Facility Team Training: Human Reliability Analysis in the PCSA

Preclosure safety analysis

28 February 2007

Topics Covered

- Purpose
- The Definition of "Human Failure Event" (HFE)
- General Approach
- Defining the Scope
- Defining the Base Case Scenario
- Identifying and Defining HFE of Concern
- Performing the Screening Analysis
- Identifying Potential Vulnerabilities
- Identifying HFE Scenarios
- Quantifying Probabilities of HFE
- Incorporating HFE into PCSA
- Special Topic: Recovery Analysis
- HFE Naming

Purpose

- The purpose of this training is to give detailed guidance to the task leaders on those aspects of the HRA that they will be responsible for performing.

The Definition of "Human Failure Event"

- Human Failure Event (HFE) - A basic event included in a fault tree or event tree that represents the human action, which results in the failure of a safety function, system, or component modeled in the PCSA.
- HFEs may contain multiple human actions, or human actions in combination with other failures, in a logic model that is quantified to get the overall probability of the HFE.
- "Human Error" is not a preferred term in current HRA.

YMP PCSA General Approach

- The HRA task will be conducted through a series of sub-tasks.
- Either the Facility Team or the HRA Team will be the lead for each sub-task and responsible for its completion.
- Regardless of which team leads a sub-task, it will be completed with support from the other team.
- Support from Operations will be obtained for those tasks where it is appropriate.

YMP PCSA General Approach

- Define the scope of analysis. (Facility Team)
- Describe the base case scenarios. (Facility Team w/ Operations support)
- Identify and define human failure events of concern. (Facility Team w/ Operations support)
- Perform screening analysis. (HRA Team)
- Identify potential vulnerabilities. (Facility Team w/ Operations support)
- Search for HFE scenarios (i.e., scenarios of concern). (Facility Team w/ Operations support)
- Quantify probabilities of human failure events. (HRA Team)
- Incorporate human failure events into the PCSA. (Facility Team)
- Evaluation of HRA/PCSA results. (HRA Lead)

Define the Scope of the Analysis

- Define the facility and its boundaries.
- Define the operations within the facility that will be considered within the HRA.
  - It is useful to break up the operations into various operational phases, for example;
    - Movement of rail cask from facility boundary to entrance vestibule.
    - Movement of cask from entrance vestibule to transfer cell.

Define the Scope of the Analysis

- Certain operations may be excluded from the scope, for example;
  - Movement of empty waste package from facility boundary to entrance vestibule
  - Such operations may be excluded because it is determined they are not risk significant
- List key assumptions that will be used in the HRA (see next slides)

Assumptions (Absolute)

- Malevolent Behavior Excluded
- Plant Personnel Always Acting in Perceived Best Interests of the Plant
  - Covers all Intentional Deviations from Processes and Procedures
  - Staff Believe Their Actions to be More Efficient or More Effective

Assumptions (Apply When Valid)

- Base assumptions
  - operating under normal conditions
  - plant will be designed to the highest quality human factors specifications
  - the operator does not need to wear protective clothing
  - licensed, qualified plant personnel
  - environment in the plant is not adverse
- Evaluate whether or not each of these applies. If not, say so and why.

Define the Scope of the Analysis

- Define the state of the design and operational information that will form the basis for the HRA
  - What YMP documents will be used as reference for the HRA?
  - What non-YMP documents and information will be used as reference for the HRA (see next slide)

Assumptions (Design/Operation)

- It is perfectly reasonable to assume for the purpose of the PCSA that the equipment design and operational characteristics that will exist at GROA facilities once they are built and operating (including crew structures, training, and interactions), is adequately represented by comparable, currently operating facilities.
  - NPP with ISFSI
  - Army Chemical Demilitarization Plants
  - Others handling/disposing large hazmat

Define the Base Case Scenario

- For each of the phases of operation considered, provide a step-by-step description of what should happen when the operation is conducted correctly.

Define the Base Case Scenario

- Include any specific assumptions
  - Operating team characteristics
  - Operation and design characteristics
  - Formal rule and procedures
  - Operator tendencies and informal rules
  - Operator expectations

Define the Base Case Scenario

- Example: Cask Movement from Preparation Area to the Transfer Pit
- Describe the Operational Phase
  - In this process the canister (MPC) has been completely prepared, the lid has been welded in place, and the top of the transfer cask has been bolted on. This phase starts at the point where the scaffolding is to be removed from around the cask. It continues through the change of the transfer lid and the movement of the cask to the transfer pit on top of the storage cask, but ends prior to the removal of the short stays and attachment of the long stays.

