Used Fuel Disposition Campaign

Deep Borehole Emplacement Mode Hazard Analysis (DBEMHA)

S. David Sevougian
Sandia National Laboratories

2015 UFDC Annual Working Group Meeting
Deep Borehole Field Test Session, June 10, 2015
Las Vegas, NV

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2015-4529PE

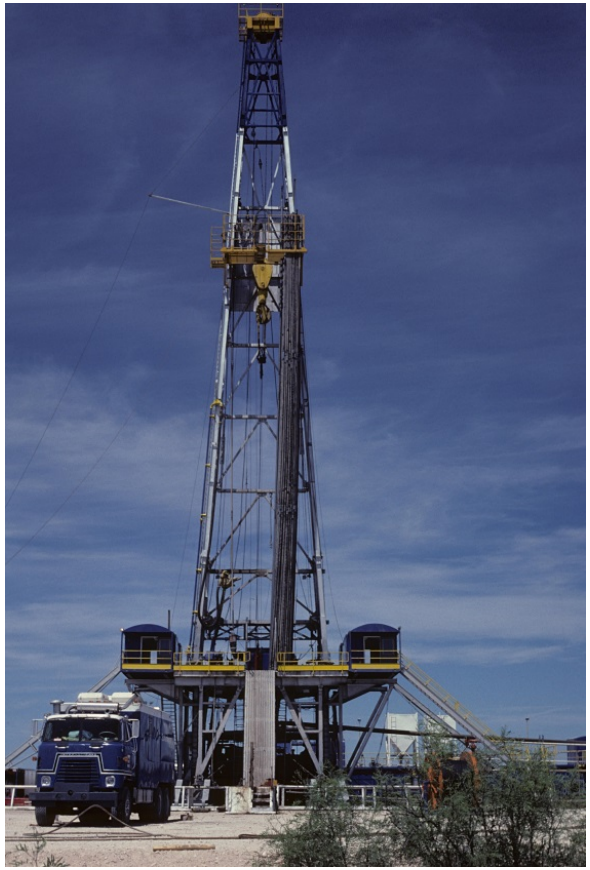
Outline

- Main purpose of DBEMHA
- Assumed limitation on event consequences
- Choice of hazard/risk analysis technique
- Discussion of ETA and FTA
- Potentially hazardous events for wireline emplacement
- Preliminary fault tree for wireline emplacement
- Accident/failure databases
- Future work

Purpose of DBEMHA

- **What accidents could occur and how likely are they during deep-borehole emplacement of waste packages?**

- **Primary steps/aspects of hazard/risk analysis:**
  1. Hazard identification and event sequence construction (*what can happen? – "causes"*)
  2. Frequency/probability analysis (*how likely is it to happen?*)
  3. Consequence analysis (*what are the consequences if it happens?*)
  4. Risk calculation (*how bad is it?* – product of frequency and consequence)
  5. Decision analysis (*how should we proceed in light of the risk?*)



© S. D. Sevougian, S.E. New Mexico, Summer 1979

Limitations on Consequence

- **Cause ⇒ Event ⇒ Consequence**
- **Prevention & Mitigation ⇒ Safety Functions/Barriers in the Design**

