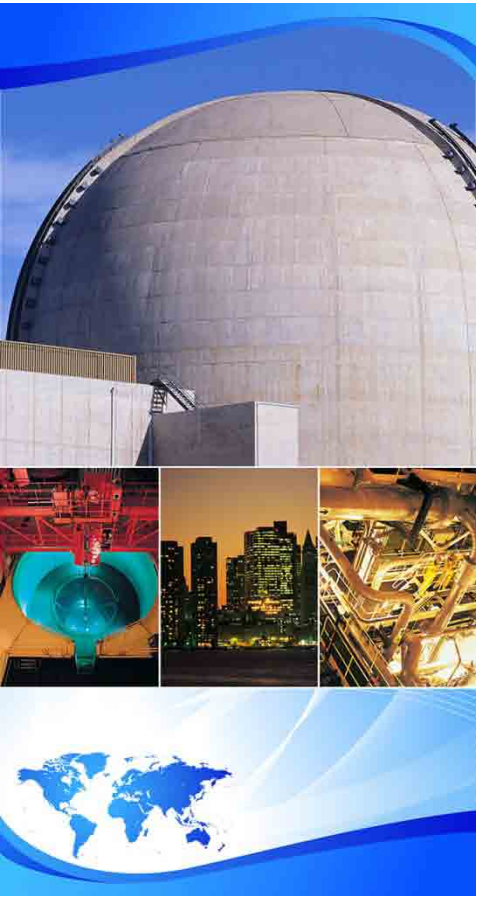
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Sandia National Laboratories

CURTISS WRIGHT Flow Control Company
SCIENTECH

SAIC Science Applications International Corporation
From Science to Solutions™



Principles of Human Reliability Analysis (HRA)

Joint NRC-RES/EPRI Fire PRA Workshop 2012
Bethesda, MD

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

Course Objectives

- Introduce Human Reliability Analysis (HRA), in the context of PRA for nuclear power plants.
- Provide students with a basic understanding of HRA:
  - What is HRA?
  - Where does HRA fit into PRA?
  - What does HRA model?
  - Is there a standard for performing HRA?
  - What guidance is there for performing HRA?
  - What are the keys to performing HRA?
  - How can we understand human error?
  - What are the important features of existing HRA methods?
  - What are the HRA concerns or issues for fire PRA?

Course Outline

- **What is HRA?**
- Where does HRA fit into PRA?
- What does HRA model?
- Is there a standard for performing HRA?
- What guidance is there for performing HRA?
- What are the keys to performing HRA?
- How can we understand human error?
- What are the important features of existing HRA methods?
- What are the HRA concerns or issues for fire PRA?
- Any final questions?

Human Reliability Analysis (HRA) ….

Is generally defined as:

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

Is developed because:

- **PRA reflects the as-built, as-operated plant**
- **HRA is needed to model the "as-operated" portion (and cross-cuts many PRA tasks and products)**

Produces:

- Identified and defined human failure events (HFEs)
- Qualitative evaluation of factors influencing human errors and successes
- Human error probabilities (HEPs) for each HFE

HRA …. (continued)

- Requires inputs from many technical disciplines, e.g.,:
  - PRA
  - Plant design and behavior
  - Engineering (e.g., thermal hydraulics)
  - Plant operations
  - Procedures and how they are used
  - Ergonomics of monitoring and control interfaces (both inside and outside control room)
  - Cognitive and behavioral science
  - Etc., etc., etc.
- Is performed by:
  - A multi-disciplinary team

Course Outline

- What is HRA?
- **Where does HRA fit into PRA?**
- What does HRA model?
- Is there a standard for performing HRA?
- What guidance is there for performing HRA?
- What are the keys to performing HRA?
- How can we understand human error?
- What are the important features of existing HRA methods?
- What are the HRA concerns or issues for fire PRA?
- Any final questions?

Overview of PRA Process

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

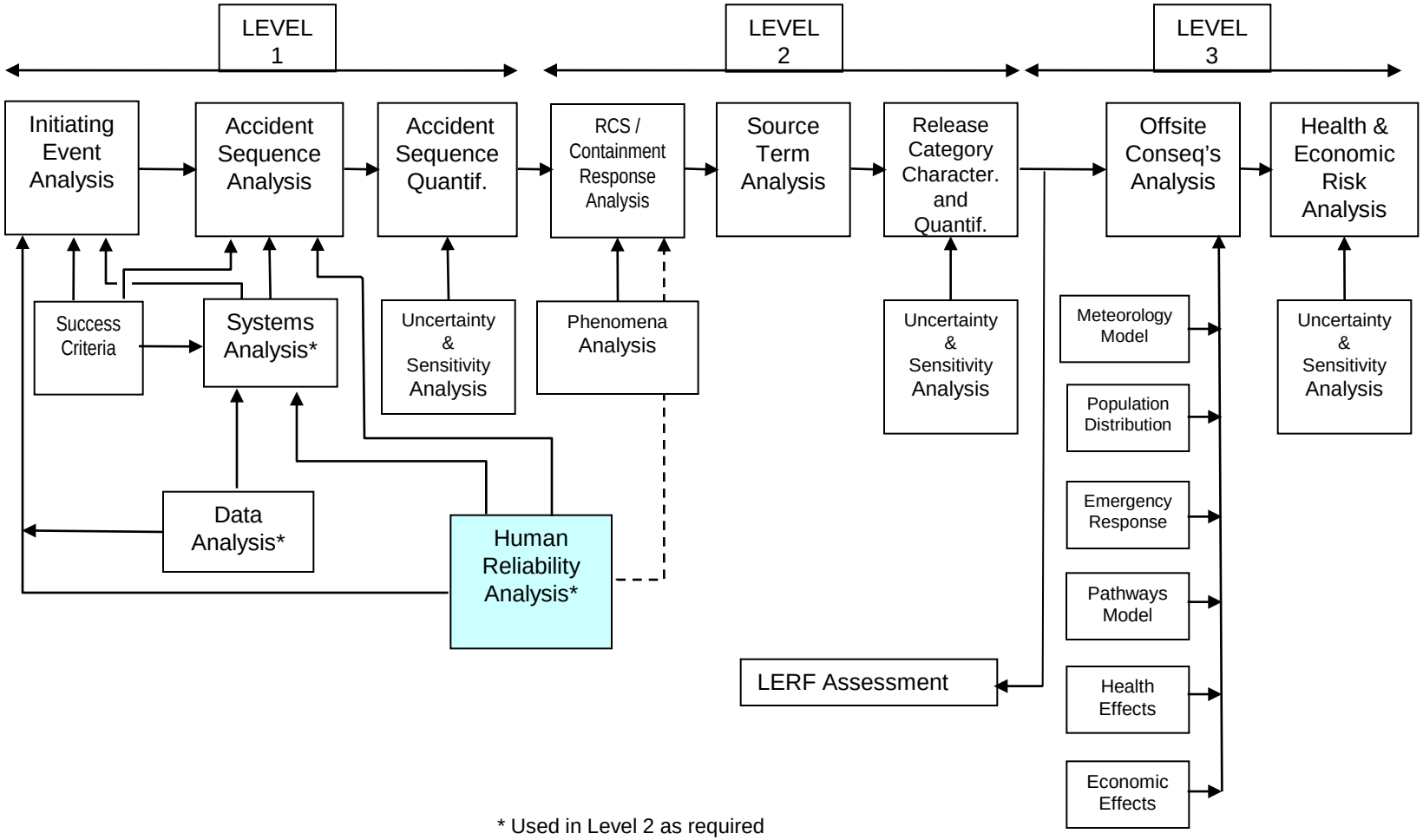
Level	An Assessment of:	Result
1	Plant accident initiators and systems'/operators' response	Core damage frequency and contributors
2	Reactor core melt, and frequency and modes of containment failure	Categorization and frequencies of containment releases
3	Public health consequences	Estimation of public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

PRA Classification

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

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

Principal Steps in PRA



* Used in Level 2 as required

Principal Steps in PRA (continued)

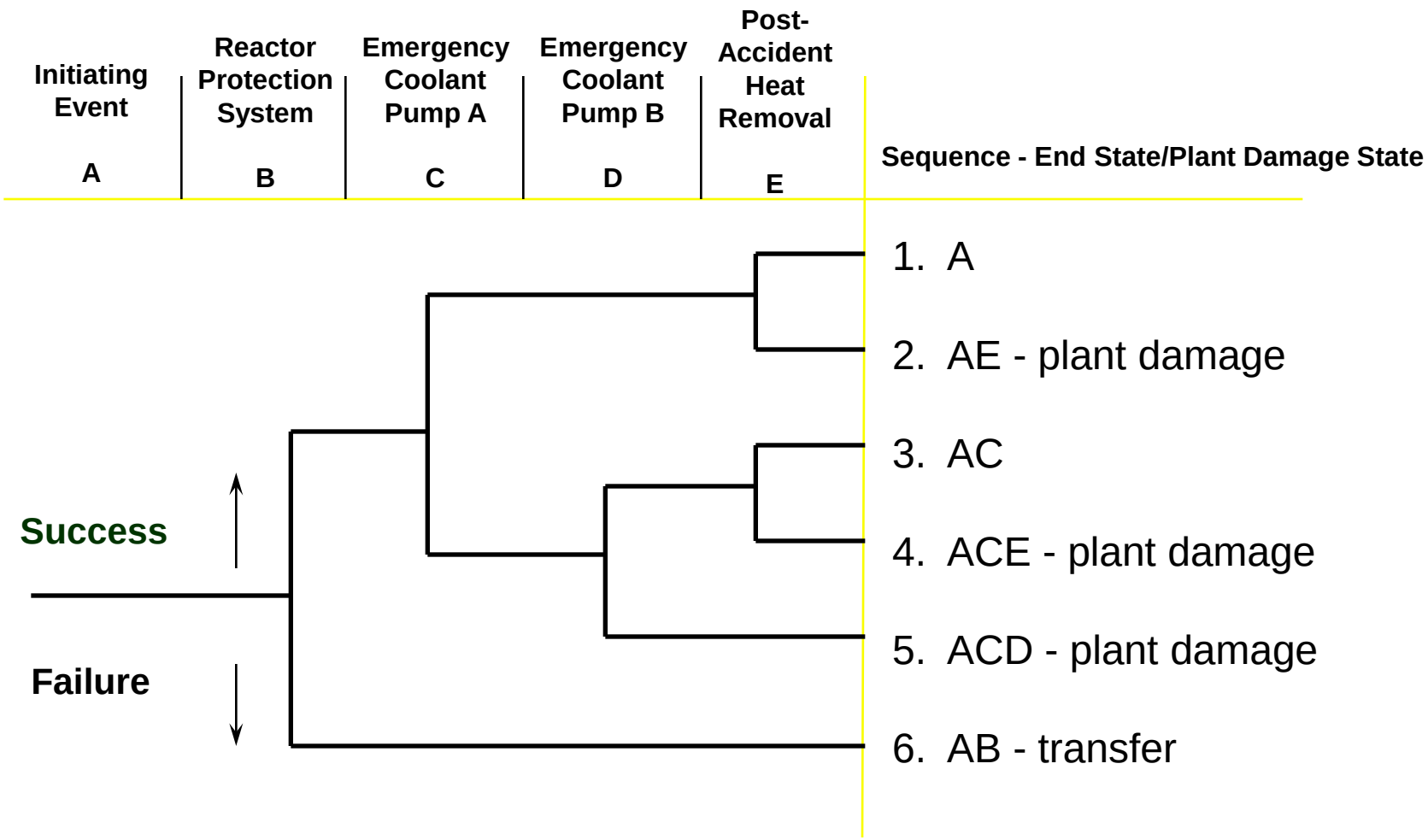
- First, we'll look at how HRA fits into Event Tree (ETs) models.

