Idaho National Laboratory

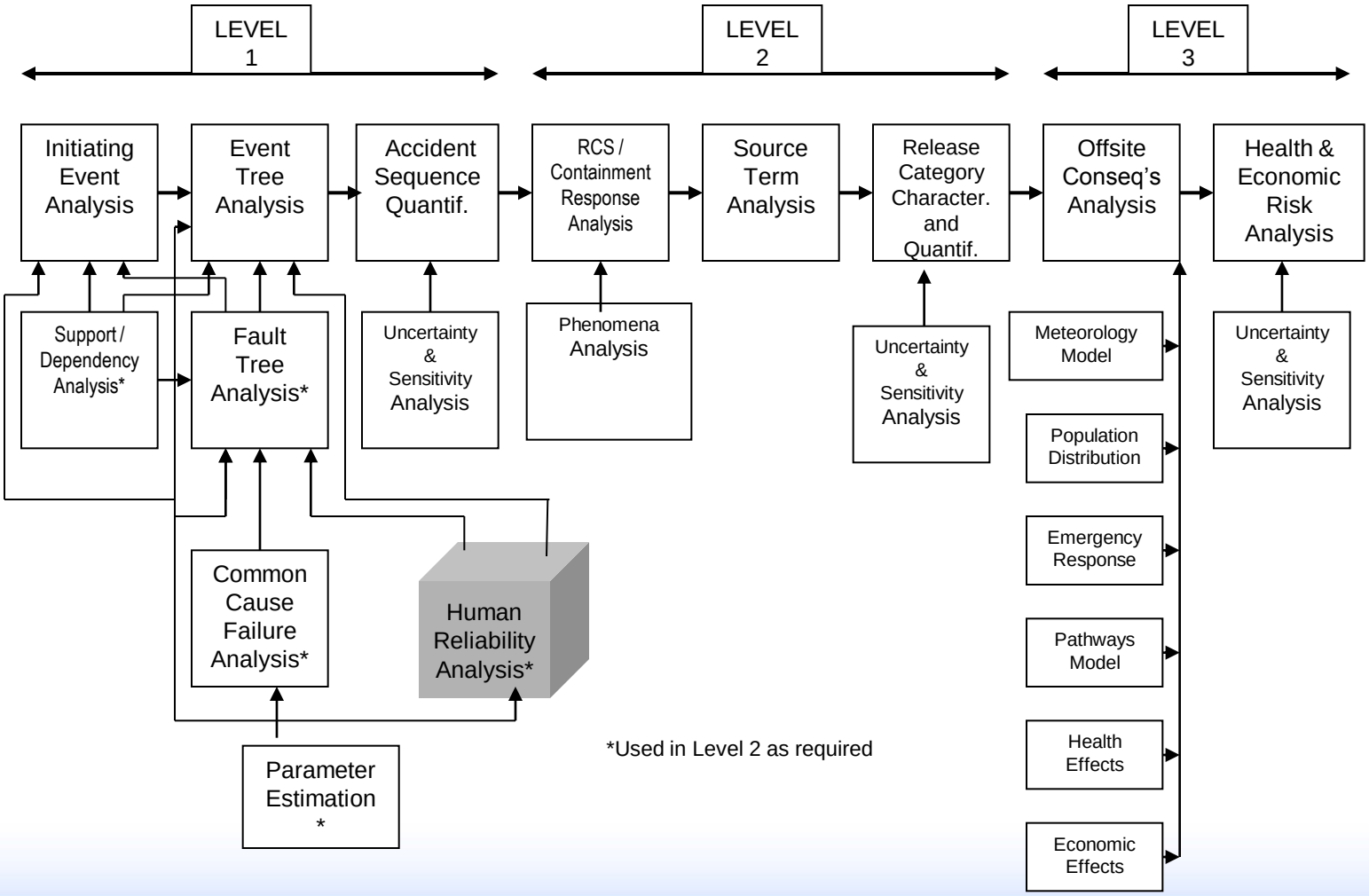
MODULE I

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-1792, HRA Good Practices, 2005**
  - **NUREG-1842, Review of HRA Methods Against Good Practices, 2006**
  - **NUREG/CR-6775, Human Performance Characterization in the Reactor Oversight Process, 2002**
  - **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)**
  - **IEEE Std. 1082-1997**
  - **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 during an accident)**

