Overview of “BSEE-2016-XXX Probabilistic Risk Assessment Procedures Guide for Offshore Applications (Partial Draft)”

Presentation to PHMSA RMWG

Bob Youngblood

March 9, 2017
Disclaimer

Views expressed by the presenter are not necessarily those of the Idaho National Laboratory or Johnson Space Center.
Summary

- NASA’s Johnson Space Center (JSC) is developing a PRA Procedures Guide for BSEE, initially scoped to deal with offshore drilling
- INL is helping JSC do that
- By agreement between JSC and BSEE, the starting point for the development was NASA’s PRA Procedures Guide
  - Development of the NASA guide was initiated after Challenger
  - The NASA guide was heavily influenced by nuclear industry PRA guidance
    - Initially (2002), mostly logic modeling, which is good at functional dependency, redundancy, etc., but rather approximate in some ways
    - Later (2011), the guide paid some attention to simulation, which is better at timing, variations in event phenomenology, ...
  - We are trying to be responsive to oil-industry risk modeling needs, not blindly assume nuclear/ NASA PRA techniques are optimal
- The Draft BSEE Guide addresses [or will address, when complete]
  - Standard high-end logic-model tools
  - More qualitative risk assessment tools
  - Simulation-enhanced PRA [placeholder for now]
  - Improved discussion of data analysis
  - Better understanding of uncertainty
  - Improved discussion of the USE of risk model results
In the Late 60’s / Early 70’s, Some Were Beginning to Advocate Modern Risk Analysis*


Principles of Unified Systems Safety Analysis [USSA]
B. John Garrick, 1970

… USSA has been evolved to both assess and monitor the level of safety while revealing necessary adjustments either in design, procedure, or both to sustain a prescribed level. … put the more analytical activities of safety analysis in context with the more routine activities of operations to assure to the extent possible their proper interactions. …

*That is, the use of logic models (event trees, fault trees) to construct and quantify a notionally complete scenario set

Two things going on:
• How safe is this facility?
• How do we best manage risk?
Why do we do risk analysis?

• To support decisions…
• … in situations characterized by
  – High stakes
  – Complexity
  – Significant uncertainty
  – Diversity of stakeholders

• One definition of risk:
  – \{scenarios, scenario frequencies, scenario consequences\} \ (Kaplan and Garrick, 1981)
    • With treatment of uncertainty…
  – A point of this definition is that just giving the decision-maker a single number (like “expected consequences”) may help, but doesn’t indicate what more would be helpful to know, or what would be helpful to fix
OVERVIEW OF HIGH-END SCENARIO-BASED PRA
Not understood in the US at the time of WASH-1400

Table 3. Conditional cut sets for the dominant sequences.

<table>
<thead>
<tr>
<th>Importance</th>
<th>Percent Contribution</th>
<th>Minimal Cut Sets (of basic events)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Tree: RCP-BUS-UV Sequence: 2-18-03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2E-006</td>
<td>70.01</td>
<td>EPS-XHE-XL-NR04H /RCS-MDP-LK-BP2 EPS-DGN-NR04H</td>
</tr>
<tr>
<td>5.3E-007</td>
<td>16.92</td>
<td>EPS-XHE-XL-NR04H /RCS-MDP-LK-BP2 EPS-DGN-NR04H</td>
</tr>
<tr>
<td>2.1E-007</td>
<td>6.77</td>
<td>EPS-XHE-XL-NR04H /RCS-MDP-LK-BP2 EPS-DGN-NR04H</td>
</tr>
<tr>
<td>3.1E-006</td>
<td>100</td>
<td>Total (all cutsets)</td>
</tr>
</tbody>
</table>

Figure 4. Event tree for station blackout.
Two things going on:
- How safe is this facility?
- How do we best manage risk?