MPC Multi purpose container

Define the Base Case Scenario

- List Initial Conditions
  - The transfer cask is sitting properly in the preparation area of the refueling floor.
  - The canister (MPC) lid is properly welded to the MPC.
  - The MPC drying/inerting process is complete.
  - The yoke is still attached to the crane.
  - The short stays have not been attached to the yoke or the transfer cask.
  - The welding scaffolding is properly configured around the transfer cask.

Define the Base Case Scenario

- Describe Each of the Process Steps – Focus on Human Actions

Remove Scaffolding from Around Transfer Cask – In succession, each scaffolding section is removed from around the cask. For each section, the crane operator will move the crane in order to be able to attach to the scaffolding. Maintenance workers attach each scaffolding section to the yoke. The operator moves each scaffolding section out of the way. The workers unhook the scaffolding section from the yoke.

A single operator is stationed on the crane. The crane will be operated in a manual mode, with visual cues being used to position the crane at each scaffold section so that the maintenance workers can attach the section. Approximately two or three workers will be in the vicinity of the scaffolding, and one of them will be in communication with the crane operator through hand signals to provide guidance on positioning the crane. Once the crane is in position, the workers will attach the crane to the scaffolding. The crane operator will move the scaffolding to an out-of-the-way location on the refueling floor. He will use a combination of his own visual observation and direction from the communicating worker. The other workers have no specific assignment during this movement. Precise placement of the scaffolding sections away from the cask is not required. Once set down, the workers will release the crane from the scaffolding, and the process will repeat until all sections are moved.

Define the Base Case Scenario

- Continue until each process step is described
  - Connect short stays to yoke and to canister (MPC) lid.
  - Connect yoke to transfer cask trunnions.
  - Move transfer cask to transfer skid.
  - Unbolt lower transfer cask lid.
  - Place transfer cask on transfer lid.
  - Bolt transfer cask to transfer lid.
  - Move transfer cask from refueling floor to transfer pit.

Identify and Define Human Failure Events of Concern

- Specify high-level HFE that can occur during each of the process steps. At this point, the details of the potential causes of the HFE and the vulnerabilities that can lead to the HFE are not fully developed.
- The identification process should cover the broad range of HFE (see next slide).

Identify and Define Human Failure Events of Concern

- HFE considerations include:
  - Time phases of HFE (when in the course of an event sequence does the error occur)
  - Error Mode of HFE (both errors of omission and errors of commission)
  - Behavior Type Associated with HFE (the occurrence of slips, lapses, and mistakes)

Time Phases of HFEs Considered

- Pre-initiator HFE
- Initiator HFE
- Post-initiator HFE
  - Non-recovery post-initiator HFE
  - Recovery post-initiator HFE (not identified at this time)

Pre-initiator HFE

- A HFE that represents actions taken before the initiating event and results in the unavailability of equipment or system that is not discovered until it is demanded during response to the initiator.
- Incorporated in system fault trees.

Initiator HFE

- A HFE that represents actions that cause or lead to an initiating event.
- Incorporated in initiating event models.

Non-Recovery Post-Initiator HFE

- A post-initiator HFE that represents operator failure to perform required proceduralized actions with front-line equipment in responding to an initiator that is the result of failure in diagnosis or implementation.
- Incorporated into event trees or top logic.

Recovery Post-Initiator HFE

- A post-initiator HFE that represents operator failures to manually actuate or manipulate front-line equipment that has failed to automatically actuate or alternatives to frontline equipment, as required.
- Adjoined to cutsets after quantification.
- Not identified prior to screening.

Error Modes Considered

- Error of Omission (EOO) - A human failure event that represents the failure to perform one or more actions that should have been taken and that then leads to an unchanged or inappropriately changed configuration with the consequences of a degraded state. Examples include the failure of an operator to initiate a required safety system or failure to actuate a component during performance of an operational task.
- Error of Commission (EOC) - A human failure event that represents one or more actions that are performed incorrectly or some other action(s) that is performed instead. It results from an overt, unsafe action that, when taken, leads to a change in configuration with the consequence of a degraded state. Examples include the inappropriate termination of a necessary safety function or an initiation of an inappropriate system or function.