Human Events in Event Trees

Nature of event trees (and where HRA fits in):

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

Simple Event Tree



System-Level Event Tree Development

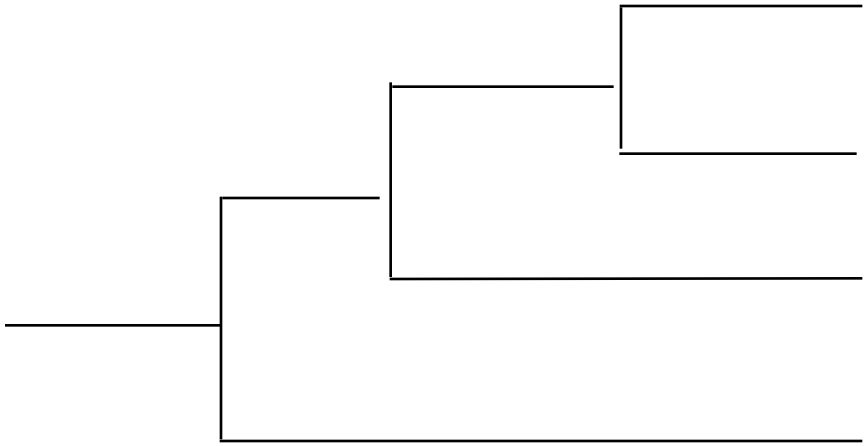
- A system-level event tree consists of an initiating event (one per tree), followed by a number of headings (top events), and sequences of events defined by success or failure of the top events
- Top events represent the systems, components, and/or human actions required to mitigate the initiating event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

System-Level Event Tree Development (continued)

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

Functional Event Tree

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



SEQ #	STATE
1	OK
2	LATE-CD
3	EARLY-CD
4	ATWS

Critical Safety Functions

Example safety functions for core and containment

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

Example BWR Mitigating Systems

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

Example PWR Mitigating Systems

Function	Systems
Reactivity Control	Reactor Protection System (RPS)
RCS Overpressure Protection	Safety valves, pressurizer Power-Operated Relief Valves (PORVs)
Coolant Injection	Accumulators, High Pressure Safety Injection (HPSI), Chemical Volume and Control System (CVCS), Low Pressure Safety Injection (LPSI), High Pressure Recirculation (may require LPSI)
Decay Heat Removal	Power Conversion System, Auxiliary Feedwater (AFW), Residual Heat Removal (RHR), Feed and Bleed (PORV + HPSI)

System Success Criteria

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

Example Success Criteria

IE	Reactor Trip	Short Term Core Cooling	Long Term Core Cooling
Transient	Auto Rx Trip or Manual Rx Trip	Power Conversion System or 1 of 3 AFW or 1 of 2 PORVs and 1 of 2 ECI	Power Conversion System or 1 of 3 AFW or 1 of 2 PORVs and 1 of 2 ECR
Medium or Large LOCA	Auto Rx Trip or Manual Rx Trip	1 of 2 ECI	1 of 2 ECR

What does HRA do with ET information?

For example, the HRA analyst:

- From initiating event and subsequent top events on ET:
  - Identifies the procedures and procedure path that lead to successful mitigation of the initiating event
- From success criteria:
  - Determines what defines an operator failure (e.g., fewer pumps started than needed, actions performed too late in time)
- From plant behavior timing provided by T-H calculations:
  - Determines what plant parameters, alarms, and other indications are available to help operators:
    - understand the plant state (initially and as the accident progresses)
    - use procedures appropriately to respond to specific accident sequence
- Any plant function-related human failure events (HFEs) can be defined.

What does HRA do with ET information? (continued)

- From the various branches on the event tree (combined with success criteria and timing information):
  - Identifies (or confirms) what operator actions, if failed, could result in “down” branches and certain plant damage states (alone or in combination with system failures) (i.e., define an HFE)
  - Identifies what specific operator actions (e.g., fails to start HPI Train A pump, turns off Safety Injection) would result in a “down” branch (i.e., define an HFE)
  - Identifies what procedure paths might be plausibly taken that would result in operator failures
  - Identifies what plant information (or missing information) might cause operators to take inappropriate procedure paths
- These inputs also can be factors influencing the selection of screening values for human failure events.

Principal Steps in PRA (continued)

- Next, we'll see how HRA is included in Fault Tree (FT) models.

Human Events in Fault Trees

Characteristics of fault trees (and where HRA fits in):

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

Human Events in Fault Trees (continued)

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

Specific Failure Modes Modeled for Each Component

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

Typical Component Failure Modes

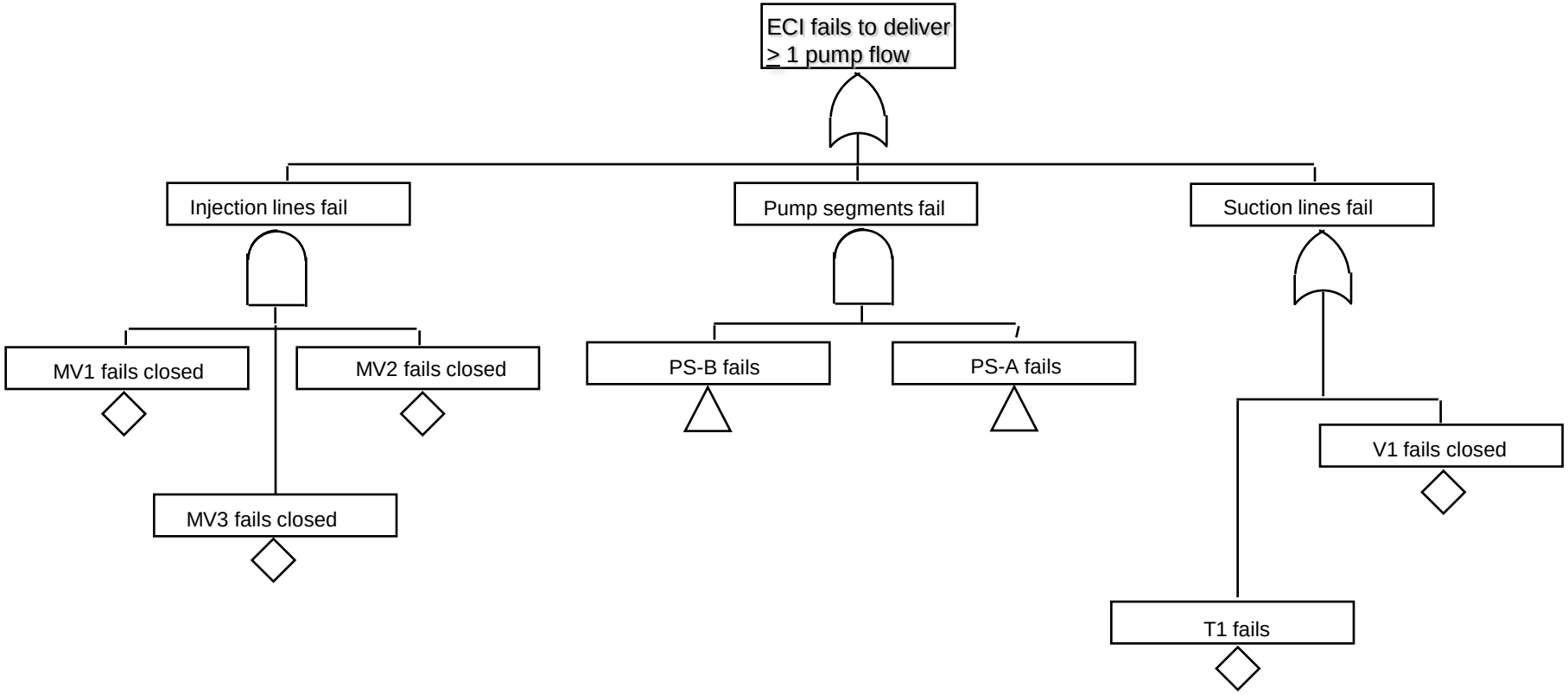
- Active Components
  - Fail to Start*
  - Fail to Run*
  - Fail to Open/Close/Operate*
- Additional “failure mode” is component is unavailable because it is out for test or maintenance

* In addition to hardware failures that have these failure modes, an operator “error of commission” (that suppresses actuation or operation, or turns off equipment) also can cause these failure modes.

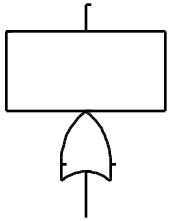
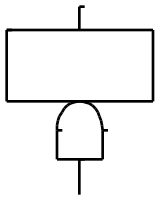
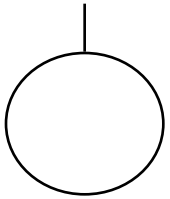
Active Components Require "Support"

- Signal needed to "actuate" component
  - Safety Injection Signal starts pump or opens valve
- If system is a "standby" system, operator action may be needed to actuate (and failure to actuate is modeled as an HFE)
- Support systems might be required for component to function
  - AC and/or DC power
  - Service water or component water cooling
  - Room cooling

Simplified Fault Tree for Failure of Emergency Coolant Injection (ECI)



Fault Tree Symbols

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

What does HRA do with FT information?

