Deep Borehole Emplacement Mode Hazard Analysis (DBEMHA)

S. David Sevougian
Sandia National Laboratories

U.S. Nuclear Waste Technical Review Board Visit
Albuquerque, NM
July 16, 2015

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. SAND2015-5341PE

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Outline

- **Purpose and approach**
- **Treatment of consequences**
- **Categories of failures/errors**
- **Choice of hazard analysis method**
- **Combined Event Tree/Fault Tree example from YMP PCSA***
- **Preliminary Event Tree/Fault Trees for wireline emplacement**
  - Drop-in-hole hazard
  - Stuck-in-hole hazard
- **Component failure databases (probabilities, frequencies)**
- **Future work, including drill string emplacement hazards**
- **References**

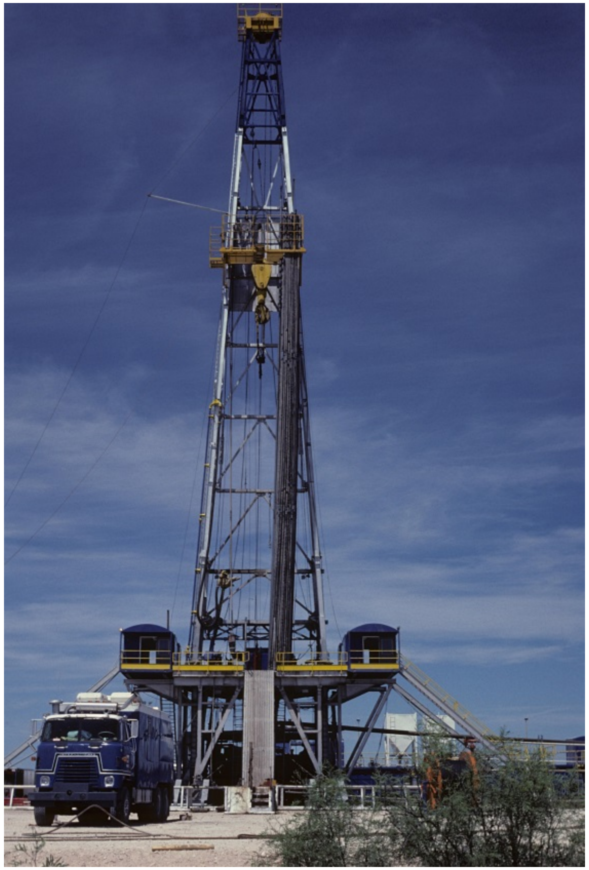
* Yucca Mountain Project Pre-closure Safety Analysis

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Purpose and Approach

- **Discriminate between emplacement mode options (*drill string* vs. *wireline*), according to**
  - 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. Consequence analysis (*what are the consequences if it happens?*)
  3. Frequency/probability analysis (*how likely is it to happen?*, including uncertainty ranges)
  4. Risk calculation (*how bad is it?* – product of frequency and consequence)
  5. Decision analysis (*how should we proceed in light of the risk?*)



Level of Consequences

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

*"Bow-tie" Diagram**

Often used for risk analysis in the oil industry

- **Level of Consequence in DBEMHA:**
  - Loss of operational capability: "yes/no"
  - Potential waste package breach condition exists: "yes/no"
    - Similar to consequences in Level 1 NPP PRA: "core damage yes/no"

* 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

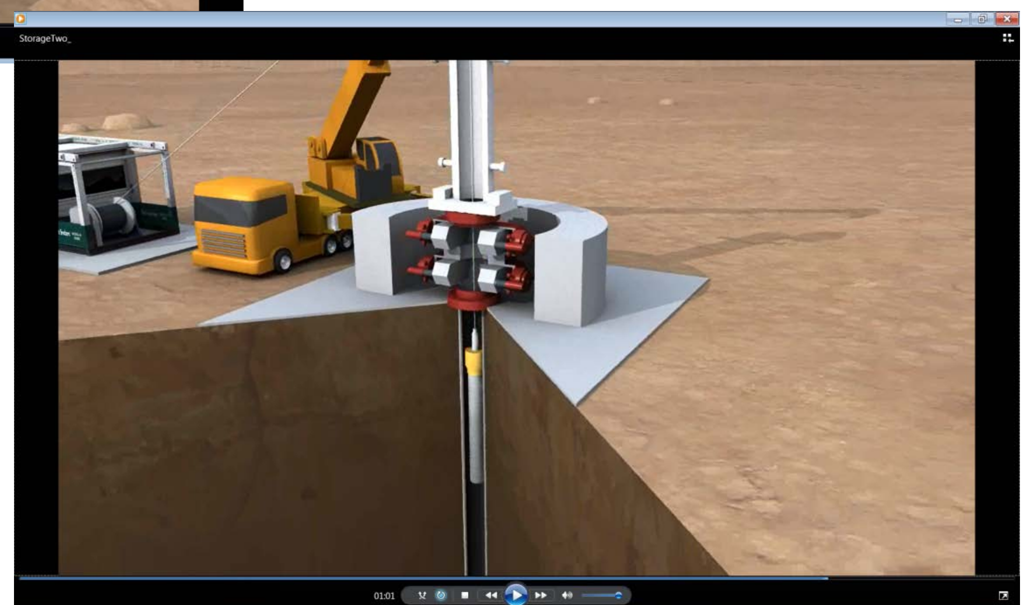
Some Assumptions & Simplifications

- **Accident analysis begins subsequent to bolting of shipping cask to wellhead (including nothing prior to reaching the site)**
- **Only internal events for now (i.e., omit seismic, weather-related, etc.)**
- **No malevolent acts**
- **No simultaneous initiating events (standard PRA practice because of low probability and because either event ceases operations)**
- **Typical risk consequences not considered at this point, such as**
  - Personnel risk (e.g., injury or fatality)
  - Environmental risks (e.g., groundwater contamination; biota damage)

Wireline Emplacement in Deep Borehole

Attach cable head to waste package

Lower waste package
through BOP and downhole



Three categories for failures/errors*

- **Hazardous events can result from either actions (e.g., human acts) or component failures (e.g. battery, sensor) or a combination—three major categories….**
- **Passive component failures (usually towards the top of a fault tree)**
  - Includes components such as the waste package, casing, tubing, and passive BOP components
  - Conditional failure probability (i.e., following a structural or thermal challenge) requires an engineering calculation (fragility and damage analysis) using process models, e.g., probability of damage/failure from mechanical stress (dropping, bumping), probability of damage/failure from thermal stresses (fire)
- **Active component failures:**
  - Includes components such as electric cable head release, wireline winch, wireline sheave wheels, interlock systems, cranes, active BOP components (rams), UPS, batteries, diesel generators, wireline (fatigue), etc.
  - Failure probability ("demand"-based) or failure frequency (time-based) come from industry and governmental reliability databases for electro-mechanical equipment
- **Human errors/failures**

* Also used to classify the "criticality" of minimal cut sets, by Rausand and Hoyland 2004, Table 3.2

Choosing a Hazard Evaluation (HE) Method

- **From:** ***CCPS (Center for Chemical Process Safety) 1992. Guidelines for Hazard Evaluation Procedures, 2nd Edition,*** **AIChE:**
  - "Selecting an appropriate HE technique is more an art than a science"
  - Detailed flow charts and criteria for choosing the best HE method (seven pages)