"Bow-tie" Diagram*

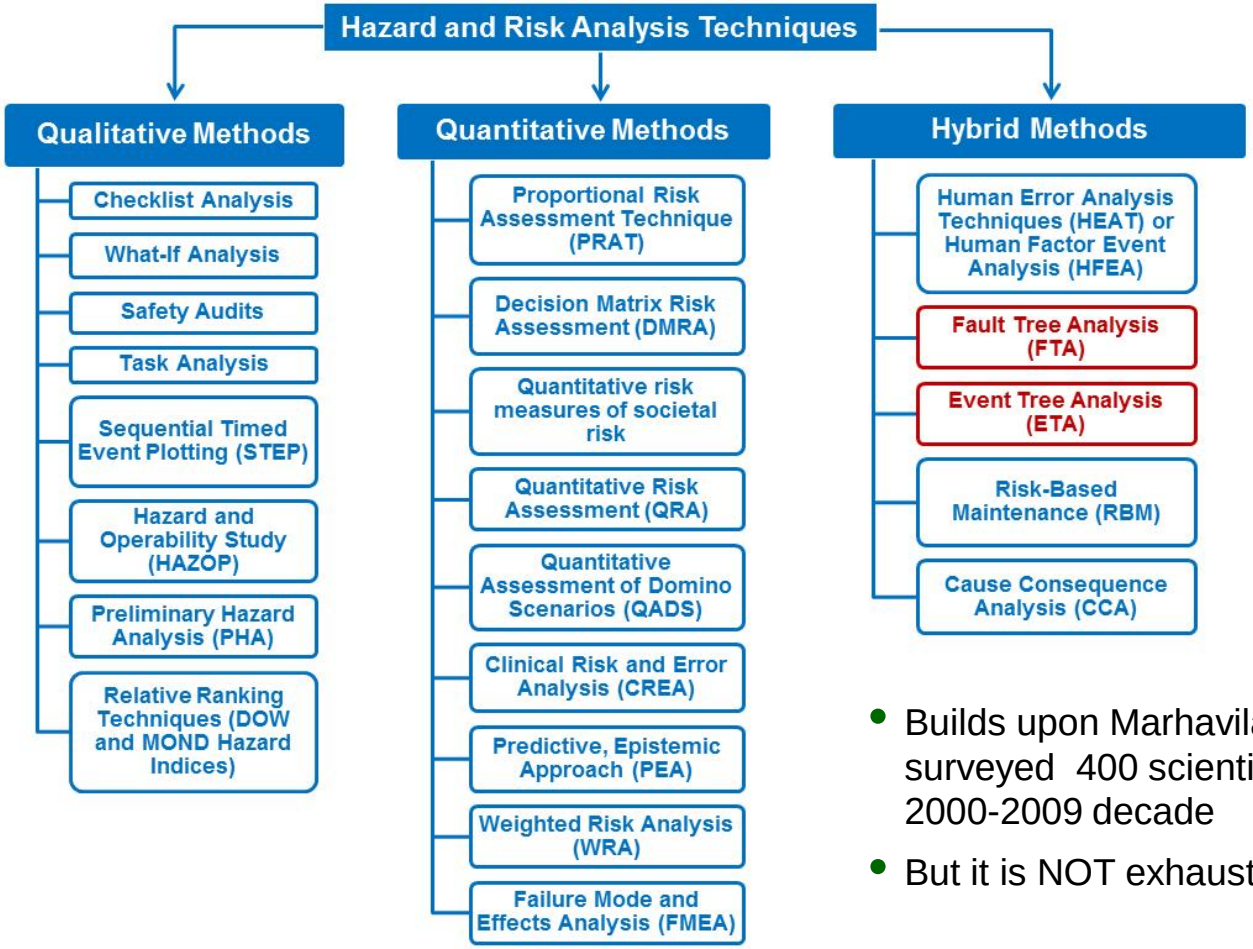
Often used for risk analysis in the oil industry

- **Key Consequence/Risk <u>Assumption</u> for DBEMHA for now:**
  - Only *one* accident "end state" or effect ⇒ "loss of control" of waste package (or waste package string)
  - Eliminates need to compute personnel (e.g., injury or fatality) risk or technical risks (e.g., environmental impact or material damage)

* Burtonshaw-Gunn, S. A. 2009. *Risk and Financial Management in Construction*, Fig. 3-8, ISBN 978-0-5660-8897-1, Ashgate, also Gower at www.gpmfirst.com

Risk/Hazard Analysis Techniques

- **After Matanovic et al. 2014, *Risk Analysis for Prevention of Hazardous Situations in Petroleum and Natural Gas Engineering:***



- Builds upon Marhavilas et al. (2011), who surveyed 400 scientific papers from the 2000-2009 decade
- But it is NOT exhaustive; others like BBN

Criteria for Choosing Hazard Evaluation Method for a Nuclear Hazard Category 2 Facility*

- **After DOE 1997. *DOE Standard: Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports.* DOE-STD-1027-92, Change Notice No. 1, September 1997:**

Type/Complexity of Facility	Facility or System Description	Recommended HE Method
Low-Complexity	• Little or no processing of materials takes place; • e.g., waste storage, vaults, tanks, cylinders, canisters.	Checklist Analysis or other simple "Hazard Analysis" that includes the following information: • Hazardous Material Quantity, Form, and Location • Energy Sources and Potential Initiating Events • Preventive Features • Mitigative Features
Single-Failure Electro-Mechanical Systems	• Relatively simple electrical and mechanical devices in which a single-failure mechanism causes a release of materials. • e.g., Simple one-step processes, single glove box operations, and small furnaces are example of such devices	Failure Modes and Effects Analysis (FMEA): "FMEA is not very efficient for large-scale systems analysis because…it examines and documents the effects of component failures having little, if any, relevance to system failure or potential release."
Systems with Redundant Barriers or Requiring Multiple Failures	• An undesired event could be uncontrolled release of hazardous material from a facility or core damage in a reactor….For each initiating event, various systems or barriers designed to prevent or to mitigate the progress of the accident are identified • e.g., fire scenarios or seismic events.	Event Tree Analysis (ETA)
Large, Moderately Complex Processes	• Is most suitable for analysis of large, moderately complex systems or processes where multiple component failures including human errors can contribute to the failure of the system or process.	Fault Tree Analysis (FTA)
Complex Fluid Processes	• Complex fluid processes involve arrays of piping, tanks, and instrumentation and control systems. • Examples of these processes include PUREX, chemical separations, isotope separations (e.g., uranium enrichment), and petrochemical processing	Hazard and Operability Studies (HAZOP): • HAZOP is a standard and widespread technique used for the analysis of chemical flow processes
High Complexity Facilities	• Highly complex facilities include multi-component transfer and control systems for which extensive instrumentation and control systems are needed. Extensive redundancy at the component, system, and safety level • Processes generally cannot be completely controlled through manual actions because the interactions between systems are too intricate for an operator to interpret in the time required for action. Thus, processes are generally characterized by large-scale monitoring and automatic control systems.	Integrated Event Tree and Fault Tree Techniques (ETs/FTs): • The specification of the use of these techniques is due to the complex system interdependencies found in such facilities. Connecting of the initiating event and ET and FT models in a structured fashion is a proven technique capable of handling, in an efficient and comprehensive fashion, the very complex nature of the system designs, interactions, and dependencies

