from the PRA. Plant-specific information may not be statistically significant. Furthermore, requiring all plants to collect the same information without a focus based on plant performance, is counter to the concept behind the Maintenance Rule.*

*Another commenter stated that the discussion of uncertainties in Part II.(B) of the proposed policy statement is appropriate. However, in the implementation of this part of the policy, care must be exercised to restrain from requiring or implying the need for massive plant-specific component level failure rate data collection programs. Several commenters expressed concerns that a new or expanded nuclear power plant experience data collection rulemaking could further burden the licensees and the resulting benefit may well be marginal.*



The Commission agrees that it should make every effort to avoid any unnecessary regulatory burdens in connection with collecting reliability and availability data. Specific comments on the types of data that should or should not be collected will be addressed in connection with proposed data collection requirements when they are published for comment.

#### Radiation Medicine

*One commenter recommended that NRC should abandon the use of the linear hypothesis in estimating radiation-induced cancer and mutation risk. The commenter further stated that the NRC's PRA implementation plan refers to risk analysis to analyze nuclear medical devices and that, "...there are no nuclear medicine devices that have risk to be analyzed."*

The International Commission on Radiation Protection, the United Nations Scientific Committee on the Effects of Atomic Radiation, and the National Academy of Sciences' Committee on the Biological Effects of Ionizing Radiation believe that, in the absence of convincing evidence that there is a dose threshold or that low levels of radiation are beneficial, the assumptions regarding a linear nonthreshold dose-effect model for cancers and genetic effects and the existence of thresholds only for certain nonstochastic effects remain appropriate for formulating radiation protection standards. NRC follows their guidelines. Although some data suggest the possible use of other models, there are still many scientists who believe there are insufficient data to deviate from the "linear" hypothesis. The issue of realism involved in continuing the use of the "linear" hypothesis is expected to be a matter of debate over the coming years.

The NRC regulates radiation medicine, which includes both nuclear medicine and radiation oncology. The intent of the policy statement concerning medical applications is to refer to medical devices containing byproduct material, in particular, those used in radiation oncology. The term "nuclear medical device" was revised in the recent status update on the PRA implementation plan (SECY-95-079) and clarified in the policy statement.

#### Nuclear Waste

*One commenter recommended that the NRC expand its use of PRA to other areas such as radiological dose assessment during the site decommissioning process. The NRC intends to consider expansion of PRA techniques into*



additional areas with the proviso that the application of these techniques to these facilities should be tempered according to the complexity of the disposal system, its uncertainties and the estimated risk.

*One commenter provided comments on several aspects of the proposed policy statement in the nuclear waste area. Regarding the scope of the policy statement, the commenter recommended that the policy statement be amended to include risk assessment applications other than power reactors. The Commission agrees with that comment. The use of PRA should be considered for those applications that involve projecting system performance for very long time periods, such as hundreds or thousands of years. The policy statement stated that the use of PRA technology should be increased in all regulatory matters. Another recommendation was to temper the commitment to PRA to reflect inherent risk differences associated with different waste management facilities. Because of inherent differences in the regulations and practices associated with the licensing of waste management facilities, the application of performance assessment (PRA is called performance assessment for waste management systems) techniques to these facilities should be tempered according to the complexity of the disposal system, uncertainties surrounding the system performance, and the estimated risk. The Commission also agrees with the comments regarding uncertainties in projecting repository performance and the use of technical expert judgment in assessing these uncertainties, but feels the PRA policy statement is not the appropriate forum to discuss these items applicable only to waste management.*

*Regarding the suggestion of describing the reasons for using the PRA and the application of PRA in regulatory activities, the Commission included the reasons for using PRA in Section III of the policy statement and added a description of the impact of PRA on the rule changes to 10 CFR Part 100 in the background discussion.*

*Another commenter expressed concern that the proposed policy statement inappropriately encouraged the use of PRA in the licensing and regulation of nuclear waste disposal facilities. The Commission disagrees with this comment since PRA techniques are acceptable in a performance assessment for the geologic repository, but are only part of the requirements for a license. The commenter was also concerned that any new regulations proposed by the Environmental Protection Agency (EPA) and the NRC's 10 CFR Part 60 for a high-level waste (HLW) disposal facility proposed for Yucca Mountain will probably prohibit use of PRA for these facilities because of Type I faults at this site. The Commission anticipates that both probabilistic and deterministic hazard assessment methodologies will be*



applied to assess the significance of faulting at Yucca Mountain. Furthermore, the Commission does not interpret 10 CFR Part 60 so as to preclude the use of PRA as a basis for licensing a proposed repository at Yucca Mountain. *The commenter did not agree with NRC's characterization of the waste disposal system as passive and believed that, at this time, there is no alternative to the use of deterministic techniques for waste disposal application because PRA techniques are in the embryonic stage.* The "Fault Tree Handbook" (NUREG-0492, January 1981) refers to "passive" as a "...mechanism (e.g., wire) whereby the output of one 'active' component becomes the input to a second 'active' component." "Passive" is generally used for "engineered" components that have no moving parts. Since there are no "engineered" components that are "active" (or causing motion in another engineered component) in the post-closure phase of the potential geologic repository at Yucca Mountain, the NRC has applied the traditional PRA concept to the waste disposal system and referred to it as a "passive system." The remanded 1985 EPA Standard, 40 CFR 190, required a probabilistic analysis for a geologic repository. The NRC has developed this type of analysis since 1970 and has attained a state of maturity for these analyses that is accepted by internationally-known organizations (e.g., Organization for Economic Cooperation and Development (OECD)/Nuclear Energy Agency (NEA)).

*A number of editorial comments were received on the role of PRAs in the licensing of waste disposal facilities. The NRC has incorporated the appropriate comments in this final PRA policy statement.*

### III. Deterministic and Probabilistic Approaches to Regulation

#### (A) *Extension and Enhancement of Traditional Regulation*

The NRC established its regulatory requirements to ensure that a licensed facility is designed, constructed, and operated without undue risk to the health and safety of the public. These requirements are largely based on deterministic engineering criteria. Simply stated this deterministic approach establishes requirements for engineering margin and for quality assurance in design, manufacture, and construction. In addition, it assumes that adverse conditions can exist (e.g., equipment failures and human errors) and establishes a specific set of design-basis events. It then requires that the licensed facility design include safety systems capable of preventing and/or mitigating the consequences of those design-basis events to protect the public health and safety.



The deterministic approach contains implied elements of probability (qualitative risk considerations), from the selection of accidents to be analyzed as design-basis accidents (e.g., reactor vessel rupture is considered too improbable to be included) to the requirements for emergency core cooling (e.g., safety train redundancy and protection against single failure). The approach by the Commission for the use of performance assessment to implement its regulations for disposal of radioactive nuclear waste (10 CFR Part 60 for high-level waste disposal and 10 CFR Part 61 for low-level waste disposal) also contains implied elements of probability. The results of the numerous calculations obtained from a performance assessment for a given performance measure and for a particular type of facility (e.g., a spectrum of values for ground-water travel time or individual dose) are expressed in terms of statistical distributions that express the probability that a given measure of performance will be attained. When this distribution is compared to the appropriate deterministic standard in the Commission's regulations, the probability of not exceeding the standard can be obtained from the part of the distribution that falls below this standard.

PRA addresses a broad spectrum of initiating events by assessing the event frequency. Mitigating system reliability is then assessed, including the potential for multiple and common cause failures. The treatment therefore goes beyond the single failure requirements in the deterministic approach. The probabilistic approach to regulation is, therefore, considered an extension and enhancement of traditional regulation by considering risk in a more coherent and complete manner. A natural result of the increased use of PRA methods and techniques would be the focusing of regulations on those items most important to safety. Where appropriate, PRA can be used to eliminate unnecessary conservatism and to support additional regulatory requirements. Deterministic-based regulations have been successful in protecting the public health and safety and PRA techniques are most valuable when they serve to focus the traditional, deterministic-based, regulations and support the defense-in-depth philosophy. In addition, PRA techniques are appropriately used when considering regulations defined in probabilistic terms, and for estimating safety of systems with very large uncertainties such as waste disposal systems (Note that PRA is called performance assessment for these waste disposal systems).

Beyond its deterministic criteria, the NRC has formulated guidance, as in the safety goal policy statement, that utilizes quantitative, probabilistic risk measures. The safety goal policy statement establishes top-level objectives to help assure safe operation of nuclear power plants.



The safety goals are intended to be applied generically and are not for plant-specific applications. For the purpose of implementation of the safety goals, subsidiary numerical objectives on core damage frequency and containment performance have been established. The safety goals provide guidance on where plant risk is sufficiently low that further regulatory action is not necessary. Also, as noted above, the Commission has been using PRA in performing regulatory analysis for the proposed backfit of cost-beneficial safety improvements at operating reactors (as required by 10 CFR 50.109) for a number of years.

(B) *Uncertainties and Limitations of Deterministic and Probabilistic Approaches*

The treatment of uncertainties is an important issue for regulatory decisions. Uncertainties exist in any regulatory approach and these uncertainties are derived from knowledge limitations. These uncertainties and limitations existed during the development of deterministic regulations and attempts were made to accommodate these limitations by imposing prescriptive, and what was hoped to be, conservative regulatory requirements. A probabilistic approach has exposed some of these limitations and provided a framework to assess their significance and assist in developing a strategy to accommodate them in the regulatory process.

Human performance is an important consideration in both deterministic and probabilistic approaches. Assessing the influence of errors of commission and organizational and management issues on human reliability is an example that illustrates where current PRA methods are not fully developed. While this lack of knowledge contributes to the uncertainty in estimated risks, the PRA framework offers a powerful tool for logically and systematically evaluating the sensitivity and importance to risk of these uncertainties. Improved PRA techniques and models to address errors of commission and the influence of organizational factors on human reliability are currently being developed.

It is important to note that not all of the Commission's regulatory activities lend themselves to a risk analysis approach that utilizes fault tree methods. In general, a fault tree method is best suited for power reactor events that typically involve complex systems. Events associated with industrial and medical uses of nuclear materials generally involve a simple system, involve radiation overexposures, and result from human error, not equipment failure. Because of the characteristics of medical and industrial events, as discussed above, analysis of these events using



relatively simple techniques can yield meaningful results. Power reactor events, however, generally involve complex systems and human interactions, can potentially involve more than one adverse consequence, and often result from equipment failures. Therefore, power reactor events can require greater use of more complex risk analysis techniques, such as fault tree analysis, to yield meaningful insights. PRA methods need to be adapted for waste disposal systems because they are passive systems subjected to interlocking natural and man-made processes and events that are dominated by complex phenomenology.

Given the dissimilarities in the nature and consequences of the use of nuclear materials in reactors, industrial situations, waste disposal facilities, and medical applications, the Commission recognizes that a single approach for incorporating risk analyses into the regulatory process is not appropriate. However, PRA methods and insights will be broadly applied to ensure that the best use is made of available techniques to foster consistency in NRC risk-based decision-making.

#### *(C) Defense-in-Depth Philosophy*

In the defense-in-depth philosophy, the Commission recognizes that complete reliance for safety cannot be placed on any single element of the design, maintenance, or operation of a nuclear power plant. Thus, the expanded use of PRA technology will continue to support the NRC's defense-in-depth philosophy by allowing quantification of the levels of protection and by helping to identify and address weaknesses or overly conservative regulatory requirements applicable to the nuclear industry. Defense-in-depth is a philosophy used by NRC to provide redundancy for facilities with "active" safety systems, e.g., a commercial nuclear power, as well as the philosophy of a multiple-barrier approach against fission product releases. Such barrier principles are mandated by the Nuclear Waste Policy Act of 1982, which provides redundancy for a geologic repository to contain and isolate nuclear waste from the human environment.

#### IV. The Commission Policy

Although PRA methods and information have thus far been used successfully in nuclear regulatory activities, there have been concerns that PRA methods are not consistently applied throughout the agency, that sufficient agency PRA/statistics expertise is not available, and that the Commission is not deriving full benefit from the large agency and industry investment in the developed risk assessment methods. Therefore, the Commission believes that an overall policy on the use of PRA in nuclear



regulatory activities should be established so that the many potential applications of PRA can be implemented in a consistent and predictable manner that promotes regulatory stability and efficiency. This policy statement sets forth the Commission's intention to encourage the use of PRA and to expand the scope of PRA applications in all nuclear regulatory matters to the extent supported by the state-of-the-art in terms of methods and data. Implementation of the policy statement will improve the regulatory process in three areas: foremost, through safety decision making enhanced by the use of PRA insights; through more efficient use of agency resources; and through a reduction in unnecessary burdens on licensees.

Therefore, the Commission adopts the following policy statement regarding the expanded NRC use of PRA:

- (1) The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
- (2) PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal for additional regulatory requirements in accordance with 10 CFR 50.109 (Backfit Rule). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.
- (3) PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.
- (4) The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.