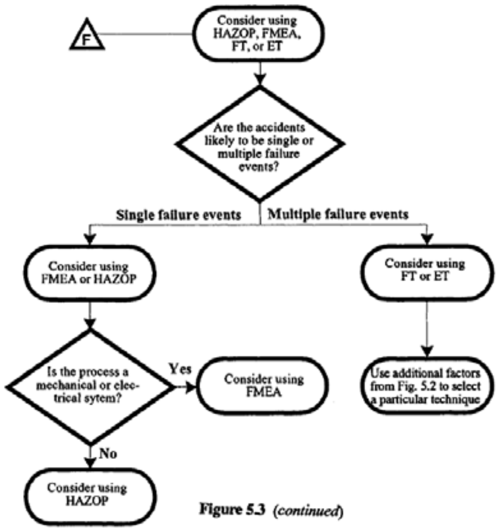


Figure 5.3 (continued)

- **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:**
  - For a <u>Nuclear Hazard Category 2 Facility</u> (facility with a potential for "significant on-site consequences):

Type/Complexity of Facility	Recommended Hazard Evaluation Method
Low-Complexity	Checklist Analysis or other simple "Hazard Analysis"
Single-Failure Electro-Mechanical Systems	Failure Modes and Effects Analysis (FMEA)
Systems with Redundant Barriers or Requiring Multiple Failures	Event Tree Analysis (ETA)
Large, Moderately Complex Processes	Fault Tree Analysis (FTA)
Complex Fluid Processes	Hazard and Operability Studies (HAZOP)
High Complexity Facilities	Integrated Event Tree and Fault Tree Techniques (ETAs/FTAs)

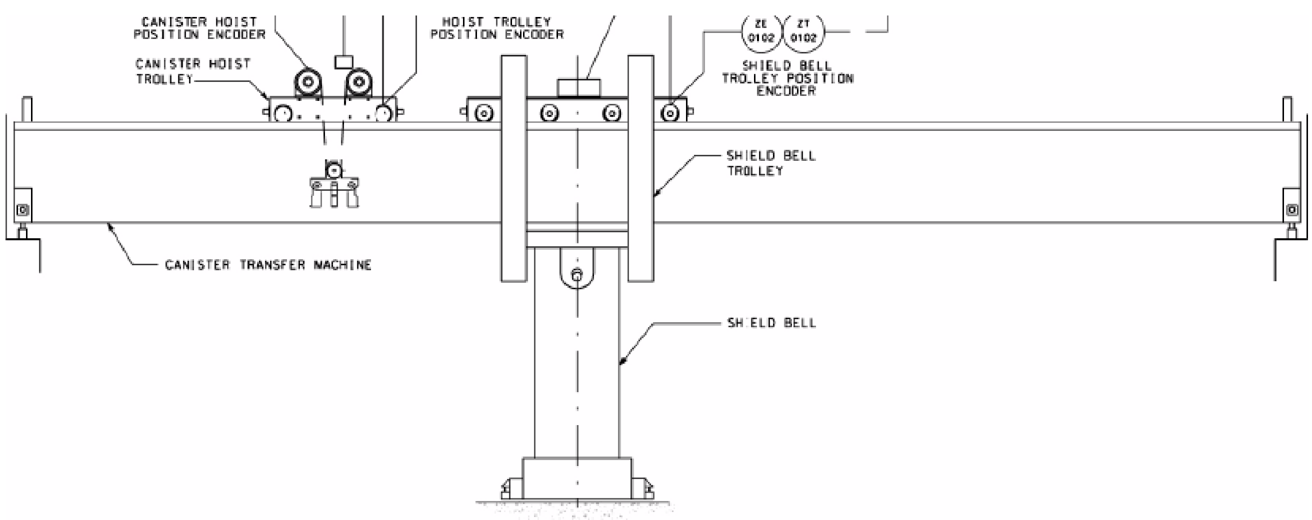
←YMP PCSA*

* Yucca Mountain Project Pre-closure Safety Analysis

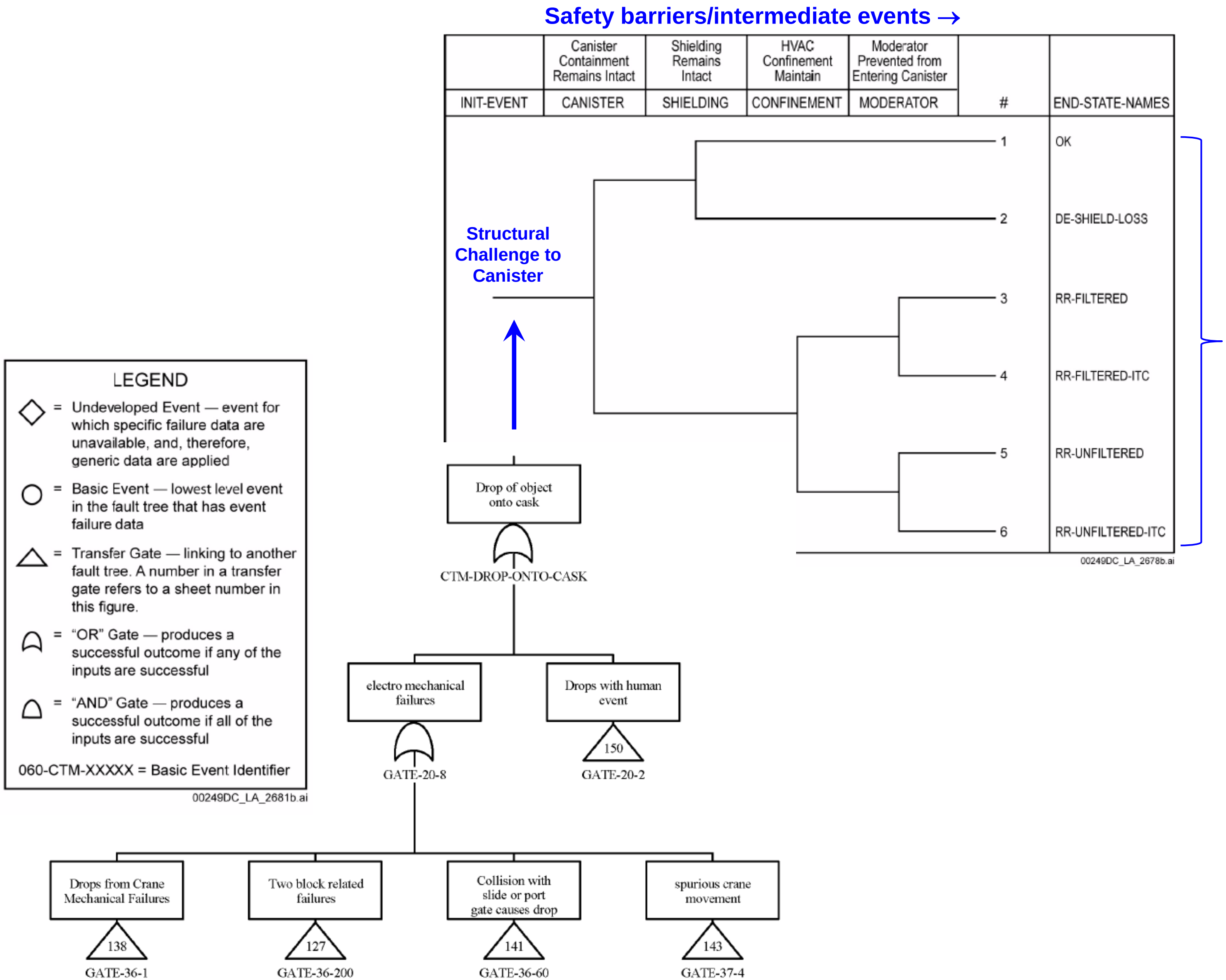
Example from Yucca Mountain Pre-Closure Safety Analysis (PCSA)