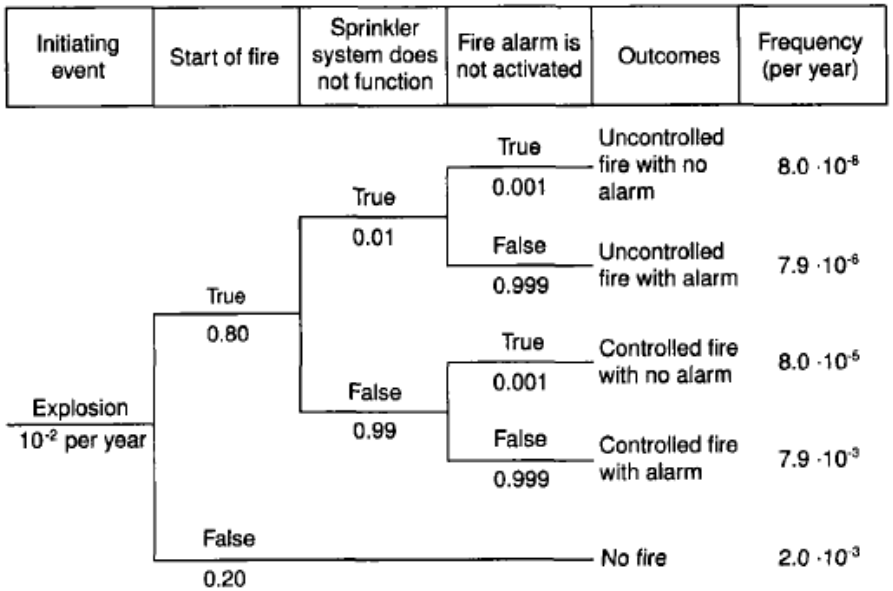
* Definition = potential for significant on-site consequences

Event Tree Analysis (ETA) Primer

- **Five major steps in an event tree analysis (e.g., after Rousand and Hoyland 2004; CCPS 1992), an *inductive* technique:**

1. Identification of an *initiating event (hazard)* causing the accident or failure of concern
2. Identification of the *safety functions* /barriers/actions/procedures, designed to mitigate the initiating event—a failure of which results in an "intermediate" or "pivotal" event
3. Construction of the *event tree*
4. Description of the resulting accident *event sequences*
5. Calculation of frequencies/probabilities: frequency of end state(s) = frequency of initiating event × probability of each intermediate event

Example event tree based on an initiating event (dust explosion) followed by subsequent events, including those associated with success/failure of safety/mitigation functions:
(1) fire may or may not break out; (2) a sprinkler system and (3) an alarm system have been installed, which may or may not function.



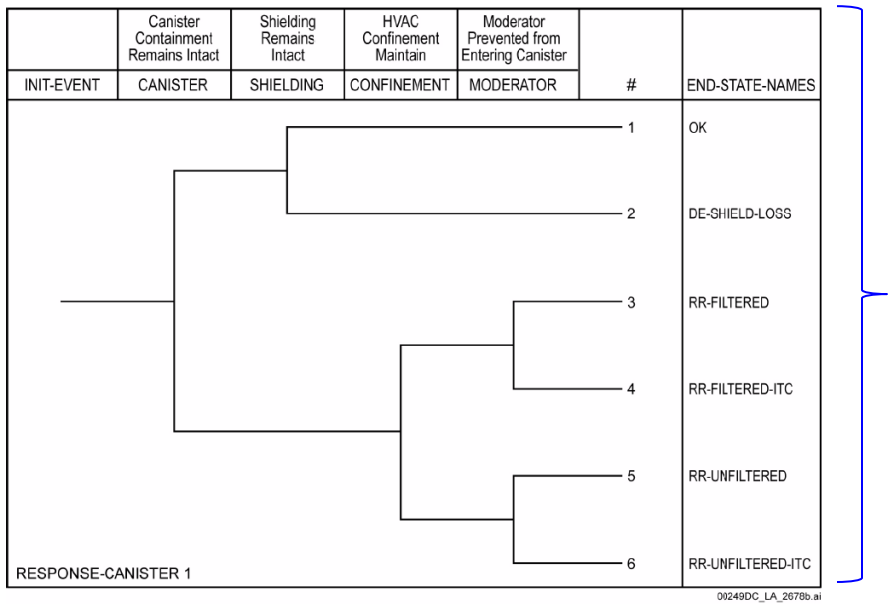
Rausand, M. and A. Hoyland 2004. *System Reliabiltiy Theory: Models, Statistical Methods, and Applications, Second Edition*, John Wiley & Sons, Inc., Hoboken, NJ.

