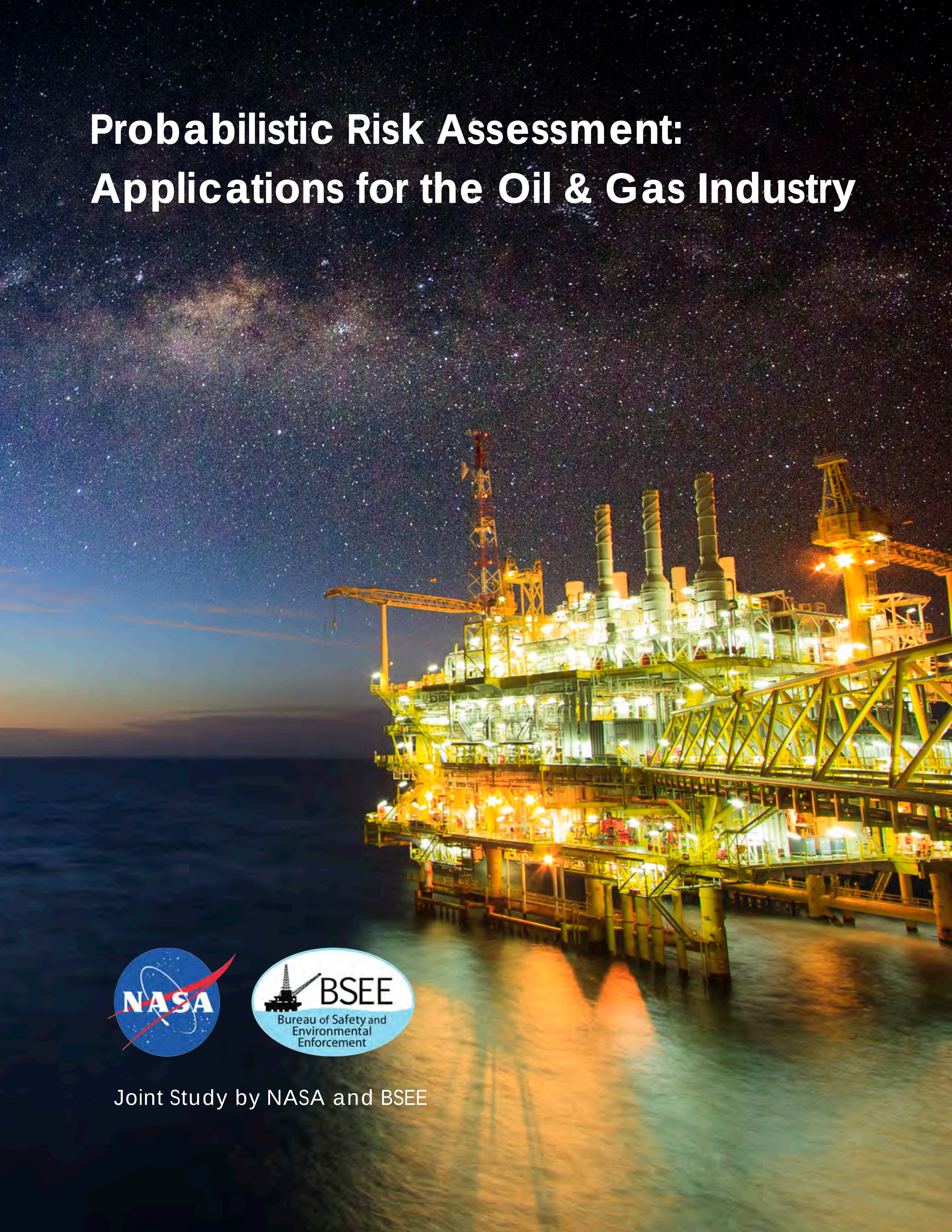
Probabilistic Risk Assessment: Applications for the Oil & Gas Industry



Joint Study by NASA and BSEE

Introduction

Probabilistic Risk Assessment (PRA) is a tool that has gained increasing popularity across several industries from nuclear power to human spaceflight to systematically and comprehensively evaluate risks associated with complex engineered facilities.