- **Combines ETA and FTA:**
  - Each "pivotal event" (i.e., intermediate event) in the PCSA event sequences was decomposed using a *fault tree* to define its probability of occurrence
- **PCSA used a well-established methodology codified in various NUREGs of the U.S. NRC (e.g., see NRC 1983)**
- **Example hazardous events associated with Canister Transfer Machine (CTM) operations inside the Canister Receipt and Closure Facility (CRCF):**

CTM: Transfers waste canister from transportation cask to waste package



Example Event Tree/Fault Tree Combination for Canister Transfer Machine (CTM)

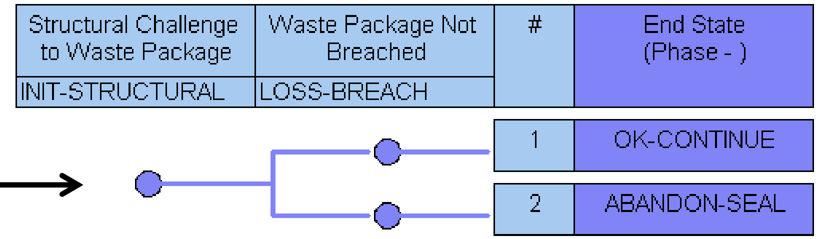


End states

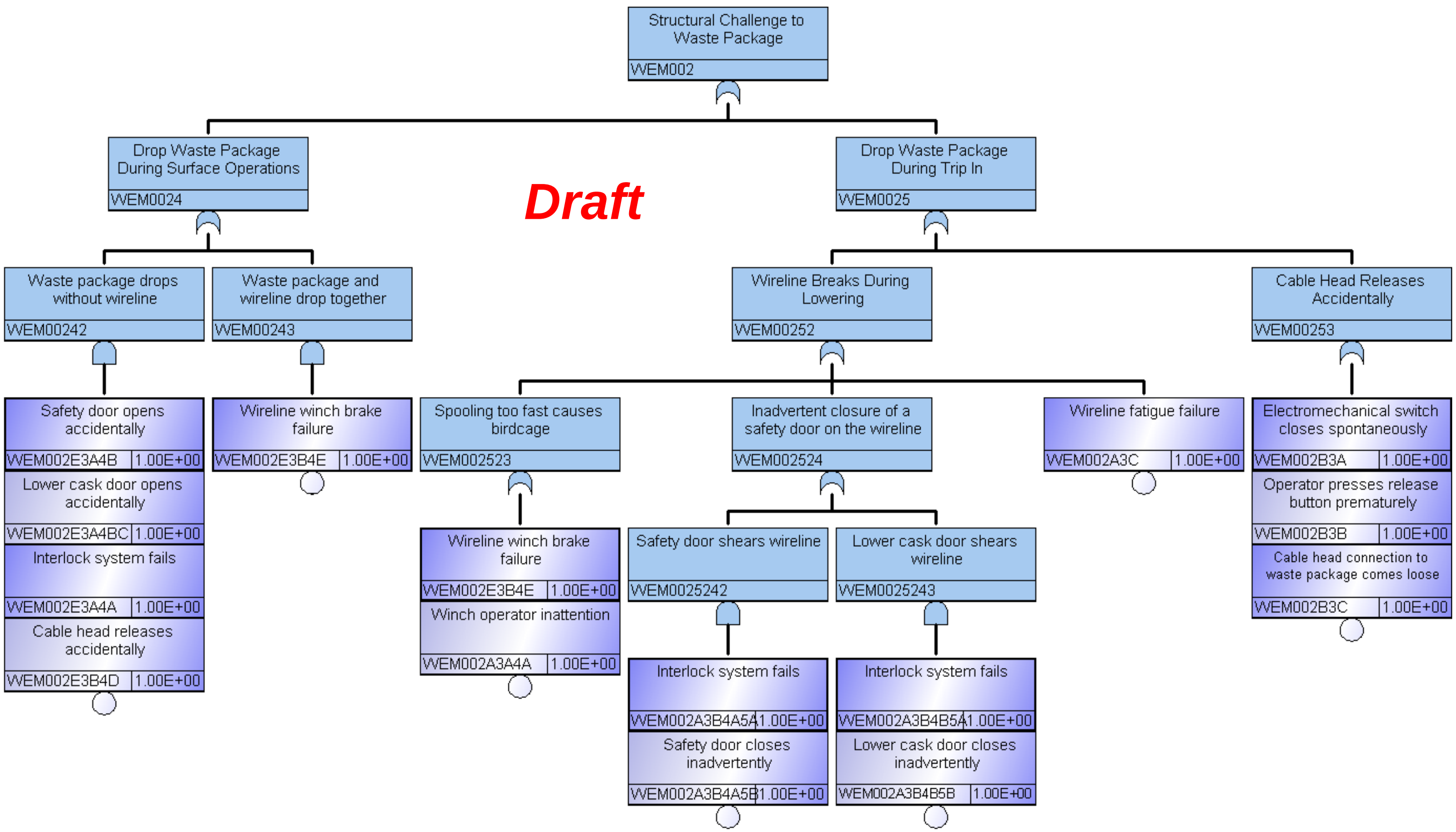
1. **OK**
2. **Direct exposure, shielding loss**
3. **Radionuclide release, filtered by HVAC**
4. **Radionuclide release, filtered by HVAC, also important to criticality**
5. **Radionuclide release, unfiltered by HVAC**
6. **Radionuclide release, unfiltered by HVAC, also important to criticality**

Preliminary "Structural Challenge" Event/Fault Trees for *Wireline* Emplacement

- **Generated with SAPHIRE v8.1.24**
- **Top and intermediate events in fault tree shown in blue; basic events shown in purple**
- **Probabilities are just placeholders**