Combined ETA/FTA for YMP PCSA*

- **Preclosure Safety Analysis (PCSA) for Yucca Mountain used combined ETA and FTA:**
  - Each "pivotal" (i.e., intermediate event) in the PCSA event sequences was decomposed using a fault tree approach to define its probability of occurrence
  - Multiple end states were defined for the PCSA (in contrast to the single end state currently being used for DBEMHA)

Safety barriers/intermediate events →

Event Sequences for transfer of a TAD canister by a Canister Transfer Machine (CTM)



End states

1. **OK**
2. **Direct exposure, shielding loss**
3. **Radionuclide release, filtered by HVAC**
4. **Radionuclide release, filtered by HVAC, also important to criticality**
5. **Radionuclide release, unfiltered by HVAC**
6. **Radionuclide release, unfiltered by HVAC, also important to criticality**

Figure 1.7-5. System-Response Event Tree for Activities Associated with the Transfer of a TAD Canister by a Canister Transfer Machine in a Canister Receipt and Closure Facility

NOTE: DE = direct exposure; INIT = initiating; ITC = important to criticality; RR = radioactive release.

* DOE (U.S. Department of Energy) 2008. *Yucca Mountain Repository License Application Safety Analysis Report*. DOE/RW-0573, Revision 1.

Fault Tree Analysis (FTA) Primer

- **Five major steps in an fault tree analysis (e.g., after Rousand and Hoyland 2004), a *deductive* technique:**
  1. Definition of the problem and the boundary conditions, including definition of "top event"
  2. Construction of the fault tree, backwards from "immediate cause events" (just below top event) to a level of "basic (initiating) events" or causes
  3. Identification of minimal "cut sets"*
  4. Qualitative analysis of the fault tree
  5. Quantitative analysis of the fault tree

*Minimal "cut set" = *smallest combination of basic events (component failures) which, if they all occur or exist simultaneously, will cause the top event to occur*

One type of failure and underlying causes for Canister Transfer Machine (CTM) operations—this is a fault tree for one of the initiating events that might compromise a canister.

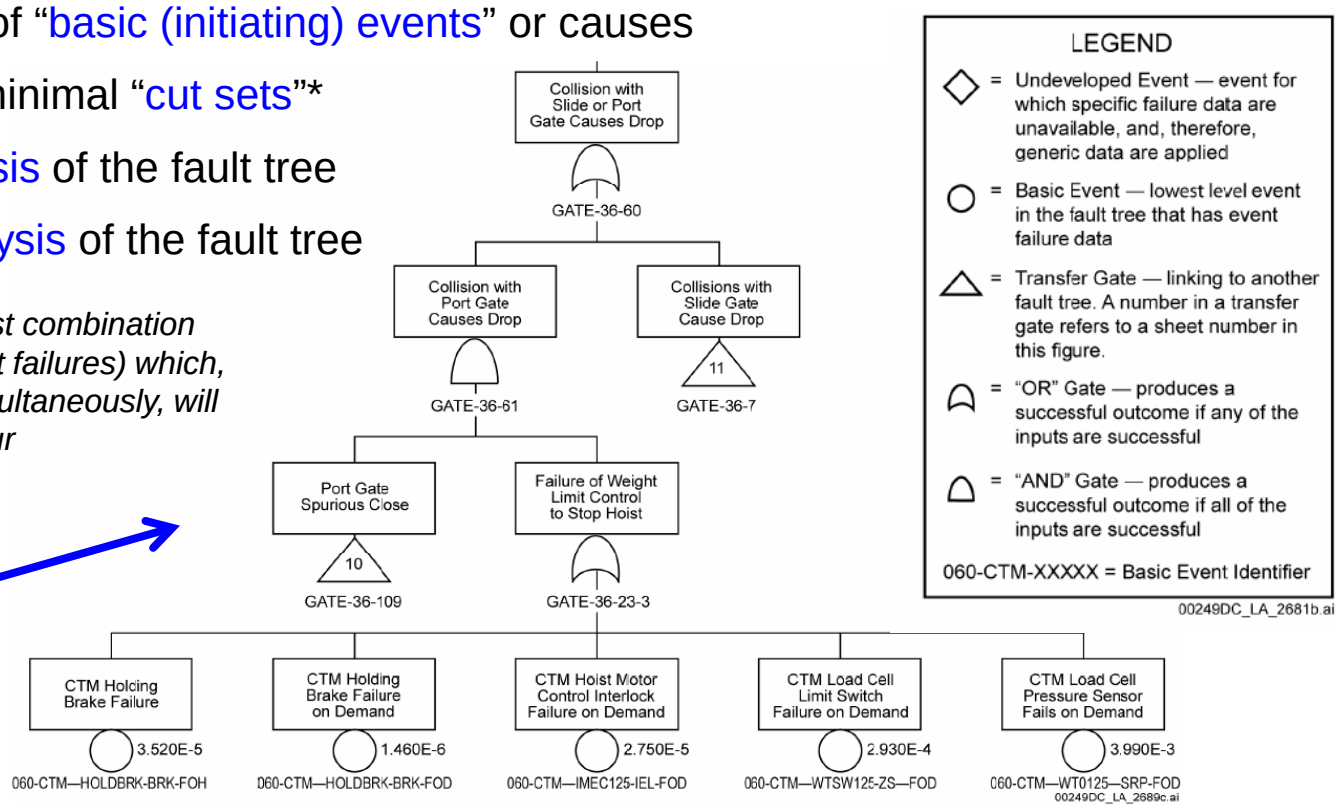


Figure 1.7-8. Example of Fault Tree of the Preclosure Safety Analysis (Sheet 9 of 12)

NOTE: CTM = canister transfer machine.