Figure 8. Use of PRA to select BDBEs.
EVOLUTION OF “PRA PROCEDURES GUIDES”
Selected “Procedures Guides”


PHMSA
Consensus Standards, “PRA Quality” concerns, Other Regulatory Guidance

• PRA standards have also been under development by the American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS):
  – ASME and ANS jointly issued an at-power Level 1 and limited Level 2 PRA standard for internal and external hazards (requirements for low power shutdown conditions to be added) (Ref. 14).2
  – ASME is developing PRA standards for new LWRs applying for design certification (DC) and COLs, and for future advanced non-LWRs. ANS is developing a Level 1 and limited Level 2 PRA standard for low-power shutdown operating mode (to be incorporated into the ASME/ANS joint standard), and is also developing Level 2 and Level 3 PRA standards.

• NRC Regulatory Guide 1.200
  – When used in support of an application, this regulatory guide will obviate the need for an in-depth review of the base PRA by NRC reviewers, allowing them to focus their review on key assumptions and areas identified by peer reviewers as being of concern and relevant to the application. Consequently, this guide will provide for a more focused and consistent review process. In this regulatory guide, the quality of a PRA analysis used to support an application is measured in terms of its appropriateness with respect to scope, level of detail, and technical acceptability.
Evolution of PRA Procedures Guides

State of the art as of ~ 1980; authored by almost the entire community of practice that existed as of 1979; focused on nuclear power plants. Not prescriptive: rather, descriptive of a buffet of techniques.

Context: Post-Three-Mile-Island; General perception of the hazard (the range of potential consequences); Recognition of the need for regulators to get beyond purely prescriptive thinking; Recognition of the need for a structured approach to risk assessment.
Comment on “getting beyond purely prescriptive thinking”

• Before the 1979 accident at Three Mile Island, the Reactor Safety Study (1975) had already illustrated some of what’s wrong with prescriptive approaches to safety analysis

• In general, prescriptive approaches…
  – … leave undone some of what ought to be done (they miss significant risk contributors)
  – … do things that ought not to be done (expend resources preventing things that are unlikely a priori, or unlikely to cause real problems even if they do occur

• Risk analysis isn’t perfect; you have to work hard to try to assure completeness and reasonableness of modeling, especially in areas where the community of practice has not reached consensus

• But it’s better than nothing, and over the years, has come to play a very important role in NRC decision-making
Evolution of PRA Procedures Guides (continued)

State of practice of fault tree / event-tree methods as of 2002-2011; authored by PRA practitioners who were also mostly conversant with NASA technologies

Context: Post-Challenger; General perception of the hazard (the range of potential consequences); Recognition of the need for a structured approach to risk assessment
BSEE PRA Guide

• Context: Post-Macondo

• Purpose
  – This Guide is intended to assist in the development of probabilistic risk assessment (PRA) of offshore drilling facilities, in order to support decision-making by Bureau of Safety and Environmental Enforcement (BSEE) and by the industry.

• Scope
  – This Guide is not a policy document, nor does it establish regulatory requirements; it discusses particular modeling techniques that have been found to be useful in a range of applications to decision-making about complex and high-hazard facilities.
Graded approach, keyed to decision support needs
Graded Approach to System Safety Analysis

Examples of Decisions
- Architecture A vs. Architecture B vs. Architecture C
- Technology A vs. Technology B
- Intervene in Process Based on Performance, vs. Do Not Intervene
- Comparison of Reliability or Performance Allocations
- Prioritization
- Contingency Plan A vs. Contingency Plan B

Decision Alternatives For Analysis

Deliberation and Ranking / Selection of Preferred Alternative (See Figure 9)

Risk & TPM Results

Yes

No

Is the Ranking / Comparison Robust?

Yes

No

Cost-Beneficial to Reduce Uncertainty?