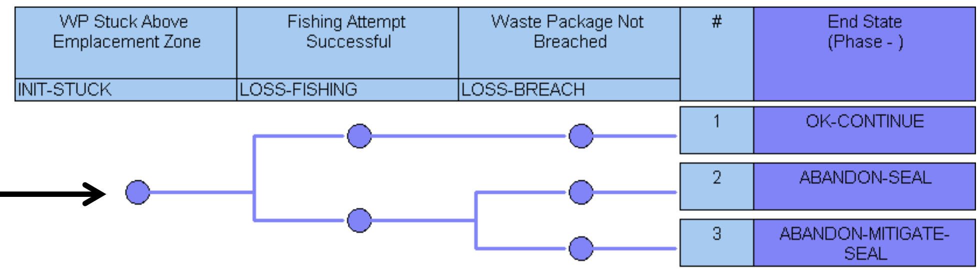


Example End States

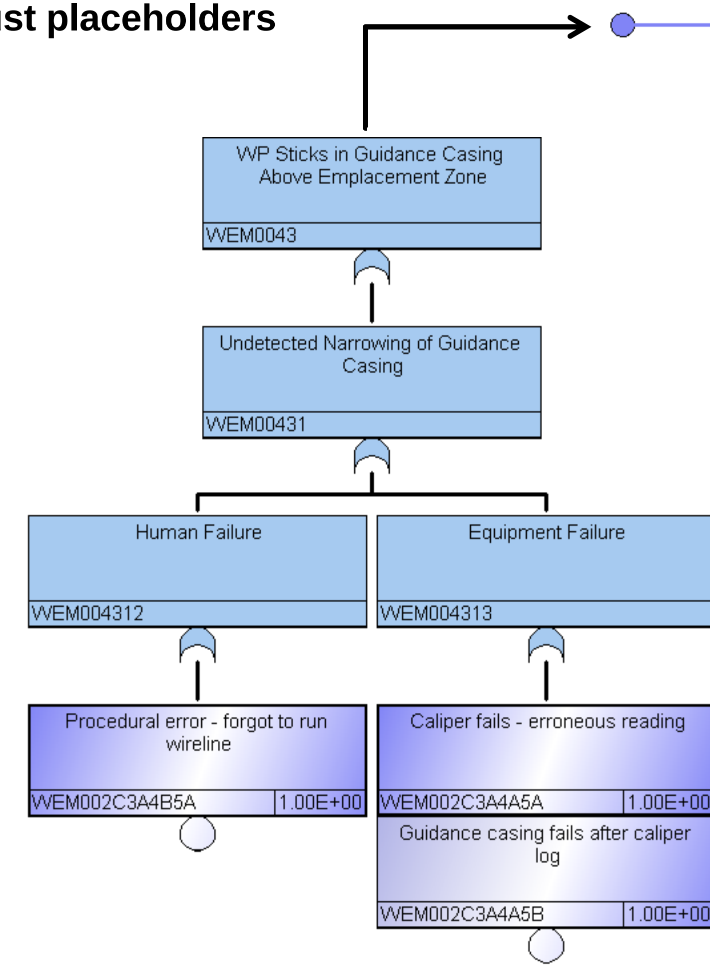


Preliminary “Stuck in Hole” Event/Fault Trees for *Wireline* Emplacement

- **Generated with SAPHIRE v8.1.24**
- **Top and intermediate events in fault tree shown in blue; basic events shown in purple**
- **Probabilities are just placeholders**



Example End States



Draft

Reliability Failure Databases for Frequency/Probability*

1. **Component failure event databases, e.g.,**
   – GIDEP (Government Industry Data Exchange Program) in the U.S.
2. **Accident and incident databases, e.g.,**
   – WOAD (World Offshore Accident Databank), by DNV (Det Norske Veritas)
   – Oil and Gas UK (co-sponsored by the UK Health and Safety Executive)
   – PSID (Process Safety Incident Database), by AIChE
3. **Component reliability databases, e.g.,**
   – OREDA (Offshore Reliability Database), by DNV
   – 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
5. **Various databases cited in YMP PCSA**

* First four major categories of "hardware" reliability databases are according to Rausand and Hoyland (2004), Sec. 14.2. Also, see Vinnem (2007), Sec. 5.9.

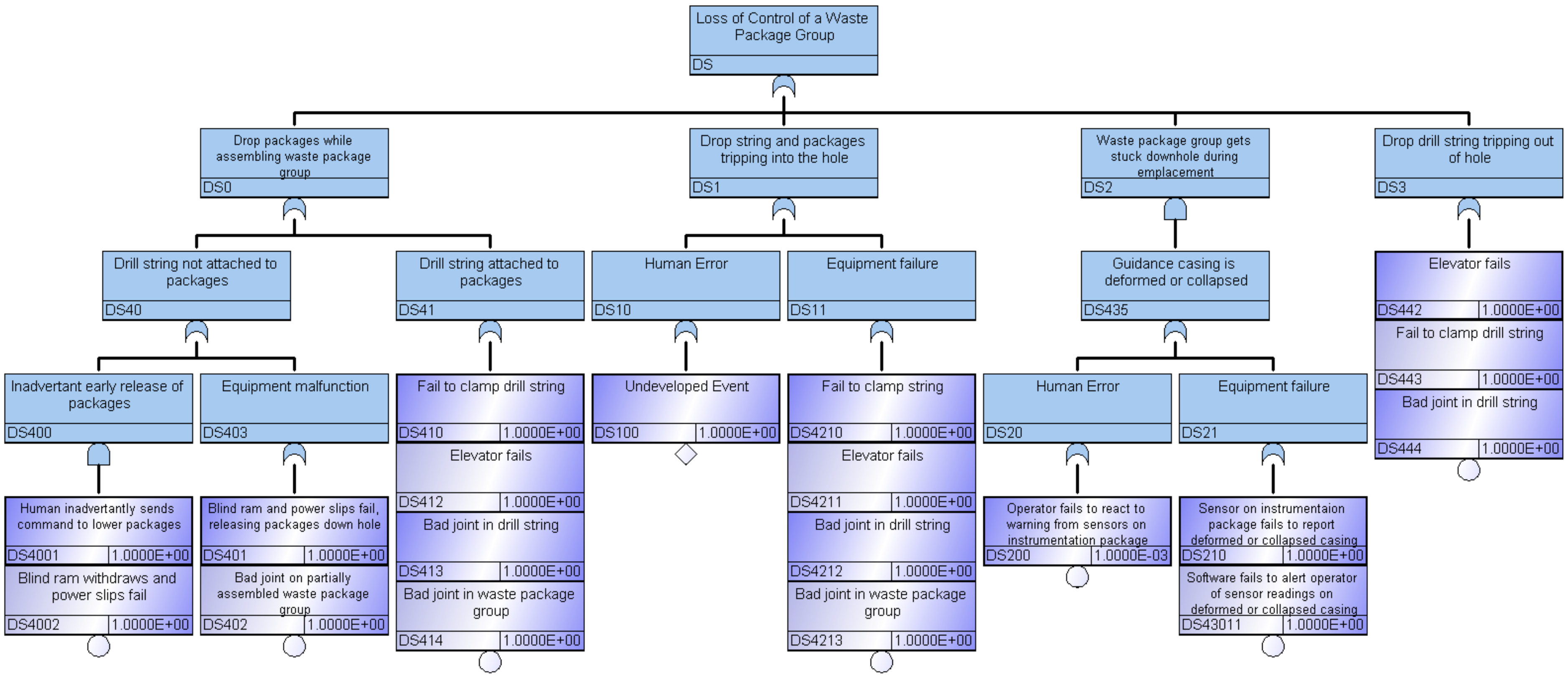
Future Work

- Generate a more detailed wireline fault tree
- Generate a detailed fault tree for drill string emplacement (see next slide)
- Refine consequence terminology and detail
- Determine available accident frequencies and failure probabilities that might be applicable to either wireline or drill string emplacement operations
- Convene an expert panel to review fault trees, accident frequencies, and failure probabilities

Thanks for your attention!