### *Policy Implications*

There are several important regulatory or resource implications that follow from the goal of increased use of PRA techniques in regulatory activities. First, the NRC staff, licensees, license applicants, and Commission must be prepared to consider changes to regulations, to guidance documents, to the licensing process, and to the inspection program. Second, the NRC staff and Commission must be committed to a shift in the application of resources over a period of time based on risk findings. Third, the NRC staff must undertake a training and development program, which may include recruiting personnel with PRA experience, to significantly enhance the PRA expertise necessary to implement these goals. Additionally, the NRC staff must continue to develop new and improved PRA methods and regulatory decision-making tools and must significantly enhance the collection of equipment and human reliability data for all of the agency's risk assessment applications, including those associated with the use, transportation, and storage of nuclear materials. However, it is recognized that there may be situations with material users where it may not be cost-effective to use PRA in their specific regulatory applications.

This policy statement affirms the Commission's belief that PRA methods can be used to derive valuable insights, perspective, and general conclusions as a result of an integrated and comprehensive examination of the design of nuclear facilities, facility response to initiating events, the expected interactions among facility structures, systems, and components, and between the facility and its operating staff.

The Commission also recognizes, and encourages, continuation of industry initiatives to improve PRA methods, applications and data collection to support increased use of PRA techniques in regulatory activities.

### V. Availability of Documents

Copies of documents cited in this section are available for inspection and/or for reproduction for a fee in the NRC Public Document Room, 2120 L Street, NW, (Lower Level), Washington, DC 20037. Copies of NUREGs cited in this document may be purchased from the Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082. Copies are also available for purchase from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.



In addition, copies of 1) SECY-94-218, "Proposed Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities," 2) SECY-94-219, "Proposed Agency-Wide Implementation Plan for Probabilistic Risk Assessment (PRA)," 3) the Commission's Staff Requirements Memorandum of September 13, 1994, concerning the August 30, 1994, Commission meeting on SECY-94-218 and SECY-94-219, and 4) the Commission's Staff Requirements Memorandum of October 4, 1994, on SECY-94-218 can be obtained electronically by accessing the NRC electronic bulletin board system (BBS) Tech Specs Plus. These four WordPerfect® 5.1 documents are located in the BBS MISC library directory under the single filename "PRAPLAN.ZIP". The WordPerfect® 5.1 file for the final policy statement on the "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities," is located in the BBS MISC library directory under the filename "PRPOLICY.ZIP". The BBS operates 24 hours a day and can be accessed through a toll-free number, 1-800-679-5784, at modem speeds up to 9600 baud with communication parameters set at 8 data bits, no parity, 1 stop bit, full duplex, and using ANSI terminal emulation.

Dated at Rockville, Maryland, this 10th day of August, 1995.

FOR THE NUCLEAR REGULATORY COMMISSION

/original signed by/

Andrew L. Bates,  
Acting Secretary of the Commission.



April 11, 1997

The Honorable Shirley Ann Jackson  
Chairman  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001

Dear Chairman Jackson:

SUBJECT: RISK-BASED REGULATORY ACCEPTANCE CRITERIA FOR PLANT-SPECIFIC  
APPLICATION OF SAFETY GOALS

In our December 6, 1996 meeting with the Commission, we committed to provide an example of how risk-acceptance criteria could be developed directly from the Safety Goals. Additionally, in a Staff Requirements Memorandum dated January 14, 1997, the Commission asked for our views on the relationship between the concept of "adequate protection," as used in the NRC regulations, and the NRC Safety Goals, from the standpoint of level of risk.

During the 440th meeting of the ACRS, April 3-4, 1997, we completed our deliberations on plant-specific application of NRC Safety Goals and the relationship between the concept of "adequate protection" and the Safety Goals. In our November 18, 1996 report on this subject, we stated that "the safety goals and subsidiary objectives can and should be used to derive guidelines for plant-specific applications." We noted that full-scope Level 3 probabilistic risk assessments (PRAs) would be necessary to use the quantitative health objectives (QHOs) directly to assess the acceptability of plant-specific risk. We also stated that this assessment of risk could be done in terms of the QHOs, along with the core damage frequency (CDF), or in terms of the CDF and large, early release frequency (LERF).

This report further discusses the need for plant-specific application of risk-acceptance criteria and the appropriateness of these criteria being derived from the Safety Goal QHO on early fatalities. The additional comments to this report provide examples of approaches that could be used to quantify lower tier acceptance criteria (i.e., LERF, or CDF and conditional containment failure probability) that will ensure that the early fatality QHO is met at each site. Quantification of the LERF at each site is needed to ensure the appropriateness of the choice of the LERF acceptance criterion proposed in draft Regulatory Guide DG-1061 and draft Standard Review Plan sections that support risk-informed, performance-based regulation.

#### Need for Plant-Specific Application

The Safety Goal Policy Statement makes it clear that the QHOs and the subsidiary goal on CDF were intended only to provide standards for the NRC to judge the overall effectiveness of its regulatory system. The Policy Statement specifically precludes enforcement of the Safety Goals on a plant-specific basis.

In the development of draft Regulatory Guide DG-1061 and the associated draft Standard Review Plan sections in support of risk-informed, performance-based regulation, the staff has found it necessary to propose risk-acceptance guidelines that can be applied on a plant-specific basis. These guidelines would be used, along with other considerations and inputs, for making judgments on the acceptability of requested changes to a licensee's current licensing basis.



Reviewing plant-specific license amendments by using risk-acceptance guidelines is a positive action toward risk-informed, performance-based regulation.

We also note that, in the longer term, the Commission may want to consider having a quantified acceptable risk level to replace the current concept of "adequate protection." This risk level could eventually serve as an objective risk-acceptance criterion for many enforcement decisions.

#### Risk-Informed, Performance-Based Regulation

The Commission has directed the staff to increase the use of PRA in the regulatory process. We have endorsed this because we believe that a risk-informed, performance-based regulatory approach will lead to increased coherence in the regulatory system, to enhanced decision-making ability, and to technically defensible bases for granting regulatory relief.

A risk-informed, performance-based regulatory system ought not be implemented without the existence of top-level risk-acceptance criteria. The obvious choices for these criteria are the NRC Safety Goal QHOs. As it is the responsibility of the NRC to license individual plants and ensure adequate protection, there seems to be no alternative to plant-specific applications.

#### Relationship Between Adequate Protection and the Safety Goals

Currently, licensing acceptance criteria are embodied in the concept of "adequate protection." With this concept, a plant that is licensed and complies fully with the applicable rules and regulations, is considered to meet the "adequate protection" standard. "Adequate protection" embodies protection of public health and safety against threats that can be quantified in terms of risk as well as threats, such as sabotage and diversion of special nuclear material, for which the risk cannot now be quantified. In the discussion that follows, the nonquantifiable aspects of adequate protection are set aside. Since there are many ways in which plants can be designed and operated within the confines of the regulations, the natural result is a spectrum of risk levels across the population of operating plants. This conclusion is consistent with the results of the recent Individual Plant Examination Program. Since each licensed plant must, by definition, provide adequate protection, the licensed plant that poses the highest level of risk places a bound on the quantified level of risk to be associated with "adequate protection."

Within the spectrum of risk, it is likely that there are plants with risk levels above the Safety Goals and other plants with risk levels below. If this is indeed the case, a single risk level that bounds "adequate protection" would be a risk level greater than the Safety Goal level. For those plants with risk levels below the Safety Goals, the difference between the plant risk and the Safety Goals can be viewed as margin. It is from some portion of this margin that plant-specific regulatory relief could be granted. For those plants with risk levels greater than the Safety Goals, the challenge will be to eventually reduce their risk to below the Safety Goal level within the confines of the backfit rule.

#### Regulatory Transparency

The unquantified "adequate protection" concept is not well understood by the general public because the public is unfamiliar with the regulatory process, the body of nuclear regulations, and associated underlying technical bases. We believe that a long-term objective of replacing the "adequate protection" concept with a well articulated and quantified "acceptable level of risk" if achievable, would enhance the public's understanding and acceptance of the regulatory process and would lead to a more uniform level of protection for all individuals living in the vicinity of nuclear plants.

We note that the use of risk-acceptance criteria such as the QHOs will add stability to the regulatory process. This is because the Safety Goals are determined primarily from considerations of societal risk, while the NRC rules



and regulations, which are now used to specify adequate protection, change with time as our understanding of reactor safety issues evolves.

#### Safety Goals as Risk-Acceptance Criteria

It is our opinion that the QHOs are the appropriate choices for risk-acceptance criteria for plant-specific applications. The Safety Goals are the expression by NRC for "how safe is safe enough." In our opinion, this is what risk-acceptance criteria ought to be. As we stated in our August 15, 1996 report, the subsidiary CDF goal should be elevated to the status of a fundamental goal. Elevating the CDF subsidiary goal to the status of a fundamental goal can be considered as a defense-in-depth principle that provides balance between prevention and mitigation.

The early fatality QHO generally controls the risks from nuclear plant operations. Our understanding of risk associated with low-power and shutdown operations, or accidents initiated by external events in which emergency response is impeded, is not yet sufficient to draw definitive conclusions concerning the limiting QHO in these situations.

Additional comments by ACRS Member T. S. Kress are presented below.

Sincerely,

/s/

R. L. Seale  
Chairman

#### Additional Comments by ACRS Member T. S. Kress

While I agree completely with the Committee's report, I think it could be augmented in two respects. First, it could make it clearer that, with respect to plant-specific application of the Safety Goals, we are making two related, somewhat radical proposals, the second more so than the first:

- 1) That lower tier risk-acceptance criteria (CDF and LERF), now being proposed in Draft Regulatory Guide DG-1061 for use in making decisions regarding requested changes to a licensee's current licensing basis, be derived directly from the prompt fatality QHO and be of such value as to bound all current sites.
- 2) That, in the long run for enforcement purposes, the prompt fatality QHO be considered as the quantification of a risk level to replace "adequate protection."

Second, guidance on how lower tier criteria are to be derived from the QHO is needed. Consequently, I am including two attachments to these additional comments (one developed by me and a complementary one developed by ACRS Senior Fellow Rick Sherry). These provide examples of how to more rigorously derive the lower tier criteria. It is suggested that the staff consider these for use if the first proposal above is to be implemented.

#### Attachments:

1. Kress, T. S., "Risk-Based Regulatory Acceptance Criteria for Plant-Specific Application of Safety Goals," March 1997
2. Sherry, R. R., "Methodology for Estimating Offsite Early Fatality Risk in the Absence of a Level 3 PRA," March 1997

#### References:

1. Staff Requirements Memorandum dated January 14, 1997, from John C. Hoyle, Secretary, NRC, to John T. Larkins, Executive Director, ACRS, Subject: Meeting with ACRS, 9:30 A.M., Friday, December 6, 1996, Commissioners'



- Conference Room.
2. Report dated November 18, 1996, from T. S. Kress, Chairman, ACRS, to Shirley Ann Jackson, Chairman, NRC, Subject: Plant-Specific Application of Safety Goals.
  3. Report dated August 15, 1996, from T. S. Kress, Chairman, ACRS, to Shirley Ann Jackson, Chairman, NRC, Subject: Risk-Informed, Performance-Based Regulation and Related Matters.
  4. U.S. Nuclear Regulatory Commission, NUREG-1560, Volume 1, Part 1, "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance," Summary Report, Draft Report for Comment, October 1996.
  5. U.S. Nuclear Regulatory Commission Draft Regulatory Guide, Draft DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," dated February 28, 1997 (Predecisional).
  6. U.S. Nuclear Regulatory Commission, Draft Standard Review Plan Chapter 19, Revision L, "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance," dated March 3, 1997 (Predecisional).



D910719

The Honorable Ivan Selin  
Chairman  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555

Dear Chairman Selin:

SUBJECT: THE CONSISTENT USE OF PROBABILISTIC RISK ASSESSMENT

During the 375th meeting of the Advisory Committee on Reactor Safeguards, July 11-13, 1991, and in earlier meetings, we discussed the unevenness and inconsistency in the use of probabilistic risk assessment (PRA) in NRC. PRA can be a valuable tool for judging the quality of regulation, and for helping to ensure the optimal use of regulatory and industry resources, so we would have liked to see a deeper and more deliberate integration of the methodology into the NRC activities. Our recommendations to this end are directed at problems that took time to develop, and are likely to take a long time to solve.

PRA is not a simple subject, so there are wide variations in the sophistication with which it is used by the various elements of NRC. There are only a few staff members expert in some of the unfamiliar disciplines -- especially statistics -- that go into a PRA, so it is not surprising that there are inconsistencies in the application of the methodology to regulatory problems.

To illustrate the problems, let us just list a few of the fundamental aspects of the use of PRA, in which different elements of the staff seem to go their own ways. These are just illustrations, but each can lead to an erroneous regulatory decision.

1. The proper use of significant figures is in principle a trivial matter, but it does provide a measure of a person's understanding of the limitations of an analysis. Yet we often hear from members of the staff who quote core-damage probabilities to three significant figures, and who appear to believe that the numbers are meaningful. It is a rare PRA in which even the first significant figure should be regarded as sufficiently accurate to play an important role in a regulatory decision, but there is something mesmerizing about numbers, which imbues them with misleading verisimilitude. They deserve respect, but not too much, and it is wrong to err in either direction.
2. Closely related is uncertainty. There is no way to know how seriously to take the results of a PRA without some estimate of the uncertainty, yet we often hear thoroughly unsatisfactory answers (some perhaps invented on the spot) when we ask about uncertainty. One of the advantages of PRA is that it provides a mechanism for estimating uncertainty, uncertainty which is equally present, but not quantified, in deterministic analyses.
3. Conservatism. A PRA should be done realistically. The proper time to add an appropriate measure of conservatism is when its results are used in the regulatory process. If the PRA itself is done with conservative assumptions (more the rule than the exception at NRC), and is then used in a conservative regulatory decision-making process, self-deception can result, or resources can be squandered.