Yes

No

Additional Uncertainty Reduction If Necessary Per Stakeholders

* NPR 8715.3C requires PRA in certain situations, e.g., human space flight
Risk-Informed Decision-Making

Decision Alternatives For Analysis
- Scoping & Determination of Methods To Be Used

Qualitative Techniques
- Identify
- Analyze

Quantitative Techniques
- Identify
- Analyze

Risk Analysis Techniques

Examples of Decisions
- Architecture A vs. Architecture B vs. Architecture C
- Technology A vs. Technology B
- Intervene in Process Based on Performance, vs. Do Not Intervene
- Comparison of Reliability or Performance Allocations
- Prioritization
- Contingency Plan A vs. Contingency Plan B

Much Existing Oil / Process Industry Practice

Deliberation and Ranking / Selection of Preferred Alternative (See Figure 9)

Yes

Risk & TPM Results

Is the Ranking / Comparison Robust?
- Yes
- No

Cost-Beneficial to Reduce Uncertainty?
- Yes
- No

Preliminary Risk & TPM Results

Additional Uncertainty Reduction If Necessary Per Stakeholders

Emphasis of both NRC and NASA PRA Procedures Guides

* NPR 8715.3C requires PRA in certain situations, e.g., human space flight
I. Examples of Decisions
- Architecture A vs. Architecture B vs. Architecture C
- Technology A vs. Technology B
- Intervene in Process Based on Performance vs. Do Not Intervene
- Comparison of Reliability or Performance Allocations
- Prioritization
- Contingency Plan A vs. Contingency Plan B

II. Risk Analysis Techniques
- Spectrum of Available Techniques
- Preliminary Risk & TPM Results

III. Deliberation and Ranking / Selection of Preferred Alternative (See Figure 9)
- Risk & TPM Results
  - Is the Ranking / Comparison Robust?
    - Yes
      - Additional Uncertainty Reduction If Necessary Per Stakeholders
    - No
      - Cost-Beneficial to Reduce Uncertainty?
        - Yes
          - Additional Uncertainty Reduction If Necessary Per Stakeholders
        - No

* NPR 8715.3C requires PRA in certain situations, e.g., human space flight*
• Section 1 – Introduction
• Section 2 – Risk Analysis Techniques
• Section 3 – Results Presentation and Interpretation

• Appendix A – Example Basic Event Naming Conventions for Fault Trees
• Appendix B – Fault Tree Gate Logic and Quantification
• Appendix C – Calculating Frequency, Reliability, and Availability Metrics
• Appendix D – Common Cause (TBD)
• Appendix E – Sources of Failure Rate and Event Data
BSEE PRA Guide – Table of Contents (cont’d)

• Appendix F – Further Discussion of Bayesian Updating
• Appendix G – Population Variability Modeling (TBD)
• Appendix H – Expert Elicitation
• Appendix I – Failure Space Based Importance Measures
• Appendix J – Prevention Worth
• Appendix K – Top Event Prevention Analysis
• Appendix L – Human Reliability
Used to develop examples for various techniques in the guide
FIGURES AND TABLES FROM THE GUIDE

Following slides are taken from the guide itself
They are shown here as representative of the style and content of the guide’s coverage
Figure 2- 1. Example of Bowtie Analysis Diagram
Figure 2-1. Typical Qualitative Risk Matrix
Figure 2-1. Notional Master Logic Diagram Related to Candidate Initiating Events
Figure 2-1. The Elements of an Accident Scenario
Figure 2-6. Event Sequence Diagram for a Well Kick from an Unexpected Overpressure Zone
Well Kick detected prior to reaching BOP


Initiating Events Leading to a Well Kick:
- Underbalanced Mud
- Overbalanced mud leaks to formation
- Swab/surge effect while tripping
- Unexpected overpressure zone

Formation fluid past the BOP

Used diverter for personnel safety

Rig performs emergency disconnect (autoshear triggered)