DOE (U.S. Department of Energy) 2008. *Yucca Mountain Repository License Application Safety Analysis Report*. DOE/RW-0573, Revision 1.

Strengths (mainly) of Fault Tree Analysis

- **Easily combines human and equipment failure (both of which are expected to be possible in DBH emplacement)**
- **Can be used to derive the probability of complex intermediate events in an event sequence**
- **Software easily available**
  - **Weakness of fault trees for DBMEHA?.... databases of frequencies and basic event probabilities?**

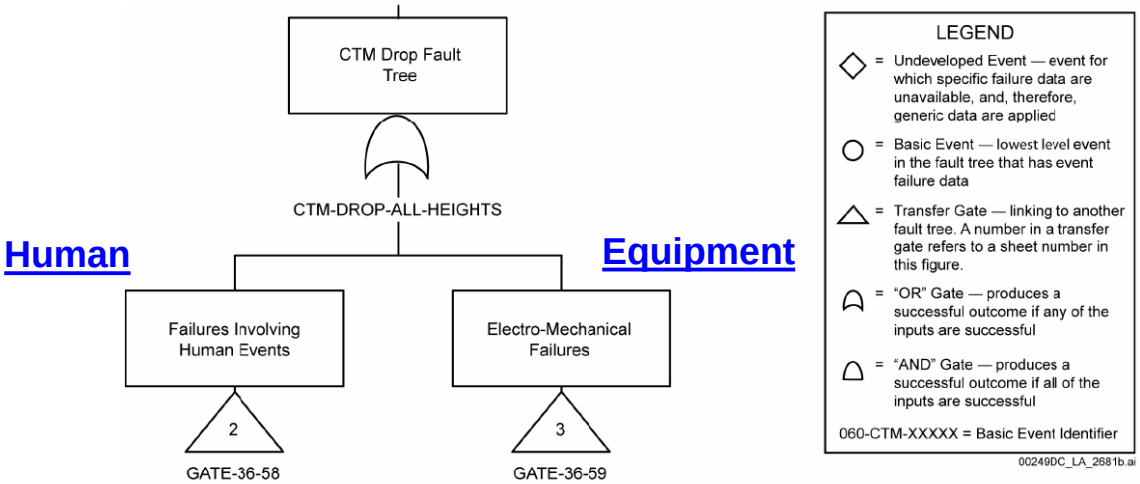


Figure 1.7-8. Example of Fault Tree of the Preclosure Safety Analysis (Sheet 1 of 12)

NOTE: CTM = canister transfer machine.

Source: BSC 2008 [DIRS 180095], Attachment B, Section B4.4.1.8.

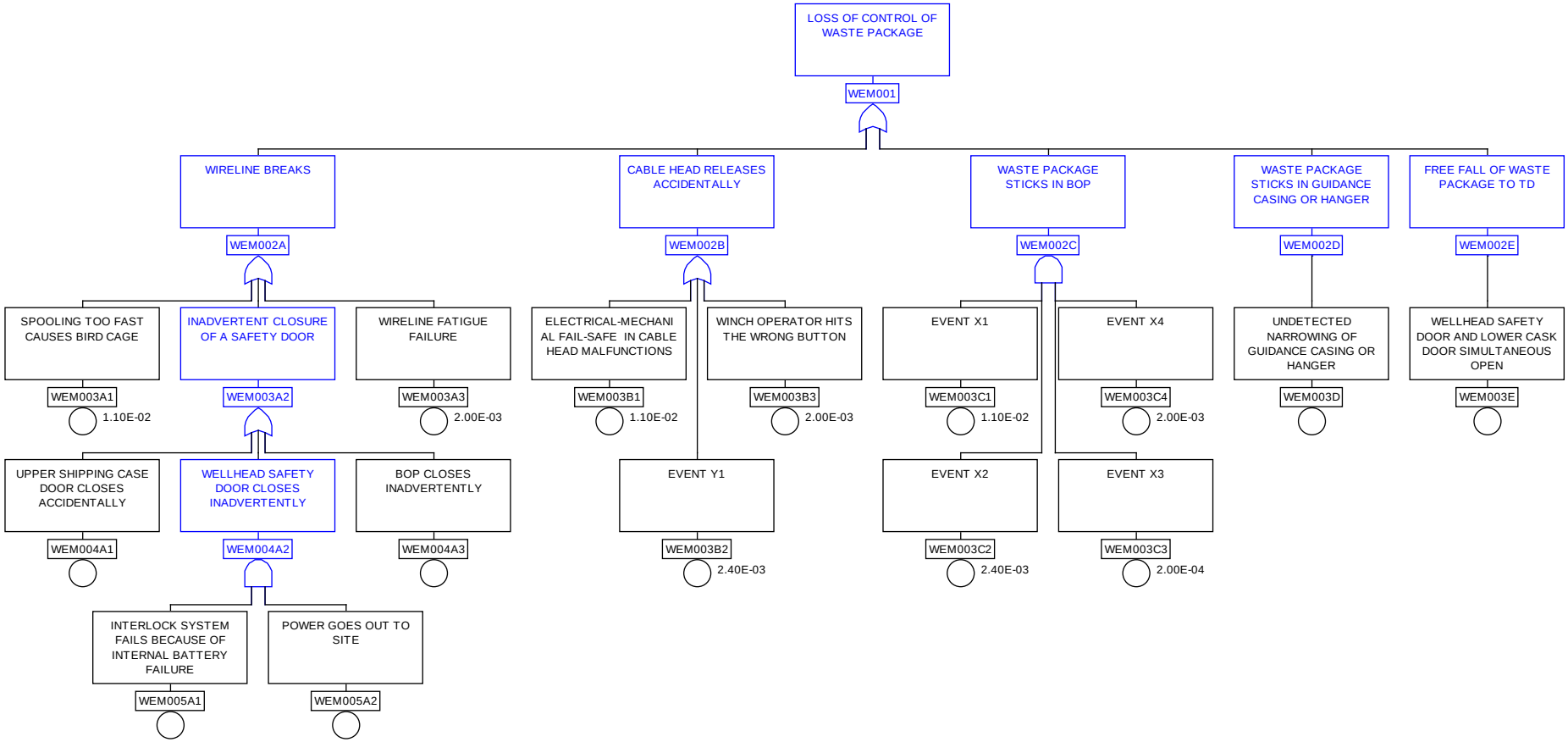
DOE (U.S. Department of Energy) 2008. *Yucca Mountain Repository License Application Safety Analysis Report*. DOE/RW-0573, Revision 1.