The inconsistent use of conservatism was illustrated by a pair of briefings at our April 1991 meeting, which included updates on proposed rules on license renewal and on maintenance. In the former case, we were told that a licensee could use PRA to add an item for later review, but never to remove one -- a one-way sieve. In the latter case we were told that PRA could be used to justify either enhancement or relaxation of maintenance requirements. Foolish consistency may be a hobgoblin, as Emerson said, but there is nothing foolish in seeking consistency in regulation.

4. The bottom line. It has been widely recognized since WASH-1400 that the bottom-line probabilities (of either core melt or immediate or delayed fatalities) are among the weakest results of a PRA, subject to the greatest uncertainties. (That doesn't mean they are useless, only that they should be used with caution and sophistication.) Yet we find staff members unaware of these subtleties, often dealing with small problems, justifying their actions in terms of the bottom-line probabilities. This is only in part due to the Backfit Rule, which almost requires such behavior; it is also inexperience and lack of sensitivity to the limitations of the methodology.



A number of staff actions and proposals use bottom-line results of a PRA as thresholds for decision making, often with the standard litany about the uncertainty in the reliability of these results. In fact, the quantified uncertainty in the bottom-line results of a PRA is just as important a number as the probability itself. It would be straightforward to employ a decision-making algorithm that prescribes a confidence level for the decision, and uses both the bottom-line probability and the uncertainty to achieve this. A further improvement would be to incorporate the consequences of erroneous decisions, what statisticians would call the loss function, into the decision-making process. The Commission has come close to this approach in its recent instructions to the staff on the diesel generator reliability question.

These are just a few examples of problems with the use of PRA in NRC, all common enough to be disturbing, and increasing in frequency as the use of PRA increases. It has been more than fifteen years since the publication of WASH-1400, a pioneering study which, despite known shortcomings, established the NRC at the forefront of quantitative risk assessment. One could have hoped that by now a coherent policy on the appropriate use of PRA within the agency, on both large and small problems, could have evolved. We recommend that:

- A. A mechanism be found (perhaps a retreat) through which the few PRA and statistical experts now scattered throughout the agency (and generally ignored) can be brought together with the appropriate senior managers and outside experts, to work toward a consistent position on the use of PRA at NRC. It could be worth the time expended. (Among other long-term benefits, such an interaction would add an element of horizontal structure to the NRC's predominantly vertical organization.)
- B. The Commission then find a way to give credence and force to that position.
- C. The Commission emphasize recruitment of larger numbers of professionals expert in PRA and statistics.
- D. The Commission consider some kind of mandate that any letter, order, issue resolution, etc., that contains or depends on a statistical analysis or PRA, be reviewed by one of the expert PRA or statistical groups.

We do not pretend that this is an easy problem. The solution involves not only a cultural shift, so that those few experts already at NRC have some impact, but also substantial enhancement of the staff capabilities. That will require incentives that only the Commission can supply. It is interesting that the Commission's Severe Accident Policy Statement, dated August 1985, stated that "within 18 months of the publication of this severe accident statement, the staff will issue guidance on the form, purpose and role that PRAs are to play in severe accident analysis and decision making for both existing and future plant designs...."

Additional comments by ACRS Members Harold W. Lewis and J. Ernest Wilkins are presented below.

Sincerely,

David A. Ward  
Chairman

Additional Comments by ACRS Members Harold W. Lewis and J. Ernest Wilkins

We thoroughly endorse this letter, and regret only that the Committee chose to ignore the parallels between the PRA problems and those in a number of other newer technologies significant to nuclear safety. Recommendation C should have included mention of some of these -- electronics and computers, for example -- which are of increasing importance. Weaknesses in those areas also need correction. Computerized protection and control systems, in particular, require the kind of sophisticated review that NRC is in no position to provide.



December 16, 1997

The Honorable Shirley Ann Jackson  
Chairman  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555-0001

Dear Chairman Jackson:

SUBJECT: TREATMENT OF UNCERTAINTIES VERSUS POINT VALUES  
IN THE PRA-RELATED DECISIONMAKING PROCESS

During the 443rd, 444th, 446th, and 447th meetings of the Advisory Committee on Reactor Safeguards, July 9-11, September 3-5, November 6-7, and December 3-6, 1997, respectively, we met with representatives of the NRC staff to discuss issues included in the Staff Requirements Memorandum dated May 27, 1997, regarding the use of uncertainty versus point values in the PRA-related decisionmaking process (Reference 1). Our Subcommittee on Reliability and Probabilistic Risk Assessment (RPRA) met with the staff and industry representatives to discuss these matters on July 7, August 28, October 21-22, and November 12-13, 1997.

#### Background

Uncertainty has always been of concern to nuclear power regulators. As early as 1956, Willard F. Libby, Acting Chairman of the Atomic Energy Commission (AEC), wrote to the Congressional Joint Committee on Atomic Energy that "it is incumbent upon the new industry and the Government to make every effort to recognize every possible event or series of events which could result in the release of unsafe amounts of radioactive material to the surroundings and to take all steps necessary to reduce to a reasonable minimum the probability that such events will occur in a manner causing serious overexposure to the public." (Reference 2)

Even though Dr. Libby used the word "probability," about 20 years would pass before systematic calculations of probabilities would be produced for the "possible event or series of events" to which he referred. The "reasonable minimum" of the unquantified probability that was achieved at that time was attained through the development and application of the concepts of defense in depth and safety margins.

Defense in depth is advocated in numerous documents as the principal means of controlling the (still unquantified) probability of accidents. For example, during the 1971 hearings on emergency core cooling, the AEC staff stated: "The safety goal, therefore, is the prevention of exposure of people to this radioactivity. This goal can be achieved with a high degree of assurance, although not perfectly [emphasis added], by use of the concept of defense in depth...The three separate lines of the defense in depth provided for power reactors are considered appropriate to reduce to an acceptable value the probability and potential consequences of radioactive releases." (Reference 3)

Although the approaches of defense in depth and safety margins have served the industry well from the safety perspective, they were intended to be conservative and, as implemented today, they impose a heavy regulatory burden. The level of safety was not quantified. The first call for a more rational approach to regulation based on improved understanding of risk came in 1967 from F. Reginald Farmer (Reference 4) of the United Kingdom Atomic Energy Authority. The Reactor Safety Study (WASH-1400) (Reference 5) soon followed in 1975. Not surprisingly, the WASH-1400 study itself proved to be conservative in some areas, e.g., the analysis of the containment, and nonconservative in others, e.g., the analysis



of earthquakes and fires. There has been tremendous progress in our understanding of the risks from nuclear power plants since that study (a history of PRA developments since WASH-1400 is given in Reference 6).

Realizing that the availability of risk numbers made it possible to reexamine the question of how safe is safe enough, the Commission issued the safety goal policy in 1986 (Reference 7). The recognition that uncertainties had to be dealt with is reflected in the following three statements from the policy statement:

Statement I: "It is the Commission's intent that the risks from all the various initiating mechanisms be taken into account to the best of the capability of current evaluation techniques."

Statement II: "To the extent practicable, the Commission intends to ensure that the quantitative techniques used for regulatory decisionmaking take into account the potential uncertainties that exist so that an estimate can be made on the confidence level to be ascribed to the quantitative results."

Statement III: "The Commission has adopted the use of mean estimates for the purposes of implementing the quantitative objectives of this safety goal policy...."

The Commission's safety goals were derived from societal considerations, i.e., independent of the PRA state of the art. Even though they were expressed both qualitatively and quantitatively, it was clear that the Commission did not intend to simply compare a PRA "point estimate" (however it was defined) with the numerical goals.

#### The Issue

As noted above, the numerical estimates that PRAs produce have been scrutinized to an extraordinary degree since the early days of WASH-1400. Sometimes the debate regarding the accuracy of these numbers detracts from the intended use of PRA.

It is not the intent to regulate on the basis of risk estimates alone (thus, "risk-informed" regulation). The objective is to gain enough confidence in the numerical probabilities of a set of accident scenarios so that the traditional approaches (defense in depth and safety margins) that have already been applied to this set can be better managed. This means either relaxing some existing requirements, if proven burdensome and non-contributing to risk reduction, or adding new requirements, if the traditional approaches have not covered some detrimental events.

The preceding discussion suggests that the question regarding the quality of PRA results ought not to be an absolute one, but, rather, a comparative one. Therefore, we offer the following observation:

#### Observation 1:

When PRA results and insights are proposed to be used in the regulatory process, the question to be asked should be: To what degree is there confidence that the use of PRA results and insights will improve on the existing regulatory system for the problem of interest?

The words "PRA results and insights" include the set of dominant scenarios to risk (or core damage, as the case may be), as well as an assessment of the uncertainties regarding the frequencies of these scenarios. The utilization of PRA results and insights depends on our confidence that their use will improve the regulations in accordance with the Commission's vision. It is definitely not a case of PRA versus the traditional approach.

In Observation 1, the key words are "will improve." There is improvement when the regulations contribute to the safe and efficient use of nuclear materials, as per the recently articulated vision of the Commission: "In implementation of its



mission, Nuclear Regulatory Commission actions enable the Nation to safely and efficiently use nuclear materials." (Reference 8)

#### Uncertainties

As our brief historical review has demonstrated, the uncertainties regarding off-normal events and incidents in nuclear power plants have been of concern since the early days of reactor regulation. In the early seventies, quantifying the uncertainties was synonymous with developing probability distributions for the failure rates and the frequencies of accident initiators. This explicit quantification of uncertainties posed a new problem to safety analysts. They soon discovered that the interpretation of the concept of probability was controversial among mathematicians. Several schools of thought were available, of which the frequentist and the Bayesian schools were dominant. When the nuclear debate was heating up in the mid-seventies, the analysts were reluctant to get involved in an additional controversy.

This attitude, although understandable in the context of the times, was unfortunate, because it led to confusion and the perception that uncertainty analysis was controversial and to be avoided. It also led to some circumlocutions. For example, the WASH-1400 treatment of failure rates is purely Bayesian, yet that voluminous report does not acknowledge this fact explicitly. Similarly, the NUREG-1150 studies (Reference 9) claimed to elicit "weighting factors" from the experts, rather than admit that they were eliciting probabilities. Although "officially," both frequentist and Bayesian viewpoints were equally valid, no PRA had been done using frequentist methods because it cannot be done. Industry-sponsored PRAs, however, have readily acknowledged using Bayesian methods in an explicit way (Reference 10).

It is now known that uncertainties in failure rates and other parameters appearing in PRA can be quantified via probability distributions using available generic and plant-specific data and appropriate Bayesian methods. The propagation of these distributions through the PRA logic diagrams is straightforward using standard computer packages. We believe that there is no excuse for failing to do an uncertainty analysis on the parameters of the PRA models. Therefore, we offer the following observation:

#### Observation 2:

The Bayesian interpretation of probability provides the appropriate framework for PRA. Probability distributions for the parameters of PRA models, e.g., failure rates, should be developed using all available evidence and propagated to produce the probability distribution of the quantity of interest, e.g., core damage frequency (CDF) and large, early release frequency (LERF).

Since regulators must confront uncertainties, it is evident that, if PRA is to be used as in our Observation 1, the probability distributions of Observation 2 must be derived. Anything less does not represent what is actually known about these failure rates. This brings up the issue of "point estimates," for which we offer the following observation:

#### Observation 3:

The only "point estimates" that are unambiguously defined are those that are summary measures of a probability distribution; e.g., the mean value, the median value, and various percentile values.

Ill-defined "point estimates," such as "best estimates," have limited utility. Point estimates are valuable for screening purposes after a convincing case has been made that the uncertainties have been handled appropriately, e.g., they are either negligible or have been bounded. In fact, the use of such point values is an important tool in screening the thousands of minimal cut sets that a PRA produces. Such use, however, should be followed by a rigorous uncertainty analysis of the dominant sequences.



The uncertainties of interest in reactor regulation have been termed "state-of-knowledge" uncertainties (Reference 11) or, more recently, "epistemic" uncertainties (References 12, 13). The parameter uncertainties that are referred to in Observation 2 are only a part of the total epistemic uncertainties. Uncertainties resulting from model assumptions and approximations are also epistemic and more difficult to quantify. Examples would include models used for evaluating severe accident phenomena in Level II PRAs.