Risk to personnel topside, possibly abandon

Continuous observe flow during shut in process

Blind shear ram successfully closes

Limited Release Well Shut In
Figure 2- 1. Example Event Tree Sequence
Figure 2-13. Event Tree Structure for Well Kick from an Unexpected Overpressure Zone
Figure 2- 1. Typical Fault Tree Structure and Symbols
Figure 2- 1. Basic Fault Tree
Frequently, you can understand a lot of what a logic model is saying from a diagram like this.
Figure 2-27. Common Cause Modeling for a 3 of 4 System
Figure 2- 1. Sources of Information for Quantification of Basic Event Likelihood
<table>
<thead>
<tr>
<th>Basic Event Type</th>
<th>Commonly-Used Models of Basic Event Probability</th>
<th>Data Required in Order to Quantify Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiating event</td>
<td>Poisson model for probability of seeing k events in time t: ( Pr(k) = e^{-\lambda t} \frac{(\lambda t)^k}{k!} ) where t: Mission time ( \lambda ): frequency</td>
<td>Number of events k in time t</td>
</tr>
<tr>
<td>Component fails on demand</td>
<td>Constant probability of failure on demand, or ( q )</td>
<td>Number of failure events k in total number of demands N</td>
</tr>
<tr>
<td>Standby component fails in time, or component changes state between tests (faults revealed on functional test only)</td>
<td>Constant standby failure rate ( Q = 1 - \frac{1 - e^{-\lambda_s T_s}}{\lambda_s T_s} ) ( T_s ): Time between tests ( \lambda_s ): Standby failure rate</td>
<td>Number of events k in total time in standby T</td>
</tr>
<tr>
<td>Component in operation fails to run, or component changes state during mission (state of component continuously monitored)</td>
<td>Constant failure rate ( U = 1 - e^{-\lambda_0 T_m} \approx \lambda_0 T_m ) ( T_m ): Mission time ( \lambda_0 ): Operating failure rate Approximation is adequate when ( \lambda_0 T_m \ll 1 )</td>
<td>Number of events k in total exposure time T (total time standby component is operating, or time the component is on line)</td>
</tr>
<tr>
<td>Component unavailable due to test</td>
<td>( Q = \frac{T_{TD}}{T_s} ) ( T_{TD} ): Test duration (only in the case of no override signal) ( T_s ): Time between tests</td>
<td>Average test duration (( T_{TD} )) and time between tests (( T_s ))</td>
</tr>
</tbody>
</table>

Component unavailable due to corrective maintenance (fault revealed only at periodic test, or preventative maintenance performed at regular intervals) \( Q = \frac{T_U}{T_T} \) \( T_U \): Total time unavailable while in maintenance (out of service) \( T_T \): Total operating time |

Component unavailable due to unscheduled maintenance (continuously monitored components) \( Q = \frac{\mu T_R}{1 + \mu T_R} \) \( T_R \): Average time of a maintenance outage ["Repair time"]. \( \mu \): Maintenance rate Number of maintenance acts r in time T (to estimate \( \mu \)) |

Standby component that is never tested. Assumed constant failure rate. \( Q = 1 - e^{-\lambda_m T_P} \) \( T_P \): Exposure time to failure \( \lambda_m \): Standby failure rate Number of failures r, in T units of (standby) time |

Common-Cause Failure Probability (Refer to Appendix D) \( \alpha_T \), through \( \alpha_m \), where \( m \) is the redundancy level \( n_k \) through \( n_m \), where \( n_k \) is the number of CCF events involving k components |

Total time out of service due to maintenance acts while system is operational, \( T_U \) and total operating time \( T_T \). |
Figure 2-37. Example Discrete Event Simulation Model
We characterize the design intent in terms of design reference missions and other requirements to be satisfied. The design itself is characterized at a level of detail appropriate to the current life cycle phase.

We specify the design for the current life cycle phase (including requirements and controls).*

We understand what is credited

We understand the nominal performance and dynamic response in design reference phases

We understand the performance allocation

We have formulated hazard controls, derived requirements, and fault protection approaches in a risk-informed manner

We present the results of analysis, conditional on an explicitly characterized baseline allocation of levels of performance, risk-informed requirements, and operating experience. We have a process for identifying departures from this baseline and/or addressing future emergent issues that are not addressed by this baseline.