Back-up Slides

Preliminary Fault Tree for *Drill String* Emplacement



Selected References

- Anderson, S. and B. A. Mostue 2012. "Risk analysis and risk management approaches applied to the petroleum industry and their applicability to IO concepts," *Safety Science* 50, 2010-2019.
- Atwood, C. L., J. L. LaChance, H. F. Martz, D. J. Anderson, M. Englehardt, D. Whitehead, and T. Wheeler 2003. *Handbook of Parameter Estimation for Probabilistic Risk Assessment*, NUREG/CR-6823, U.S. Nuclear Regulatory Commission, Washington DC 20555, ADAMS #ML032900131, SAND2003-3348P, Sandia National Laboratories, Albuquerque, NM.
- Aven, T. and J. E. Vinnem 2007. *Risk Management: With Applications from the Offshore Petroleum Industry*, Springer-Verlag London Limited.
- Aven, T., J. E. Vinnem, and H. S. Wiencke 2007. "A decision framework for risk management, with application to the offshore oil and gas industry," *Reliability Engineering and System Safety* 92, 433-448.
- BORA (Barriere & Operajonell Riskoanalyse) 2007. *Operational Risk Analysis—Total Analysis of Physical and Non-physical Barriers, BORA Handbook Rev 00*, June 26, 2007, Preventor AS, Jan Erik Vinnem, Ulstadvn 8, P.O. Box 56, 7541 Klaebu, Norway, http://preventor.no/projects/bora-barrier-and-operational-risk-analysis/
- Brandsaeter, A. 2002. "Risk assessment in the offshore industry," *Safety Science* 40, 231-269.
- BSC 2009. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. 060-PSA-CR00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ENG.20090112.0004. November 2008.
- Calixto, E. 2013. *Gas and Oil Reliability Engineering Modeling and Analysis*, Gulf Professional Publishing (an imprint of Elsevier), Waltham, MA 02451, ISBN 978-0-12-391914-4.
- CCPS (Center for Chemical Process Safety) 1992. *Guidelines for Hazard Evaluation Procedures, 2nd Edition with Worked Examples*, American Institute of Chemical Engineers, New York, New York, 1992.
- CSB (US Chemical Safety and Hazard Investigation Board) 2014. *Investigation Report, Volumes 1 and 2:* Explosion *and Fire at the Macondo Well*, CSB, 2175 K Street, Washington DC 20037, June 5, 2014. http://www.csb.gov/macondo-blowout-and-explosion/
- DOE (U.S. Department of Energy) 2008. *Yucca Mountain Repository License Application Safety Analysis Report.* DOE/RW-0573, Revision 1. U.S. Department of Energy, Washington, D.C. (http://www.nrc.gov/waste/hlw-disposal/yucca-lic-app/yucca-lic-app-safety-report.html#1)
- DOE (U.S. Department of Energy) 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. U.S. Department of Energy, Washington, D.C. 20585

Selected References (cont.)

- Gran B.A., R. Bye, O.M. Nyheim, E.H. Okstad, J. Seljelid, S. Sklet, J. Vatn, and J.E. Vinnem 2012. "Evaluation of the Risk OMT model for maintenance work on major offshore process equipment," *Journal of Loss Prevention in the Process Industries* 25, 582-593.
- Marhavilas, P. K., D. Koulouriotis, and V. Gemeni 2011. "Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000-2009," *Journal of Loss Prevention in the Process Industries* 24, 477-523.
- Matanovic, D., N. Gaurina-Medimurec, and K. Simon 2014. *Risk Analysis for Prevention of Hazardous Situations in Petroleum and Natural Gas Engineering*, Engineering Science Reference (an imprint of IGI Global), Hershey, PA 17033, ISBN 978-1-4666-4777-0.
- NAIIC 2012. *The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission*, The National Diet of Japan, 2012.
- NORSOK 2001. *NORSOK Standard Z-013, Risk and Emergency Preparedness Analysis, Rev.2.*, Norwegian Technology Centre, Oslo, Norway.
- NRC (Nuclear Regulatory Commission) 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis*, NUREG-1624, U.S. Nuclear Regulatory Commission, Washington DC 20555, ADAMS #ML003719212.
- NRC (Nuclear Regulatory Commission) 1998. *Nuclear Fuel Cycle Facility Accident Analysis Handbook*, NUREG/CR-6410, U.S. Nuclear Regulatory Commission, Washington DC 20555, ADAMS #ML072000468.
- NRC (Nuclear Regulatory Commission) 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, Volumes 1 and 2*, NUREG/CR-2300, U.S. Nuclear Regulatory Commission, Washington DC 20555, ADAMS # ML063560439 and ML063560440.
- Pitblado R., B. Bain, A. Falck, K. Litland, and C. Spitzenberger 2012. "Frequency data and modification factors used in QRA studies," *Journal of Loss Prevention in the Process Industries* 24, 249-258.
- Rausand, M. and A. Hoyland 2004. *System Reliabiltiy Theory: Models, Statistical Methods, and Applications, Second Edition*, John Wiley & Sons, Inc., Hoboken, NJ.
- Skogdalen, J. E. and J. E. Vinnem 2012. "Quantitative risk analysis of oil and gas drilling, using Deepwater Horizon as case study," *Reliability Engineering and System Safety* 100, 58-66.
- Skogdalen, J. E. and J. E. Vinnem 2011. "Quantitative risk analysis offshore—Human and organizational factors," *Reliability Engineering and System Safety* 96, 468-479.

Selected References (cont.)

- Smith, C. L. and S. T. Wood 2011. *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8*, NUREG/CR-7039, Volumes 1 through 7, U.S. Nuclear Regulatory Commission, Washington DC 20555, June 2011.
- Thaheem, M. J., A. De Marco, and K. Barlish. 2012. "A Review of Quantitative Analysis Techniques for Construction Project Risk Management," in *Proceedings of the Creative Construction Conference 2012*, ed: M. Hajdu and M. J. Skibniewski, Budapest, Hungary, June 30 – July 3, 2012, ISBN 978-963-269-297-5, Diamond Congress Ltd., Budapest, www.diamond-congress.hu
- Vesely, W. E., F.F. Goldberg, N.M. Roberts, and D.F. Haasl (1981). *Fault Tree Handbook*, NUREG–0492, Office of Nuclear Regulatory Research. U.S. Nuclear Regulatory Commission: Washington DC, January 1981.
- Vinnem, J. E. 2007. *Offshore Risk Assessment: Principles, Modelling and Applications of QRA Studies*, 2nd Edition, Springer-Verlag London Limited 2007.
- Vinnem, J.E., R. Bye, B.A. Gran, T. Kongsvik, O.M. Nyheim, E.H. Okstad, J. Seljelid, and J. Vatn 2012. "Risk modelling of maintenance work on major process equipment on offshore petroleum installations," *Journal of Loss Prevention in the Process Industries* 25, 274-292.
- Vinnem, J. E., T. Aven, T. Husebo, J. Seljelid, and O. J. Tveit 2006. "Major hazard risk indicators for *monitoring* of trends in the Norwegian offshore petroleum sector," *Reliability Engineering and System Safety* 91, 778-791.