Model uncertainty is the key to any use of PRA results. When events or processes are modeled poorly or not at all, there is uncertainty that has not been quantified, in the sense that it is not part of the probability distributions produced by propagating parameter uncertainties. The fact that uncertainty is not quantified does not mean, however, that nothing is known about it. The PRA structure provides a good framework within which these uncertainties can be assessed qualitatively through sensitivity analyses or other means (see, for example, Reference 14). These uncertainties exist independently of whether or not they are quantified in PRAs. Recalling Observation 1, use of PRA insights must include a qualitative description of unquantified uncertainties, in addition to those that have been quantified. Any PRA-based argument for easing the regulatory requirements of the traditional approach is weakened when the unquantified uncertainties are very large and pertinent to the application. Therefore, we offer the following observation:

Observation 4:

Regulatory decisions must be made in the light of all the relevant uncertainties. These include the uncertainties quantified in PRAs, as well as significant unquantified uncertainties. Although "point" values, defined as in Observation 3, can be useful for screening purposes, they are summary measures of the probability distributions and should not be the sole basis for decisionmaking.

The deliberation on uncertainties that we are recommending is best accomplished by considering the scenarios that dominate the event of interest. The set of dominant scenarios is one of the most important results of PRA and has been proven to be very useful in risk management (Reference 15). A discussion of the overall uncertainties without a discussion of the sources of uncertainties is of limited value. Thus, we offer the following observation:

Observation 5:

The dominant scenarios should be an integral part of the deliberation on uncertainties.

The regulatory decisions of immediate interest are those related to requests for changes in the current licensing basis (CLB). In discussing uncertainties, it is important to consider possible benefits of the proposed change. For example, a change that reduces the regulatory burden in certain areas could allow the reallocation of resources to more risk significant issues and activities. Therefore, we offer the following observation:

Observation 6:

The unquantified uncertainties associated with a proposed change in the CLB should include the possible beneficial impact of the proposed change on plant safety.

Finally, we note that the decisionmaking process described in Regulatory Guide 1.174 treats uncertainties and point values in a manner consistent with our recommendations as discussed in our report dated December 11, 1997. (Reference 16)



Sincerely,

/s/

R. L. Seale  
Chairman

References:

1. Staff Requirements Memorandum dated May 27, 1997, from John C. Hoyle, Secretary of the Commission, to John T. Larkins, ACRS, Subject: Meeting with Advisory Committee on Reactor Safeguards on Friday, May 2, 1997.
2. Letter dated March 14, 1956, from Willard F. Libby, Acting Chairman of the Atomic Energy Commission, to Senator B. Hickenlooper, Joint Committee on Atomic Energy, reproduced in: D. Okrent, Nuclear Reactor Safety, The University of Wisconsin Press, Madison, 1981.
3. Testimony of the AEC Regulatory Staff at a Public Rulemaking Hearing on Interim Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Reactors on January 27, 1972, Issued December 28, 1971, U. S. Atomic Energy Commission.
4. F. Reginald Farmer, "Reactor Safety and Siting: A Proposed Risk Criterion," Nuclear Safety, Vol. 8, No. 6, pp. 539-548, Nov.-Dec. 1967.
5. U. S. Nuclear Regulatory Commission, NUREG-75/014, "Reactor Safety Study, An Assessment of Accident Risks in U.S. Nuclear Power Plants, WASH-1400," October 1975.
6. Eric S. Beckjord, Mark C. Cunningham, and Joseph A. Murphy, "Probabilistic Safety Assessment Development in the United States 1972-1990," Reliability Engineering and System Safety, Vol. 39, pp. 159-170, 1993.
7. U. S. Nuclear Regulatory Commission, "Safety Goals for the Operation of Nuclear Power Plants: Policy Statement," Federal Register, Vol. 51, p. 30028, August 21, 1986.
8. U.S. Nuclear Regulatory Commission, "Strategic Plan: Fiscal Year 1997 - Fiscal Year 2000," September 1997.
9. U. S. Nuclear Regulatory Commission, NUREG-1150, "Severe Accident Risks: An Assessment for Five US Nuclear Power Plants," December 1990.
10. Pickard, Lowe, and Garrick, Inc., Westinghouse Electric Corporation, and Fauske & Associates, Inc., "Zion Probabilistic Safety Study," Report prepared for Commonwealth Edison Company, Chicago, 1981.
11. Stanley Kaplan and B. John Garrick, "On the Quantitative Definition of Risk," Risk Analysis, Vol. 1, No. 1, pp. 11-28, March 1981.
12. George E. Apostolakis, "A Commentary on Model Uncertainty," in U. S. Nuclear Regulatory Commission, NUREG/CP-0138, Proceedings of Workshop I in Advanced Topics in Risk and Reliability Analysis: Model Uncertainty, Its Characterization and Quantification, October 20-22, 1993.
13. Gareth W. Parry, "The Characterization of Uncertainty in Probabilistic Risk Assessments of Complex Systems," Reliability Engineering and System Safety, Vol. 54, pp. 119-126, 1996.
14. Dennis Bley, Stanley Kaplan, and David Johnson, "The Strengths and Limitations of PSA: Where We Stand," Reliability Engineering and System Safety, Vol. 38, pp. 3-26, 1992.
15. Mardyros Kazarians, Nathan Siu, and George Apostolakis, "Risk Management Application of Fire Risk Analysis," Proceedings of the First International



Symposium on Fire Safety Science, pp. 1029-1038, C.E. Grant and P.J. Pagni, Editors, Hemisphere Publishing Corporation, New York, 1986.

16. Report dated December 11, 1997, from R. L. Seale, Chairman, ACRS, to Shirley Ann Jackson, Chairman, NRC, Subject: "Proposed Final Regulatory Guide 1.174 and Standard Review Plan Chapter 19 for Risk-Informed Performance-Based Regulation"



# NRC INSPECTION MANUAL

OTSB

---

PART 9900: TECHNICAL GUIDANCE

---

STS30DEG.TG

## RESOLUTION OF DEGRADED AND NONCONFORMING CONDITIONS

Issue Date: 10/08/97

9900 Degraded Conditions



RESOLUTION OF  
DEGRADED AND NONCONFORMING CONDITIONS

Table of Contents

	<u>Page</u>
1.0 P U R P O S E A N D SCOPE.....	1
2.0 DEFINITIONS.....	1
2.1 C u r r e n t L i c e n s i n g Basis.....	1
2.2 D e s i g n Basis.....	2
2.3 D e g r a d e d Condition.....	2
2.4 N o n c o n f o r m i n g Condition.....	2
2.5 F u l l Qualification.....	2
3.0 BACKGROUND.....	2
4.0 D I S C U S S I O N O F N O T A B L E PROVISIONS.....	4
4.1 P u b l i c H e a l t h a n d Safety.....	4
4.2 O p e r a b i l i t y Determinations.....	4
4.3 The Current Licensing Basis and 1 0 C F R 5 0 A p p e n d i x B.....	4
4.4 Discovery of an Existing But Previously U n a n a l y z e d C o n d i t i o n o r Accident.....	4
4.5 Justification for Continued Operation (JCO).....	4
4.5.1 Background.....	4



4.5.2	J	C	O
	Definition.....		
	.....4		
4.5.3	Items	for	Consideration
	JCO.....		in a
			5
4.5.4	Discussion	of	Industry-Type
	JCOs.....		5
4.6	R e a s o n a b l e	A s s u r a n c e	o f
	Safety.....		5
4.7	E v a l u a t i o n	o f	C o m p e n s a t o r y
	Measures.....		6
4.8	F i n a l	C o r r e c t i v e	
	Action.....		7
REFERENCE.....			
	.....8		



RESOLUTION OF  
DEGRADED AND NONCONFORMING CONDITIONS

1.0 PURPOSE AND SCOPE

To provide guidance to NRC inspectors on resolution of degraded and nonconforming conditions affecting the following systems, structures, or components (SSCs):

- (i) Safety-related SSCs, which are those relied upon to remain functional during and following design basis events (A) to ensure the integrity of the reactor coolant pressure boundary, (B) to ensure the capability to shut down the reactor and maintain it in a safe shutdown condition, or (C) to ensure the capability to prevent or mitigate the consequences of accidents that could result in potential offsite consequences comparable to the 10 CFR Part 100 guidelines. Design basis events are defined the same as in 10 CFR 50.49(b)(1).
- (ii) All SSCs whose failure could prevent satisfactory accomplishment of any of the required functions identified in (i) A, B, and C.
- (iii) All SSCs relied on in the safety analyses or plant evaluations that are a part of the plant's current licensing basis. Such analyses and evaluations include those submitted to support license amendment requests, exemption requests, or relief requests, and those submitted to demonstrate compliance with the Commission's regulations such as fire protection (10 CFR 50.48), environmental qualification (10 CFR 50.49), pressurized thermal shock (10 CFR 50.61), anticipated transients without scram (10 CFR 50.62), and station blackout (10 CFR 50.63).
- (iv) Any SSCs subject to 10 CFR Part 50, Appendix B.
- (v) Any SSCs subject to 10 CFR Part 50, Appendix A, Criterion 1.
- (vi) Any SSCs explicitly subject to facility Technical Specifications (TS).
- (vii) Any SSCs subject to facility TS through the definition of operability (i.e., support SSCs outside TS).
- (viii) Any SSCs described in the FSAR.

This guidance is directed toward NRC inspectors that are reviewing actions of licensees that hold an operating license. Although this guidance generally reflects existing staff practices, application on specific plants may constitute a backfit. Consequently, significant differences in licensee practices should be discussed with NRC management to ensure that the guidance is applied in a reasonable and consistent manner for all licensees.



## 2.0 DEFINITIONS:

### 2.1 Current Licensing Basis

Current licensing basis (CLB) is the set of NRC requirements applicable to a specific plant, and a licensee's written commitments for assuring compliance with and operation within applicable NRC requirements and the plant-specific design basis (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect. The CLB includes the NRC regulations contained in 10 CFR Parts 2, 19, 20, 21, 30, 40, 50, 51, 55, 72, 73, 100 and appendices thereto; orders; license conditions; exemptions, and Technical Specifications (TS). It also includes the plant-specific design basis information defined in 10 CFR 50.2 as documented in the most recent Final Safety Analysis Report (FSAR) as required by 10 CFR 50.71 and the licensee's commitments remaining in effect that were made in docketed licensing correspondence such as licensee responses to NRC bulletins, generic letters, and enforcement actions, as well as licensee commitments documented in NRC safety evaluations or licensee event reports.

### 2.2 Design Basis

Design basis is that body of plant-specific design bases information defined by 10 CFR 50.2.

### 2.3 Degraded Condition

A condition of an SSC in which there has been any loss of quality or functional capability.

### 2.4 Nonconforming Condition

A condition of an SSC in which there is failure to meet requirements or licensee commitments. Some examples of nonconforming conditions include the following:

1. There is failure to conform to one or more applicable codes or standards specified in the FSAR.
2. As-built equipment, or as-modified equipment, does not meet FSAR descriptions.
3. Operating experience or engineering reviews demonstrate a design inadequacy.
4. Documentation required by NRC requirements such as 10 CFR 50.49 is not available or deficient.

### 2.5 Full Qualification

Full qualification constitutes conforming to all aspects of the current licensing basis, including codes and standards, design criteria, and commitments.



### 3.0 BACKGROUND

A nuclear power plant's SSCs are designed to meet NRC requirements, satisfy the current licensing basis, and conform to specified codes and standards. For degraded or nonconforming conditions of these SSCs, the licensee may be required to take actions required by the Technical Specifications (TS). The provisions of Title 10 of the Code of Federal Regulations (10 CFR), Part 50, Appendix B, Criteria XVI, may apply requiring the licensee to identify promptly and correct conditions adverse to safety or quality. Reporting may be required in accordance with Sections 50.72, 50.73, and 50.9(b) of 10 CFR Part 50, 10 CFR Part 21, and the Technical Specifications (TS). Collectively, these requirements may be viewed as a process for licensees to develop a basis to continue operation or to place the plant in a safe condition, and to take prompt corrective action. Changes to the facility in accordance with 10 CFR 50.59 may be made as part of the corrective action required by Appendix B. The process displayed by means of the attached chart titled, "Resolution of Degraded and Nonconforming Conditions," recognizes these and other provisions that a licensee may follow to restore or establish acceptable conditions. These provisions are success paths that enable licensees to continue safe operation of their facilities.

### 4.0 DISCUSSION OF NOTABLE PROVISIONS

#### 4.1 Public Health and Safety

All success paths, whether specifically stated or not, are first directed to ensuring public health and safety and second to restoring the systems, structures, or components (SSCs) to the current licensing basis of the plant as an acceptable level of safety. Identification of a degraded or nonconforming condition that may pose an immediate threat to the public health and safety requires the plant to be placed in a safe condition.

Technical Specifications (TS) address the safety systems and provide Limiting Conditions for Operation (LCOs) and Allowed Outage Times (AOTs) required to ensure public health and safety.

#### 4.2 Operability Determinations

For guidance on operability see the Inspection Manual, Part 9900, "OPERABLE/OPERABILITY: ENSURING THE FUNCTIONAL CAPABILITY OF A SYSTEM OR COMPONENT," and see the Inspection Manual, Part 9900, "STANDARD TECHNICAL SPECIFICATIONS STS SECTION 1, OPERABILITY."

#### 4.3 The Current Licensing Basis and 10 CFR 50, Appendix B

The design and operation of a nuclear plant is to be consistent with the current licensing basis. Whenever degraded or nonconforming conditions of SSCs subject to Appendix B are identified, Appendix B requires prompt corrective action to correct or resolve the condition. The licensee must establish a time frame for completion of corrective action. The timeliness of this corrective action should be commensurate with the safety significance of the issue.