The Bureau of Safety and Environmental Enforcement (BSEE), in partnership with the National Aeronautics and Space Administration (NASA), is exploring the ability of PRA to assist in the evaluation and communication of risk in the offshore oil & gas industry.

With the boundaries of exploration, development, and production facing challenges from harsher environments and new technologies, understanding the risks involved becomes more important than ever to ensure continued high levels of safety and environmental protection. By exploring the use of PRA, BSEE is considering the potential of PRA as a tool that can provide additional insights into the levels of risk involved in challenging offshore operations as well as facilitate communication with the industry on how to best manage those risks. This paper presents a context for PRA in terms of current risk assessment practices in the industry, identifies the benefits of PRA, and provides a description of the PRA tool.

A Context for Probabilistic Risk Assessment

Not every situation requires a quantitative approach; however, PRA is appropriate for complex engineering hardware that has critical human interaction and multiple pathways to catastrophic failure.

Concept of Risk Management

Risk management includes the principles, framework, and processes for managing risks effectively. Risk events are characterized as a combination of both the probability and consequences of undesired events. Therefore, risk management efforts are focused on a combination of the following: eliminating or reducing the probability of an undesired event; and reducing or mitigating the consequences of the undesired event should it occur. While many risk management practices are in use on the Outer Continental Shelf (OCS) and in the broader oil and gas industry, at their core they all follow the same process—identify, analyze, evaluate, control, communicate, and monitor.

Risk management for most offshore oil and gas operators begins with a multi-disciplinary approach to early well and facility design planning. These planning processes are embedded within management systems that provide a framework for all of the operating and safety management activities of the organization. Organizational risk management processes are also provided within American Petroleum Institute (API) standards and recommended practices as well as International Organization for Standardization (ISO) standards.

Qualitative versus Quantitative Risk Assessment

Qualitative risk assessment is commonly based on experience or expertise and results in categorical estimates of risk. Quantitative risk assessment leverages empirical data to determine and assign numerical values to risks. Risk assessment activities are used to identify sources of risks, their causes, and consequences. Risk assessment techniques are selected, which may be qualitative or quantitative, to help decision makers better understand the risks. Risk assessment helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action. Finally, decisions are made to determine if existing risk controls should be modified or additional controls added to provide further prevention or mitigation of risk.

Choosing the appropriate risk assessment approach or combination of approaches is a key step in supporting the decision-making process, where options are evaluated against the risks associated with each choice. Both qualitative and quantitative risk assessments provide decision makers with the knowledge required to properly control and communicate the risk. Selection of a suitable risk assessment approach should reflect the evaluation of the technical and operational challenges. Qualitative assessments, involving expert judgment, may be sufficient for many operations, such as simple operations where the level of risk is dependent on fewer variables and where uncertainties are relatively low. Quantitative assessments, however, can offer additional insight when the operation or technology is more complex; decisions regarding the effectiveness of risk controls and potential consequences are dependent on many variables; multiple paths to failure exist; the magnitude of risk is greater; or uncertainties are higher. Ultimately, choosing the appropriate risk assessment method is also for proper communication of risk between the operator, the regulator, and other stakeholders.

Qualitative Assessment

Qualitative assessments are commonly used in oil and gas risk management and are valuable first steps in the risk analysis process. They add rigor and structure to the common risk assessment method of brainstorming. Examples of qualitative assessments can include:

Hazard Identification (HAZID)	HAZID is a structured brainstorming technique for the identification of all significant hazards associated with the particular activity under consideration. Usually conducted in the beginning of the project, it is the starting point to conducting qualitative assessment of major accident risks.
Hazard and Operability (HAZOP)	HAZOP is a systematic approach to identifying hazards and operability problems in design and operations occurring as a result of deviations from the intended range of process conditions. Complex designs usually are assessed as a series of smaller nodes.
Bowtie Analysis	Bowties are a visual risk assessment method focused on a single event and the threats (cause) and consequences (effect). They are more commonly used to analyze major accident events such as loss of containment, facility explosion, fire, etc. Bowties can illustrate relationships between hazards, controls and an organization's safety management systems, otherwise known as "barriers."
Failure Modes and Effects Analysis (FMEA)	FMEA is a subjective analysis of facility equipment, potential failure modes and the effects of those failures on the equipment or facilities. The failure mode is simply a description of how the equipment failed. The effect is the incident, consequence or system response to the failure.
Job Hazard Analysis (JHA)	JHA is a hazard analysis of a completed procedure to identify any additional hazards to people or process prior to putting it in the field. In some cases, JHA is a general job-related safety analysis.

