Using Hazards Analysis Techniques to Identify Pertinent Scenarios for Criticality Safety Analyses

Chris Dean, Vice President
Government Operations

Sandi Larson,
Criticality Safety Manager

NuclearSafety
Associates

June 16, 2010

Overview

- Description of the hazards analysis process
- Hazard identification philosophy
- Screening identified scenarios
- Hazard evaluation process
  - Use of HA to support DC arguments
  - Defense-in-depth
  - Determining adequacy of controls
- Documentation

NuclearSafety Associates

Hazard Analysis Process

- Define the process
- Perform hazard identification
- Perform screening to eliminate initiating events from consideration based on credibility or inability to produce undesired consequence
- Analyze the contingencies (hazard evaluation)

NuclearSafety Associates

Hazard Analysis Process (Cont'd)

- Develop controls necessary for double contingency and to maintain an acceptable risk of operation
- Document the hazard analysis (CSE)

Process Description

- Define the scope and boundaries of the process to be considered; include maintenance and all operational activities
- Provide process flow description
- Identify all materials, quantities, and properties
- Identify process equipment and procedures
- Provide drawings or diagrams of system for illustration
- Describe previous analyses

NuclearSafety Associates

Hazard Identification

- Identification of process upset conditions (deviations from design intent)
- Consideration of all deviations is documented for completeness
- Utilizes a team approach
- Requires use of standardized documentation format

NuclearSafety Associates

Hazard Identification (Cont'd)

- Method used is typically determined by complexity of the operation
  - What-If/Checklist
  - Hazard and Operability Study (HAZOP)
- Uses established process boundaries, but:
  - Considers external events which can impact the system
  - Considers effects of interacting systems

NuclearSafety Associates

Hazard Identification (Cont'd)

- In commercial facilities, criticality analysts can utilize the hazard identification results conducted as part of the Integrated Safety Analysis (ISA) process to identify DC scenarios
  - Conducted at the correct level of detail
  - Ensures consistency and integration with the ISA
- Hazard identification for DOE safety basis document development is not typically conducted at the level of detail required to support the CSE

NuclearSafety Associates

What-if Hazard Identification Table

No.	What-If	Causes	Consequences	Safeguards	Comments
Process Zone 1: Shipping Container Receipt					
1.1	What if certified shipping container is received damaged?	• Truck damage during transportation • Damaged container sent by shipper	• Structural damage • Damaged shipping container • Damage to fissile material in package	• Receipt inspection • Driver qualification • Shipper's quality assurance program	
1.2	What if truck impacts building or dock?	• Driver error • Brake failure • Weather	• Structural damage • Damaged shipping container • Damage to fissile material in package • Personnel injury	• Robust shipping container • Driver qualification • Site speed limit	Truck backs up to dock to unload
1.3	What is load contains more containers than expected?	• Shipper error	• Maximum allowed Criticality Safety Index (CSI) for the shipment may be violated	• Shipper's quality assurance program	

NuclearSafety Associates

Hazard Screening

- Initiating events are screened to determine the nature of analysis required
- Some events do not present an NCS hazard
  - No impact on NCS parameters
  - No credible mechanism for event to occur
- Such events and their disposition are documented in the screening process
- Scenarios impacting criticality that require further analysis are carried forward for evaluation

NuclearSafety Associates

What-if Hazard Screening Results Table

No.	What-If	Causes	Consequences	Screening Results	Justification	Carries Forward?
Process Zone 1: Shipping Container Receipt						
1.1	What if certified shipping container is received damaged?	• Truck damage during transportation • Damaged container sent by shipper	• Structural damage • Damaged shipping container • Damage to fissile material in package	• Insufficient mass involved to support criticality	• The 1 shipping container involved contains less than the minimum subcritical mass of fissile material	No
1.2	What if truck impacts building or dock?	• Driver error • Brake failure • Weather	• Structural damage • Damaged shipping container • Damage to fissile material in package • Personnel injury	• Unmitigated scenario is not credible to result in criticality	• Damage to certified shipping containers would be minimal due to backing speed	No
1.3	What is load contains more containers than expected?	• Shipper error	• Allowed Criticality Safety Index (CSI) may be violated	• Infinite array of this shipping container is not subcritical		Yes

NuclearSafety Associates

Hazard Evaluation Process

- Goal for scenarios requiring further evaluation:
  - Demonstrate double contingency
  - Show unmitigated scenario is non-credible
- For credible criticality scenarios, identify primary and secondary barriers to criticality
- Multiple primary or secondary barriers may be provided as defense-in-depth strategy
  - Must be clear what is relied upon for DC
  - Identify which failures constitute a loss of DC control
- DC barriers must be clearly identified to ensure proper application of CM and QA elements