Slips/Lapses and Mistakes

- Slip/Lapses - An action performed where the outcome of the action was not as intended due to some failure in execution. Slips are errors that result from attentional failures while lapses are errors that result from failures in memory recall.
- Mistake - An action performed as intended, but the intention is wrong. Mistakes are typically failures in activities performed in monitoring (especially deciding what to monitor and how frequently to monitor), situation assessment, or response planning.
- "If the intention is not appropriate, this is a mistake. If the action is not what what was intended, this is a slip." [Norman, 1983]

Identify and Define Human Failure Events of Concern

- HFE during movement of transfer cask from preparation area to transfer pit.
  - Operator topples cask during scaffold movement.
  - Operator drops cask during lowering into transfer pit.
  - Operator improperly sets up crane rigging following maintenance
  - Exposure due to operator failure to monitor for radiation after cask drop into transfer pit

Identify and **Define** Human Failure Events of Concern

- Operator topples cask during scaffold movement.
  - The cask falls on its side while the crane operator is moving the scaffolding away from the sides of the cask.
  - This is a human-induced initiating event.
  - This can occur either as the result of errors during movement of the crane (error of commission, slip) or because the crane was not properly disengaged from the cask prior to moving the scaffolding (error of omission, slip/lapse).

Perform Screening Analysis

- At this point in the HRA, the Facility Team will provide the HRA team with the information developed and then meet with them for discussions.
- The HRA team will select and document screening HEP values and work with the Facility Team to screen the HFE.

Identify Potential Vulnerabilities

- Identify vulnerabilities to human failure for each operational phase.
- These are those aspects of the human action that could contribute to a human failure.
- These may apply to a specific action, a specific operational phase, or all operational phases.

Performance Influencing Factors

- Vulnerabilities are quite often associated with performance influencing factors (PIF)
  - Design of procedures and/or training
  - Job aids (e.g., special tools, remote cameras, binoculars)
  - Time pressure

Performance Influencing Factors

- Environmental conditions (e.g., noise, temperature extremes, protective clothing)
- Prevention devices (e.g., limit switches, interlocks, mechanical stops)
- Warning devices (e.g., alarms)
- Task challenge (i.e., level of stimulation and interest)
- Oversight/feedback (i.e., level of teamwork)

Identify Potential Vulnerabilities

- Performance influencing factors are general and always exist.
- Vulnerabilities are the specific negative manifestations of these PIF as they relate to the HFE being evaluated.
- Vulnerabilities need to be identified and documented for the HRA.

Identify Potential Vulnerabilities

- Vulnerabilities can be grouped, identified, and described generically at a high level when they may apply to multiple HFE.
- Ultimately, which of these generic vulnerabilities apply to each HFE needs to be specified.

Identify Potential Vulnerabilities

- Examples of High Level Definitions:
  - *Limited Nature of Procedures* – Spent fuel operations are not highly proceduralized, but depend primarily on skills learned and additional training experiences. The vast majority of the activities do not use written procedures at all, and with few exceptions even those that include procedures do not have any formal checklists or verbal confirmation requirements spelled out.
  - *Communication Difficulties* – Hand signals are also used by members of the team to communicate, but there is no guarantee that the intended recipient will see these signals (or even be looking for them). There may be quite a bit of difficulty in getting their attention in a timely fashion. Signals may also be interpreted improperly, especially given that there does not appear to be a firmly established convention for the meaning of all the signals.
  - *Limited Indicators and Job Aids* – Compared to the control panel and local indicators and other job aids that are common in the power plant operations, those that exist in spent fuel operations are quite limited. Processes are controlled by visual cues.
  - *Visual Challenges* – The crane operator needs to lean out over the crane bridge, and the view of an operation is essentially only from directly above. Many of the potential errors that could occur are related to vertical position, which cannot be determined from above. In addition, even the view from above may be obstructed. Thus, the operator is often put in the position of being the hands for someone else's eyes.
  - *Unchallenging Activities* – The activities involved in spent fuel handling are, in general, quite simple in nature. In addition, the speed of the movements is quite slow, so each action takes a long time to complete. Basically, this is mostly boring work. There is ample opportunity for diversion and distraction, and an air of informality and complacency can easily exist within and amongst the team members.

Identify Potential Vulnerabilities

- Example of Specific HFE Vulnerabilities – Cask Drop During Scaffold Movement:
  - *Limited Nature of Procedures* – There are no written procedures for this operation. Training consists of a video.
  - *Communication Difficulties* – If the maintenance workers notice a problem, they will need to get the attention of the crane operator. They will not have the convenience of communication headsets, so they will need to yell or attract the operator with hand signals. There is quite a bit of noise in the area, so voices may not be heard. Hand signals are unlikely to be noticed unless the workers can determine where the operator is looking and can get in his line of sight.
  - *Visual Challenges* – The operator will have a slightly obstructed view from his location on the crane bridge to the scaffolding and cask below. In addition, his focus will tend to be ahead of the scaffolding rather than directly at it, to be sure that the path is clear of personnel and obstructions.