The time frame governing corrective action begins with the discovery of the condition, not with the time when it is reported to the NRC. In determining whether the licensee is making reasonable efforts to complete corrective action promptly, NRC will consider whether corrective action was taken at the first opportunity, as determined by safety significance (effects on operability, significance of degradation) and by what is necessary to implement the corrective action. Factors that might be included are the amount of time required for design, review, approval, or procurement of the repair/modification; availability of specialized equipment to perform the repair; or the need to be in a hot or cold shutdown to implement the actions. The NRC expects time frames longer than the next refueling outage to be explicitly justified by the licensee as part of the deficiency tracking documentation. If the licensee does not resolve the degraded or nonconforming condition at the first available opportunity or does not appropriately justify a longer completion schedule, the staff would conclude that corrective action has not been timely and would consider taking enforcement action.

#### 4.4 Discovery of an Existing But Previously Unanalyzed Condition or Accident

In the course of its activities, the licensee may discover a previously unanalyzed condition or accident. Upon discovery of an existing but previously unanalyzed condition that significantly compromises plant safety, the licensee shall report that condition in accordance with 10 CFR 50.72 and 50.73, and put the plant in a safe condition.

For a previously unanalyzed condition or accident that is considered a significant safety concern, but is not part of the design basis, the licensee may subsequently be required to take additional action after consideration of backfit issues (see Section 50.109(a)(5)).

#### 4.5 Justification for Continued Operation (JCO)

##### 4.5.1 Background

The license authorizes the licensee to operate the plant in accordance with the regulations, license conditions and the TS. If an SSC is degraded or nonconforming but operable, the license establishes an acceptable basis to continue to operate and the licensee does not need to take any further actions. The licensee must, however, promptly identify and correct the condition adverse to safety or quality in accordance with 10 CFR Part 50, Appendix B, Criterion XVI.

The basis for this authority to continue to operate arises because the TS contain the specific characteristics and conditions of operation necessary to obviate the possibility of an abnormal situation or event giving rise to an immediate threat to public health and safety. Thus, if the TS are satisfied, and required equipment is operable, and the licensee is correcting the degraded



or nonconforming condition in a timely manner, continued plant operation does not pose an undue risk to public health and safety.

Under certain defined and limited circumstances, the licensee may find that strict compliance with the TS would cause an unnecessary plant action not in the best interest of public health and safety. NRC review and action is required prior to the licensee taking actions that are contrary to compliance with the license conditions or TS unless an emergency situation is present such that 10 CFR 50.54(x) and (y) is applied. A JCO, as defined herein for general NRC purposes, is the licensee's technical basis for requesting NRC responses to such action.

#### 4.5.2 JCO Definition

A Justification for Continued Operation<sup>1</sup> (JCO) is the licensee's technical basis for requesting authorization to operate in a manner that is prohibited (e.g., outside TS or license) absent such authorization. The preparation of JCOs does not constitute authorization to continue operation.

#### 4.5.3 Items for Consideration in a JCO

Some items which are appropriate for consideration in a licensee's development of a JCO include:

- o Availability of redundant or backup equipment
- o Compensatory measures including limited administrative controls
- o Safety function and events protected against
- o Conservatism and margins, and
- o Probability of needing the safety function.
- o PRA or Individual Plant Evaluation (IPE) results that determine how operating the facility in the manner proposed in the JCO will impact the core damage frequency.

#### 4.5.4 Discussion of Industry-Type JCOs

Currently, some licensees refer to two other documents or processes as JCOs that are not equivalent to and do not perform the same function as the NRC-recognized JCO (as defined in 4.5.2). This is an acceptable industry practice and to the extent the industry JCO fulfills other NRC requirements, the JCOs will be selectively reviewed and audited accordingly.

---

<sup>1</sup> Regulations, generic letters, and bulletins may provide direction on specific issue JCOs, which do not require that they be submitted. Licensees may also use the JCO for situations other than for operating in a prohibited manner. The JCO term has been used in Generic Letters 88-07 on Environmental Qualifications of Electrical Equipment and 87-02 on Seismic Adequacy. Licensees should continue to follow earlier guidance regarding the preparation of JCOs on specific issues.



In the first industry-type JCO, the licensee may consider the entire process depicted in the attached chart as a single JCO that includes such things as the basis for operability, PRA, corrective action elements, and alternative operations.

In the second industry-type JCO, the licensee may consider the documentation that is developed to support facility operation after the operability decision has been made as a JCO. This documentation can cover any or all of the items listed under "Interim Operation" on the attached chart.

Although the "JCO" is used differently by some licensees, the NRC concern is that the operability decision is correct, documentation of licensee's actions are appropriate, and submittals to the NRC are complete. The licensee's documentation of the JCO's is normally proceduralized through the existing plant record system, which is auditable.

#### 4.6 Reasonable Assurance of Safety

For SSCs that are not expressly subject to TS and that are determined to be inoperable, the licensee should assess the reasonable assurance of safety. If the assessment is successful, then the facility may continue to operate while prompt corrective action is taken. Items to be considered for such an assessment include the following:

- o Availability of redundant or backup equipment
- o Compensatory measures including limited administrative controls
- o Safety function and events protected against
- o Conservatism and margins, and
- o Probability of needing the safety function.
- o PRA or Individual Plant Evaluation (IPE) results that determine how operating the facility in the manner proposed in the JCO will impact the core damage frequency.

#### 4.7 Evaluation of Compensatory Measures

In its evaluation of the impact of a degraded or nonconforming condition on plant operation and on operability of SSCs, a licensee may decide to implement a compensatory measure as an interim step to restore operability or to otherwise enhance the capability of SSCs until the final corrective action is complete. Reliance on a compensatory measure for operability should be an important consideration in establishing the "reasonable time frame" to complete the corrective action process. NRC would normally expect that conditions that require interim compensatory measures to demonstrate operability would be resolved more promptly than conditions that are not dependent on compensatory measures to show operability, because such reliance suggests a greater degree of degradation. Similarly, if an operability determination is based



upon operator action, NRC would expect the nonconforming condition to be resolved expeditiously.

On July 21, 1997, the Nuclear Energy Institute (NEI) submitted to the NRC a guidance document, NEI 96-07 [Final Draft], "Guidelines for 10 CFR 50.59 Safety Evaluations." Part of this guidance relates to applicability of 10 CFR 50.59 to degraded and nonconforming conditions. With respect to the use of compensatory measures, the guidance states:

- If an interim compensatory action is taken to address the condition and involves a procedure change or temporary modification, a 10 CFR 50.59 review should be conducted and may result in a safety evaluation. The intent is to determine whether the compensatory action itself (not the degraded condition) impacts other aspects of the facility described in the SAR.

The staff concludes that this is an acceptable approach for dealing with compensatory actions within the context of a corrective action process.

In considering whether a compensatory measure may affect other aspects of the facility, a licensee should pay particular attention to ancillary aspects of the compensatory measure that may result from actions taken to directly compensate for the degraded condition. As an example, suppose a licensee plans to close a valve to isolate a leak. Although that action would temporarily resolve the leak, it has the potential to affect flow distribution to other components or systems, may complicate required operator responses, or could have other effects that should be evaluated before the compensatory measures are implemented. In accordance with 10 CFR 50.59, should the evaluation determine that implementation of the compensatory action itself would involve a TS change or an unreviewed safety question (USQ), NRC approval, in accordance with 10 CFR 50.90 and 50.92, is required prior to implementation of the compensatory action.

#### 4.8 Final Corrective Action

The responsibility for corrective action rests squarely on the licensee. A licensee's range of corrective action could include (1) full restoration to the SAR-described condition, (2) NRC approval for a change to its licensing basis to accept the as-found condition as is, or (3) some modification of the facility other than restoration to the original FSAR condition. If corrective action is taken so that the degraded or nonconforming condition is restored to its original configuration, no 10 CFR 50.59 evaluation is required. The 10 CFR 50.59 process is entered when the final resolution to the degraded or nonconforming condition is to be different than the established FSAR requirement. At this point, the licensee is planning (in a prospective sense) to make a change to



the facility or procedures as described in the SAR. The proposed change is now subject to the evaluation process established by 10 CFR 50.59. A change can be safe, but can still require NRC approval. The proposed final resolution can be under staff review and not affect the continued operation of the plant, because interim operation is being governed by the processes of the operability determination and corrective action of Appendix B.

In two situations, the identification of a final resolution or final corrective action would trigger a 10 CFR 50.59 evaluation, unless another regulation applies (i.e., 10 CFR 50.55a): (1) when a licensee decides to change its facility or procedures to something other than full restoration to the FSAR-described condition, as the final corrective action, or (2) when a licensee decides to change its licensing basis as described in the SAR to accept the degraded or nonconforming condition as its revised licensing basis. This guidance is consistent with the July 21, 1997, revision of NEI 96-07.

#### Change to Facility or Procedures

The first circumstance is if the licensee plans for its final resolution of the degraded or nonconforming condition to include other change(s) to the facility or procedures in order to cope with the (uncorrected, including only partially corrected) nonconforming condition. Rather than fully correcting the nonconforming condition, the licensee decides to restore capability or margin by another change. In this case, the licensee needs to evaluate the change from the SAR-described condition to the final condition in which the licensee proposes to operate its facility. If the 10 CFR 50.59 evaluation concludes that a change to the TS or a USQ is involved, a license amendment must be requested, and the corrective action process is not complete until the approval is received, or other resolution occurs.

#### Change to Current Licensing Basis

The other situation is a final resolution in which the licensee proposes to change the current licensing basis to accept the as-found nonconforming condition. In this case, the 10 CFR 50.59 evaluation is of the change from the SAR-described condition to the existing condition in which the licensee plans to remain (i.e., the licensee will exit the corrective action process by revising its licensing basis to document acceptance of the condition). If the 10 CFR 50.59 evaluation concludes that a change to the TS or a USQ is involved, a license amendment must be requested, and the corrective action process is not complete until the approval is received, or other resolution occurs. In order to resolve the degraded or nonconforming condition without restoring the affected equipment to its original design, a licensee may need to obtain an exemption from 10 CFR Part 50 in accordance with 10 CFR 50.12, or relief from a design code in accordance with 10 CFR 50.55a. The use of 10 CFR 50.59, 50.12, or 50.55a in fulfillment of Appendix B corrective action requirements does not relieve the licensee of the responsibility



to determine the root cause, to examine other affected systems, or to report the original condition, as appropriate.

In both of these situations, the need to obtain NRC approval for a change (e.g., because it involves a USQ) does not affect the licensee's authority to operate the plant. The licensee may make mode changes, restart from outages, etc., provided that necessary equipment is operable and the degraded condition is not in conflict with the TS or the license. The basis for this position was previously discussed in Section 4.5.1.

#### ENFORCEMENT

If the licensee, without good cause, does not correct the nonconformance at the first available opportunity, the staff concludes that the licensee has failed to take prompt corrective action and, thus, is in violation of 10 CFR Part 50 Appendix B (Criterion XVI).<sup>2</sup> When the NRC concludes that corrective action to implement the final resolution of the degraded or nonconforming condition is not prompt, or that the operability determination is not valid, enforcement action (Notice of Violation, orders) will be taken. Enforcement action may include restrictions on continued operation.

Implementation of complete corrective action within a reasonable time frame does not mitigate the potential for taking enforcement action for the root causes that initially created the degraded or nonconforming condition or for violations of other regulatory requirements. The nonconforming condition may have resulted from (1) earlier changes performed without a 10 CFR 50.59 evaluation or (2) inadequate reviews; or may be a *de facto* change for which the facility never met the SAR description. The staff may determine that the "change" from the FSAR-described condition to the discovered nonconforming condition involved a USQ (or a TS change), and that enforcement action is appropriate for the time frame up to time of discovery.

#### 5.0 REFERENCE

See attached charts titled, "Resolution of Degraded and Nonconforming Conditions."