Human Reliability Analysis (HRA)

- **Starts with the basic premise that the humans are, in effect, part of the system. Thus, nuclear power plants and systems which comprise them are "human-machine systems."**
- **Identifies and quantifies the ways in which human actions contribute to the;**
  - **Initiation**
  - **Propagation**
  - **Termination of accident sequences**

"Human Reliability" is the probability that a person will:

❶ **Correctly perform some system-required activity, and**

❷ **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**
    - **Sometimes captured in equipment failure data**
  - **As a contribution or cause to initiating events**
    - **Usually implicitly included in data used to quantify initiating event frequencies**
  - **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 RCS in accordance with the EOPs)**
    - **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 informatic 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	 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

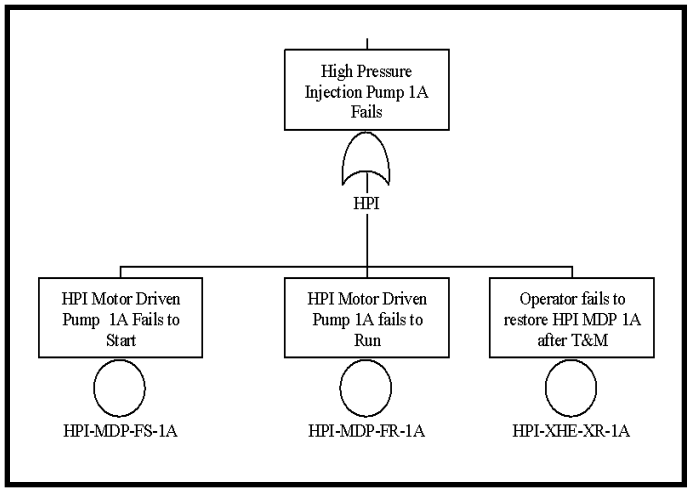
- Generally, two types of human errors are defined:
  - Errors of omission
    - Failure to perform a required action or step, e.g., failure to initiate feed-and-bleed
  - Errors of commission
    - Action performed incorrectly or wrong action performed, e.g., opening the wrong valve, turning off safety injection
- Normally only errors of omission and very simple errors of commission (slips) are modeled due to uncertainty in being able to identify errors of commission, and lack of modeling and quantification methods to address errors of commission
  - ATHEANA (A Technique for Human Error Analysis) research program is directed at errors of commission

HRA Process

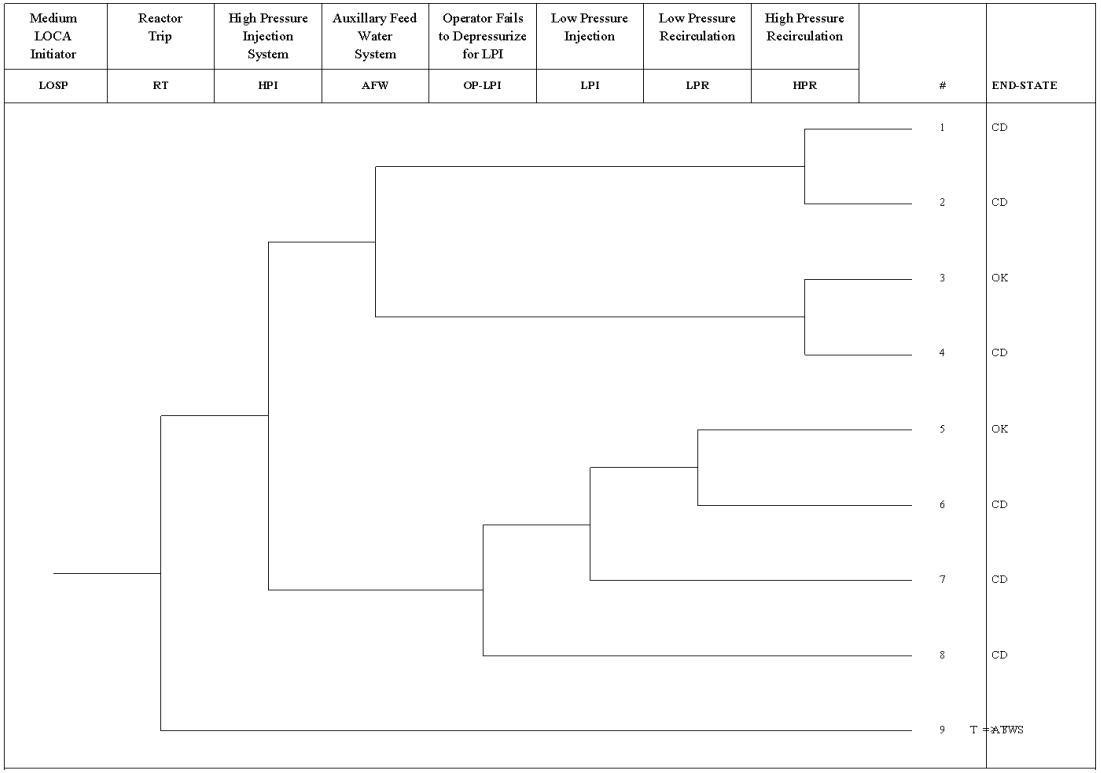
- **Identify Human Errors to be considered in plant models:**
  - **Normal Plant Ops**
    - **Identify potential errors involving miscalibration or failure to restore equipment by observing test and maintenance**
  - **Upset Conditions**
    - **Determine potential errors in manipulating equipment in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