Qualitative assessments are effective at identifying many risks and consequences associated with oil and gas exploration and production. Companies have used these results to successfully develop and implement risk management and safety programs. While effective at identification of the hazards, qualitative assessments do not quantify the probabilities of events, and therefore, make assigning any type of risk rating subjective and often difficult. Low probability, high consequence events are not defined as well as they might be with more quantitative methods.

Quantitative Assessment

Quantitative risk assessment involves the assignment of data-supported numeric values in the assessment of probability and consequence. It commonly follows an initial qualitative assessment, focusing on the highest-priority risks identified. Quantitative risk assessment can account for the compounding of effects between multiple scenarios or events, as with the Quantitative Risk Assessment method briefly described in the table below. The method accounts for compounding effects by quantifying the possible outcomes and the probability of their occurrence, allowing risk-informed decision-making in the presence of uncertainty. There are multiple methods for performing quantitative risk assessment and many are used regularly in the oil and gas industry. Some common quantitative approaches include:

Layers of Protection Analysis	Semi-quantitative method that analyzes one incident scenario (cause-consequence pair) at a time, using predefined values for the initiating event frequency, independent protection layer failure probabilities, and consequence severity, in order to compare a scenario risk estimate to risk criteria for determining where additional risk reduction or more detailed analysis is needed. Scenarios are identified elsewhere, typically using a scenario-based hazard evaluation procedure such as a HAZOP study.
Failure Mode & Effect Criticality Analysis (FMECA)	A variation of FMEA that includes an estimate of the potential frequency and severity of consequences of a failure mode. FMECA can be both qualitative and quantitative based on the approach. The Quantitative FMECA uses a Quantitative Criticality Analysis and the Qualitative FMECA uses a Qualitative Criticality Analysis.
Event Tree Analysis	Graphical model represents the various event chains that can occur as a result of an initiating event. Used quantitatively to determine the probability or frequency of different consequences arising from the hazardous event. (May be used in PRA.)
Fault Tree Analysis	Graphical model representing various combinations of equipment failures and human errors that can result in system failures or hazardous events. Output is a failure-logic diagram based upon Boolean logic gates. Used quantitatively to allow system-failure probability or frequency to be calculated. (May be used in PRA.)
Quantitative Risk Assessment (QRA)	The systematic development of numerical estimates of the expected frequency and severity of potential incidents associated with a facility or operation based on engineering evaluation and mathematical techniques. QRA's have traditionally been utilized to quantify risks in the design and operation of offshore installations to predict and quantify the direct effects of dispersion of gas or released fluids; overpressures due to explosions; size and duration of fires; structural impact from collisions, falling objects; and escape, evacuation and rescue capacity during major accident event scenarios.
Probabilistic Risk Assessment (PRA)	PRA is a systematic and comprehensive methodology to evaluate risks associated with every life-cycle aspect of a complex engineered technological entity. PRA involves the assignment of numeric values in the assessment of probability and consequence, and commonly follows an initial qualitative analysis, focusing on the highest-priority risks identified. It allows for the compounding of effects between multiple scenarios or events. It does this by quantifying the probability of possible outcomes allowing risk-informed decision-making in the presence of uncertainty. PRA attempts to consider all events and consequences in one assessment, allowing for a more robust estimation of risk.

The process of performing a quantitative assessment can be as simple as basic probability calculations or as complicated as multiple regression models and Monte Carlo simulations. Often quantitative assessments are performed with the assistance of commercially available computer software.