Potential Hazardous Events for *Wireline* Emplacement in Deep Borehole

Event Identifier	Description of Potential Hazardous Event (based on sequential emplacement steps)	Risk Mitigation Measures, Assumptions, and Other Notes	Screening decision (include/exclude)
Top event	***Loss of control of waste package***		include
Immediate-cause event	Wireline breaks		include
Immediate-cause event	Cable head releases accidentally		include
Immediate-cause event	Waste package "sticks" in BOP		include
Immediate-cause event	Waste package sticks in guidance casing or hanger on trip in		include
Immediate-cause event	Waste package falls out of shipping cask to TD; all safety doors/rams fail	Risk mitigation measure: Cask/wellhead-safety-door/blind-ram interlock system	include
Aggregate event (not basic)	Inadvertent closure of a safety door or ram		include
Basic event	Prior to attachment of cable head, the operator mistakenly opens the lower door on the shipping cask instead of the upper one, dropping package onto the "safety door" in the wellhead below	Risk mitigation measure: Door/ram/wireline hoist interlock system, including a "deadman" lock out (in case of loss of power or inadvertent energization). This event is not considered to be "loss of control".	exclude
Basic event	Upper cask door closes accidentally after cable head is attached but while lower cask door is still closed.	Risk mitigation measure: A restraint to prevent upper door closing is set prior to cable head attachment. Furthermore, the package has "no where to go" at this point, so no loss of control	exclude
Basic event	Cable head pulls loose, dropping the package on the lower cask door, because operator accidentally tried to spool the cable upward beyond the range-limiting pin	Risk mitigation assumption: Such a drop within the cask would be small and not cause damage to the package, the cask, or the lower door.	exclude
Basic event	Lower cask door closes inadvertently on the wireline		include
Basic event	Lower cask door closes inadvertently on the waste package	Risk mitigation assumption: Waste package is strong enough to be structurally unaffected.	exclude
Basic event	Upper cask door closes inadvertently on the wireline		include
Basic event	Wellhead safety door closes inadvertently on the wireline		include
Basic event	Wellhead safety door closes inadvertently on the waste package	Risk mitigation assumption: Waste package is strong enough to be structurally unaffected.	exclude
Basic event	BOP closes inadvertently on the wireline		include
Basic event	BOP (blind ram) closes inadvertently on the waste package	Risk mitigation assumption: Waste package is strong enough to be structurally unaffected.	exclude
Basic event	Bird cage of wireline	Risk mitigation measure: Automated speed and tension control on wireline winch	include
Basic event	Wireline fatigue failure	Risk mitigation measure: Schlumberger TuffLINE cable	include
Basic event	Wireline winch failure		include
Basic human event	Operator spools waste package "past TD" or "past previous waste package"	Risk mitigation measure: Procedural and software controls; "crush box" on bottom of waste package	include
Basic human event	Operator pushes cable head release button prematurely		include
Basic event	Electrical-mechanical fail-safe in cable head malfunctions and releases waste package early		include
Basic event	Undetected narrowing of guidance or tieback casing or associated hangers	Risk mitigation measure: Caliper log run prior to waste package emplacement trip	include
Basic event	Lightning strike	Risk mitigation measure: Procedural: no operations during threats of severe weather	include
Basic event	Site-wide power failure	Risk mitigation measure: UPS battery backup	include
Basic event	Cable head fails to release while package is at TD	May not result in a loss of control	exclude
Basic event	Cable head releases on trip out with waste package still attached, releasing package to free fall to the bottom	Requires a joint underlying event with a very low probability, i.e., cable head failed to actuate at TD and tension guage does not indicate this extra weight on the trip out	exclude