Examples of Incorporating Human Actions Into a PRA Model:

Basic events on fault trees



Top events on event trees



Recovery actions added by applying recovery rules to minimal cut set results

```
If EPS-DGN-FS-A * EPS-DGN-FS-B then
    RECOVERY = OPERATOR-RECOVERS-DGNS;
endif
```

Idaho National Laboratory

HRA Process (cont.)

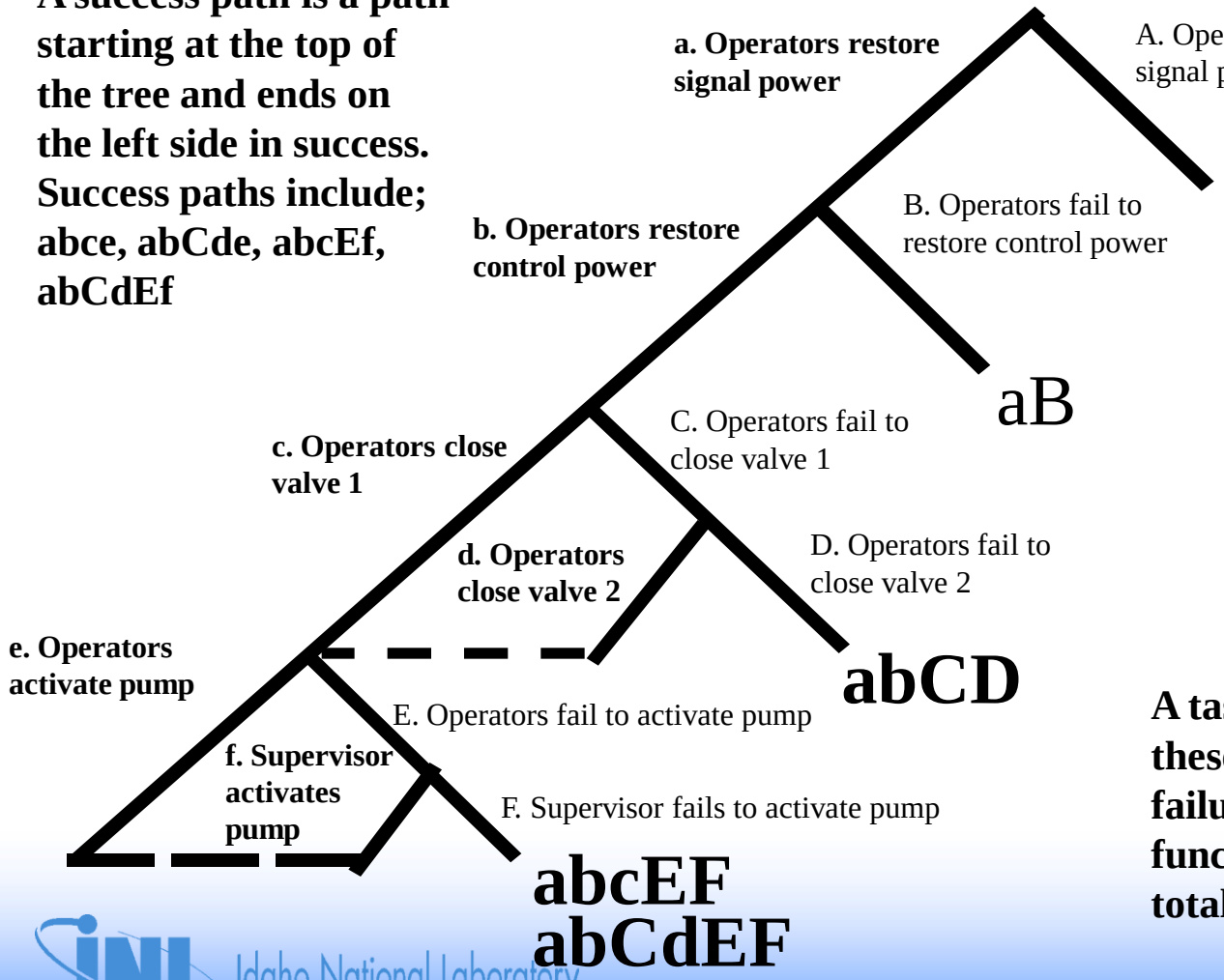
- **Perform screening analysis**
  - **Uses deliberately conservative estimates of human error probability**
    - **Screening methods include ASEP**
  - **Leaves smaller set of human failure events for more detailed analysis**