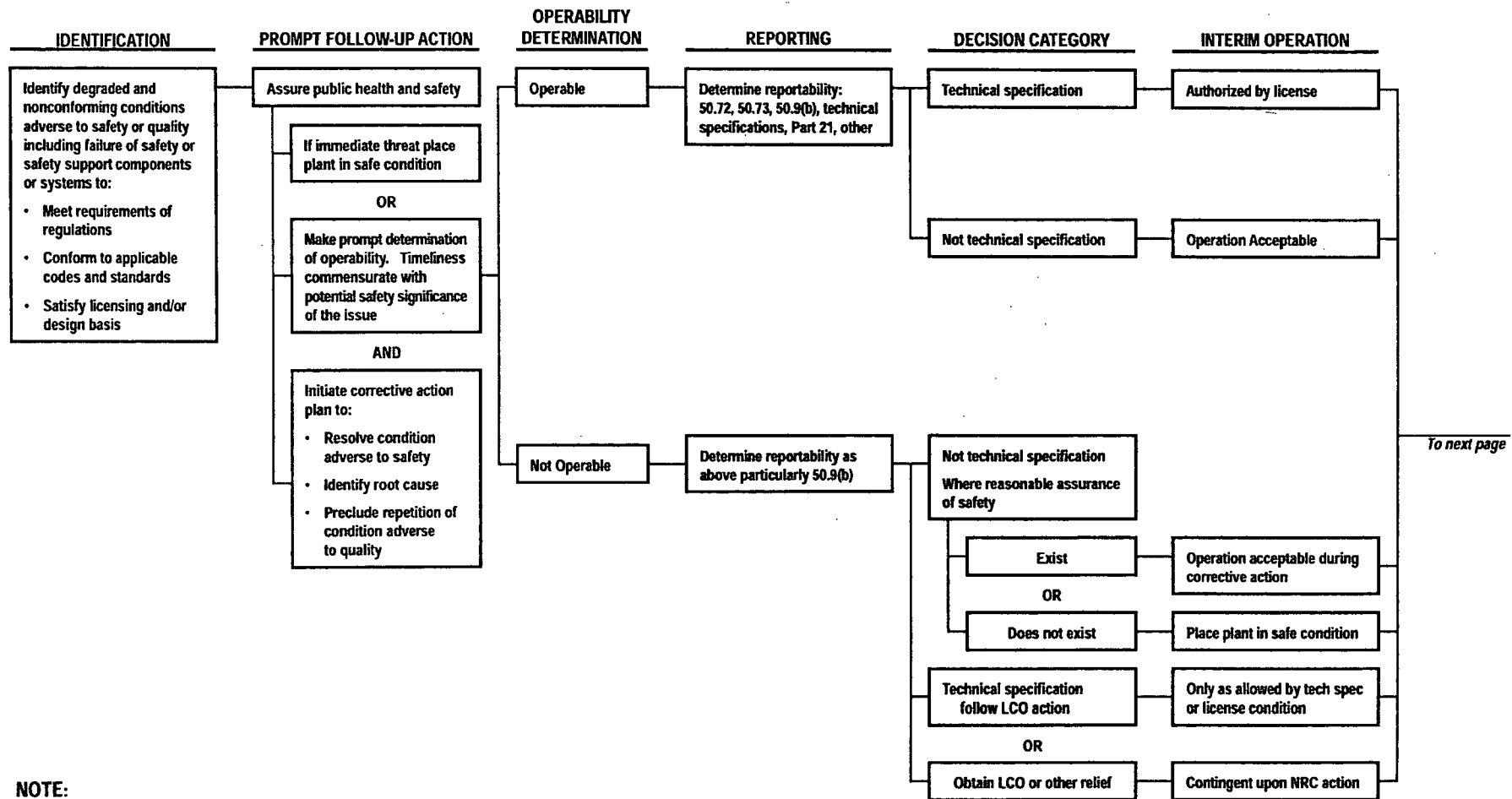
END

---

<sup>2</sup> Since Appendix B is only applicable to safety-related SSCs, this approach could not be used if the delay in resolution of a nonconforming condition from the SAR involved only non-safety-related SSCs and did not affect any safety-related SSCs. However, NRC expects licensees to take corrective action for nonconformances with the SAR consistent with Criterion XVI in a time frame commensurate with safety.



# RESOLUTION OF DEGRADED AND NONCONFORMING CONDITIONS

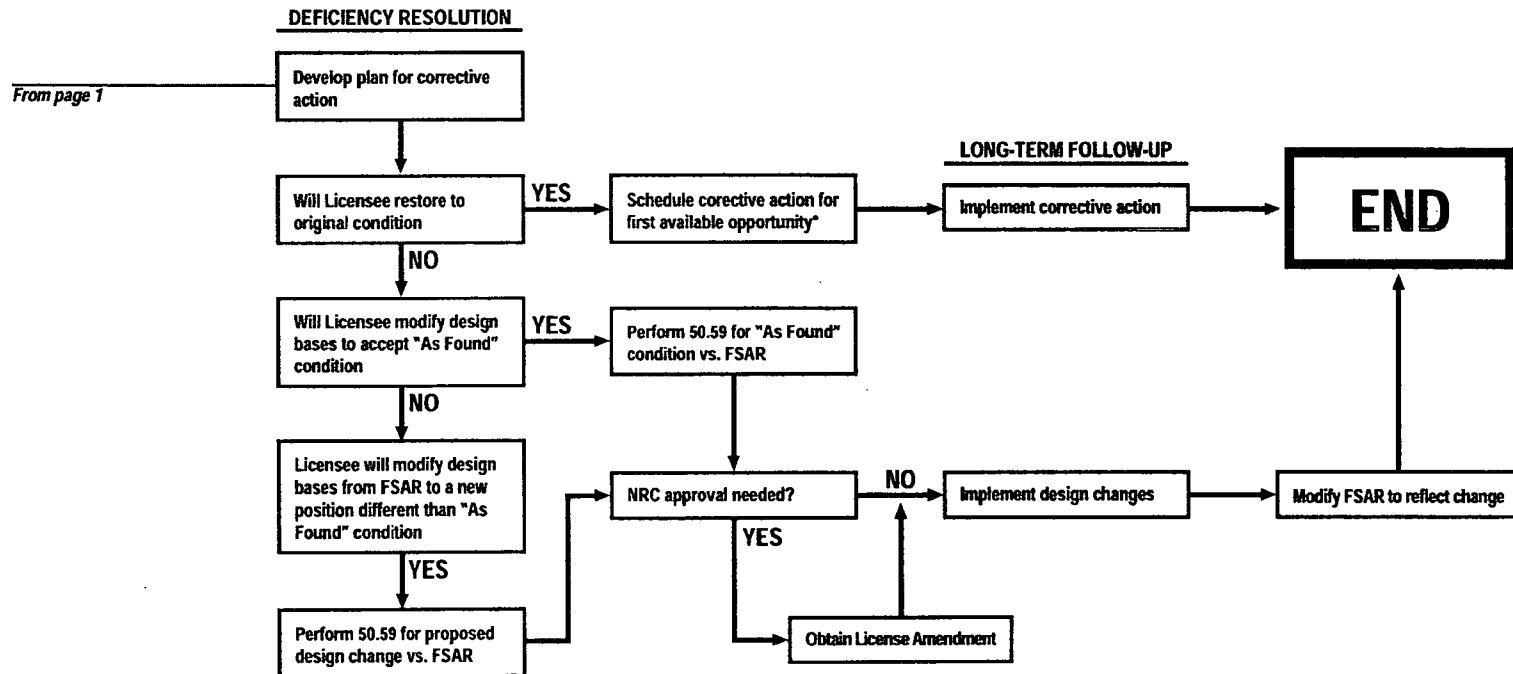


## NOTE:

Bulletins and generic letters, among others may provide guidance specific to an issue but counter to the generally accepted approach herein. Examples of deviations from the above approach include generic letter 88-07 on environmental qualification of electrical equipment and generic letter 87-02 on seismic adequacy (See use of JCO)



# RESOLUTION OF DEGRADED AND NONCONFORMING CONDITIONS



\* See section 4.3











# NRC INSPECTION MANUAL

OTSB

---

PART 9900: TECHNICAL GUIDANCE

---

STS100P.STS

OPERABLE/OPERABILITY:  
ENSURING THE FUNCTIONAL CAPABILITY OF A SYSTEM OR COMPONENT



program is implemented to restore full qualification. This is consistent with the plant TS being the controlling document for making decisions about plant operations, while 10 CFR Part 50, Appendix B, Criterion XVI, Corrective Action, is the requirement document for dealing with restoring equipment qualification.

The principle of treating the related concepts of operability and restoration of qualification separately is to ensure that the operability determination is focused on safety and is not delayed by decisions or actions necessary to plan or implement the corrective action, i.e., restoring full qualification.

#### 5.4 Determining Operability and Plant Safety is a Continuous Decision-Making Process

Licensees are obligated to ensure the continued operability of SSCs as specified by TS, or to take the remedial actions addressed in the TS. For other SSCs which may be in a degraded or nonconforming condition, it must be determined whether a condition adverse to quality exists and whether corrective actions are needed. Operability is verified, as discussed above, by day-to-day operation, plant tours, observations from the control room, surveillances, test programs, and other similar activities. Deficiencies in the design basis or safety analysis or problems identified by the operability verification lead to the operability determination process by which the specific deficiency and overall capability of the component or system are examined. The process, in one form or another, is ongoing and continuous. As a practical matter, decision making requires good information and takes time. However, the process used by licensees should call for prompt and continuous attention to deficiencies and potential system inoperabilities. In addition, the licensee's process should call for immediately declaring equipment inoperable when reasonable expectation of operability does not exist or mounting evidence suggests that the final analysis will conclude that the equipment cannot perform its specified safety function(s).

#### 5.5 Timeliness of Operability Determinations

Timeliness of operability determinations should be commensurate with the safety significance of the issue. Once the deficiency has been identified and the specific component or system has been identified, the determination can be made regarding the capability to perform the specified function(s). There is not an explicit requirement in the regulations for the timing of the decision. As discussed further in Section 6.0, timeliness is important and is determined by the safety significance of the issue. The Allowed Outage Times (AOTs) contained in TS generally provide reasonable guidelines for safety significance.

#### 5.6 Timeliness of Corrective Action

Timeliness of corrective action (i.e., the requirements in 10 CFR Part 50, Appendix B, Criterion XVI, for "prompt" corrective action) should be commensurate with the safety significance of the corrective action.



on the licensee's reasonable expectation that the SSC is operable and that the prompt determination process will support that expectation.

In the absence of reasonable expectation that the SSC is operable, the SSC is to be declared inoperable immediately. Subsequent evaluation may conclude that an SSC declared inoperable is in fact operable. The licensee's actions subsequent to declaring an SSC inoperable are guided by the regulations, TS, plant procedures, and so forth. In addition, the licensee should determine when and under what circumstances the system became inoperable so that reporting requirements may be met and NRC followup actions may properly reflect the circumstances and the licensee's efforts to correct and prevent recurrences. In summary, an SSC is either operable or inoperable at all time. "Indeterminate" is not a recognized state of operability.

## 6.9 Use of Probabilistic Risk Assessment in Operability Decisions



Probabilistic risk assessment (PRA) is a valuable tool for the relative evaluation of accident scenarios while considering, among other things, the probabilities of occurrence of accidents or external events. The definition of operability states; however, that the SSC must be capable of performing its specified function(s). The inherent assumption is that the occurrence conditions or event exists and that the safety function can be performed. The use of PRA or probabilities of the occurrence of accidents or external events is not acceptable for making operability decisions.

However, PRA may provide valid and useful supportive information for a licensee amendment. The PRA is also useful for determining the safety significance of SSCs. The safety significance, whether determined by PRA or other analyses, is a necessary factor in decisions on the appropriate "timeliness" of operability determinations. Specific guidance on the timeliness of determinations is presented in Section 5.5.

## 6.10 Environmental Qualification

When the NRC or licensee identifies a potential deficiency in the environmental qualification of equipment (i.e., a licensee does not have an adequate basis to establish qualification), the licensee is expected to make a prompt determination of operability, to take immediate steps to establish a plan with a reasonable schedule to correct the deficiency, and to write a Justification for Continued Operation (JCO) (See Note below), which will be available for NRC review. The licensee may be able to make a finding of operability using analysis and partial test data to provide reasonable assurance that the equipment will perform its safety function(s) in its accident environment when called upon to do so. The licensee should also show that subsequent failure of the equipment will not result in significant degradation of any safety function or provide misleading information to the operator.

NOTE: The JCO referred to in questions of equipment qualification is specifically addressed by Generic Letter 88-07 dated April 7, 1988. This environmental qualification "JCO" includes an operability determination. It also states that the licensee should evaluate whether the findings are reportable under 10 CFR 50.72, 10 CFR 50.73, 10 CFR Part 21, the Technical Specifications, or any other pertinent reporting requirements, including 10 CFR 50.9.

The following actions should be taken if a licensee is unable to demonstrate equipment operability:



Date: October 1, 1996

MEMORANDUM TO: Frederick Hebdon, Director

Project Directorate II-3

Division of Reactor Projects I/II

FROM: Edward J. Butcher, Chief

Probabilistic Safety Assessment Branch

Division of Systems Safety and Analysis

SUBJECT: INTERIM STAFF GUIDANCE ON THE USE OF PRA IN THE 10 CFR 50.59 PROCESS -  
FOLLOW UP ON RESPONSE TO TIA 95-013

As stated in my July 30, 1996 memorandum to you regarding the St. Lucie TIA (95-013), we have been formulating SPSB staff guidance on the use of PRA and associated methodologies in the 10 CFR 50.59 process.

Attached to this memorandum is our recently completed interim staff guidance on the subject. We have concluded that licensees should not make changes under 10 CFR 50.59 based on the numerical results of a PRA or related probabilistic analysis. The guidance addresses the rule as it currently is, and not what it "could or should" be or what it may become as a result of the recently initiated NRC staff action plan. SPSB will keep abreast of development, and participate in the implementation, of the staff action plan and update our guidance as appropriate.

If you have any questions regarding our policy on review of 10 CFR 50.59 evaluations or our interim staff guidance, please contact John O. Schiffgens at 415-1074 (E-mail: JOS).