- From the top events and types of equipment modeled in the fault tree:
  - Identify and define any human failure events (HFEs) that could result in system, train, or component failures (e.g., starting, actuating, opening/closing)
- From review of procedures and other documents related to testing and maintenance:
  - Identify and define operator failures to restore systems, trains, or components following testing or maintenance
  - Determine the frequency of testing and preventive maintenance
  - Determine what post-testing and post-maintenance checks are performed
- These inputs also can be used in selecting appropriate screening values for HFEs.

Course Outline

- What is HRA?
- Where does HRA fit into PRA?
- **What does HRA model?**
- Is there a standard for performing HRA?
- What guidance is there for performing HRA?
- What are the keys to performing HRA?
- How can we understand human error?
- What are the important features of existing HRA methods?
- What are the HRA concerns or issues for fire PRA?
- Any final questions?

Human Reliability Analysis

- Starts with the basic premise that the humans can be represented as either:
  - A component of a system, or
  - A failure mode of a system or component.
- Identifies and quantifies the ways in which human actions initiate, propagate, or terminate accident sequences.
- Human actions with both positive and negative impacts are considered in striving for realism.
- A difficult task in a PRA since the HRA analyst needs to understand the plant hardware response, the operator response, the accident progression modeled in the PRA.
- Not everything the operator does is modeled in the PRA!

Human Reliability Analysis Objectives

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

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

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

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

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

Ref. ASME RA-Sa-2009

Categories of Human Failure Events in PRA

- Operator actions can occur throughout the accident sequence:
  - Before the initiating event (i.e., pre-initiator)
  - As a cause of the initiating event
  - After the initiating event (i.e., post-initiator)

Categories of Human Failure Events: Pre-Initiator HFEs

- Sometimes called “latent errors” because they are not revealed until there is a demand for the affected system (after the initiating event).
- Examples:
  - Failure to restore valve lineup following routine system testing
  - Failure to rack-in pump breaker in following preventive maintenance
  - Mis-calibration of instruments
- Most frequently relevant outside main control room
- Some of these failures are captured in equipment failure data.
- For HRA, the focus is on equipment being left misaligned, unavailable, or not working exactly right (accounting for post-test/post-maintenance verification).

Categories of Human Failure Events: Initiating-Event Related

- Operator actions can contribute to the occurrence of or **cause initiating events** (i.e., human-induced initiators)
- In PRAs, such events are most often
  - Included implicitly in the data used to quantify initiating event frequencies, and
  - Therefore not modeled explicitly in the PRA
- Operator actions can be particularly relevant for operating conditions other than power operation
  - Human-caused initiating events can have unique effects (e.g., causing drain-down of reactor or RCS during shutdown)
  - Actions that cause initiating events may also have implications for subsequent human response (i.e., dependence can be important)

Categories Of Human Failure Events: Post-Initiator HFEs

- **Post-initiator HFEs** account for failures associated with response to an initiating event
- Typically reflect failure to take necessary action (in main control room or locally)
  - Failure to initiate function of manually-actuated system
  - Failure to back up an automatic action
  - Failure to recover from other system failures
    - Reconfigure system to overcome failures (e.g., align electrical bus to alternative feed)
    - Make use of an alternative system (e.g., align fire water to provide pump cooling)
- Most often reflect failure to take actions called for by procedures

Other Classifications of Human Failure Events

- Another way to classify human failure events (HFEs) from the perspective of the PRA is:
  - Error of omission (EOO)
  - Error of commission (EOC)
- Errors of omission (EOOs):
  - *A human failure event resulting from a failure to take a required action, leading to an unchanged or inappropriately changed and degraded plant state.*
  - Examples:
    - Failure to start auxiliary feedwater system
    - Failure to block automatic depressurization system signals

Other Classifications of HFEs (continued)

- Errors of commission (EOCs):
  - *A human failure event resulting from a well-intended but inappropriate, overt action that, when taken, leads to a change in the plant and results in a degraded plant state.*
  - Often, these events represent "good" operating practice, but applied to the wrong situation (especially, when understanding the situation is difficult).
  - Examples:
    - Prematurely terminating safety injection (because operators think SI is not needed; but for the specific situation, SI is needed).

Other Classifications of HFEs (continued)

- Pre-initiator HFEs can be either EOOs or EOCs:
  - These HFEs usually represent failures in execution (i.e., failures to accomplish the critical steps; these steps are typically already decided so no decision-making is required).
  - Execution failures are often caused by inattention (or over-attention) failures
  - Examples:
    - Inattention: Skipped steps (especially, following interruptions or other distractions)
    - Over-attention: Repeated or reversed steps

Other Classifications of HFEs (continued)

- Most post-initiator HFEs that are modeled are EOOs:
  - These HFEs can represent either failures in execution or cognitive failures (such as failures in diagnosis of the plant condition or decision-making regarding procedure use for a particular situation).
  - Most PRAs ***only include*** EOOs; however, EOCs have been involved in many significant accidents, both in nuclear power industry and others.
  - Later, we'll see that the fire PRA methodology for NFPA-805 requires that certain EOCs be addressed.

Course Outline

- What is HRA?
- Where does HRA fit into PRA?
- What does HRA model?
- **Is there a standard for performing HRA?**
- What guidance is there for performing HRA?
- What are the keys to performing HRA?
- How can we understand human error?
- What are the important features of existing HRA methods?
- What are the HRA concerns or issues for fire PRA?
- Any final questions?

Standard for HRA?

- NRC's Regulatory Guide 1.200 provides staff position for one approach in determining the technical adequacy of a PRA to support a risk-informed activity
- The staff position, in determining technical adequacy, defines a technically acceptable base PRA
- For each technical element (e.g., HRA)
  - Defines the necessary attributes and characteristics of at technically acceptable HRA
  - Allows use of a standard in conjunction with a peer review to demonstrate conformance with staff position
  - Endorses ASME/ANS standard and NEI peer review guidance (with some exceptions)

Standard for HRA? (continued)

- RG 1.200 specifies what is needed in a technically acceptable PRA/HRA
- ASME/ANS PRA standard defines requirements*
  - Specifies **what** you need to do.
- These standard requirements have been established to ensure PRA quality commensurate with the type of PRA application and/or regulatory decision

*The use of the word "Requirements" is Standard language and is not meant to imply any regulatory requirement

Standard for HRA? (continued)

- The standard provides two levels of technical requirements:
  - High level requirements (HLRs)
  - Supporting requirements (SRs)
- The HLRs provide the minimum requirements for a technically acceptable baseline PRA. The HLRs are defined in general terms and reflect the diversity of approaches and accommodate future technological innovations.
- The SRs define the requirements needed to accomplish each HLR

Standard for HRA? (continued)

- In defining the SRs, the standard recognizes that, depending on the application, the level of detail, the level of plant specificity and the level of realism can vary
- Three capability categories are defined, and the degree to which each is met increases from Category I to Category III
- Each SR is defined to a different “Capability Category”
- Within a PRA, even the HRA element can be a mixture of capability categories.

Standard for HRA? (continued)

- Capability Category I:
  - Scope and level of detail are sufficient to identify relative importance of contributors down to system or train level.
  - Generic data and models are sufficient except when unique design or operational features need to be addressed.
  - Departures from realism have moderate impact on results.
- Capability Category II:
  - Scope and level of detail are sufficient to identify relative importance of significant contributors down to component level, including human actions.
  - Plant-specific data and models are used for significant contributors.
  - Departures from realism have small impact on results.

Standard for HRA? (continued)

- Capability Category III:
  - Scope and level of detail are sufficient to identify relative importance of contributors down to component level, including human actions.
  - Plant-specific data and models are used for all contributors.
  - Departures from realism have negligible impact on results.

Objective of HRA Technical Element in ASME/ANS PRA Standard

The objective of the human reliability element of the PRA is to ensure that the impacts of plant personnel actions are reflected in the assessment of risk in such a way that:

- Both pre-initiating event and post-initiating event activities are addressed
- Logic model elements are defined to represent the effect of such personnel actions
- Plant-specific and scenario-specific factors are accounted for
- Human performance issues are addressed in an integral way so that issues of dependency are captured

PRA Standard Requirements for HRA

ASME HRA **High Level Requirements** Compared

Pre-Initiator	**Post Initiator**
A – Identify HFEs	E – Identify HFEs
B – Screen HFEs	
C – Define HFEs	F – Define HFEs
D – Assess HEPs	G – Assess HEPs
	H – Recovery HFEs
I – Document HFEs/HEPs	

ASME/ANS Standard Post-Initiator HRA High Level Requirements (HLRs)

- Examples of High Level Requirements (HLRs) for post-initiator HFEs:

HLR-HR-E

A systematic review of the relevant procedures shall be used to identify the set of operator responses required for each of the accident sequences

HLR-HR-F

Human failure events shall be defined that represent the impact of not properly performing the required responses, consistent with the structure and level of detail of the accident sequences.

ASME/ANS Standard Post-Initiator HRA High Level Requirements

- Examples (continued):

HLR-HR-G

The assessment of the probabilities of the post-initiator HFEs shall be performed using a well defined and self-consistent process that addresses the plant-specific and scenario-specific influences on human performance, and addresses potential dependencies between human failure events in the same accident sequence.

HLR-HR-H

Recovery actions (at the cutset or scenario level) shall be modeled only if it has been demonstrated that the action is plausible and feasible for those scenarios to which they are applied. Estimates of probabilities of failure shall address dependency on prior human failures in the scenario

ASME/ANS Standard Pre- and Post-Initiator HRA High Level Requirements

- Examples (continued):

HLR-HR-I

The HRA shall be documented consistent with the applicable supporting requirements (HLR-HR-I).

ASME/ANS Standard Post-Initiator HRA Supporting Requirements (SRs)

- Examples of Supporting Requirements (SRs) for post-initiator HFEs:

HR-E1

When identifying the key human response actions review (a) the plant-specific emergency operating procedures, and other relevant procedures (e.g., AOPs, annunciator response procedures) in the context of the accident scenarios (b) system operation such that an understanding of how the system(s) and the human interfaces with the system is obtained. (All Capability Categories)

ASME/ANS Standard Post-Initiator HRA Supporting Requirements (SRs)

- Examples (continued):

HR-G1

Capability Category I: Use conservative estimates (e.g., screening values) for the HEPs of the HFEs in accident sequences that survive initial quantification.

Capability Category II: Perform detailed analyses for the estimation of HEPs for significant HFEs. Use screening values for HEPs for non-significant human failure basic events.

Capability Category III: Perform detailed analyses for the estimation of human failure events.