While there are exceptions, quantitative risk assessment approaches in the domestic offshore oil and gas industry and globally typically use simple versions of the detailed analysis tools that are available (primarily due to unavailability of safety integrity or experience data with which to perform causal analysis). Therefore, many quantitative approaches may not support detailed analysis of uncertainty, common cause failures, and human reliability, in contrast to Probabilistic Risk Assessment (PRA).

Probabilistic Risk Assessment

Probabilistic Risk Assessment is a quantitative method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance. PRA attempts to consider all events associated with the consequences of interest in one assessment, allowing for a more robust risk assessment.

Because of its logical, systematic, and comprehensive approach, PRA has repeatedly proven capable of uncovering design and operational weaknesses that had escaped even some of the best deterministic safety and engineering experts. NASA has found that relying on expert judgment alone may result in the mischaracterization of the likelihood of failure events. Not every situation requires a quantitative approach; however, PRA is appropriate for complex engineering hardware that has critical human interaction and multiple pathways to catastrophic failure.

Brief History of PRA

The early beginnings of PRA are found in the U.S. nuclear industry. In the 1970's, scientists needed to quantify how reactor design improvements could reduce the risk of a catastrophic release of radioactive core material, as plans were being drawn for larger reactors to be located near population centers. The need to quantify and evaluate design improvements led to the introduction of what would be known as Probabilistic Risk Assessment (PRA).

In 1975, the Nuclear Regulatory Commission (NRC) published the Reactor Safety Study WASH-1400. This study is universally accepted as the first "modern" PRA analysis and set the foundation for PRA to become a major component of risk analysis for the U.S. nuclear industry. It utilized both fault trees and event trees to analyze the systems of power plants.

The NRC identified three fundamental steps in the assessment process: identify the problem, determine the initiating events, and estimate the frequency of those events. Even though the study made major strides in understanding and quantifying the risk of operating nuclear power plants, it received criticism. However, interest in PRA was revitalized after a review of the Three Mile Island accident (March 1979) revealed the type of accident that caused the damage had been predicted by the Reactor Safety Study four years earlier.

The NRC continued to develop and advance the use of PRA, and in 1983, it released the *PRA Procedures Guide*[1], which provided a standardized method for performing PRA. Over the next decade, the state of the art of PRA was continually improved, and in 1995, the NRC issued the PRA policy statement that said, in part:

> *The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach, and supports the NRC's traditional defense-in-depth philosophy.*[2]

In the early 2000's, NASA sought to enhance its risk management capabilities by hiring several PRA analysts with strong experience in the nuclear power industry. The analysts began to quietly argue for an expanded role of PRA in major NASA programs.

In February 2003, Space Shuttle *Columbia* was lost on reentry when a piece of insulation foam broke off from the external tank and struck the wing leading edge of the Shuttle. Recognizing that the cause of this accident was a low-probability, high-consequence event, NASA committed to strengthening its safety and mission assurance capabilities. PRA was adopted and embraced by the Space Shuttle Program, the International Space Station Program, and every subsequent human exploration program at NASA.

---

[1] NUREG/CR-2300.

[2] 60 FR 42622; August 16, 1995.

Benefits of PRA

The ultimate goal of performing a PRA is to support decision-making and risk management.

PRA has repeatedly proven capable of uncovering design and operational weaknesses that had escaped even some of the best deterministic safety and engineering experts.

The ultimate goal of performing a PRA or other quantitative/qualitative risk assessment techniques is to support decision-making and risk management. In the context of making decisions about complex, high-hazard systems, “risk” is usefully conceived as a set of triplets: failure scenarios, likelihoods of those scenarios, and their actual consequences. It is important to focus on these elements rather than focusing on simpler, higher-level quantities, such as “expected consequences.” Risk management involves prevention or reduction of the frequency of scenarios having undesirable consequences. This requires understanding the elements of adverse scenarios so that they can be prevented.