HRA Process (cont.)

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

Sample HRA Event Tree

A success path is a path starting at the top of the tree and ends on the left side in success. Success paths include; abce, abCde, abcEf, abCdEf



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

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

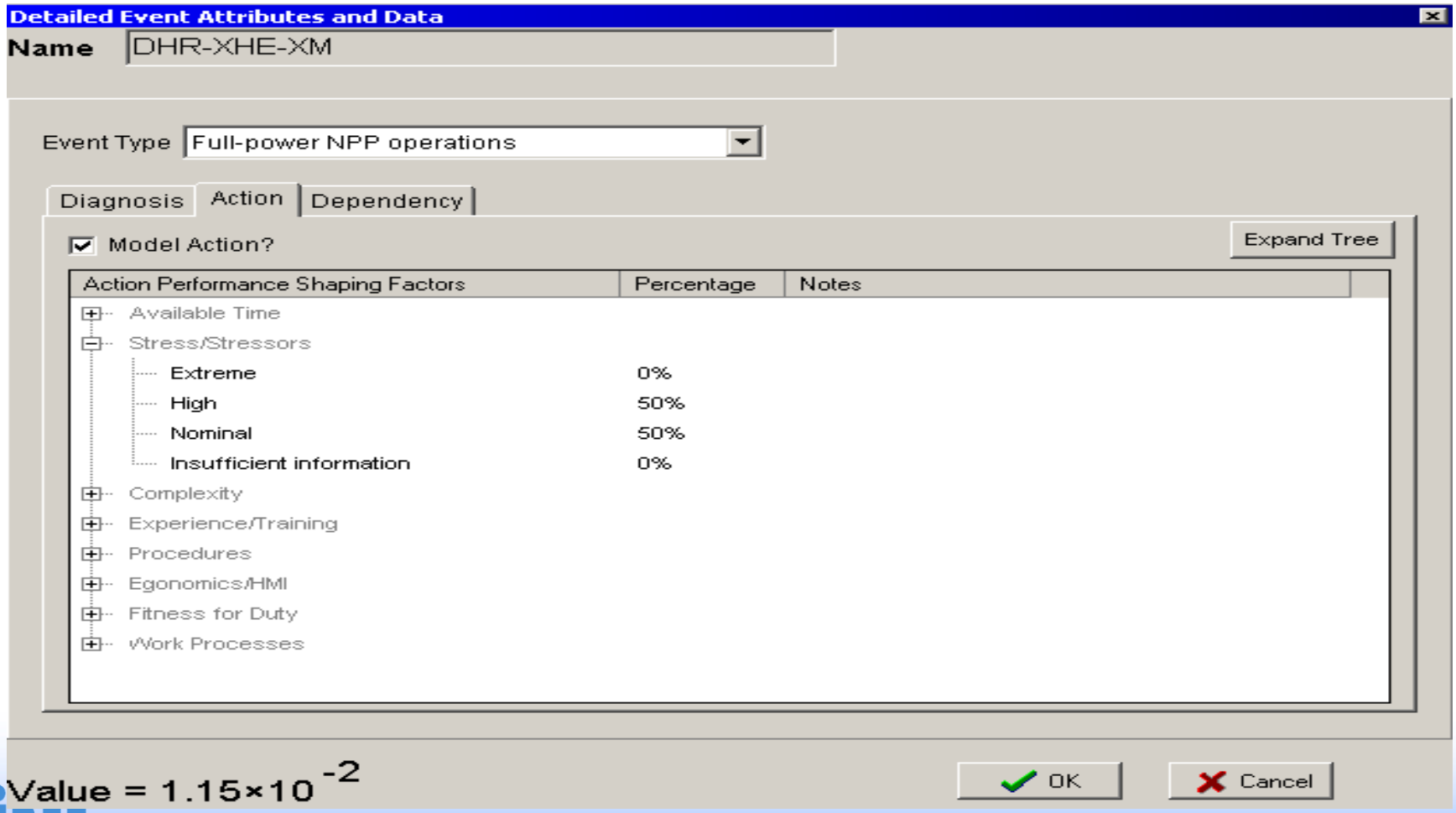
Performance Shaping Factors (PSFs)