We have performed our analyses and established the following results:
- Aggregate risk results
- Dominant accident scenarios
- Comparison with threshold/goal
- Established baseline for precursor analysis

In addition to reviewing existing information sources and operating experience, we have applied the best processes known to us for identifying previously unrecognized safety hazards

We recognize the limits of our safety models: we have evaluated the caliber of evidence used in models, and have performed uncertainty and sensitivity analyses. To the extent practicable, we have addressed the completeness issue, and have developed a thorough understanding of key phenomenology and assumptions

We have provided some defense against currently unrecognized safety issues (safety margin)

We have demonstrated that no further improvements to the design or operations are currently net-beneficial (risk is as low as reasonably practicable)

We carried out a process to identify significant safety improvements, but no candidate measures have been identified

We have determined that further improvements in safety would unacceptably affect schedule

We have determined that further improvements in safety would incur excessive performance penalties

We have determined that further improvements in safety would incur excessive cost

We understand the implementation aspects needed to achieve the level of safety claimed, and commit to the necessary measures.

We have confirmed that allocated performance is feasible

We understand how to monitor and assure ongoing satisfaction of allocated performance levels, and there are commitments to implement these measures

We have identified and prioritized risks in the risk management program

We continue to evaluate operational experience for the presence of accident precursors

---

**Figure 3-1. "Claims Tree"**

---

*This is "how safe" we are (or will be), how we know it, and what we are doing to make sure that it comes true (or remains true).*

This is our technical basis for the claim:

- Evidence, including operating experience, testing, associated engineering analysis, and a comprehensive, integrated, scenario-based design and safety analysis
- A credible set of performance commitments, deterministic requirements, and implementation measures.