ASME/ANS Standard Post-Initiator HRA Supporting Requirements (SRs)

- Examples (continued):

HR-G6

Check the consistency of the post-initiator HEP quantifications. Review the HFEs and their final HEPs relative to each other to check their reasonableness given the scenario context, plant history, procedures, operational practices, and experience. (All Capability Categories)

ASME/ANS Standard: Supporting and Fire HRA-Specific Requirements

- The standard is for an at-power Level 1/LERF PRA for both internal and external hazards
- The requirements in the PRA standard for internal events provide the requirements for the base PRA model
- The other hazards (e.g., internal fires) build upon the base PRA model for internal events
- In general, the HRA requirements (both HLRs and SRs) for internal events apply to the other hazards (e.g., fire, seismic).
- The Fire HRA Track presented this week will identify HLRs and SRs specifically applicable in performing fire HRA/PRA.

Course Outline

- What is HRA?
- Where does HRA fit into PRA?
- What does HRA model?
- Is there a standard for performing HRA?
- **What guidance is there for performing HRA?**
- What are the keys to performing HRA?
- How can we understand human error?
- What are the important features of existing HRA methods?
- What are the HRA concerns or issues for fire PRA?
- Any final questions?

HRA Guidance – How To….

- From our last presentation:
  - The standard specifies **what** you need to do.
  - Guidance, on the other hand, is a description of **how-to** do something…..
- In this presentation, we will discuss three different types of HRA guidance associated with:
  1. HRA processes
  2. Other HRA tools or approaches
  3. HRA quantification methods

HRA Processes

- An HRA process is a prescribed set of steps for **how to** perform an HRA.
- Usually, an HRA process explicitly identifies steps that are also products of HRA, i.e.,
  1. Identification and definition of human failure events (HFEs),
  2. Quantification of each HFE (i.e., assignment of human error probabilities (HEPs)),
  3. Qualitative analysis that supports #1 and #2, and
  4. Documentation of all of the above.

HRA Processes (continued)

- Not many HRA processes have been published.
- Usually, the HRA process provides both:
  1. Steps for **how to** perform HRA, and
  2. **How to** perform the steps.
- Two examples of published stand-alone HRA processes are:
  - EPRI's " SHARP1 – A Revised Systematic Human Action Reliability Procedure," EPRI TR-101711, December 1992
  - NRC's "Good Practices for Implementing Human Reliability analysis (HRA)," NUREG-1792, April 2005

* "Stand-alone" means that they are not connected with a specific HRA quantification method.

HRA Processes (continued)

- SHARP1:
  - Written to provide a “user-friendly tool” for utilities in preparing Individual Plant Examinations (IPEs) back in the early 1990s.
  - Written to enhance the original SHARP, developed in 1984, to:
    - Address review comments
    - Incorporate the experience and insight gained in intervening years
  - Described as a “framework…for incorporating human interactions into PRA…” with emphasis on the iterative nature of the process.
  - Structured in “stages” to provide additional guidance for systematically integrating HRA into the overall plant logic model of the PRA.
  - Describes and compares selected HRA methods for quantification.
  - Includes four case studies.

HRA Processes (continued)

- SHARP1 describes how to formulate a project team to perform HRA.
- SHARP1 is organized into four “stages” to define clearly the interactions with major PRA tasks:
  - Stage 1: Human Interaction Event Definition and Integration into Plant Logic Model
  - Stage 2: Human Interaction Event Quantification
  - Stage 3: Recovery Analysis
  - Stage 4: Internal Review
- The original seven steps in SHARP still apply (but are captured within these four stages).

HRA Processes (continued)

- SHARP1 uses three broad categories of human interactions:
  - Type A: Pre-initiating event interactions
  - Type B: Initiating event interactions
  - Type C: Post-initiating event interactions
    - CP: Actions dictated by operating procedures and modeled as essential parts of the plant logic model
    - CR: Recovery actions
- SHARP1 emphasizes the importance of dependencies between human interactions (especially with respect to premature screening of important interactions) and defines four classes of dependencies.

HRA Processes (continued)

- SHARP1 provides detailed guidance on **how to** define and place HFEs into the plant logic model, including:
  - example event trees and fault trees
  - comparisons of procedure steps with what an HFE represents
  - detailed accounts for four case studies
- SHARP1 provides some discussion of influence and/or performance shaping factors, but there is no particular emphasis on this topic.
- Qualitative HRA is not explicitly identified or discussed, but is incorporated into different “stages”

HRA Processes (continued)

- NRC's "Good Practices for HRA":
  - Written to establish "good practices" for performing HRA and to assess the quality of HRA, when it is reviewed.
  - Are generic in nature; not tied to any specific methods or tools.
  - Written to support implementation of RG 1.200 for Level 1 and limited Level 2 internal event, at-power PRAs (using direct links between elements of "good practices" and RG 1.200).
  - Consequently, written ultimately to address issues related to PRA quality and associated needs for confidence in PRA results used to support regulatory decision-making.
  - Developed using the experience of NRC staff and its contractors, including lessons learned from developing HRA methods, performing HRAs, and reviewing HRAs.

HRA Processes (continued)

- NRC's "Good Practices" (GPs) address the following:
  - HRA team formation and overall guidance (2 GPs), e.g.,
    - Should use a multidisciplinary team
    - Should perform field observations
  - Pre-initiator HFEs (15 GPs), e.g.,
    - In identifying HFEs, should review procedures for all routine testing and maintenance
    - In quantifying HFEs, it is acceptable to use screening values if: a) the HEPs are clearly overestimates and b) dependencies among multiple HFEs are conservatively accounted for.
    - In quantifying HFEs, should account for the most relevant plant- and activity-specific performance shaping factors (PSFs).

HRA Processes (continued)

- NRC's "Good Practices" (GPs) address (continued):
  - Post-initiator HFEs (17 GPs), e.g.,
    - In identifying HFEs, should review post-initiator related procedures and training.
    - In modeling (a.k.a., defining) HFEs, should define such that they are plant- and accident sequence-specific.
    - In quantifying HFEs, should address both diagnosis and response execution failures.
    - In adding recovery actions, should consider a number of aspects (e.g., whether cues will be clear and timely, whether there is sufficient time available, whether sufficient crew resources exist)
  - Errors of commission (2 GPs), e.g.,
    - Recommend to identify and model potentially important EOCs.

HRA Processes (continued)

- NRC's "Good Practices" (GPs) address (continued):
  - HRA documentation (1 GP), i.e.,
    - Should allow a knowledgeable reviewer to understand the analysis enough that it could be approximately reproduced and the same resulting conclusion reached.
- Does not explicitly address human-induced initiating events, but GPs for pre-initiator HFEs and post-initiator HFEs also should apply to HFEs that induce initiating events.

HRA Processes (continued)

- Neither SHARP1 nor NRC's "Good Practices" specify or dictate:
  - Which HRA method should be used to perform HRA quantification
  - Any specific HRA tools or approaches for performing HFE identification and definition, and qualitative analysis
- In fact, often an HRA method does not:
  - Provide an accompanying and explicit HRA process for applying that specific method, and/or
  - Specify which (or that any) HRA process (e.g., SHARP) should be used to apply the specific method.
- Consequently, it usually is up to the HRA analyst to decide on selecting and applying an explicit HRA process to follow.

HRA Processes (continued)

- However, there are a few HRA quantification methods that provide a specific HRA process.
- Examples of such methods:
  - THERP (NUREG/CR-1278)
  - ATHEANA (NUREG-1624, Rev. 1)
  - Fire HRA Guidelines (NUREG-1921/EPRI TR 1023001, to be published)
- For both ATHEANA and the Fire HRA Guidelines, the HRA process steps include explicit guidance for certain steps or use of HRA tools, such as:
  - Approaches for identifying HFEs (e.g., EOCs)
  - Approaches or techniques for doing certain aspects of qualitative HRA (e.g., determining if an operator action is feasible and, therefore, suitable to be included in PRA)

Course Outline

- What is HRA?
- Where does HRA fit into PRA?
- What does HRA model?
- Is there a standard for performing HRA?
- What guidance is there for performing HRA?
- **What are the keys to performing HRA?**
- How can we understand human error?
- What are the important features of existing HRA methods?
- What are the HRA concerns or issues for fire PRA?
- Any final questions?

What are the keys to performing HRA?

<u>The</u> key is to….

What are the keys to performing HRA?

…understand the problem.

What are the keys to performing HRA?

- Why do you need to "understand the problem"?
  1. To be able to identify, define, and model (i.e., place appropriately in the plant logic model) HFEs such that they are consistent with, for example:
     - the specific accident sequence
     - associated plant procedures and operations
     - expected plant behavior and indications
     - engineering calculations that support the requirements for successful accident mitigation
     - consequences that are risk-significant

What are the keys …? (continued)

- Why do you need to "understand the problem"? (continued)

2. To appropriately select an HRA quantification method to (usually) indirectly represent how operators are expected to behave, based on, for example:
    - their procedures and training
    - plant-specific (and maybe even crew-specific) styles for responding to accidents
    - plant-specific operating experience
    - general understanding of human error, behavior and cognitive science, human factors and ergonomics
    - knowledge of HRA methods and their underlying bases
3. To support and justify the HFEs and their quantification

What are the keys …? (continued)

- How do you develop this understanding?
  - Perform an appropriately thorough **qualitative analysis**, performed **iteratively** and **repeatedly** throughout the entire HRA process until the final HRA quantification is done.
- How do you know when are you done?
  - Usually, one or more of the following has occurred:
    - The accident sequence analyst tells you that you should move on to a new problem/HFE (that is more risk-significant).
    - Your deadline has arrived.
    - Your money is spent.

What are the keys …? (continued)

- Increasingly, the HRA/PRA recognizes the importance of HRA qualitative analysis.
- More focus on qualitative analysis is appearing in recent or upcoming HRA/PRA guidance, e.g.,
  - Joint EPRI/NRC-RES Fire HRA guidance (NUREG-1921/EPRI TR 1023001, to be published)
  - ATHEANA (NUREG-1624, Rev. 1)
  - EPRI's HRA Calculator
- This emphasis is supported or based on recent studies such as:
  - "International HRA Empirical Study – Phase 1 Report" (NUREG/IA-0216, Volume 1, 2009)

What are the keys to performing HRA?

An important key to building an understanding of the problem is…

What are the keys to performing HRA?

context.

What are the keys to performing HRA?