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Active Component Reliability Data Sources from YMP PCSA*

*** From BSC (2009, Sec. C1.2): "The data source had to be widely available, not proprietary." References from Table C1.2-1 and Sec. C5.**

- C5.1 *AIChE (American Institute of Chemical Engineers) 1989. *Guidelines for Process Equipment Reliability Data with Data Tables.* G-07. New York, New York: American Institute of Chemical Engineers, Center for Chemical Process Safety. TIC: 259872. ISBN: 978-0-8169-0422-8.
- C5.5 *Blanton, C.H. and Eide, S.A. 1993. *Savannah River Site, Generic Data Base Development (U).* WSRC-TR-93-262. Aiken, South Carolina: Westinghouse Savannah River Company. TIC: 246444.
- C5.6 *Borkowski, R.J.; Kahl, W.K.; Hebble, T.L.; Fragola, J.R.; Johnson, J.W. 1983. *The In Plant Reliability Data Base for Nuclear Plant Components: Interim Report-The Valve -Component.* NUREG/CR-3154; ORNL/TM-8647. Oak Ridge, TN: Oak Ridge National Laboratory. ACC: MOL.20071129.0315.
- C5.7 BSC 2007 (Bechtel SAIC Company). *Waste Form Throughputs for Preclosure Safety Analysis.* 000-PSA-MGRO-01800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071106.0001.
- C5.8 *Canavan, K.; Gregg, B.; Karimi, R.; Mirsky, S.; and Stokley, J. 2004. *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report.* 1009691. Palo Alto, California: Electric Power Research Institute. TIC: 257542.
- C5.10 *Derdiger, J.A.;Bhatt, K.M.;Siegfriedt, W.E. 1981. *Component Failure and Repair Data for Coal-Fired Power Units.* EPRI AP-2071. Palo Alto, CA: Electric Power Research Institute. TIC: 260070.
- C5.11 *Dhillon, B.S. 1988. *Mechanical Reliability: Theory, Models and Applications.* AIAA Education Series. Washington, D.C.: American Institute of Aeronautics & Astronautics. TIC: 259878.
- C5.12 *DOD (U.S. Department of Defense) 1991. *Military Handbook, Reliability Prediction of Electronic Equipment.* MIL-HDBK-217F. Washington, D.C.: U.S. Department of Defense. TIC: 232828.
- C5.13 *Drago, J.P.; Borkowski, R.J.; Fragola, J.R.; and Johnson, J.W. 1982. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Data Report The Pump Component.* NUREG/CR-2886. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071219.0222.
- C5.14 *E.I. du Pont de Nemours & Company 1981. *Some Published and Estimated Failure Rates for Use in Fault Tree Analysis.* Wilmington, Delaware: E.I. du Pont de Nemours & Company. TIC: 260092.

Active Component Reliability Data Sources from YMP PCSA (cont.)

- C5.15 *Eide, S.A.; Gentillon, C.D.; Wierman, T.E.; and Rasmuson, D.M. 2005. *Analysis of Station Blackout Risk.* Volume 2 of *Reevaluation of Station Blackout Risk at Nuclear Power Plants.* NUREG/CR-6890. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071114.0165.
- C5.16 *Eide, S.A.; Wierman, T.E.; Gentillon, C.D.; Rasmuson, D.M.; and Atwood, C.T. 2007. *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.* NUREG/CR-6928. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071211.0229.
- C5.17 *Federal Railroad Administration. 2004. "Train Accidents by Cause from Form FRA F 6180.54." Washington, D.C.: U.S. Department of Transportation, Federal Railroad Administration. Accessed 03/12/2004. ACC: MOL.20040311.0211. URL: http://safetydata.fra.dot.gov/OfficeofSafety/Query/Default.asp
- C5.20 *Framatome ANP (Advanced Nuclear Power) 2001. *Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study -1985-1999.* Lynchburg, Virginia: Framatome Advanced Nuclear Power. ACC: MOL.20011018.0158.
- C5.21 *HID Corporation [n.d.]. Ruggedized Card Reader/Ruggedized Keypad Card Reader. Dorado 740 and 780. Irvine, California: HID Corporation. TIC: 260007.
- C5.22 *IEEE (Institute of Electrical and Electronics Engineers) Std 493-1997. 1998. *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems.* New York, New York: Institute of Electrical and Electronics Engineers. TIC: 243205. ISBN 1-55937-969-3.
- C5.23 *IEEE Std 500-1984 (Reaffirmed 1991). 1991. *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations.* New York, New York: Institute of Electrical and Electronics Engineers. TIC: 256281.
- C5.24 *Kahl, W.K. and Borkowski, R.J. 1985. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report - Diesel Generators, Batteries, Chargers, and Inverters.* NUREG/CR-3831. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071212.0181.
- C5.25 *Laurus Systems [n.d.]. Instruments and Software Solutions for Emergency Response and Health Physics. Ellicott City, Maryland: Laurus Systems. TIC: 259965.

Active Component Reliability Data Sources from YMP PCSA (cont.)

- C5.26 Lloyd, R.L. 2003. *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002.* NUREG-1774. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050802.0185.
- C5.28 *Miller, C.F.; Hubble, W.H.; Trojovsky, M.; and Brown, S.R. 1982. *Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants from January 1, 1976 to December 31, 1980.* NUREG/CR-1363, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071219.0223.
- C5.32 *Moss, T.R. 2005. *The Reliability Data Handbook. 1st* Edition. New York, NY: ASME Press (American Society of Mechanical Engineers). ISBN: 0-7918-0233-7. TIC: 259912.
- C5.35 NRC 1980. *Control of Heavy Loads at Nuclear Power Plants.* NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.
- C5.37 *NSWC (Naval Surface Warfare Center) 1998. *Handbook of Reliability Prediction Procedures for Mechanical Equipment.* NSWC-98/LE1. West Bethesda, Maryland: Naval Surface Warfare Center, Carderock Division. TIC: 245703.
- C5.38 *Peltz, E.; Robbins, M.; Boren, P.; Wolff, M. 2002. "Using the EDA to Gain Insight into Failure Rates.z" *Diagnosing the Army's Equipment Readiness: The Equipment Downtime Analyzer.* Santa Monica, CA: RAND. TIC: 259917. ISBN: 0-8330-3115-5.
- C5.39 *Reece, W.J.; Gilbert, B.G.; and Richards, R.E. 1994. *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Volume 5: Data Manual, Part 3: Hardware Component Failure Data.* NUREG/CR-4639, Vol. 5, Rev. 4. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071220.0209.
- C5.40 *Denson, W.; Chandler, G.; Crowell, W.; Clark, A.; and Jaworski, P. 1994. *Nonelectronic Parts Reliability Data 1995.* NPRD-95. Rome, New York: Reliability Analysis Center. TIC: 259757.
- C5.41 *SAIC (Science Applications International Corporation) 2002. *Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment.* Report No. SAIC-00/2641. Volume I. Abingdon, Maryland: Science Applications International Corporation. ACC: MOL.20071220.0210.
- C5.42 *SINTEF Industrial Management 1992. *OREDA, Offshore Reliability Data Handbook.* 2nd Edition. Trondheim, Norway: OREDA. ISBN: 825150188.1
- C5.43 *SINTEF Industrial Management 2002. *OREDA, Offshore Reliability Data Handbook.* 4th Edition. Trondheim, Norway: OREDA. ISBN: 8214027055. TIC: 257402.
- C5.45 *Trojovsky, M. 1982. *Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, January 1, 1972 to April 30, 1980.* NUREG/CR-1205, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20080207.0024.
- C5.46 *Zentner, M.D.; Atkinson, J.K.; Carlson, P.A.; Coles, G.A.; Leitz, E.E.; Lindberg, S.E.; Powers, T.B.; and Kelly, J.E. 1988. *N Reactor Level 1 Probabilistic Risk Assessment: Final Report.* WHC-SP-0087. Richland, Washington: Westinghouse Hanford Company. ACC: MOL.20080207.0021