PRA is essentially an advanced risk analysis method that overcomes many limitations of qualitative techniques. In general, the choice of techniques in a given decision analysis needs to be made in light of the magnitude of consequences associated with the decision, the complexity involved in analyzing the possible outcomes, the uncertainties, the diversity of stakeholders involved, and perhaps other considerations. The magnitude of the consequences of accidents can include fatalities or health effects, adverse environmental effects, significant expense, and perhaps other adverse effects on the operating company or other stakeholders.

When PRA is selected as the suitable technique for advanced risk analysis, applicable end states are identified so that the results of the analysis will present appropriate risk metrics to support decision-making. The PRA will produce a list of risks that can be ranked by their expected frequency of occurrence, such as the example in Table 1. The example in Table 1 is simplified, as the typical results from the PRA have a comprehensive set of scenarios that can be in millions. Most often the bulk of the risk is concentrated in a much shorter list (e.g., top 10 to 20 items).

Unexpected Overpressure Zone **and** Failure of the Blind Shear Ram to Close/Shut In the Well While Drilling	1.05E-05
Unexpected Overpressure Zone **and** Human Error - Failure to Recognize and Act on a Well Kick	9.30E-06
Incorrect Mud Density **and** Failure of the Blind Shear Ram to Close/Shut In the Well While Running Casing	4.50E-06
Unexpected Overpressure Zone **and** Common Cause Failure of the Blue/Yellow Pods to Operate the Blind Shear Ram	4.40E-06
Unexpected Overpressure Zone **and** Failure of the Blind Shear Ram to Close/Shut In the Well While Drilling due to Tool Joint in the Blind Shear Ram Plane	4.10E-06
Unexpected Overpressure Zone **and** Failure of the Blind Shear Ram to Close/Shut In the Well While Tripping	3.90E-06
Incorrect Mud Density **and** Human Error - Failure to Recognize and Act on a Well Kick	3.80E-06

Table 1: Notional Scenario Risk Ranking Example

Ranking Expected Contributions of Initiating Events

Once individual scenarios are quantified and there is confidence that the results reflect the current state of knowledge, the individual scenarios are reviewed to determine if there are any high-risk outliers that need to be addressed. The results can be grouped in numerous ways to provide insights that might otherwise be hidden when addressing individual scenarios. For instance, as shown in Figure 1, combining individual scenarios leading to a release of hydrocarbons by an Initiating Event would show the most likely challenge to the blowout preventer (BOP). By knowing the expected frequencies of Initiating Events leading to consequences of interest, it may be possible to reduce the challenges to the BOP by maintenance, operational strategies, or future design considerations.