Preliminary, Simplified Fault Tree for Wireline Emplacement

- **Generated with demo version of CAFTA (from EPRI):**
- **Future fault trees to be generated with SAPHIRE v.8.x.x**



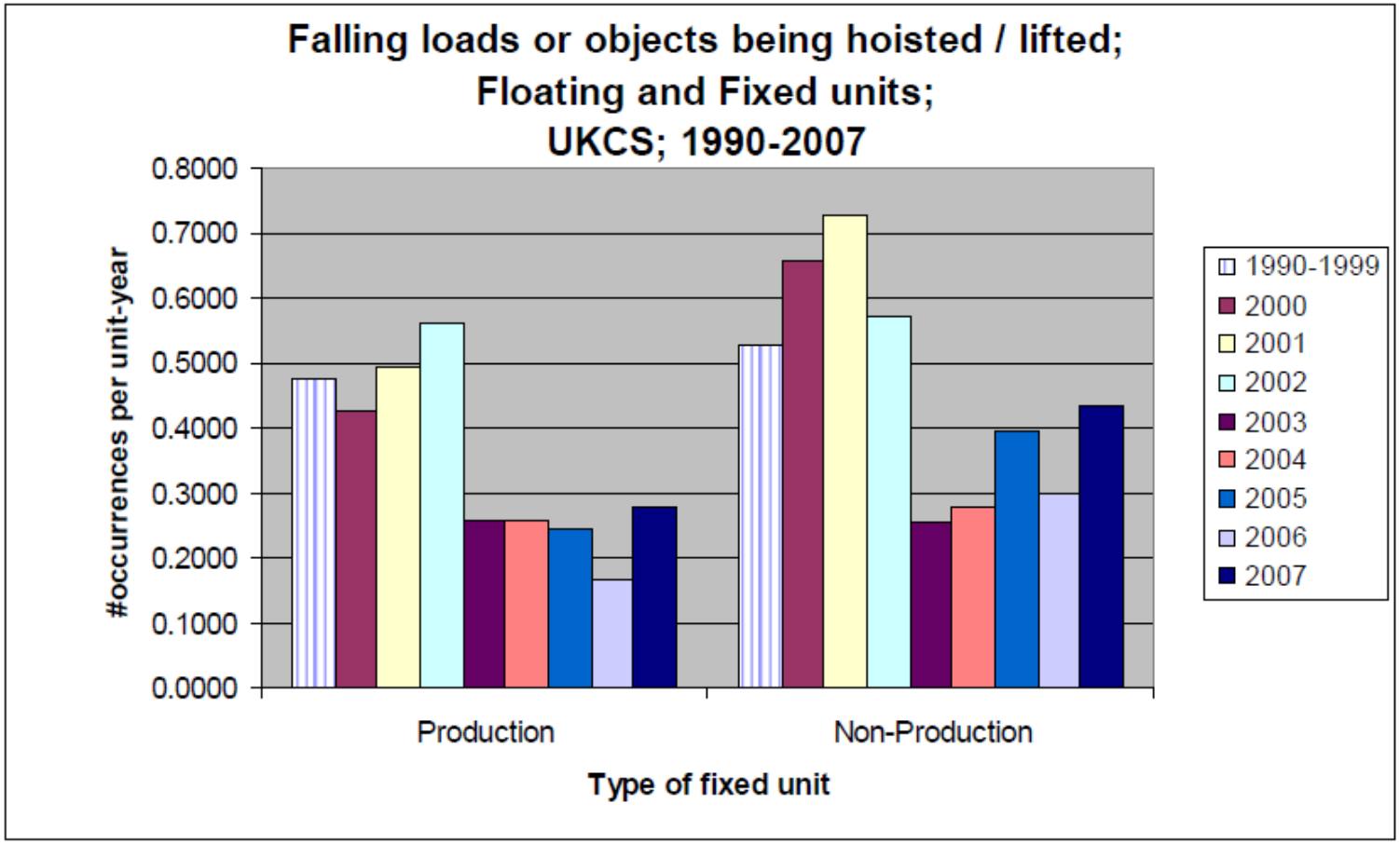
Some Databases for Accident Frequency and Failure Probabilities