The nature and specificity of the claim, and the character of the underlying evidence, depend on the life cycle phase at which the safety case is being applied.
<table>
<thead>
<tr>
<th>#</th>
<th>Prob/Freq</th>
<th>Cut Set Contribution %</th>
<th>Cut Set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>5.598E-4</td>
<td>100</td>
<td>Displaying 10 Cut Sets, (9794 Original)</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2.471E-4</td>
<td>44.14</td>
<td>DRILLING : sequence 14-1</td>
<td>Well Kick While Drilling</td>
</tr>
<tr>
<td>1</td>
<td>1.000E+0</td>
<td></td>
<td>DRILLINGKICK</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>3.530E-4</td>
<td></td>
<td>BOP-POD-YLBL-CCF</td>
<td>Common cause failure of blue and yellow pods</td>
</tr>
<tr>
<td>1</td>
<td>7.000E-1</td>
<td></td>
<td>/ROV</td>
<td>ROV intervention unsuccessful</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>LARGERELEASEOV</td>
<td>Added through Event Tree Add</td>
</tr>
<tr>
<td>2</td>
<td>2.000E-4</td>
<td>35.73</td>
<td>DRILLING : sequence 16</td>
<td>Well Kick While Drilling</td>
</tr>
<tr>
<td>2</td>
<td>1.000E+0</td>
<td></td>
<td>DRILLINGKICK</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2.000E-4</td>
<td></td>
<td>DRL-HUM-ERR-001</td>
<td>Kick not properly detected</td>
</tr>
<tr>
<td>3</td>
<td>9.531E-5</td>
<td>17.03</td>
<td>DRILLING : sequence 14-2</td>
<td>Well Kick While Drilling</td>
</tr>
<tr>
<td>3</td>
<td>9.531E-5</td>
<td></td>
<td>DRILLINGKICK</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3.530E-4</td>
<td></td>
<td>BOP-POD-YLBL-CCF</td>
<td>Common cause failure of blue and yellow pods</td>
</tr>
<tr>
<td>3</td>
<td>9.000E-1</td>
<td></td>
<td>/CAPSTACK</td>
<td>Well Capping unsuccessful</td>
</tr>
<tr>
<td>3</td>
<td>3.000E-1</td>
<td></td>
<td>ROV- FTR-001</td>
<td>ROV intervention unsuccessful</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>LARGERELEASECAP</td>
<td>Added through Event Tree Add</td>
</tr>
<tr>
<td>4</td>
<td>1.000E-5</td>
<td>1.80</td>
<td>DRILLING : sequence 14-3</td>
<td>Well Kick While Drilling</td>
</tr>
<tr>
<td>4</td>
<td>1.000E+0</td>
<td></td>
<td>DRILLINGKICK</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3.530E-4</td>
<td></td>
<td>BOP-POD-YLBL-CCF</td>
<td>Common cause failure of blue and yellow pods</td>
</tr>
<tr>
<td>4</td>
<td>1.000E-1</td>
<td></td>
<td>CAP-LKG-001</td>
<td>Well capping unsuccessful</td>
</tr>
<tr>
<td>4</td>
<td>9.500E-1</td>
<td></td>
<td>/RELIEFWELL</td>
<td>Relief Well unsuccessful</td>
</tr>
<tr>
<td>4</td>
<td>3.000E-1</td>
<td></td>
<td>ROV-FTR-001</td>
<td>ROV intervention unsuccessful</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>LARGERELEASERELIEF</td>
<td>Added through Event Tree Add</td>
</tr>
<tr>
<td>5</td>
<td>4.699E-6</td>
<td>0.84</td>
<td>DRILLING : sequence 14-1</td>
<td>Well Kick While Drilling</td>
</tr>
<tr>
<td>5</td>
<td>1.000E+0</td>
<td></td>
<td>DRILLINGKICK</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2.590E-3</td>
<td></td>
<td>BOP-POD-FTR-BLUE</td>
<td>Blue pod (standby) fails to run</td>
</tr>
<tr>
<td>5</td>
<td>2.590E-3</td>
<td></td>
<td>BOP-POD-FTR-YELLOW</td>
<td>Yellow pod (operating) fails to run</td>
</tr>
<tr>
<td>5</td>
<td>7.000E-1</td>
<td></td>
<td>/ROV</td>
<td>ROV intervention unsuccessful</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>LARGERELEASEOV</td>
<td>Added through Event Tree Add</td>
</tr>
<tr>
<td>6</td>
<td>1.811E-6</td>
<td>0.32</td>
<td>DRILLING : sequence 14-2</td>
<td>Well Kick While Drilling</td>
</tr>
<tr>
<td>6</td>
<td>1.000E+0</td>