NuclearSafety Associates

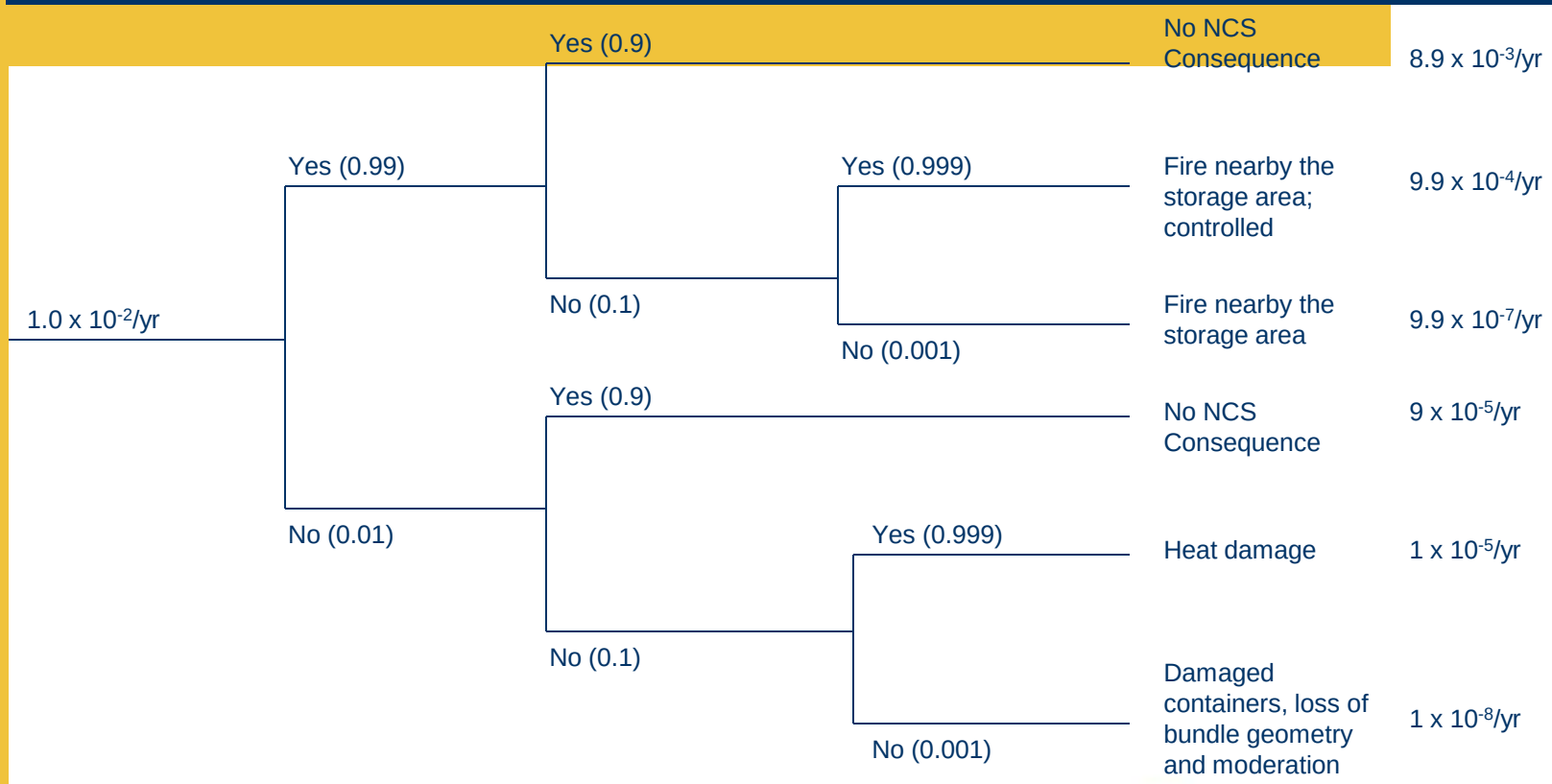
Hazard Evaluation Process (Cont'd)

- Event tree analysis is particularly helpful to illustrate the initiating events and barriers to accidental criticality
- Event trees can be quantified to assist in defending adequacy of controls or arguments for scenario incredibility

NuclearSafety Associates

Event Tree Analysis – Scenario 1

Fuel leak from vehicle	Fuel does not reach storage area	Fuel does not ignite and cause fire	Sprinkler system works		
A	B	C	D	Outcome	Frequency



NuclearSafety Associates

Defensible Basis for Events

Item	Event Description	Frequency or Probability	Source/Basis
A	Fuel leak from a vehicle at the rollup door or other location in the facility	1.0×10^{-2}/yr	Fuel leak is based on failure of a fuel tank due to long-term deterioration or impact to the tank during vehicle movement. Based on vehicle inspections for commercial vehicles, inspection prior to entering site, the typical location of fuel tanks on vehicles and low speed operations, this was assigned a low event frequency.
B	Fuel does not flow to the storage area to pool	0.99	This is based on a leak with sufficient fuel available that occurs inside the building, spreads away from the leak location rapidly, and flows past the floor drains near the storage area that would tend to mitigate such liquid pooling.
C	Fuel does not ignite and cause a fire when leak occurs	0.9	Ignition sources in this area could be concurrent hot work, hot brakes on the vehicle, or electrical faults.
D	Sprinkler system actuates and controls or extinguishes the fire	0.999	Credited as a well-maintained and adequately designed engineered feature.

NuclearSafety Associates

Identification of Criticality Barriers

- Two credited barriers in the example are a passive design feature that precludes fuel pooling and an active fire sprinkler system
- Barriers must be selected based on:
  - Consideration of common-mode failures
  - DC is clearly demonstrated
  - Frequency of accidental criticality demonstrated to be acceptable (qualitative or quantitative)
  - Preferred design approach

NuclearSafety Associates

Parameter Discussion

- Discuss each NCS parameter (mass, enrichment, volume, etc.) and the contingent conditions associated with each
- Specifically reference the scenarios identified in the hazard ID section
- State controls on each parameter as appropriate
- For other parameters, state that no control is applied
- Provide sufficient discussion/analysis such that compliance with double contingency is evident and clearly stated

NuclearSafety Associates

Documentation

- Scope and process description
- All necessary CSE elements and documentation of each HA process
- Hazard identification and screening process can be included as appendices
- Parameter discussion
- Limits and controls for criticality safety
- Technical basis for control selection and reliability

NuclearSafety Associates

Conclusions

- HA process adds significant rigor and defensibility to criticality analyses
  - Understanding of the process and upset conditions
  - Adequacy of controls
- Can illustrate the logic in a criticality accident scenario to assist in identification of barriers and supporting DC arguments
- Helps to ensure effectiveness of credited controls

NuclearSafety Associates