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

Typical PSFs Considered in HRA

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

Example of Incorporating PSFs into a Human Error Basic Event



(SAPHIRE Risk Assessment Software used for this example)

How Human Actions Are Incorporated Into PRA Model

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

Sources of HRA Data

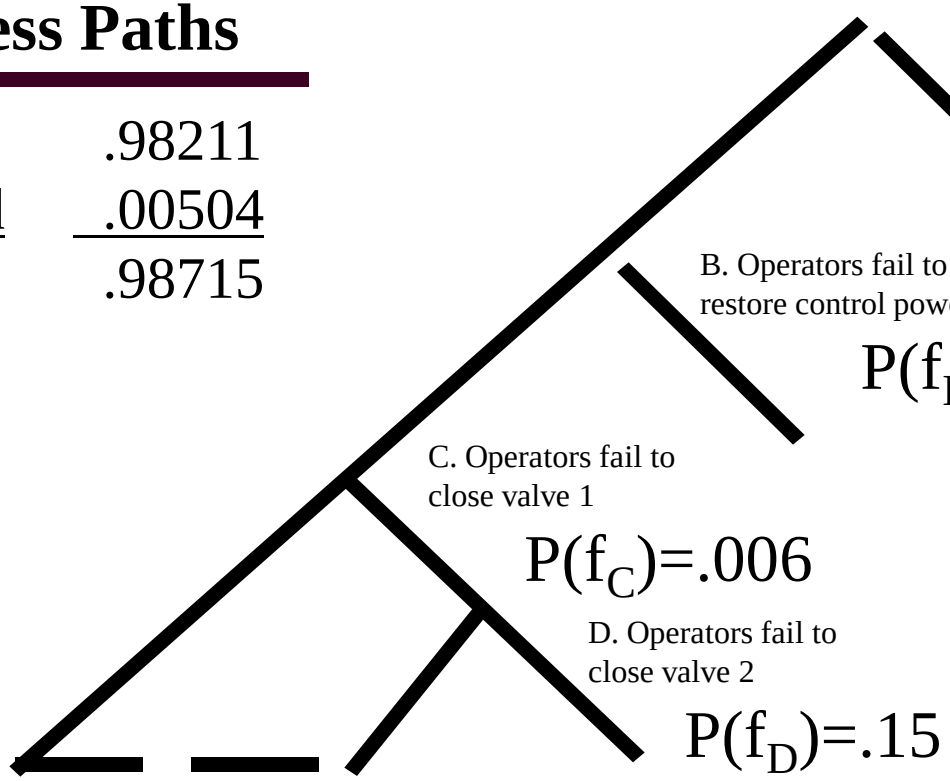
- Nuclear and allied industries
- Military
- Nuclear plant simulators
- Expert elicitation