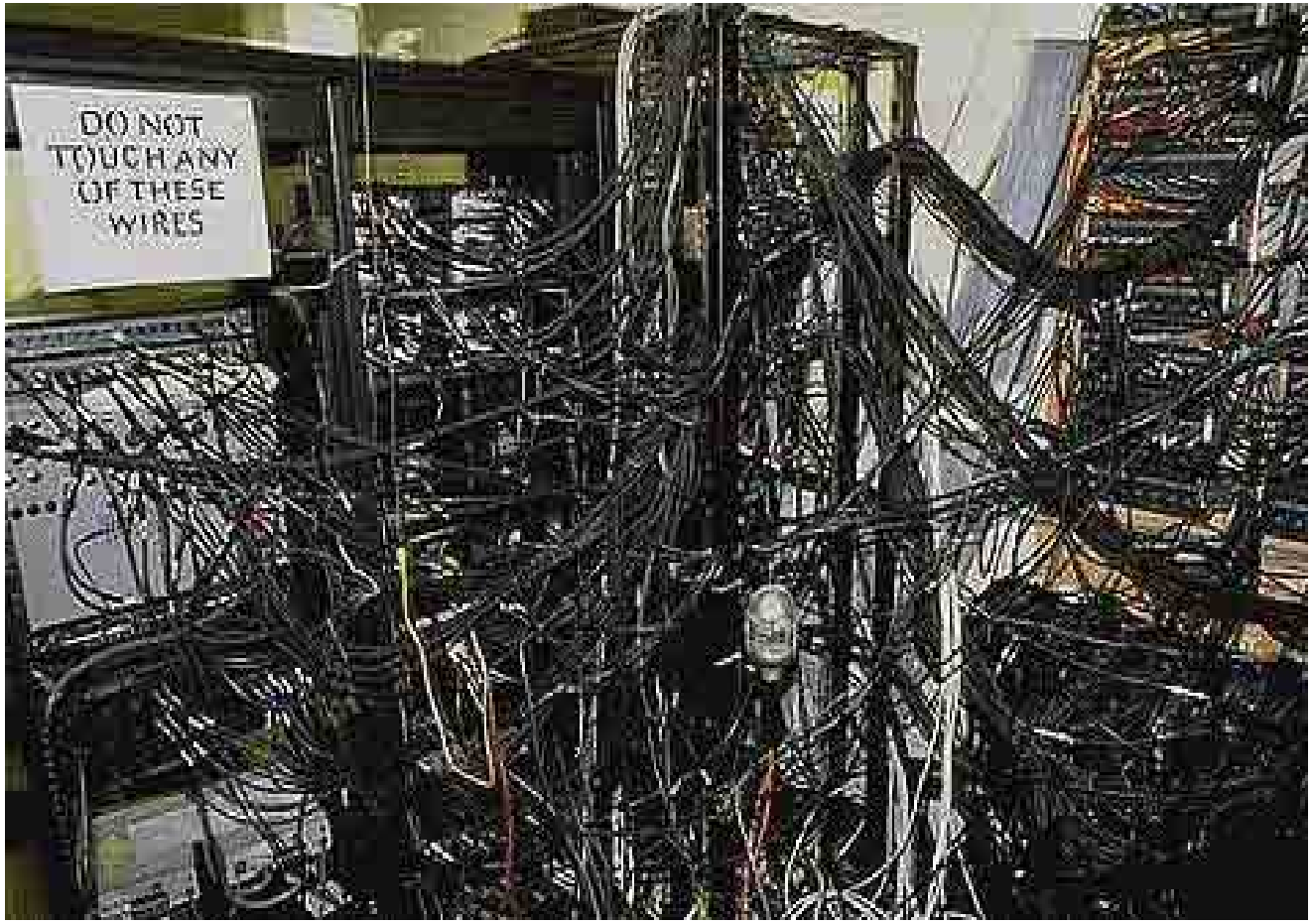
- Context has long been recognized as important, e.g.,
  - SHARP1 (1992) discusses the importance of addressing human interactions for plant-specific and accident sequence-specific scenarios.
- However, a commonly held belief, still evident in popular accounts of incidents and reflected in how some people regard what new technologies ought to accomplish, is:
  - If we could just eliminate the human, we'd never have any problems.
- This corresponds with the so-called "blame culture" or "human-as-a-hazard" view

What are the keys …? (continued)

- Of course, the “human” here is the one on the “sharp end,” i.e., the last one to “touch” any equipment or try to respond to an accident.
- But, humans also are involved in design, planning, inspection, testing, manufacturing, software development, etc., etc., etc.

- Let’s look at some everyday examples of what humans on the “sharp end” have to contend with as a way of understanding the impact of “context” and how we may be “set up” for failure.

What are the keys to performing HRA?



What are the keys to performing HRA?

What are the keys to performing HRA?

What are the keys … HRA? (continued)

- Recent research on human error and human actions involved in serious accidents has contributed to building a new perspective on the role of humans in technology and the role of context.
- Examples of research/researchers include:
  - James Reason, *Human Error*, 1990, *Managing the Risks of Organizational Accidents*, 1997, *The Human Contribution: Unsafe Acts, Accidents and Heroic Recoveries*, 2008.
  - Donald R. Norman, *The Design of Everyday Things*, 1988.
  - E. M. Roth and R.J. Mumaw, *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies*, NUREG/CR-6208, 1994.
  - Others, such as: Eric Hollnagel, David Woods, Micah Endsley

What are the keys …? (continued)

- Some of the key messages from this body of research are:
  - The operator is often "set-up" for failure …
    - …by prior events, pre-existing conditions, failed or misleading information, unusual and unfamiliar plant conditions and configurations, procedures that don't match the situation, and so on.
  - But, he doesn't always fail…
    - …"[E]ven the best [trouble-shooters] have bad days. It is my impression that the very best trouble-shooters get it right about half the time. The rest of us do much worse." (Reason, *The Human Contribution*, page 66)
  - So, he's the "last line of defense" …
    - …after all other previous designs and plans have failed.

What are the keys …? (continued)

<u>Suggestions for some practical exercises on context</u>

1. You want a book off the shelf in your living room. You even go to the living room to get the book. However, after you return to your home office, you discover that you never got the book.
2. You have a doctor's appointment. Despite reminding yourself of the location for the doctor's office while you drive away from home, you end up at your children's school instead.
3. You drive yourself to work every day on the same route, you have a good driving record, and you drive defensively. Somehow, you end up in a collision with another vehicle.

All unlikely, right? Now, think about how the context might "cause" you to make one of these mistakes.

What are the keys …? (continued)

Suggestions for some practical exercises on context

1. In Reason's *Human Error*, the context was an interruption, namely knocking a bunch of books off the shelf. After picking up all the books, you forget why you were there in the first place.
2. I've done this. I got distracted by thinking about a work problem and/or was focused on the radio music. My "automatic pilot" kicked in and, instead of stopping at the doctor's office (~1 mile before the turnoff to the school), I did what I usually do 2x per day – drove to the school.
3. This one is easy (i.e., lot of options for added context).
   - Potential distractions, e.g.: Call coming in on the cell phone, passengers in car (*Bring Your Child to Work Day*?), etc.
   - Added challenges, e.g.: Rain/ice/snow, fogged or iced up windows, road construction.
   - Unexpected equipment problems, e.g.: "Fuel low" light comes on, run out of windshield washer fluid.

Course Outline

- What is HRA?
- Where does HRA fit into PRA?
- What does HRA model?
- Is there a standard for performing HRA?
- What guidance is there for performing HRA?
- What are the keys to performing HRA?
- **How can we understand human error?**
- What are the important features of existing HRA methods?
- What are the HRA concerns or issues for fire PRA?
- Any final questions?

How can we understand human error?

Lesson 1:

How can we understand human error?

Human error is <u>not</u> random.

How can we understand human error?

- But, why does human error seem random?
- Remember our exercise about context?
  - How many different possible contexts would you estimate can influence your everyday life?
  - For the actions typically addressed by HRA, the range of contexts has been constrained to:
    - Existing, licensed and operating nuclear power plants (NPPs)
    - NPP accidents represented in Level 1, at-power, internal events PRA
    - Actions taken by licensed operators
    - Operator actions taken (mostly) in the control room (that has been extensively designed and redesigned, reviewed and re-reviewed)
    - Operator actions that are addressed by Emergency Operating Procedures (EOPs) (that have been validated and demonstrated with decades of experience)
    - Operator actions that are adequately trained
    - Etc., etc., etc.

How can we understand human error?

Lesson 2:

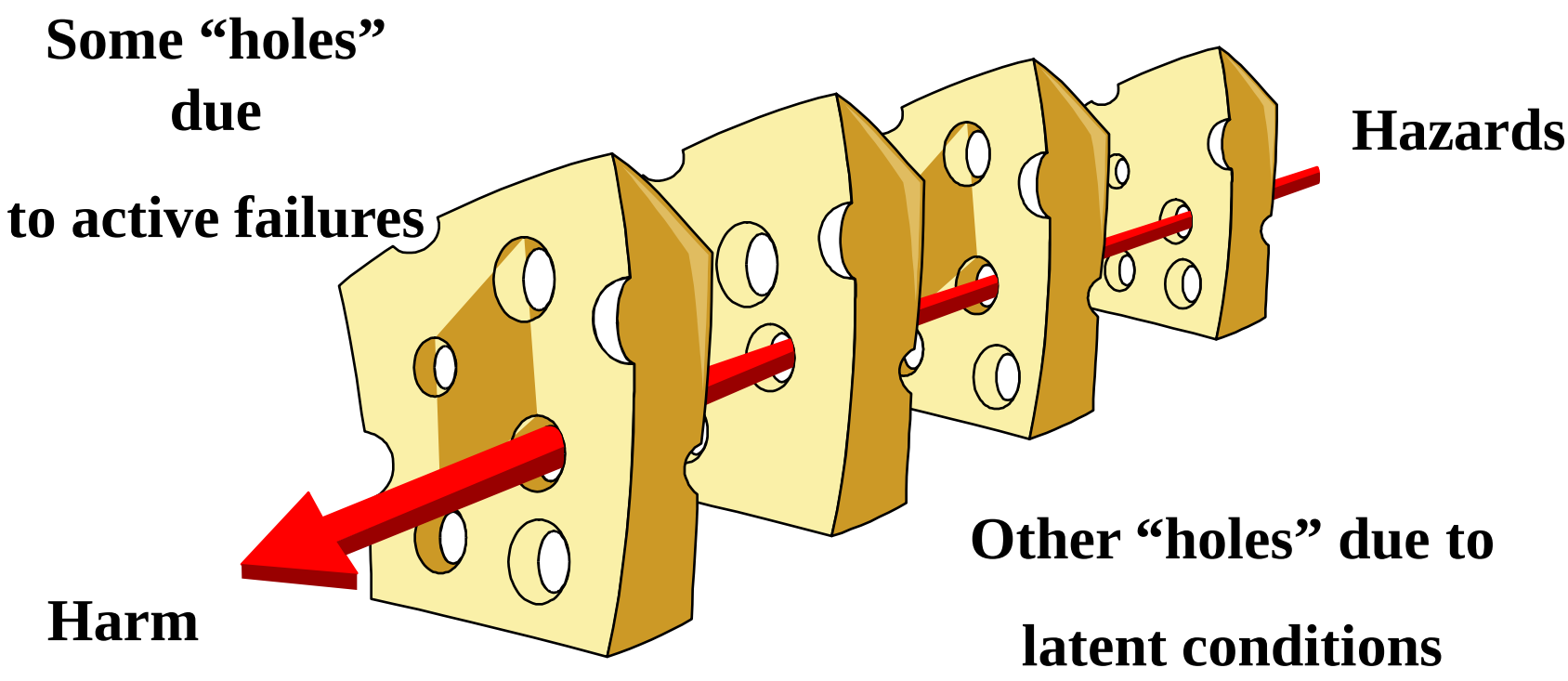
How can we understand human error?