Problems Encountered During Wireline and CT Operations

Activity	% failure on first run	% failure on second run	Comments
WL run to EOT in 2-3/8" tubing	14%		improve if cool water circulated[4]
WL run to EOT in larger tubing	<2%		
WL Plug setting	5%		Assumes low scale, low paraffin environment
WL Plug pulling	20%	15%	Debris over plug is major problem
CT Plug Setting	10 to 15%		Problems in sensitivity and depth control
CT plug pulling	10 to 15%		
WL Perforating	2%to 3%	<1%	detonator/conductivity problems, assumes tubing is open to TD[32]
CT Perforating	5% to 8%	3%	detonator/gun-to-gun failure, assumes tubing is open to TD[32]
Tubing Puncher Charge	5%		Depends on magnetic decentralizer operation[33]
Tube cut off, below packer	75%	75%	Incomplete cut without tension[29]
Tube cut off, above packer	20%	20%	Insufficient overpull, coatings & heavy or alloy pipe[29,30]
Sliding Sleeve Operation	10 to 50%		depends on age, corrosion and debris, improve with CT impact tool on CT

Event Tree Analysis (ETA)

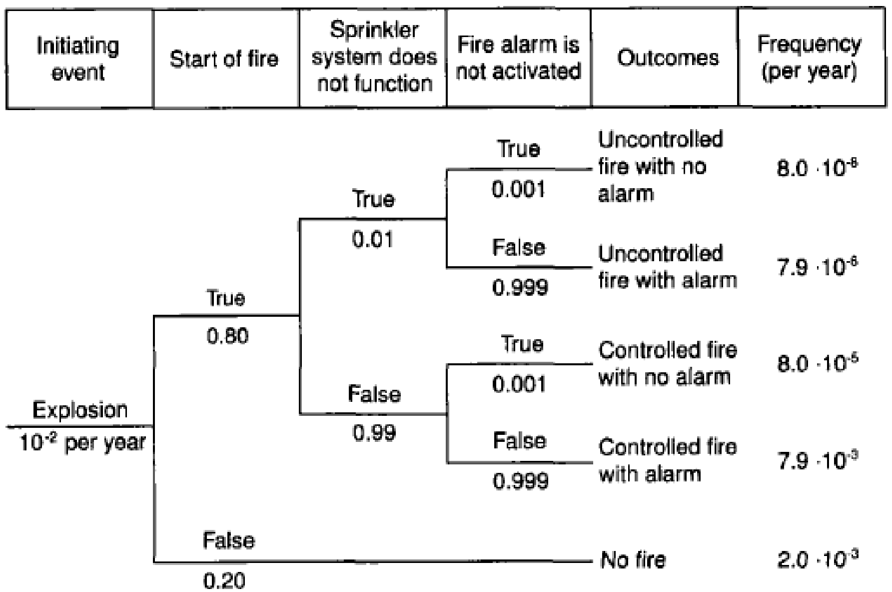
- **Major steps in an event tree analysis (e.g., after Rausand and Hoyland 2004; CCPS 1992), an *inductive* technique:**

1. Identification of an *initiating event (hazard)* causing the accident or failure
2. Identification/design of *safety functions* /barriers/procedures to mitigate the initiating event—failure of a barrier results in an *"intermediate" 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*

End States



*Convention: Upper branches represents success ("true"), while lower branches represent failure ("false").

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

Fault Tree Analysis (FTA)—with an example from the YMP PCSA*

- **Five major steps in an fault tree analysis (e.g., after Rausand 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 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 (e.g., component failures) which, if they all occur or exist, will cause the top event to occur*

Fault tree for one of the *initiating events* that might compromise a canister in the YMP Canister Transfer Machine (CTM)

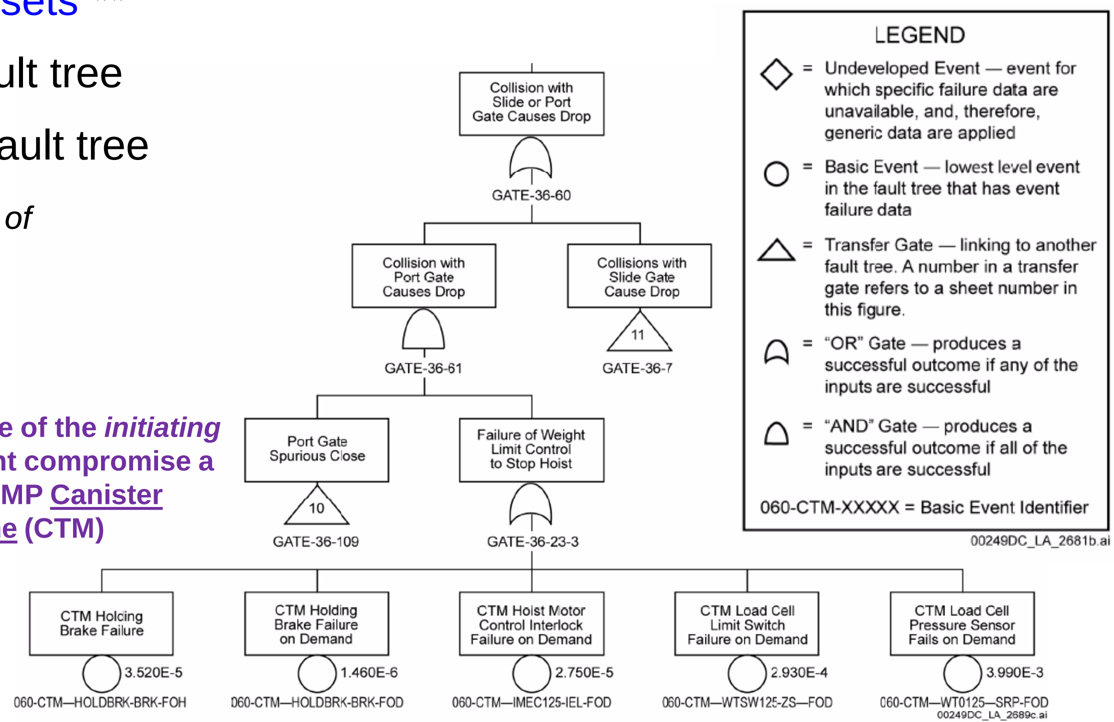


Figure 1.7-8. Example of Fault Tree of the Preclosure Safety Analysis (Sheet 9 of 12)

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.