HRA Event Tree Quantification

Plug HEP data into the model and calculate paths and total HEP

Success Paths

abc	.98211
abCd	.00504
Total	.98715



Failure Paths

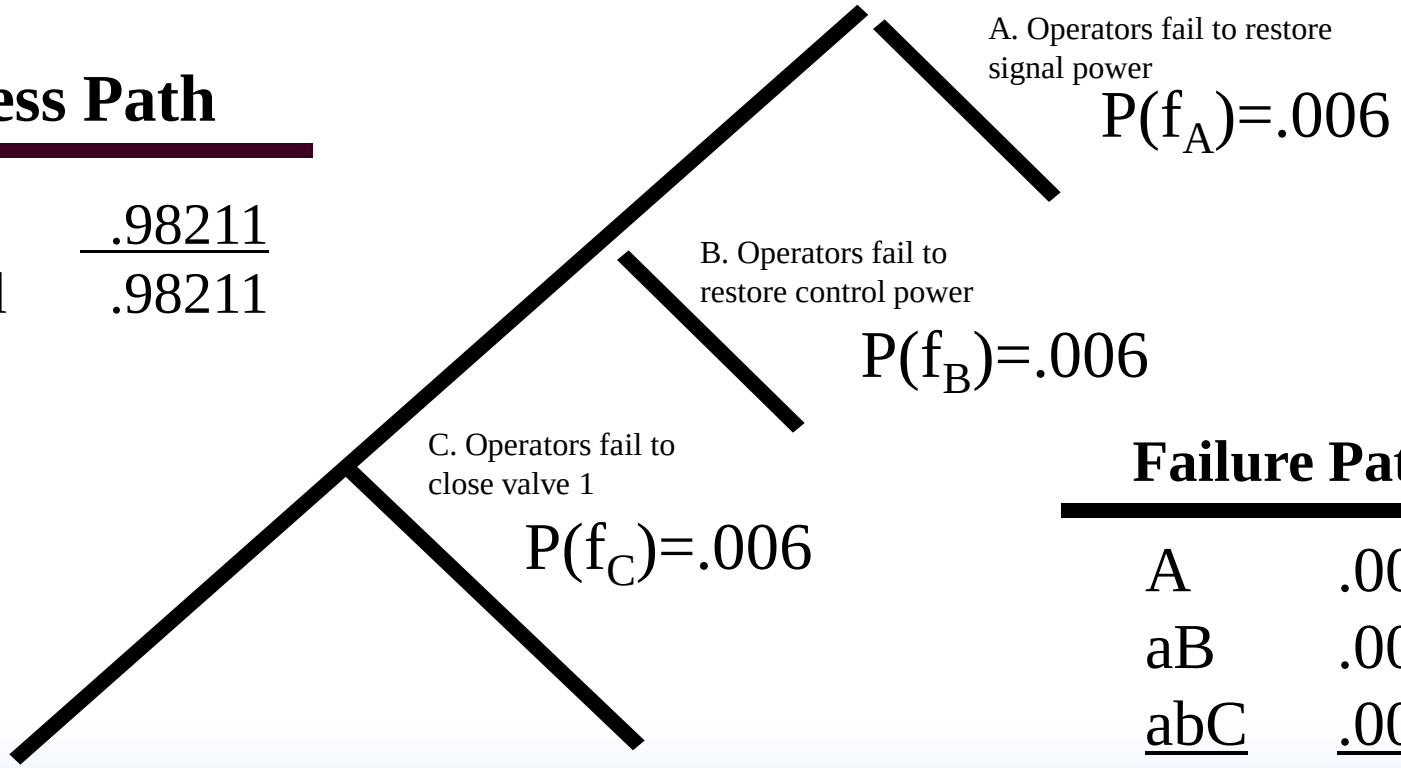
A	.006
aB	.00596
abCD	.00089
Total	.01285

HRA Event Tree Quantification

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

Success Path

abc	.98211
Total	.98211



Failure Paths

A	.006
aB	.00596
abC	.00593
Total	.01789

HRA Strengths and Limitations

- **Major Strength:**
  - **HRA identifies areas where improvements may be made in training, procedures, and equipment to reduce risk**
- **Limitations:**
  - **Lack of consensus as to which modeling and quantification approach to use (many 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**

ATHEANA (A Technique for Human Event Analysis)

- NRC Research project to develop a methodology and implementation guidance for addressing errors of commission
- NUREG-1624, Technical Basis And Implementation Guidelines For A Technique For Human Event Analysis (ATHEANA)
- 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

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.**