Human error is not the "cause" of a mishap.

How can we understand human error?

- Remember….
  - **The operator is often "set-up" for failure …**
  - **And, the operator is on the "sharp-end" (i.e., simply the last one to touch "the problem").**
- To illustrate this concept, here is Reason's Swiss Cheese model of event causation (1990 and 1997)

The 'Swiss Cheese' Model of Event Causation



Successive layers of defenses, barriers, & safeguards

How can we understand human error?

Lesson 3:

How can we understand human error?

Human error can be predicted.

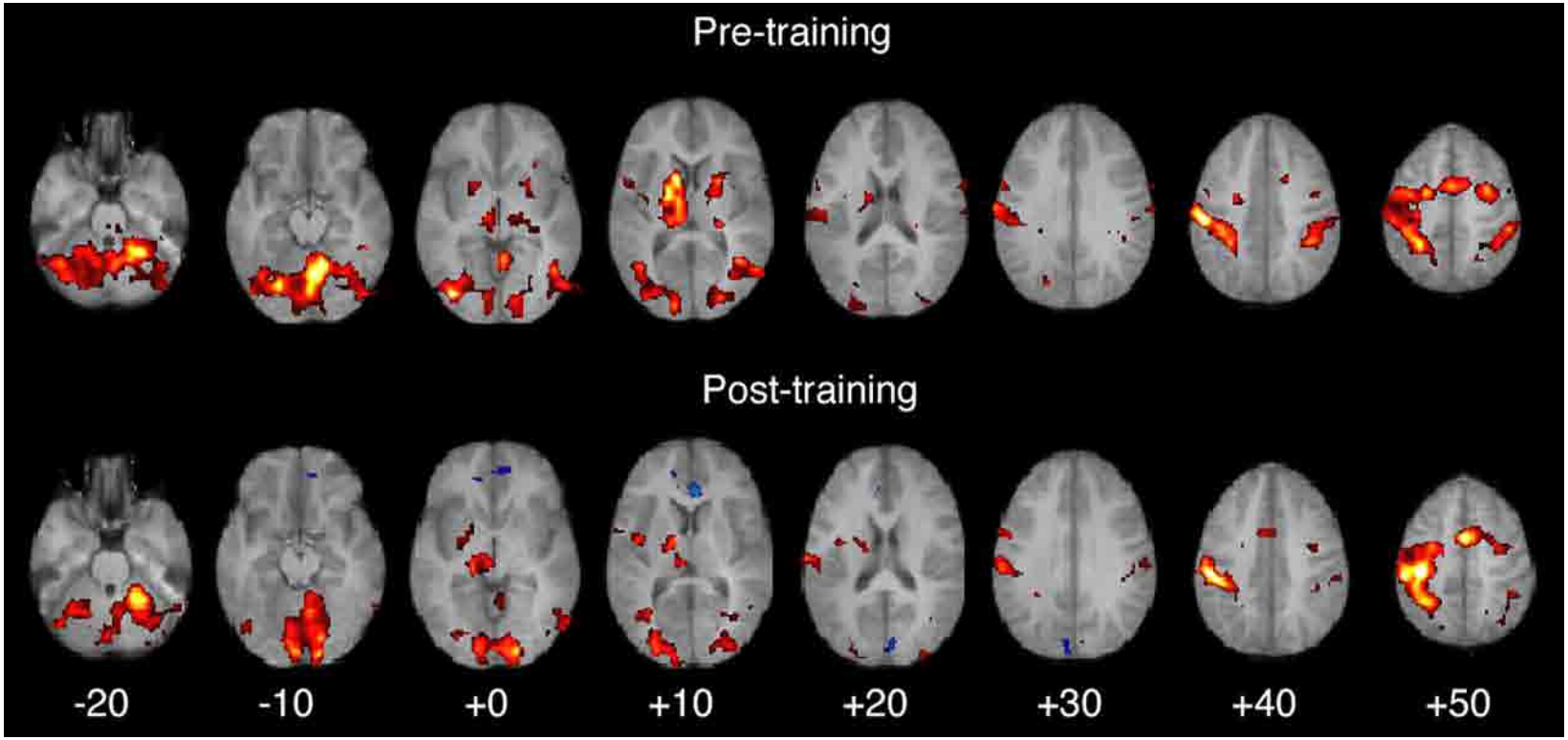
Human error can be predicted because…

- People's behavior is almost always rational
  - adaptive – i.e., goals are achieved
  - satisficing – i.e., best under the circumstances
- People's actions will tend to be
  - practical
    - people do what "works"
  - economical
    - people act so as to conserve resources
- And, in the case of NPPs, we have lots of rules and regulations to follow that are taken seriously; this further constrains likely behaviors and influences that HRA must model.

Human error can be predicted because…

- People follow familiar paths
  - Maximize use of habits (good *and* bad)
  - Minimize 'cognitive strain'
- People use 'rapid pattern-matching' to detect and interpret faults and errors
  - Very effective at detecting most problems, but
  - Not very effective at detecting our own errors
- People also use…
  - "shortcuts, heuristics, and expectation-driven actions."
  - efficiency-thoroughness trade-offs

Practiced actions become ‘automatic’…



…whether we want them to or not.

How can we understand human error?

Lesson 4:

How can we understand human error?

By combining Lessons #1 through #3…

How can we understand human error?

Human errors are not isolated breakdowns, but rather are the result of the same processes that allow a system's normal functioning.

How can we understand human error… for HRA/PRA?

- First, previous PRA studies serve as guides for what types of operator actions are important to include in PRA models, what factors are the most important influences on operator performance, and so on.

- Second, HRA methods are developed principally for operators in NPPs; consequently, some basic understanding and expectations of NPP operator behavior, control room design, procedure use, operator training and education, etc. has been “built-in” the methods.

How can we understand human error… for HRA/PRA? (continued)

- Third, HRA methods attempt to bridge the gap between the real operational experience in NPPs and psychology by:
  - filtering out behaviors, performance influences, and other factors that are not typically important for operator response to accident scenarios modeled in PRAs
  - Providing the HRA analyst with a focused set of issues to address in NPP HRA/PRA
- Fourth, the HRA analyst should perform qualitative HRA tasks (i.e., make plant-specific assessments and observations of operator performance in order to identify which factors or issues are important for the specific plant and study).

How can we understand human error … for HRA/PRA? (continued)

- As part of qualitative analysis, the HRA analyst further develops an understanding and ability to predict operator actions by addressing…
  - The context for the operator action

- The context includes both:
  1. Plant/facility conditions, configuration, and behavior, and
  2. Operator behavior influencing factors (sometimes called "performance shaping factors" (PSFs), performance influencing factors (PIFs), or driving factors)

How can we understand human error … for HRA/PRA? (continued)

- Performance shaping factors usually capture important behavior-influencing aspects of, for example:
  - Time available (often not defined as a PSF, but a **very** important factor)
  - Procedures
  - Operator training
  - Human-machine interfaces
  - Action cues and other indications
  - Crew staffing and organization
  - Crew communication
- The important aspects of these factors can change with the plant/facility, NPP operation, operator action and location, etc.

How can we understand human error… for HRA/PRA? (continued)

- Then, the HRA analyst can match up the results of qualitative HRA with aspects of HRA quantification methods to predict <u>why</u> such potential operator failures might occur, e.g.,
  - Classifications, categories, or types of operator failures:
    - Errors of omission and commission (dependent on the PRA model for definition)
    - Slips/lapses, mistakes, and circumventions
    - Skill-, rule-, and knowledge-based errors
  - Explanations of operator failures using information processing models, e.g.,
    - Failures in detection, situation assessment, response planning, and/or response execution
  - Explanations of operator failures using a filtered set of "causes" (i.e., cause-based models)
  - Explanation of operator failures using performance shaping factors

How can we understand human error… for HRA/PRA? (continued)

- Which approach for explaining operator failure do you use?
  - **Depends** on a variety of factors but, especially, the type of operation or action being modeled.
  - Often helpful to use more than one way of classifying operator failure because different HRA quantification methods…
    - Use different classification and categorization schemes
    - Emphasize different PSFs, driving factors, or other elements of context
    - Represent different types of operator actions, behavior models, and so forth
  - Which approach helps to best explain why the HRA analyst thinks the operator might fail?

How can we understand human error?

- So, it's important for an HRA analyst to do his best to
  - "Understand the problem" by understanding the context, operator actions and potential failures or errors, etc. (i.e., perform some HRA qualitative analysis)
  - Match "the problem" to the HRA method that best represents the critical aspects of "the problem
- In other words, HRA method selection is important and should be done after you have some "understanding of the problem," including the likely operator actions and potential operator failures ("errors").
- In the next presentation topic, we'll summarize some of the important features of existing HRA methods.

Course Outline

- What is HRA?
- Where does HRA fit into PRA?
- What does HRA model?
- Is there a standard for performing HRA?
- What guidance is there for performing HRA?
- What are the keys to performing HRA?
- How can we understand human error?
- **What are the important features of existing HRA methods?**
- What are the HRA concerns or issues for fire PRA?
- Any final questions?

What are the important features of existing HRA methods?

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

What are the important features of existing HRA methods?

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

What are the important features of existing HRA methods?