Search for HFE Scenarios

- For unscreened HFE, construct specific scenarios that can lead to the occurrence of the HFE.
- "HAZOP-like" thought process.
- Establish the "error forcing context"
  - Include relevant equipment conditions
  - Consider human factors concerns (e.g., vulnerabilities as performance influencing factors)

Search for HFE Scenarios

- HFE includes all the aspects of the failure, including (as necessary) equipment failures that enable or influence the HFE.
- HFE models can be very simple (e.g., "anded" contributors) or more involved (e.g. "and/or" combinations of contributors)

Search for HFE Scenarios

- Operator Topples Cask During Scaffold Movement
  - Operator fails to completely clear scaffolding from cask **AND**
  - Scaffolding hooks on cask **AND**
  - Operator fails to notice that cask is being pulled over **AND**
  - Operator does not responds to warning from workers
- Operator Leaves Canister Lid Ajar
  - Operator fails to align canister lid over canister **AND**
  - Lid fails to properly seat **AND**
  - Maintenance workers fail to notice lid not in place **AND**
  - Radiation levels are not properly monitored **OR** radiation monitors fail **OR** warning of high radiation is not acknowledged

Search for HFE Scenarios

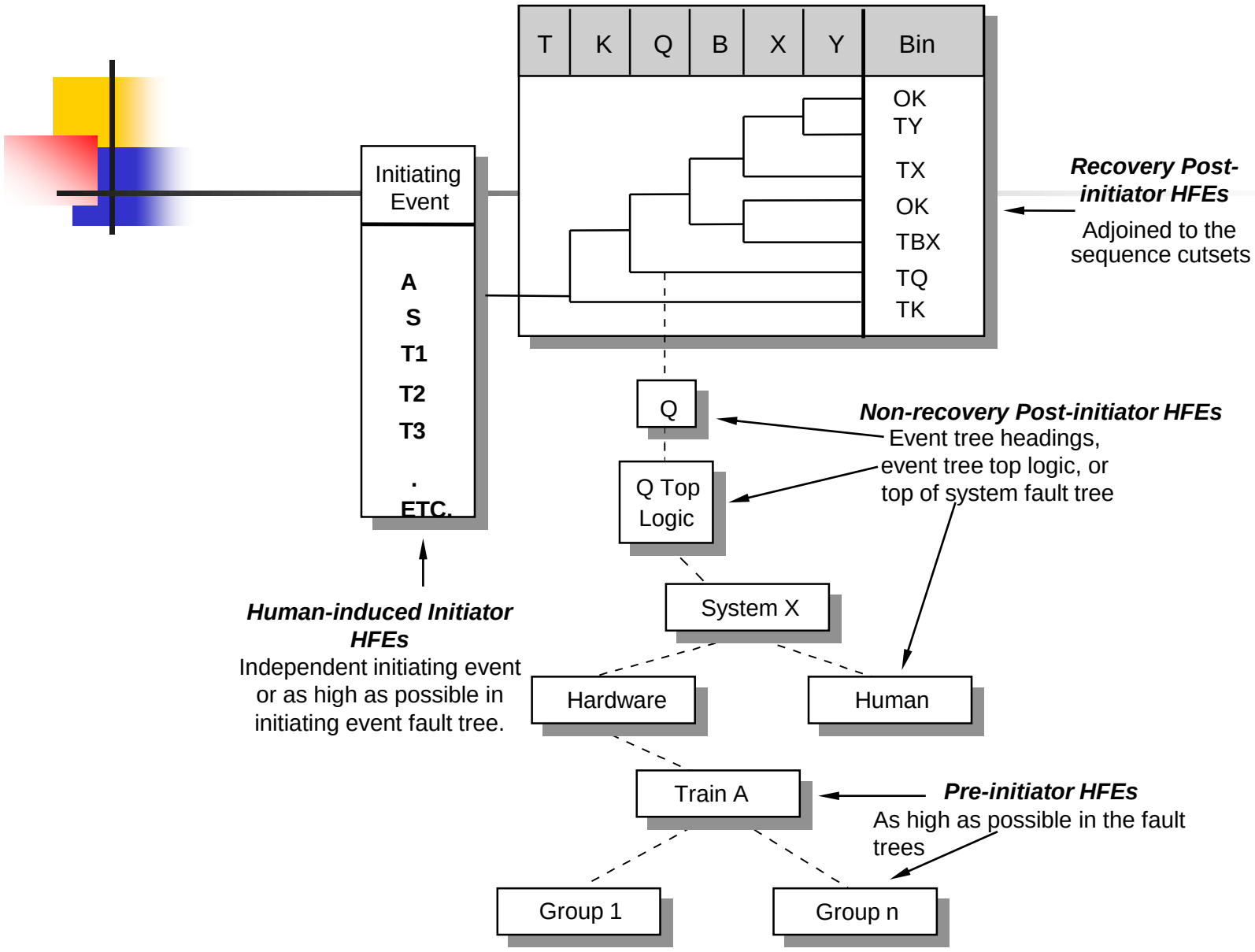
- Operator Topples Cask During Scaffold Movement
  - *Operator fails to completely clear scaffolding from cask* – Before moving each scaffolding section to its storage location, the operator needs to lift it slightly off the floor and move it directly away from the cask. The operator fails to do this properly, leaving the scaffolding in a position where it can hook on the cask as it is moved across the floor.
  - *Scaffolding hooks on cask* - If the scaffolding is not sufficiently cleared from the cask, it will impact the cask as the operator moves the scaffolding to its final location. It may simply bounce of the side of the cask, or it may hook on the cask and begin to pull it over.
  - *Operator fails to notice that cask is being pulled over* - The operator will have a slightly obstructed view from his location on the crane bridge to the scaffolding and cask below. In addition, his focus will tend to be ahead of the scaffolding rather than directly at it, to be sure that the path is clear of personnel and obstructions.
  - *Operator does not responds to warning from workers* - The maintenance workers will be observing the movement of the scaffolding in preparation for unhooking it from the crane when it reaches its destination, so they will almost assuredly notice that it has hooked the cask. They will need to get the attention of the crane operator. They will not have the convenience of communication headsets, so they will need to yell or attract the operator with hand signals. There is quite a bit of noise in the area, so voices may not be heard. Hand signals are unlikely to be noticed unless the workers can determine where the operator is looking and can get in his line of sight.
  - Scenario-specific vulnerabilities
    - Lack of visual cues for crane operator
    - Communication deficiencies