<td></td>
<td>DRILLINGKICK</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2.590E-3</td>
<td></td>
<td>BOP-POD-FTR-BLUE</td>
<td>Blue pod (standby) fails to run</td>
</tr>
<tr>
<td>6</td>
<td>2.590E-3</td>
<td></td>
<td>BOP-POD-FTR-YELLOW</td>
<td>Yellow pod (operating) fails to run</td>
</tr>
<tr>
<td>6</td>
<td>9.000E-1</td>
<td></td>
<td>/CAPSTACK</td>
<td>Well Capping unsuccessful</td>
</tr>
<tr>
<td>6</td>
<td>3.000E-1</td>
<td></td>
<td>ROV-FTR-001</td>
<td>ROV intervention unsuccessful</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>LARGERELEASECAP</td>
<td>Added through Event Tree Add</td>
</tr>
<tr>
<td>7</td>
<td>5.295E-7</td>
<td>0.09</td>
<td>DRILLING : sequence 14-4</td>
<td>Well Kick While Drilling</td>
</tr>
<tr>
<td>7</td>
<td>1.000E+0</td>
<td></td>
<td>DRILLINGKICK</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>2.590E-3</td>
<td></td>
<td>BOP-POD-FTR-BLUE</td>
<td>Blue pod (standby) fails to run</td>
</tr>
<tr>
<td>7</td>
<td>2.590E-3</td>
<td></td>
<td>BOP-POD-FTR-YELLOW</td>
<td>Yellow pod (operating) fails to run</td>
</tr>
<tr>
<td>7</td>
<td>9.000E-1</td>
<td></td>
<td>/CAPSTACK</td>
<td>Well Capping unsuccessful</td>
</tr>
<tr>
<td>7</td>
<td>3.000E-1</td>
<td></td>
<td>ROV-FTR-001</td>
<td>ROV intervention unsuccessful</td>
</tr>
<tr>
<td>8</td>
<td>1.912E-7</td>
<td>0.03</td>
<td>DRILLING : sequence 14-3</td>
<td>Well Kick While Drilling</td>
</tr>
<tr>
<td>8</td>
<td>1.000E+0</td>
<td></td>
<td>DRILLINGKICK</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>3.530E-4</td>
<td></td>
<td>BOP-POD-YLBL-CCF</td>
<td>Common cause failure of blue and yellow pods</td>
</tr>
<tr>
<td>8</td>
<td>1.000E-1</td>
<td></td>
<td>CAP-LKG-001</td>
<td>Well capping unsuccessful</td>
</tr>
<tr>
<td>8</td>
<td>5.000E-2</td>
<td></td>
<td>REL-WELL-LKG-001</td>
<td>Relief well not successful on first attempt</td>
</tr>
<tr>
<td>8</td>
<td>3.000E-1</td>
<td></td>
<td>ROV-FTR-001</td>
<td>ROV intervention unsuccessful</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td>LARGERELEASERELIEF2</td>
<td>Added through Event Tree Add</td>
</tr>
<tr>
<td>9</td>
<td>4.942E-8</td>
<td>&lt; 0.01</td>
<td>DRILLING : sequence 19-1</td>
<td>Well Kick While Drilling</td>
</tr>
<tr>
<td>9</td>
<td>1.000E+0</td>
<td></td>
<td>DRILLINGKICK</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>3.530E-4</td>
<td></td>
<td>BOP-POD-YLBL-CCF</td>
<td>Common cause failure of blue and yellow pods</td>
</tr>
<tr>
<td>9</td>
<td>2.000E-4</td>
<td></td>
<td>DRL-HUM-ERR-001</td>
<td>Kick not properly detected</td>
</tr>
<tr>
<td>9</td>
<td>7.000E-1</td>
<td></td>
<td>/ROV</td>
<td>ROV intervention unsuccessful</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td>LARGERELEASERELIEF</td>
<td>Added through Event Tree Add</td>
</tr>
<tr>
<td>10</td>
<td>2.471E-8</td>
<td>&lt; 0.01</td>
<td>DRILLING : sequence 15-1</td>
<td>Well Kick While Drilling</td>
</tr>
<tr>
<td>10</td>
<td>1.000E+0</td>
<td></td>
<td>DRILLINGKICK</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>3.530E-4</td>
<td></td>
<td>BOP-POD-YLBL-CCF</td>
<td>Common cause failure of blue and yellow pods</td>
</tr>
<tr>
<td>10</td>
<td>1.000E-4</td>
<td></td>
<td>EDL-HUM-ERR-001</td>
<td>Emergency disconnect fails</td>
</tr>
<tr>
<td>10</td>
<td>7.000E-1</td>
<td></td>
<td>/ROV</td>
<td>ROV intervention unsuccessful</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td>LARGERELEASEOV</td>
<td>Added through Event Tree Add</td>
</tr>
</tbody>
</table>
Figure 3 - 1. Example Frequency of Exceedance Curve
Figure 3- 1. Example Probability Density Function