*** Yucca Mountain Project Pre-closure Safety Analysis**

Strengths 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 ("pivotal") events in an event sequence

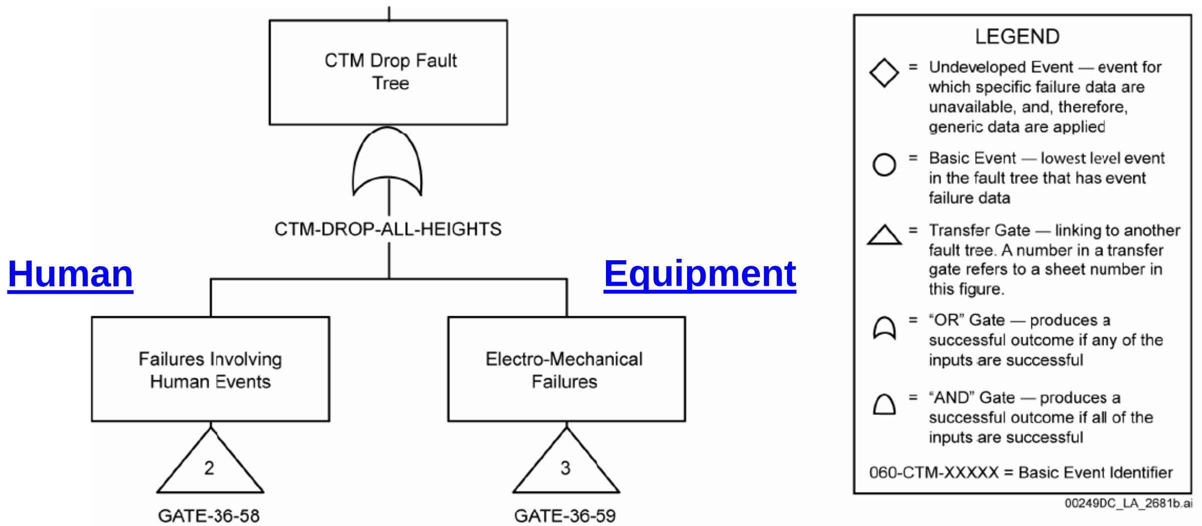


Figure 1.7-8. Example of Fault Tree of the Preclosure Safety Analysis (Sheet 1 of 12)

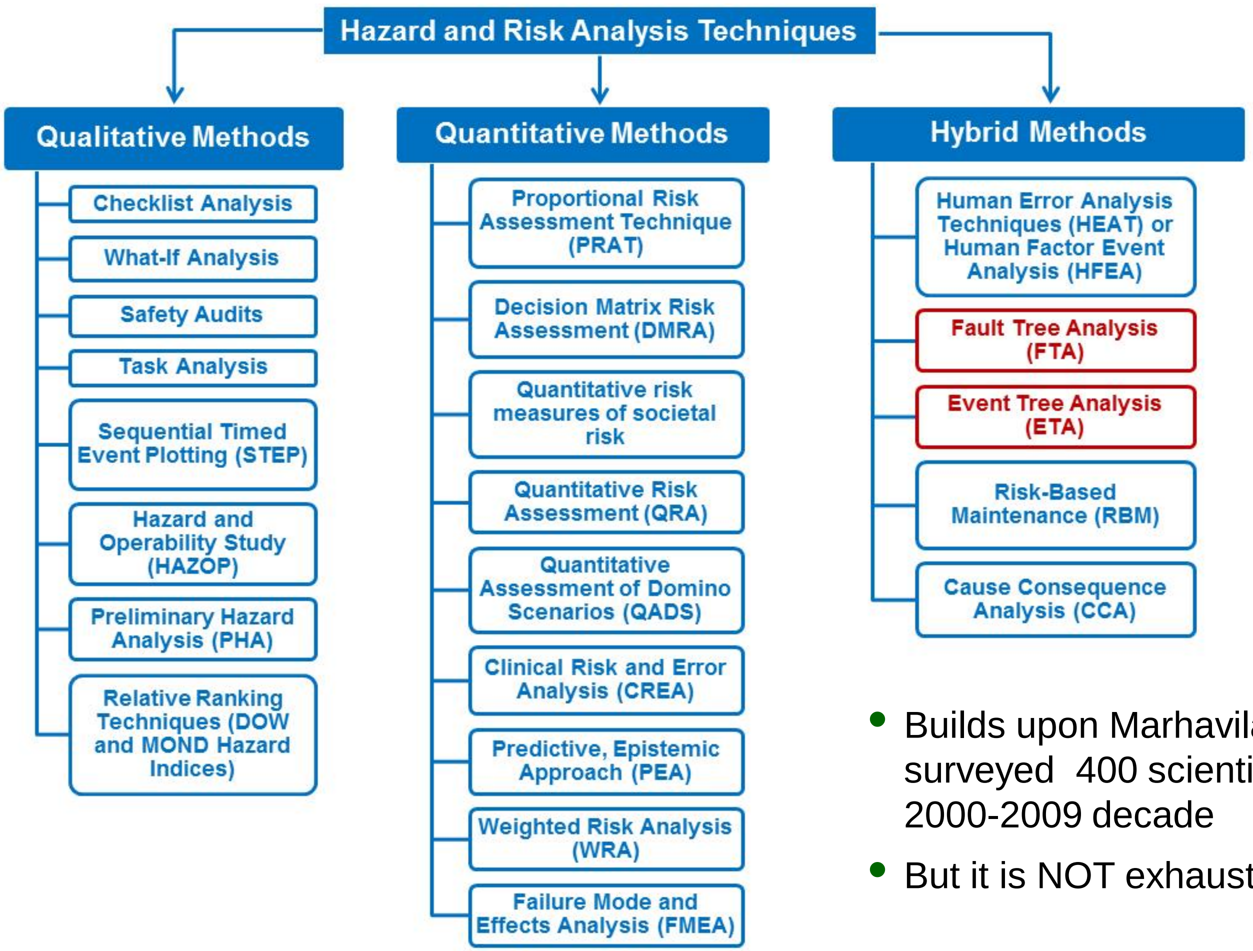
NOTE: CTM = canister transfer machine.

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.

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

Potential "Internal" Hazardous Events for *Wireline* Emplacement—based on emplacement steps

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	Drop waste package during surface operations	<u>Risk prevention measure</u>: Cask/wellhead-safety-door/blind-ram interlock system	include
Immediate-cause event	Drop waste package during trip into hole		include
Immediate-cause event	Waste package sticks in guidance casing or hanger during trip into hole		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	<u>Risk prevention measure</u>: 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.	<u>Risk prevention measure</u>: 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	<u>Risk prevention assumption</u>: 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	<u>Risk prevention assumption:</u> 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

Potential "Internal" Hazardous Events for *Wireline* Emplacement—based on emplacement steps (cont.)

Event Identifier	Description of Potential Hazardous Event (based on sequential emplacement steps)	Risk Mitigation Measures, Assumptions, and Other Notes	Screening decision (include/exclude)
Basic event	Wellhead safety door closes inadvertently on the waste package	Risk prevention 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 prevention assumption: Waste package is strong enough to be structurally unaffected.	exclude
Basic event	Bird cage of wireline	Risk prevention measure: Automated speed and tension control on wireline winch	include
Basic event	Wireline fatigue failure	Risk prevention 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 prevention 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 prevention measure: Caliper log run prior to waste package emplacement trip	include
Basic event	Site-wide power failure	Risk prevention 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