- Overall, many HRA methods have been developed:
  - THERP (published in 1983) was first; developed to support first nuclear power plant PRA effort (WASH-1400 [1975])
  - Many methods developed in the 1990s to support a growing number of PRA studies (e.g., IPEs)
  - In the 2000s, HRA method development continued with a focus on cognitive/decision-making, e.g.,
    - So-called "second-generation" methods developed to capture advances in behavior and cognitive science
- In general, each HRA method represents (usually, implicitly), <u>as developed</u>:
  1. A perspective on human error (e.g., what performance shaping factors are important), and
  2. A snapshot in time (with respect plant design, operations, etc.).
- <u>As applied</u>, HRA methods have been used to represent human behavior in other timeframes, technologies, etc. – <u>must be cautious though!</u>

What are the important features of existing HRA methods?

- To-date, the principal focus of HRA methods development has been on supporting Level 1, at-power, internal events PRA.
- However, existing HRA methods have been applied to other kinds of problems:
  - Low power and shutdown HRA/PRA for nuclear power plants (e.g., NUREG/CR-6144 and NUREG/CR-6145).
  - NASA PRAs for space shuttle
  - DOE's license application for Yucca Mountain waste repository
- In some cases, these applications have explicitly expanded or adapted existing HRA methods (in recognition that the method is not being applied exactly as intended)
- And, there have been other cases….

THERP: Technique for Human Error Rate Prediction (NUREG/CR-1278, 1983)

- This is the most extensively documented and the most widely used (and misused) HRA technique. The handbook has four main sections:
  - Basic concepts.
  - Method for analysis and quantification of human performance.
  - Human performance models and HEPs.
  - Tables of HEPs and examples.

- Simplified version developed as “Accident Sequence Evaluation Program Human Reliability Analysis Procedure” in NUREG/CR-4772, 1987
  - Referred to as “ASEP”

THERP (continued)

- THERP:
  - Is applicable to pre- and post-initiator HFEs
  - Provides a cognitive model based on time reliability correlations
- THERP models **execution errors** using task analysis, e.g.,
  - Tasks are reviewed to identify critical steps
  - Each critical step has two failure modes
    - Error of omission
    - Errors of commission
  - HFE can be represented in a HRA event tree
- THERP provides human error probabilities in Chapter 20 tables
  - Intended to be assigned as "branch" probabilities in HRA event tree
  - Limited number of PSFs used to adjust HEPs
  - Recovery and dependencies are addressed

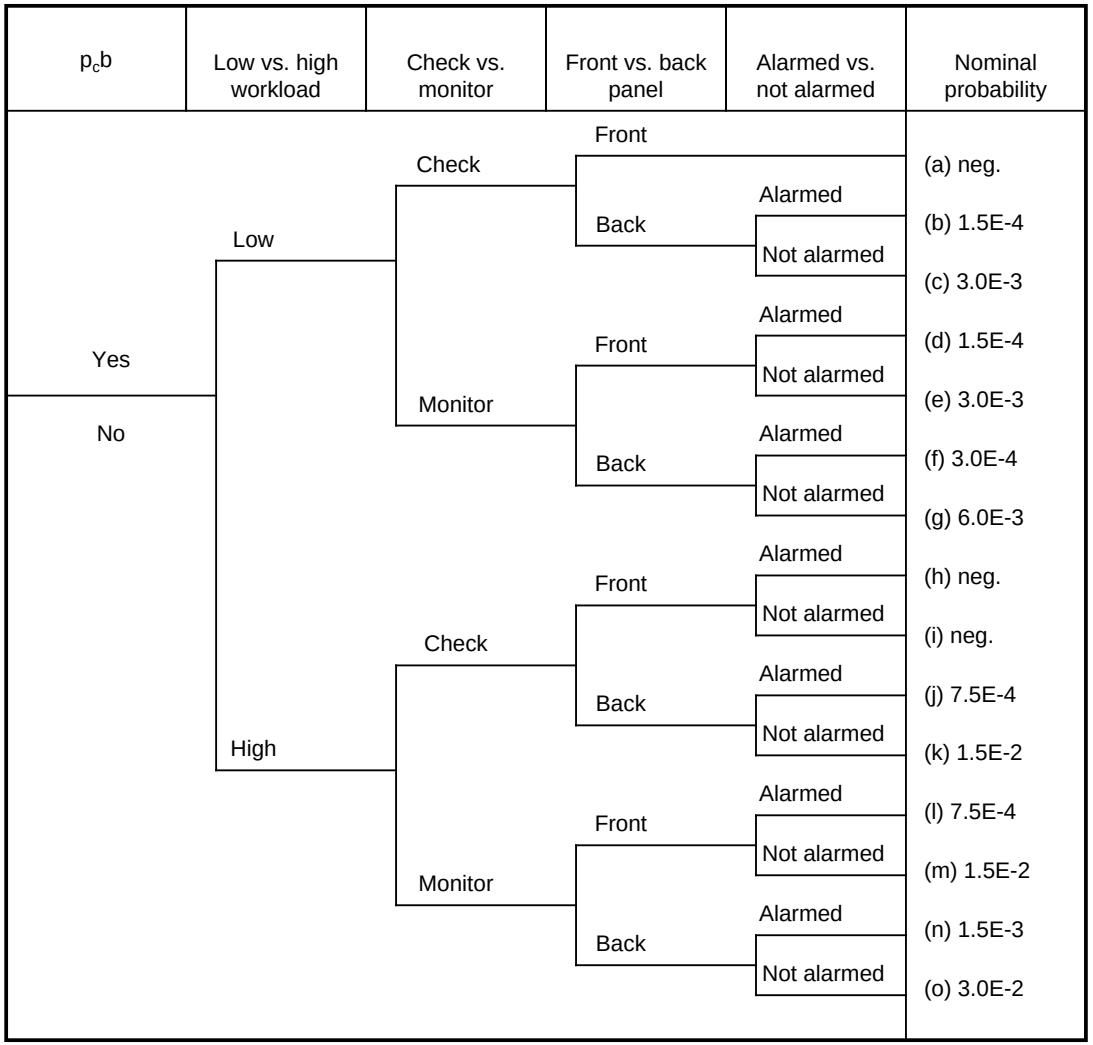
Cause-Based Decision Tree (CBDT) Method (EPRI)

- CBDT consists of a series of 8 decision trees to address potential causes of errors, produces HEPs based on those decisions.
- Four (i.e., half) of the decision trees involve the man-machine cue interface:
  - Availability of relevant indications (location, accuracy, reliability of indications)
  - Attention to indications (workload, monitoring requirements, relevant alarms)
  - Data errors (location on panel, quality of display, interpersonal communications)
  - Misleading data (cues may not match procedure, need for training in cue recognition, etc.)

CBDT (continued)

- Another four decision trees involve the man-procedure interface:
  - Procedure format (visibility and salience of instructions, place-keeping aids)
  - Instructional clarity (standardized vocabulary, completeness of information, training provided)
  - Instructional complexity (e.g., avoid use of "not" statements, complex use of terms such as "and," "or," etc.)
  - Potential for deliberate violations (unquestioning belief in instructional adequacy, lack of awareness of availability and consequences of alternatives, etc.)
- For time-critical actions, the CBDT is supplemented by a time-reliability correlation (TRC)

Example CBDT decision-tree: data not attended to



EPRI HRA Calculator

- Software tool
- Uses SHARP1 as the HRA framework/HRA process (EPRI TR-100259)
- Post-initiator HFE methods:
  - For diagnosis, uses CBDT (decision trees) and/or HCR/ORE (time based correlation)
  - For execution, THERP for manipulation
- Pre-initiator HFE methods:
  - Uses THERP and ASEP to quantify pre-initiator HFEs

ATHEANA – NUREG-1624, Rev. 1 and NUREG-1880

- Provides an HRA process, an approach for identifying and defining HFEs (especially for EOCs), an HRA quantification method, and a knowledge-base (including analyzed events and psychological literature)
- Provides a structured search for problem scenarios and unsafe actions
- Focuses on the error-forcing context
- Uses the knowledge of domain experts (e.g., operators, pilots, operator trainers)

ATHEANA – NUREG-1624, Rev. 1 and NUREG-1880 (continued)

- Links plant conditions, performance shaping factors (PSFs) and human error mechanisms
- Consideration of dependencies across scenarios
- Attempts to address PSFs holistically (considers potential interactions)
- Structured search for problem scenarios and unsafe actions
- Developed by the USNRC:
  - NUREG-1624, Rev.1 was published first (2000) and is more detailed
  - NUREG-1880 was published later (2007), is a user's guide, and contains the full, expert elicitation quantification approach

Course Outline

- What is HRA?
- Where does HRA fit into PRA?
- What does HRA model?
- Is there a standard for performing HRA?
- What guidance is there for performing HRA?
- What are the keys to performing HRA?
- How can we understand human error?
- What are the important features of existing HRA methods?
- **What are the HRA concerns or issues for fire PRA?**
- Any final questions?

What are the HRA concerns or issues for fire PRA?

What are the HRA concerns or issues for fire PRA?

- Actually, there are some different issues for HRA to address in fire PRA, such as:
  - New HFEs to identify, e.g.,
    - Fire response operator actions in fire procedures
  - Errors of Commission (EOCs) to identify and define, e.g.,
    - Per the Standard, the possibility that operators respond to spurious indications as if they are “real” must be considered.
    - Is there a way to limit the number of EOCs modeled in the fire PRA?
  - New environmental hazards to model as performance shaping factors (PSFs), e.g.:
    - Fire effects of smoke, heat, and toxic gases on operators
    - Impact of breathing apparatus and protective gear on operator performance, including communications
  - More challenging contexts, e.g.,
    - Potentially wide variations in size, location, and duration of fires and their effects on plant systems and functions

What are the HRA concerns or issues for fire PRA?

- Some different issues for fire HRA: (continued)
  - Different types of decisions, e.g.,
    - Operator judgment on whether to abandon the control room
  - Other PSFs or influencing factors, e.g.,
    - Design of ex-control room equipment control locations and alternate shutdown panels

- But, this, and more, will be addressed in the Fire HRA track, starting tomorrow.

Course Outline

- What is HRA?
- Where does HRA fit into PRA?
- What does HRA model?
- Is there a standard for performing HRA?
- What guidance is there for performing HRA?
- What are the keys to performing HRA?
- How can we understand human error?
- What are the important features of existing HRA methods?
- What are the HRA concerns or issues for fire PRA?
- **Any final questions?**

Backup slides

Simple Example of HRA Application – Using SPAR-H

- In order to get a idea of how HRA is performed, let's talk about a simple HRA example.
- First, we'll give a little background on the HRA method used, SPAR-H
- Then, we'll discuss the example.