Attachment: As stated

DISTRIBUTION

Docket File

SPSB File

LWiens

ATTACHMENT 1

THE PROBABILISTIC SAFETY ASSESSMENT BRANCH (SPSB)

INTERIM STAFF GUIDANCE

ON THE USE OF PROBABILISTIC RISK ASSESSMENT (PRA)

IN THE 10 CFR 50.59 PROCESS

A. BACKGROUND

Over the past year the Commission has expressed renewed interest in issues related to Title 10, Code of Federal Regulations, Part 50, Section 59 (10 CFR 50.59), as discussed in memorandums to the staff dated October 27 and November 30, 1995. Specifically, the staff was requested to reexamine the adequacy of the regulatory framework that authorizes licensees to make changes to their facilities



without prior approval of the NRC and to explore ways of improving the 10 CFR 50.59 process.

In response, the staff reevaluated the process and prepared an action plan to address the matters of concern, as discussed in a memorandum from James M. Taylor, Executive Director for Operations (EDO) to Shirley A. Jackson, Commission Chairman dated April 15, 1996. The action plan addresses consistency of guidance and evaluation of NRC inspection activities with the goal of identifying actions which can be undertaken to improve licensee implementation and NRC oversight of the process. The action plan objectives include staff development of guidance for improving "unreviewed safety question (USQ)" determinations by providing direction on a) the extent to which short and long term compensatory actions may be considered as part of a change under 10 CFR 50.59, b) the extent to which PRA techniques may be useful in evaluating the effects on safety of a change under 10 CFR 50.59, and c) the meaning of "margin of safety" relative to numerical parameters, methods of analysis, calculated results of safety analyses, and licensing limits.

In addition to the staff's April 15 response to the Commission, on April 9, 1996 the staff updated Part 9900: 10 CFR Guidance in the NRC Inspection Manual, "10 CFR 50.59 - Interim Guidance on the Requirements Related to Changes to Facilities, Procedures and Tests (or Experiments)." This interim guidance clarifies current staff practices with respect to 10 CFR 50.59, beyond that which is already contained in NRC Inspection Manual, Part 9900, "10 CFR 50.59 - Changes to Facilities, Procedures and Tests (or Experiments)," dated January 1, 1984. Also, recent guidance to the staff on the scope of 10 CFR 50.59 evaluations is contained in NRC Inspection Manual, Inspection Procedure (IP) 37001, "10 CFR 50.59 Safety Evaluation Program," dated December 29, 1992.

The provisions according to which a licensee may make decisions concerning the need for prior Commission approval before implementing a change in the facility or procedures described in the safety analysis report, or conducting a test, or experiment not described in the safety analysis report (i.e., before implementing a CTE) are described in 10 CFR 50.59. Specifically, the regulation states, in part, the following:

"(a)(1) The holder of a license authorizing operation of a production or utilization facility may

(i) make changes in the facility as described in the safety analysis report,

(ii) make changes in the procedures as described in the safety analysis report, and

(iii) conduct tests or experiments not described in the safety analysis report,

without prior Commission approval, unless the proposed change, test or experiment involves a change in the technical specifications incorporated in the license or an unresolved safety question.

(2) A proposed change, test, or experiment shall be deemed to involve an unreviewed safety question

(i) if the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis report may be increased; or

(ii) if a possibility for an accident or malfunction of a different type than any evaluated previously in the safety analysis report may be increased; or

(iii) if the margin of safety as defined in the basis for any technical specification is reduced." (underlining added)

The NRC has statutory responsibility for licensing and regulating nuclear facilities and materials (which includes, among other things, protecting public health and safety) and for conducting research in support of the licensing and regulatory process. Agency functions are carried out through a) standards setting and rulemaking, b) technical reviews and studies, c) conduct of public hearings, d) issuance of authorizations, permits, and licenses, e) inspection, investigation and enforcement, f) evaluation of operating experience, and g) confirmatory research. These functions are directed toward defining what is



necessary to protect public health and safety (i.e., appropriate goals and criteria for safe design, maintenance, and operation of nuclear facilities and use of nuclear materials) and determining what practices are "safe enough" (i.e., satisfy established safety goals and criteria). With regard to 10 CFR 50.59, NRC oversight of licensee use of the provisions of the rule is accomplished by inspection of CTEs and technical review (or audit) of "50.59 safety evaluations" which document the bases for the determination that a CTE does not involve an unreviewed safety question.

The Licensee, on the other hand, has responsibility for proposing and implementing the safe design of - and safe maintenance and operation practices for - its facilities, as well as for satisfying NRC regulations and requirements. The NRC encourages licensees to look beyond the regulations in evaluating the safety of its facilities and operating practices. Hence, licensees are encouraged to develop and implement plant-specific and industry guidelines, to the extent that, at the same time, the guidelines are consistent with NRC regulations and requirements. When appropriate, NRC may endorse industry guidelines as an acceptable method of complying with a particular regulation.

A joint NUMARC/NSAC working group developed a 10 CFR 50.59 guidance document, NSAC-125. Although NSAC-125 may be of some value in performing a 10 CFR 50.59 evaluation, caution must be exercised in its use since, due to its misinterpretation of parts of the rule, it has not been endorsed by the staff. In this regard, it is important to note that the provisions of the rule (which must be satisfied in order to implement CTEs without prior Commission approval) are not concerned, for example, with the magnitude of an increase in the probability of occurrence or the consequences of an accident or with the magnitude of the reduction in safety margin but, rather, with whether the probability of occurrence or the consequences may increase or whether the safety margin is reduced.

## B. OBJECTIVE

The objective of this document is to put forth and discuss interim guidance developed by the Probabilistic Safety Assessment Branch (SPSB) concerning interpretation of a specific rule, 10 CFR 50.59, and the role of a particular technology, probabilistic risk assessment (PRA) and associated methodologies, in satisfying the provisions of the rule. The guidance addresses the rule as it currently is, and not what it "could or should" be or what it may become as a result of the NRC staff action plan. SPSB will keep abreast of development, and participate in the implementation, of the staff action plan and update this guidance as appropriate.

## C. DISCUSSION

### The Rule

Any discussion of 10 CFR 50.59 must begin with the recognition that the implicit premise of the rule is that by satisfying its provisions a licensee's CTE is by definition "safe," hence, no safety analysis needs to be submitted to the NRC for approval and no safety evaluation by the NRC staff is necessary. Consequently, the language of the rule, as well as its intent, is critical.

#### 1. Language

The difficulty with promulgating a rule includes the choice of language to unambiguously convey the intent of the rule and the development of guidance to assure uniform compliance and

enforcement. Insights on key elements of the rule and associated terminology can be obtained from the above mentioned memorandum from EDO Taylor to Chairman Jackson, Part 9900: 10 CFR Guidance in the NRC Inspection Manual, and Inspection Procedure 37001. However, three elements of the rule which have a direct bearing on the use of PRA in the 10 CFR 50.59 process are discussed below.

#### Probability

As employed in the rule, the meaning of probability needs to be considered in the context of the licensing approach used in the time frame when 10 CFR 50.59 was promulgated and FSARs for current



plants were prepared. Until recently, estimates (with a few exceptions) of accident and equipment malfunction probability were qualitative, inferred from deterministic considerations and engineering judgement and not discussed in the FSAR. Although PRA and associated methodologies now provide a means for quantitative calculation of changes in probability associated with changes in SSC, procedures, tests or experiments, quantitative results, in general, can not be used as a basis for regulatory decisions without appropriate standards for the particular application of PRA and adequate guidance for interpretation of results (see also the discussion below under "The Use of PRA," along with other relevant considerations).

### Evaluated Previously

As used in 10 CFR 50.59, i.e., as in "probability of occurrence of an accident or malfunction of equipment previously evaluated" - and in - "possibility for an accident or malfunction of a different type than any evaluated previously," the phrase "evaluated previously" (or previously evaluated) has been historically taken to refer to "accident or malfunction of equipment" in the former as it does in the latter, and not to the "probability of occurrence." As noted above, in the past, quantitative estimates of the probability of occurrence of an accident or malfunction of equipment was generally not done. Hence, almost no such information is incorporated in an FSAR and estimates of change must either be qualitative and inferred from deterministic considerations and engineering judgement or, if quantitative, they must be from calculations with recent models of current equipment and configurations, and not from calculations incorporated in analyses "evaluated previously in the safety analysis report." With regard to the latter, however, since neither PRA nor associated methodologies were employed in the FSAR, their application to the assessment of the accident or equipment being evaluated was never reviewed and approved by the staff. Consequently, the validity of the results from such applications is questionable, making the conclusions based on them inappropriate bases for a 50.59 safety evaluation. (See also the discussion below, under "The Use of PRA.")

### 50.59 Safety Evaluation

Licensees are required to maintain records of changes in the facility and procedures and of tests and experiments carried out under the provisions of Section 10 CFR 50.59. "These records must include a written safety evaluation which provides the bases for the determination that the change, test, or experiment does not involve an unreviewed safety question." The "50.59 safety evaluation" is to be primarily a three step "screening analysis" of the possibility of an adverse safety impact associated with a CTE as opposed to a safety analysis of whether the actual impact of the CTE is acceptable from a public health and safety perspective.

The first step is to determine whether the CTE involves a structure, system, or component (SSC), or procedure described in the most recently updated FSAR submitted to the NRC in accordance with 50.71(e) and the second is to determine whether the description of the SSC or procedure would be affected by the change. If the conclusion from either step in the analysis is negative the CTE may be implemented under 10 CFR 50.59 because, as is implied by the rule, a change important to safety is not involved. If the conclusion from both steps is positive, the third step, evaluating the CTE against the USQ provisions of the rule, is necessary.

In order to implement a CTE without prior Commission approval, the product of the third step in the "screening analysis" (i.e., the written safety evaluation) must show that the CTE can not reasonably be expected to a) increase "the probability of occurrence or the consequences of an accident or malfunction of equipment ..." or b) create "a possibility for an accident or malfunction of a different type ..." or c) reduce "the margin of safety as defined in the basis for any technical specification."

Essentially, a "50.59 safety evaluation" is to determine whether a "safety analysis," requiring NRC staff review prior to implementation, is needed in order to support making the CTE.

The reference point for evaluation of the CTE is the FSAR. FSAR analyses are deterministic and based on the single failure criterion and a host of postulated events. By contrast, a typical analysis utilizing PRA or PRA associated methodologies would employ all current and documented information available



on the probability of initiating events and the availability and reliability of the facility systems, system configurations, and procedures, as needed. It is because of this approach that the most important accidents identified by PRA involve more than a single failure. 10 CFR 50.59, however, does not require consideration of accidents involving multiple failures making PRA an inappropriate tool for 50.59 safety evaluations.

## 2. Intent

Generally, NRC regulations and associated guidance specify what activities are to be considered potentially safety significant and what safety and process requirements are to be met to assure public health and safety. In the case of 10 CFR 50.59, the rule provides regulatory flexibility and reduces unnecessary burden on the NRC staff and licensees by allowing licensees to implement CTEs without first going through the NRC's public assessment and approval process. Such CTEs are to be clearly not detrimental to public health and safety (i.e., "such as to not exceed the bounds of the licensing and design basis of the facility" as described in the updated FSAR or affect the plant technical specifications). The regulation is to make non-safety significant changes less burdensome.

10 CFR 50.59 is not intended to allow potentially safety significant CTEs to be implemented based on "unreviewed safety analyses." That is, the 50.59 safety evaluation should not involve new, unreviewed analytical assumptions or methods (i.e., assumptions and methods not previously reviewed and approved by the NRC). For example, an analysis of an accident or malfunction of equipment previously evaluated with a current, commonly used computer code (i.e., one with NRC approved models and assumptions) that was not used in the "previous evaluation," would probably not constitute an unreviewed safety analysis. By contrast, a PRA analysis with plant and modification specific models and assumptions would constitute an unreviewed safety analysis.

As discussed below, under "The Use of PRA," if new, unreviewed analytical assumptions or methods are necessary to support the CTE, it is likely that the CTE involves a USQ, hence, implementation of the CTE under the provisions of 10 CFR 50.59 is questionable. In this case, either the CTE should not be implemented or, prior to implementation, an analysis to support the safety conclusion should be submitted to the NRC for staff approval according to the provisions of 10 CFR 50.90. It should be emphasized that (a) a determination that a USQ exists does not mean that the proposed CTE is "unsafe," just that it is significant and needs to be reviewed by the NRC prior to implementation, and (b) the purpose of a staff review of a 10 CFR 50.90 submittal for any licensee proposed CTE is to understand the licensee's analysis, to verify that the analysis is acceptable, and to determine whether the conclusions reached are in accordance with NRC regulations and not detrimental to public health and safety.

### The Use of PRA

Probabilistic Risk Assessment (PRA) logically and quantitatively relates the performance of parts to the performance of the whole. For example, applied to a nuclear power plant, it may be used to analyze component and system unavailabilities together with initiating event frequencies to obtain core damage frequencies.

