NASA Quantitative Risk Assessment Applied to the Oil & Gas Industry

AIAA Annual Technical Symposium
May 6, 2016

David Kaplan
NASA/Johnson Space Center
david.i.kaplan@nasa.gov
Agenda

• Brief Introduction to Probabilistic Risk Assessment (PRA)
• History of PRA
• Bureau of Safety and Environmental Enforcement (BSEE)
• NASA – BSEE Interagency Agreement
Probabilistic Risk Assessment (PRA) is a comprehensive, structured, and logical analysis method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance.

--Introduction; page 1-1
PRA’s systematically connect design, logic, operations, human interaction and external influences for all aspects of large complex machines/processes to detect dependencies and effects that the human mind just could not track and grasp on its own

- PRA’s take into account external events
- PRA’s take into account Human Error and Common Cause
- PRA’s link functional dependency of systems and operations
- PRA’s perform uncertainty analysis
- PRA’s do all of this in an Integrated model
PRA’s are used to model and quantify rare events

- If we had 100,000 space stations operating for 40 years each with a catastrophic failure of 500 of them we could do standard statistics to estimate the probability of catastrophic failure of a space station.

- However we have only one space station and it has had minimal experience and no catastrophic failures. Therefore there will rarely be any statistically significant data since it is in rare event territory.
History of PRA: Nuclear Power Industry

1st PRA:

WASH-1400 REACTOR SAFETY STUDY

1970

1975

1980

Three Mile Island Accident
March 28, 1979

All new Nuclear Plants are licensed by the NRC based on PRA
History of PRA: NASA

PRA's for Human Space Flight [led by team at JSC]

Space Shuttle

International Space Station

Constellation Program

Orion Capsule

Cross Program

Commercial Crew
Probabilistic Risk Assessment (PRA)

Probabilistic Risk Assessment Flow

End States
- List of consequence of interest
- Sequences of operation
- Timelines
- Operational Procedures
- Operational Rules/Assumptions
- Malfunction Procedures

Master Logic Table/Diagram
- List of Initiating Events
- Hazard Reports
- Functional Analyses
- FMEAs
- Previous risk assessments
- External event assessment

Event Trees
- Fault Trees
- Data Analyses
- SAPHIRE

Cut Sets
- Contributors
- Failure Scenario Combinations

Examples:
- Loss of life
- Loss of facility
- Shutdown
- Fire
- Blowout
- Leak
- Exceeding limits

Risk Levels for Selected End States

Relative Risk Drivers

- Training Manuals
- System Architecture
- Engineering Expertise
- P&IDs
- Human Error
- Common Cause

- Customer Data
- Industry Databases
  - OREDA
  - ICON
  - Well Master
- NPRD db
- EPRD db
- Other Assessments
Scenarios involving human error provide a significant risk contribution.

Scenarios involving human error provide a significant risk contribution.
Shell *PERDIDO* Deepwater Platform
Qualitative Risk Assessment

Fault tree

Event tree

- **Fault tree**
  - no flow into barrel E
    - and
    - no flow from pipe B
    - or
      - pipe B not fed
        - or
          - barrel D empty
          - or
            - pump A broken
      - or
        - pump A broken
    - or
      - no flow from pipe C
      - or
        - pipe C not fed
          - or
            - barrel D empty
            - or
              - pump A broken

- **Event tree**
  - Liquid Release (Two-Phase)
    - Obstructed release
      - Yes
        - UVCE/FF
          - Pool fire
            - Final event
              - Explosion + Pool fire
              - Flash fire + Pool fire
              - Release not ignition
    - No
      - Immediate ignition
        - Jet fire + Pool fire
          - Explosion + Pool fire
          - Flash fire + Pool fire
        - Release not ignition
Basic BowTie

Threat
- Prevention Control

Hazard

Top event

Consequence
- Mitigation Control
- Mitigation Control

Threat
- Prevention Control

Mitigation Control
- Mitigation Control

Escalation Factor
- Escalation Factor Control

Escalation Factor
- Escalation Factor Control
Qualitative Barrier Analyses

Deepwater Horizon 8 Key Findings
The Minerals Management Service (MMS) was an agency of the United States Department of the Interior that managed the nation's natural gas, oil and other mineral resources on the outer continental shelf (OCS).

Formed: January 19, 1982
Renamed: May 19, 2010
Dissolved: October 1, 2011

Deepwater Horizon
April 20, 2010
Mission Statement: The Bureau of Safety and Environmental Enforcement (BSEE) works to promote safety, protect the environment, and conserve resources offshore through vigorous regulatory oversight and enforcement.
Bureau of Safety and Environmental Enforcement

BSEE Alaska Region Office
3801 Centerpoint Dr Ste 500
Anchorage, AK 99503

BSEE Pacific Region Office
760 Paseo Camarillo
Suite 102, 1st Floor
Camarillo, CA 93010

BSEE Gulf of Mexico Region Office
1201 Elmwood Park Blvd
New Orleans, LA 70123
BSEE, NASA Announce Agreement to Examine Risk Offshore

03/17/2016
WASHINGTON

The Bureau of Safety and Environmental Enforcement (BSEE) and The National Aeronautics and Space Administration (NASA) have announced a five-year agreement allowing BSEE to capitalize on the best risk management approaches from the aeronautics industry to inform stakeholders and further strengthen worker and environmental safety protections on the Outer Continental Shelf.

"Both BSEE and NASA work in harsh and uncompromising environments, relying on cutting edge technology to go deeper and further than previously thought possible," said BSEE Director Brian Salerno. "This partnership brings together technical experts from BSEE and NASA to focus on the specific risks associated with offshore operations so that we can continue to find ways to improve safety for offshore workers and protect the environment."

Under the agreement, NASA will assist BSEE in achieving three primary objectives:

- further develop BSEE’s risk management capability through the use of NASA’s probabilistic risk assessment technique.
- evaluate, design, and test technologies and hardware, including emerging technologies and best available and safest technologies; and
- assess failures and near miss occurrences using the resources and expertise of NASA’s accredited failure analysis laboratory at the Johnson Space Center in Houston.

Used by NASA, probabilistic risk assessment is a technique to quantitatively model risk. It was used in the modeling of the Space Shuttle Program and is presently being used for the International Space Station and Orion deep space capsule programs.

"Whether the task takes one to deep space, or into the deep ocean, the analysis of the environment, training of personnel and risk mitigation factors are similar," said Jack James, technology transfer strategist at the Johnson Space Center. "NASA is pleased to work with BSEE, and we endeavor to learn best practices from each other."