SPAR-H

- Simplified methodology used by the NRC in SPAR models
  - Divides human error probability into two parts:
  - Diagnosis, and
  - Action
  - Allows consideration of dependencies between actions
  - Based on concept of basic human error probability (i.e., nominal error probability) influenced by performance shaping factors

SPAR-H: Performance Shaping Factors

- Performance Shaping Factor (PSF):
  - *A factor that influences human error probabilities as considered in a PRA's human reliability analysis and includes such items as level of training, quality/availability of procedural guidance, time available to perform an action, etc*. (Ref. ASME/ANS RA-Sa-2009)
- SPAR-H Performance Shaping Factors:
  1. Available Time
  2. Stress
  3. Complexity
  4. Experience/Training
  5. Procedures
  6. Ergonomics
  7. Fitness for Duty
  8. Work Processes

SPAR-H: How to compute HEPs

- Diagnosis and Action error probabilities based on factors that quantitatively address each PSF

$P_{diagnosis} = BHEP_{diag} * F_{Avail.Time} * F_{Stress} * F_{Complexity} * F_{Exp./Training} * F_{Proc} * F_{Ergonomics} * F_{FFD} * F_{Work\ Proc.}$

$P_{action} = BHEP_{action} * F_{Avail.Time} * F_{Stress} * F_{Complexity} * F_{Exp./Training} * F_{Proc} * F_{Ergonomics} * F_{FFD} * F_{Work\ Proc.}$

Where:

  - $BHEP_{diag} = 0.01 = 1E\text{-}2$
  - $BHEP_{action} = 0.001 = 1E\text{-}3$

- Total Human Error Probability is the sum of the diagnosis and action error probabilities, i.e.,

$$P_{Total} = P_{diagnosis} + P_{action}$$

Example of How to Assess SPAR-H PSF: Available Time for Diagnosis

- Available time refers to the amount of time that an operator or a crew has to diagnose an abnormal event
- A shortage of time can affect the operator's ability to think clearly and consider alternatives
  - Definitions:
  - Inadequate time - P (failure) = 1.0 - If the operator cannot diagnose the problem in the amount of time available, no matter what s/he does, then failure is certain
  - Barely adequate time (x 10) - 2/3 the average time required to diagnose the problem is available
  - Nominal time (x 1) - on average, there is sufficient time to diagnose the problem
  - Extra time (x 0.1) - time available is between one to two times greater than the nominal time required, and is also greater than 30 minutes
  - Expansive time (x 0.01) - time available is greater than two times the nominal time required and is also greater than a minimum time of 30 minutes; there is an inordinate amount of time (a day or more) to diagnose the problem.

SPAR-H Example: Development of HEP for SI/CS Recirculation

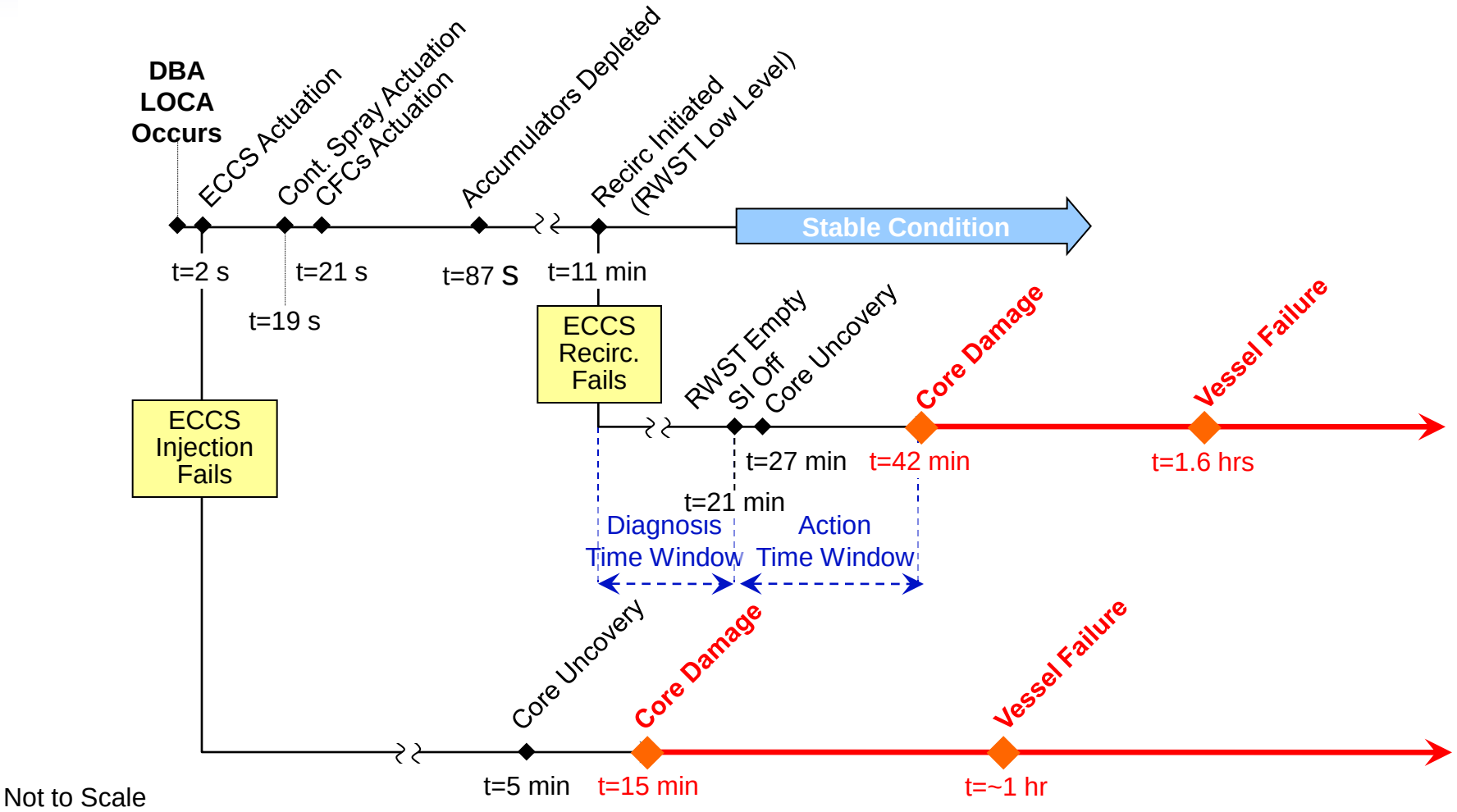
Alignment of SI/CS Recirculation

- Entry Condition:
  - Low RWST level
- Caution:
  - Steps must be performed without delay
- Key Steps:
  - Start CW cooling to SI Heat Exchanger
  - Check sump level
  - Open containment sump valves
  - Close RWST valve

Boundary Conditions – SI/CS Recirc

- Well trained, proceduralized operator action
- Pumps will trip on Low-low RWST level
- Cue for Action: Low RWST level alarm
  - Time window for diagnosis:
  - Time to low RWST level – time to low-low RWST level
  - Time window for action:
  - Time to core damage – time to low-low RWST level

Large LOCA Timelines (One Division Injecting)



Not to Scale

SPAR-H DIAGNOSIS WORKSHEET

Human Action: Operator fails to align SI/CS for Recirculation from the Containment Sump

Diagnosis HEP = 5.00E-04

PSFs	PSF Levels	Multiplier for Diagnosis		If non-nominal PSF levels are selected, please note specific reasons in this column
1. Available Time	Inadequate[a]	1.0		
	Barely adequate ≈2/3 x nominal	10		
	Nominal time	**1**	x	
	Extra time (between 1 and 2 x nominal and > than 30 min)	0.1		
	Expansive (> 2 x nominal and > 30 min)	0.01		
2. Stress	Extreme	5		Occurrence of "the" design basis event is expected to elevate stress levels. At this point there is no threat to personnel safety so "High" is selected.
	High	**2**	X	
	Nominal	1		
3. Complexity	Highly	5		Symptoms of a LOCA are obvious and well known.
	Moderately	2		
	Nominal	1		
	Obvious diagnosis	**0.1**	x	
4. Experience/Training	Low	10		Design basis LOCAs are integral part of operator training.
	Nominal	1		
	High	**0.5**	x	
5. Procedures	Not available	50		Procedures are clear and designed for such scenarios.
	Incomplete	20		
	Available, but poor	5		
	Nominal	1		
	Diagnostic/symptom oriented	**0.5**	X	
6. Ergonomics	Missing/Misleading	50		
	Poor	10		
	Nominal	**1**	X	
	Good	0.5		
7. Fitness for Duty	Unfit[a]	1.0		
	Degraded Fitness	5		
	Nominal	**1**	X	
8. Work Processes	Poor	2		
	Nominal	**1**	X	
	Good	0.8		

a - Total failure probability = 1.0, regardless of other PSFs

SPAR-H ACTION WORKSHEET

Human Action: Operator fails to align SI/CS for Recirculation from the Containment Sump

Action HEP = 1.00E-04

PSFs	PSF Levels	Multiplier for Diagnosis		If non-nominal PSF levels are selected, please note specific reasons in this column
1. Available Time	Inadequate[a]	1.0		Action itself is very quick: opening of a valve. Given the 17 minutes available, this is ample time.
	Time available ≈ time required	10		
	Nominal	1		
	Available > 5x time required	**0.1**	X	
	Available > 50x time required	0.01		
2. Stress	Extreme	5		Occurrence of "the" design basis event is expected to elevate stress levels. At this point there is no threat to personnel safety so "High" is selected.
	High	**2**	X	
	Nominal	1		
3. Complexity	Highly	5		
	Moderately	2		
	Nominal	**1**	X	
4. Experience/Training	Low	3		Design basis LOCAs are integral part of operator training.
	Nominal	1		
	High	**0.5**	X	
5. Procedures	Not available	50		
	Incomplete	20		
	Available, but poor	5		
	Nominal	**1**	X	
6. Ergonomics	Missing/Misleading	50		
	Poor	10		
	Nominal	**1**	X	
	Good	0.5		
7. Fitness for Duty	Unfit[a]	1.0		
	Degraded Fitness	5		
	Nominal	**1**	X	
8. Work Processes	Poor	2		
	Nominal	**1**	X	
	Good	0.5		

a - Total failure probability = 1.0, regardless of other PSFs

Diagnosis HEP =	5.00E-04
Action HEP =	1.00E-04
Total HEP =	6.00E-04