Quantify Probabilities of HFE

- At this point in the HRA, the Facility Team will provide the HRA Team with the information developed and then meet with them for discussions.
- The HRA Team will select the quantification method, work with the Facility Team to create the HFE model (obtaining equipment failure probabilities as needed), and quantify and document the HEP values.

Incorporate HFE into the PCSA

- Pre-initiator HFE are incorporated in system fault trees.
- Initiator HFE are incorporated in initiating event models.
- Non-recovery post-initiator HFE are incorporated into event trees or top logic.


T
K
Q
B
X
Y
Bin
OK
TY
TX
OK
TBX
TQ
TK
Initiating Event
A
S
T1
T2
T3
.
ETC.
Recovery Post-initiator HFEs
Adjoined to the sequence cutsets
Q
Non-recovery Post-initiator HFEs
Event tree headings, event tree top logic, or top of system fault tree
Q Top Logic
System X
Hardware
Human
Human-induced Initiator HFEs
Independent initiating event or as high as possible in initiating event fault tree.
Train A
Pre-initiator HFEs
As high as possible in the fault trees
Group 1
Group n

Recovery Analysis

- Recovery analysis is performed *after* the model has been quantified and the dominant sequences have been identified.
- Cut sets are reviewed to identify, based on analyst team judgment (including both Facility Team and HRA Team) recovery alternatives.

Recovery Analysis

- Analysis process is the same as for other HFE, except there is no screening step.
  - Describe base case scenario (successful recovery).
  - Identify HFE of concern (failed recovery).
  - Identify vulnerabilities (what affects HFE).
  - Search for HFE scenarios (HAZOP).
  - Quantify HEP.
  - Incorporate in model (append to cutsets).

HFE Naming

- All HFE are to be named in the following convention:
- FACL-SYST-DFNITONA-TYPFM, where:
  - FACL is the facility identifier.
  - SYST is the system identifier.
  - DFNITON is a free form field for the analyst to define the HFE. This could be such things as TADDROP, IMPACT, or whatever else the analyst deems appropriate to describe the event. For HFE related to the failure of an individual component, the P&ID component ID number can be used.
  - A is the unique HFE identifier to differentiate between HFE that otherwise would have the same combination of FACL-SYST-DFNITON (e.g., 1 for the first such event, 2 for the second, etc.).
  - TYPFM is the generic identifier (type code) for components and HFEs. Allowable values for TYPFM were specified in a draft appendix D of PCSA-DI-006 distributed by e-mail.

HRA Team

- Will closely work with you on your areas of responsibility
  - Paul Amico
  - Erin Collins
  - Doug Orvis