- **Most databases are commercial ($$$)**

1. **Component failure event databases, e.g.,**
   - GIDEP (Government Industry Data Exchange Program) in the U.S. (free)
2. **Accident and incident databases, e.g.,**
   - MARS (Major Accident Reporting System), supported by the E.U.
   - PSID (Process Safety Incident Database), by AIChE
   - WOAD (World Offshore Accident Databank), by DNV (Det Norske Veritas)
   - BLOWOUT, the SINTEF offshore blowout database (maintained by the Foundation for Scientific and Industrial Research in Trondheim, Norway)
   - Oil and Gas UK (co-sponsored by HSE, the UK Health and Safety Executive)
3. **Component reliability databases, e.g.,**
   - OREDA (Offshore Reliability Database), by DNV
   - RADS (Reliability and Availability Data System), by the U.S. NRC
   - NPRD (Nonelectronic Parts Reliability Database), by RAIC, a DoD center
   - PERD (Process Equipment Reliability Database), by AIChE
4. **Common cause failure databases**
   - CCFDB (Common-Cause Failure Database), by the U.S. NRC

Example Statistics from Oil and Gas UK, April 2009

- **Accident Statistics for Offshore Units on the UK Continental Shelf, 1990-2007, co-sponsored by the UK HSE**



Future Work

- Generate a more detailed wireline fault tree with SAPHIRE
- Generate a fault tree for drillstring emplacement
- Determine available accident frequencies and failure probabilities that might be applicable to either wireline or drillstring emplacement operations
- Convene an expert panel to review fault trees, accident frequencies, failure probabilities, and overall methodology

Thanks for your attention!

Back-up Slides

Example of a Human Error Fault Tree

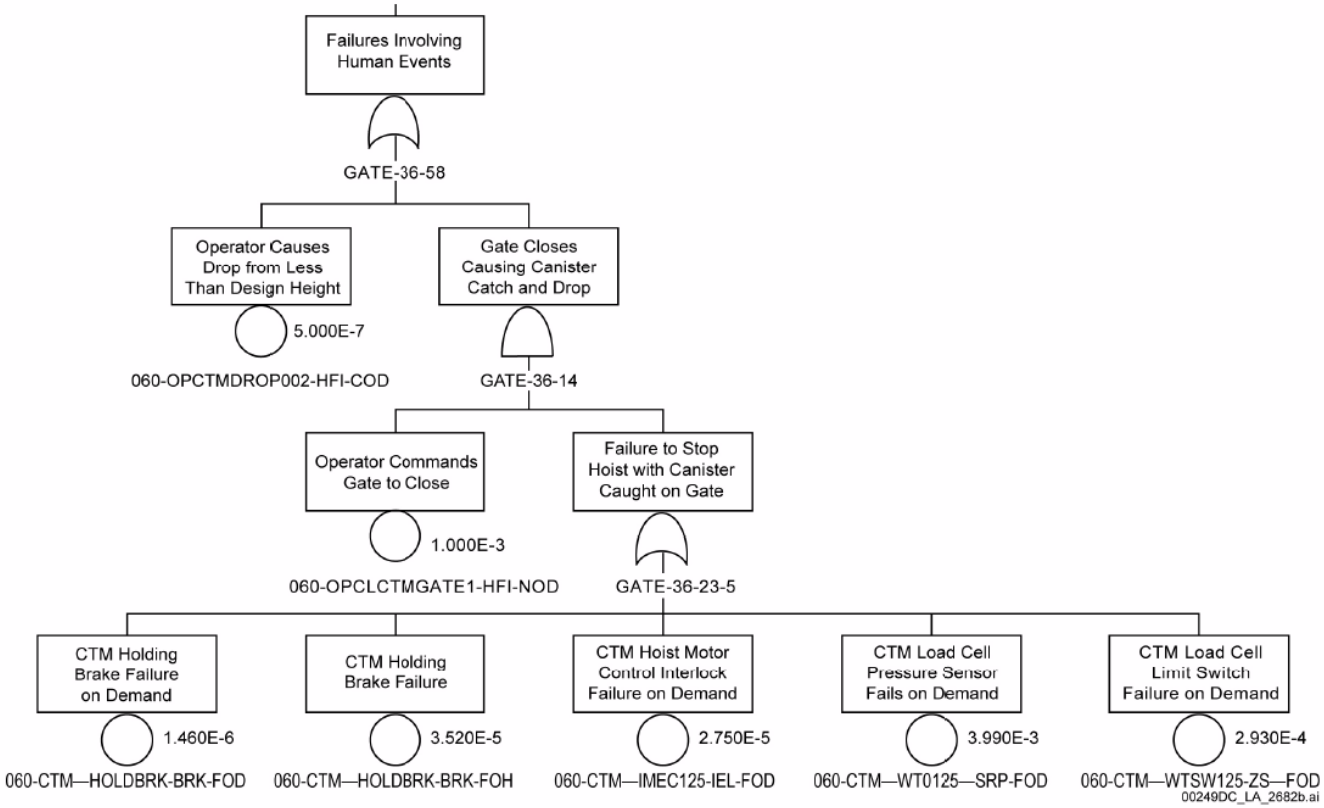


Figure 1.7-8. Example of Fault Tree of the Preclosure Safety Analysis (Sheet 2 of 12)

NOTE: CTM = canister transfer machine.

Source: BSC 2008 [DIRS 180095], Attachment B, Section B4.4.1.8.

DOE (U.S. Department of Energy) 2008. *Yucca Mountain Repository License Application Safety Analysis Report*. DOE/RW-0573, Revision 1.