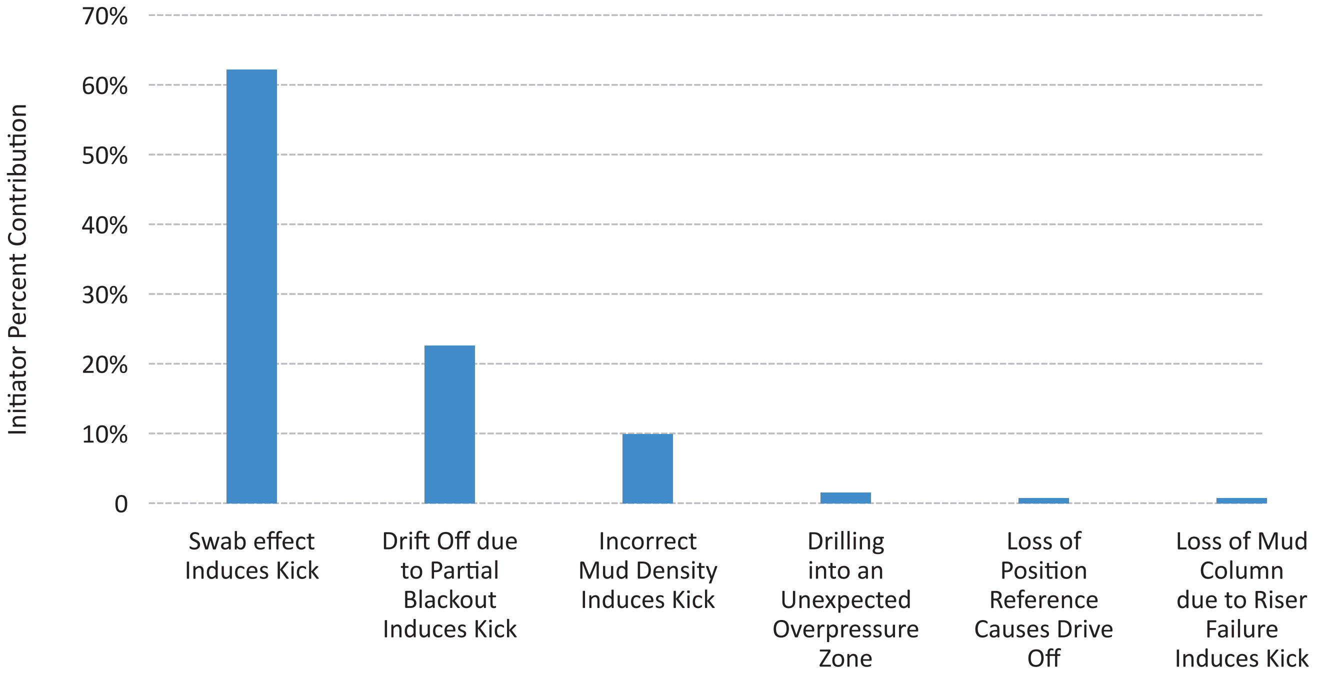


Figure 1: Notional Initiating Event Ranking Leading to a Well Kick
Data in this figure does not represent any particular facility. Rankings may be different for slightly different designs or operational procedures/practices.

This type of parsing can also be done on a variety of levels including system contributions, functional contributions, and consequences.

Identifying Common Failure Points or Modes

Most PRA software contains built-in functions that provide sensitivity studies, called importance measures, which can also be useful in determining the collective significance of events in different ways. Often times, many individual scenarios that are not risk drivers may have a common contributor. Individually, these scenarios may not appear to contribute much to the overall risk; however, if there is a common weak link, that component may be a significant contributor to the overall risk.

Identifying Low-Frequency, High-Consequence Failure Points

Another importance measure frequently used is called the Risk Achievement Worth (RAW). This importance measure is the equivalent of a "what if" sensitivity study in which each event failure is assumed to be failed and the impact to the overall risk is measured in terms of the percentage increase in risk. This measure can highlight single-failure points that are usually designed robustly and therefore do not show up as a top risk driver, but if failed will result in a serious consequence. The RAW can also highlight events that are involved in multiple lower-risk scenarios. Support system components, such as those within systems like electric power generation or distribution, often fall into this category. This importance measure can be particularly useful for situations involving planned or unplanned maintenance. When planning maintenance, knowing how much the risk is increased when a system or component is out of service can allow planning to minimize the time or plan around critical operational time periods to reduce risk. For unplanned maintenance, a high RAW would indicate the need for compensatory actions to be taken if a system or component goes out of service. On the other hand, it may show very little additive risk for certain systems or components if they are out of service and allow operations to continue nominally until repairs can be completed.

Accounting for Uncertainties

In addition to the risk rankings provided by PRA, the analysis also provides a measure of uncertainty around both the inputs and results. Failure rates and probabilities are inherently uncertain, so providing a range on events and results can help to inform users of the true state of knowledge regarding the results. Figure 2 is a notional example of how the probabilities from individual events are combined to produce an uncertainty in the end states and how different end states can be compared, not only by their best-estimate mean values but also with the accompanying uncertainty for each which is represented by the width of the box in the figure.