There are at least two ways to utilize the unique features of PRA. One emphasizes the logical process for relating component unavailabilities and reliabilities in order to obtain the probabilities of system failure on demand and gain insights into their impact on core damage, radioactive release, and public health. This results in a better understanding of the plant and its potential vulnerabilities to severe accidents. The other emphasizes the "bottom-line" numerical results of PRA and focuses on changes in some measure of risk as a function of specific modifications to plant configuration, design, or procedures in support of proposed actions. The former is more exploratory (e.g., the PRA calculations incorporated in an individual plant examination, IPE) and the latter more definitive (e.g., the PRA analysis of a proposed allowed outage time change of a limiting condition for operation in a particular technical specification).

The power of PRA is that it provides an integrated perspective for evaluating the strengths and weaknesses (i.e., assessing the risk significance) of plant design, available equipment configurations, and operating procedures. In addition, PRA provides a mechanism for focusing dialog between the



licensee and the NRC staff on the most important details of issues being analyzed. In this regard, it should be noted that a) in some cases the variety of assumptions and models employed by expert analysts to describe complex systems and system interactions can yield considerably different results, and b) guidance for the appropriate use of PRA in nuclear regulation is being developed by the staff and is, in some aspects, application specific. Consequently, it is inappropriate to accept PRA results without their basis, i.e., without understanding how the results were generated. For the foreseeable future, essentially all use of PRA in regulatory applications will require NRC staff review, in particular, those applications which emphasize numerical results. Specifically, with regard to the use of PRA in the 10 CFR 50.59 process:

a) The first question is, "Can the results of PRA analyses be useful in 10 CFR 50.59 evaluations?" The rule allows licensees to implement CTEs to their facilities unless they involve a change in technical specifications or a USQ. Since PRA would have nothing to contribute to deciding whether a proposed CTE involves a change in existing technical specifications, applying PRA in 10 CFR 50.59 evaluations would be exclusively associated with USQ determinations.

The applicability of PRA to USQ criterion 50.59(a)(2)(i) hinges on the proper interpretation of this section of the rule. Provided the phrase "if the CTE may increase the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated ..." is interpreted as it historically has been, in a qualitative sense, PRA related methodologies could have limited applicability in 10 CFR 50.59 evaluations, if appropriately utilized (i.e., as discussed below).

With regard to 50.59(a)(2)(ii), the possibility that the CTE may create an accident or malfunction (of a different type than any evaluated previously in the updated FSAR) must first be determined before it can be addressed with PRA and associated methodologies. That is, the CTE must fail to satisfy this provision of the rule before PRA can be used to analyze the malfunction or accident of a different type to obtain its probability or frequency of occurrence.

With regard to 50.59(a)(2)(iii), PRA is currently outside the scope of safety margin definition methodology (which is deterministic), hence, irrelevant to 50.59(a)(2)(iii).

b) The next question then becomes, "How may PRA be utilized in making 50.59(a)(2)(i) USQ determinations?" There is a problem with utilizing PRA in the definitive or quantitative sense for such purposes (in addition to the "evaluated previously" and limited scope problems discussed in section 1 under "The Rule"). The reason being that, in a properly structured PRA, equipment, procedures, tests, and experiments that "can not" significantly contribute to risk are typically screened out of the analysis or are subsumed into "supercomponents" or subsystems for which the total probability of failure is available or is estimated without explicitly modeling all its component parts (e.g., as is done for diesel generators). Hence, quantitatively, if CTEs are specifically included in the PRA analysis, they contribute some amount (although sometimes relatively small) to the mathematical probability of failure and it can be concluded that any such CTE with a higher failure probability than existed before will "increase the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety" without performing the PRA analysis.

Although use "in the definitive or quantitative sense" may be the "natural or correct" way of utilizing PRA in a safety analysis submitted for review (i.e., in connection with a 10 CFR 50.90 submittal), a 10 CFR 50.59 written evaluation should not be such an analysis. It should be a screening analysis concerned with whether there may be an increase not with how large it may be. Therefore, for this reason, together with that presented in the previous paragraph, as well as those discussed under "The Rule" (above), the staff has concluded that it is not appropriate for a licensee to base 10 CFR 50.59 evaluations on the numerical results of a PRA analyses.

c) It may be argued, however, that utilizing PRA in an exploratory sense (i.e., to gain insights) is appropriate in screening analyses (i.e., to decide, in a more qualitative sense, on whether there is reasonable expectation of an increase in likelihood). Such calculations de-emphasize numerical results, with their associated implications of certitude, and often lead to results and safety conclusions which, once revealed, stand on their own, i.e., are relatively independent of the PRA model that revealed them



and associated plant data.

To the extent that they stand on their own, i.e., are self explanatory, insights from PRA calculations may be appropriately incorporated in 10 CFR 50.59 evaluations. The important point here is that "whether the methodology used to gain understanding or insights leading to the 10 CFR 50.59 conclusions is reviewed and approved by the staff or not" is immaterial provided the conclusions are not dependent on, or a function of, the methodology. For example, analyses with PRA methodology a) may show that the proposed CTE negatively impacts some paths leading to successful equipment or safety system performance, but positively impacts others, so that the net effect is that it is not reasonable to expect an increase in the likelihood of (i.e., there is no discernable impact on the) "occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated ..." or b) they may reveal alternate reliable means of achieving success with other minor changes in design or equipment or equipment configurations or procedures that would result in a CTE permissible under 10 CFR 50.59 (i.e., changes for which it is not reasonable to expect an increase in the likelihood of "occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated ..." or one that would actually decrease it). It may be possible to justify such conclusions without reference to the PRA analysis or its methodological details or numerical results, even though PRA analyses were used to reach them.

#### D. CONCLUSIONS

As noted above, if a new analysis involving assumptions and models not previously reviewed and approved by the staff is necessary to support a proposed CTE, implementation of the CTE under the provisions of 10 CFR 50.59 is questionable and a USQ likely exists. In this case, either the CTE should not be implemented or, prior to implementation, the analysis required to support the safety conclusion should be submitted to the staff for review according to the provisions of 10 CFR 50.90.

PRA techniques are increasingly being used to provide risk insights into the design and operation of nuclear facilities. The acceptability of PRA results depend not only on the application of the techniques (e.g., assumptions and models) and the quality of the data, but on how the results are interpreted and used in the decision making process. The acceptability of a 10 CFR 50.59 determination, were it to be based on PRA bottom-line numerical results, would likewise depend on how the PRA results were obtained and interpreted. However, if the determination is based on the logic associated with the PRA, it depends on how well the results of the analysis, and the conclusions drawn from them, are justified or substantiated by the design and operation of the plant and the proposed CTE. Furthermore, without adequate substantiation as to whether the findings and the CTE make sense, an estimated probability alone (no matter the magnitude) would lack the assurance needed to implement the CTE under 10 CFR 50.59. In fact, once the results are logically substantiated and characterized, numerical probabilistic results are of little consequence and may actually be a distraction in the decision making process. Accordingly, licensees should not make changes under 10 CFR 50.59 based on the numerical results of a PRA or related probabilistic analysis.



## Acronyms and Abbreviations

AC	Alternating current
ACRS	Advisory Committee on Reactor Safeguards
ADS	Automatic depressurization system
ADV	Atmospheric dump valve
AEOD	Office for Analysis and Evaluation of Operational Data
AFW	Auxiliary feedwater
AOP	Abnormal Operating Procedure
AOT	Allowed outage time
AOV	Air-operated valve
APB	Accident progression bin
APET	Accident progression event tree
ASEP	Accident Sequence Evaluation Program
ASP	Accident Sequence Precursor
ATHEANA	A Technique for Human Event Analysis
ATWS	Anticipated transient without scram
BC	Boundary condition
BNL	Brookhaven National Laboratory
BTP	Branch Technical Position
BWR	Boiling water reactor
BWROG	BWR Owners' Group
BWST	Borated water storage tank
CCDF	Complementary cumulative distribution function
CCDP	Conditional core damage probability
CCF	Common-cause failure
CCI	Core-concrete interaction
CDF	Core damage frequency
CDFM	Conservative Deterministic Failure Margin
CDP	Core damage probability
CE	Combustion Engineering
CEOG	Combustion Engineering Owners' Group
CFR	Code of Federal Regulations
CLB	Current licensing basis
CRD	Control rod drive
CSIP	Charging/safety injection pump
CST	Condensate storage tank
CW	Circulating water
DBA	Design basis accident
DC	Direct current
DCH	Direct containment heating
DF	Decontamination factor
DFSD	Dominant functional sequence diagram
DHR	Decay heat removal
ECCS	Emergency core-cooling system
EDG	Emergency diesel generator
EOOS	Equipment Out of Service System
EOP	Emergency Operating Procedure
EPA	Environmental Protection Agency
EPRI	Electric Power Research Institute
ESF	Engineered safeguards feature
ESW	Emergency service water
ESWGR	Emergency switchgear



ET	Event tree
FCI	Fuel-coolant interaction
FIVE	Fire-Induced Vulnerability Evaluation
FMEA	Failure modes and effects analysis
FSAR	Final Safety Analysis Report
FT	Fault tree
F-V	Fussell-Veseley (importance)
FW	Feedwater
GE	General Electric
GL	Generic Letter
HCLPF	High confidence, low probability of failure
HCR	Human Cognitive Reliability
HEP	Human error probability
HHSI	High-head safety injection
HLW	High-level waste
HPCI	High-pressure coolant injection
HPCS	High-pressure core spray
HPI	High-pressure injection
HPSI	High-pressure safety injection
HRA	Human reliability analysis
HVAC	Heating, ventilation, and air conditioning
HX	Heat exchanger
IE	Initiating event
INEEL	Idaho National Engineering and Environmental Laboratory
INPO	Institute for Nuclear Plant Operations
IPE	Individual Plant Examination
IPEEE	Individual Plant Examination for External Events
IREP	Interim Reliability Evaluation Program
ISA	Integrated Safety Analysis
ISI	In-service inspection
ISLOCA	Interfacing system loss-of-coolant accident
IST	In-service testing
JCO	Justification for Continued Operation
LCO	Limiting Condition for Operation
LER	Licensee Event Report
LERF	Large early release frequency
LLNL	Lawrence Livermore National Laboratory
LLW	Low-level waste
LOCA	Loss-of-coolant accident
LOOP	Loss of offsite power
LOSP	Loss of offsite power
LP&S	Low power and shutdown
LPCI	Low-pressure coolant injection
LPCS	Low-pressure core spray
LPI	Low-pressure injection
LPSI	Low-pressure safety injection
LPZ	Low population zone
LWR	Light water reactor
MAAP	Modular Accident Analysis Program
MACCS	MELCOR Accident Consequence Code System
MCS	Minimal cut set
MDP	Motor-driven pump
MGL	Multiple Greek letter
MOV	Motor-operated valve



MSIV	Main steam isolation valve
MSP	Maintenance and Surveillance Program
NCV	Non-cited violation
NEI	Nuclear Energy Institute
NMSS	Office of Nuclear Materials Safety and Safeguards
NOED	Notice of Enforcement Discretion
NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission
NRR	Office Nuclear Reactor Regulation
OOS	Out of service
ORAM	Outage Risk Assessment and Management
ORNL	Oak Ridge National Laboratory!cell
OSHA	Occupational Safety and Health Administration
P&ID	Piping and instrumentation diagram
PA	Performance assessment
PCC	PRA Coordinating Committee
PCS	Power conversion system
PDS	Plant damage state
PM	Preventive maintenance !tbl
PORV	Power-operated relief valve
POS	Plant operating state
PRA	Probabilistic risk assessment
PRT	Plant response tree
PSA	Probabilistic safety assessment
PSF	Performance shaping factor
PTFG	PRA Training Focus Group
PTS	Pressurized thermal shock
PWR	Pressurized water reactor
QA	Quality Assurance
QHO	Quantitative health objective
QRA	Quantitative risk analysis
RAW	Risk achievement worth
RBCCW	Reactor building closed cooling water
RCIC	Reactor core isolation cooling
RCP	Reactor coolant pump
RCS	Reactor coolant system
RES	Office of Nuclear Regulatory Research
RG	Regulatory Guide
RHR	Residual heat removal
RI	Resident Inspector
RPS	Reactor protection system
RRW	Risk reduction worth
RSS	Reactor Safety Study
RWST	Refueling water storage tank
S/D	Shutdown
SAR	Safety Analysis Report
SBO	Station blackout
SDC	Shutdown cooling
SER	Safety Evaluation Report (Staff Evaluation Report for IPE/IPEEE)
SG	Steam generator
SGTR	Steam generator tube rupture
SHARP	Systematic Human Action Reliability Procedure
SI	Safety injection
SIT	Safety injection tank



SLOCA	Small loss-of-coolant accident
SNL	Sandia National Laboratory
SRA	Senior Reactor Analyst
SRI	Senior Resident Inspector
SRP	Standard Review Plan
SRV	Safety/relief valve
SSC	Systems, structures, and components
SSET	Support state event tree
STG	Source term group
SW	Service water
SWGR	Switchgear
TBCCW	Turbine building closed cooling water
TDP	Turbine-driven pump
TER	Technical Evaluation Report
THERP	Technique for Human Error Rate Prediction
TRC	Time reliability correlation
VCT	Volume control tank
WOG	Westinghouse Owners' Group