Figure 3- 2. Example Cumulative Probability Distribution
Figure 3- 1. Example Comparison of End State Distributions
Figure K-2. Process for Confirming Overall Performance Based on Items Credited in the Assurance Case
Next Generation Nuclear Plant Licensing Basis Event Selection White Paper (INL/EXT-10-19521)

Farmer

Event

DBE: Design-Basis Event

BDBE: Beyond-Design-Basis Event

Two things going on:
- How safe is this facility?
- How do we best manage risk?

Four things going on:
- How safe is this facility?
- How do we best manage risk?
- How do we best manage safety?
- How do we best manage radiation safety?

Figure 8. Use of PRA to select BDBEs.
• NASA’s Johnson Space Center (JSC) is developing a PRA Procedures Guide for BSEE, initially scoped to deal with offshore drilling

• INL is helping JSC do that

• By agreement between JSC and BSEE, the starting point for the development was NASA’s PRA Procedures Guide
  – Development of the NASA guide was initiated after Challenger
  – The NASA guide was heavily influenced by nuclear industry PRA guidance
    • Initially (2002), mostly logic modeling, which is good at functional dependency, redundancy, etc., but rather approximate in some ways
    • Later (2011), the guide paid some attention to simulation, which is better at timing, variations in event phenomenology, …
  – We are trying to be responsive to oil-industry risk modeling needs, not blindly assume nuclear/ NASA PRA techniques are optimal

• The Draft BSEE Guide addresses [or will address, when complete]
  – Standard high-end logic-model tools
  – More qualitative risk assessment tools
  – Simulation-enhanced PRA [placeholder for now]
  – Improved discussion of data analysis
  – Better understanding of uncertainty
  – Improved discussion of the USE of risk model results
PARKING LOT
<table>
<thead>
<tr>
<th>Topic</th>
<th>NASA Guide Section</th>
<th>Draft BSEE Guide Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Risk Management</td>
<td>2</td>
<td>2.1</td>
</tr>
<tr>
<td>PRA Overview</td>
<td>3</td>
<td>2.2.1-2.2.5, Appendices A, B</td>
</tr>
<tr>
<td>Scenario Development</td>
<td>4</td>
<td>2.1, 2.2.1-2.2.5, Appendix C</td>
</tr>
<tr>
<td>Data Collection and Parameter Estimation</td>
<td>5</td>
<td>2.2.6, Appendix E, Appendix G (TBD)</td>
</tr>
<tr>
<td>Uncertainty Analysis</td>
<td>6</td>
<td>2.2.6, Appendices F, G</td>
</tr>
<tr>
<td>Common Cause Failures</td>
<td>7</td>
<td>Appendix D (TBD)</td>
</tr>
<tr>
<td>Human Reliability</td>
<td>8</td>
<td>Appendix L (TBD)</td>
</tr>
<tr>
<td>Software Risk</td>
<td>9</td>
<td>???</td>
</tr>
<tr>
<td>Physical and Phenomenological Models</td>
<td>10</td>
<td>2.3.1 (TBD)</td>
</tr>
</tbody>
</table>

Cross Reference Matrix showing how NASA PRA Guide corresponds to BSEE’s (1 of 2)
Cross Reference Matrix showing how NASA PRA Guide corresponds to BSEE’s (2 of 2)

<table>
<thead>
<tr>
<th>Topic</th>
<th>NASA Guide Section</th>
<th>Draft BSEE Guide Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probabilistic Structural Analysis</td>
<td>11</td>
<td>2.3.1 (TBD)</td>
</tr>
<tr>
<td>Uncertainty Propagation</td>
<td>12</td>
<td>2.2.6</td>
</tr>
<tr>
<td>Presentation / Interpretation of Results</td>
<td>13</td>
<td>3, Appendices I, J, K</td>
</tr>
<tr>
<td>Launch Abort Models</td>
<td>14</td>
<td>N/A</td>
</tr>
<tr>
<td>Probability basics</td>
<td>Appendix A</td>
<td>???</td>
</tr>
<tr>
<td>Failure distributions</td>
<td>Appendix B</td>
<td>2.2.6</td>
</tr>
<tr>
<td>Bayesian inference</td>
<td>Appendix C</td>
<td>2.2.6, Appendices F, G</td>
</tr>
<tr>
<td>Modeling examples</td>
<td>Appendix D</td>
<td>2.2</td>
</tr>
<tr>
<td>Simulation example</td>
<td>Appendix E</td>
<td>2.3</td>
</tr>
<tr>
<td>Configuration Control</td>
<td>N/A</td>
<td>???</td>
</tr>
</tbody>
</table>