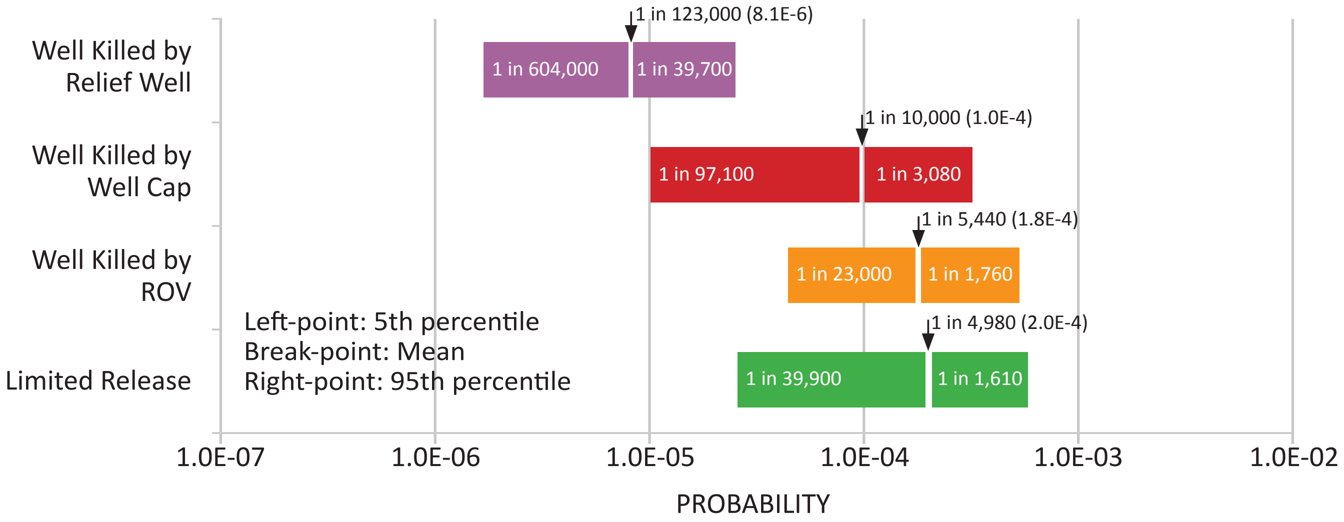


Figure 2: Notional Example of End State Probabilities with Uncertainty

By reviewing the results in these different ways, risk managers get a clear picture of what the top risk scenarios are and what components/systems contribute to the risk and why. This information can then be used to identify prudent design changes and operational procedure enhancements and to define maintenance strategies to minimize risk.

Integrated Approach

Another significant benefit from performing a PRA is the gain in knowledge of the facility design and operations by integrating all aspects of a facility from component reliabilities to human error and external phenomena. This in-depth knowledge can allow both regulators and operators to have a common understanding of the risks involved and support decision-making to enhance both operations and safety.

Description of a PRA

A PRA is useful (and the effort is justified) when decision-making involves high stakes in a complex situation. New technologies and extreme environments, such as high-pressure high-temperature deep water wells, are excellent candidates for considering use of the PRA in assessing risks. PRA can be used to evaluate risks associated with every lifecycle aspect of a complex engineered technological entity, from concept definition through design, construction and operation, and removal from service. With respect to the planning and design phases in particular, utilizing PRA may offer a practical opportunity to lower risks when it is relatively less costly to implement changes by identifying and evaluating risks and building in controls. Developing a comprehensive set of risk scenarios to provide decision-makers with the best informed picture of threats and mitigation opportunities is a special challenge, and systematic methods are needed for development and quantification of such an assessment. PRA is one of the most comprehensive methods for that task.

The PRA results in a fully developed listing of individual scenarios that can lead to a consequence of interest along with the frequency of occurrence. Each scenario produced by the PRA contains an Initiating Event and, usually, one or more pivotal events leading to a consequence of interest, commonly called an End State of the PRA. As modeled in most PRAs, an Initiating Event is a deviation from normal operation that requires some kind of response from personnel or one or more systems. The pivotal events (similar to mitigations or barriers) in a scenario include successes and failures of responses to the Initiating Event or possibly the occurrence or nonoccurrence of external conditions such as severe weather. The scenario End State(s) are defined according to the decisions being supported by the analysis, in terms of the type and severity of consequences, ranging from completely successful outcomes to losses of various kinds, such as a loss of containment.

Figure 3 shows the overall steps involved in performing a PRA.

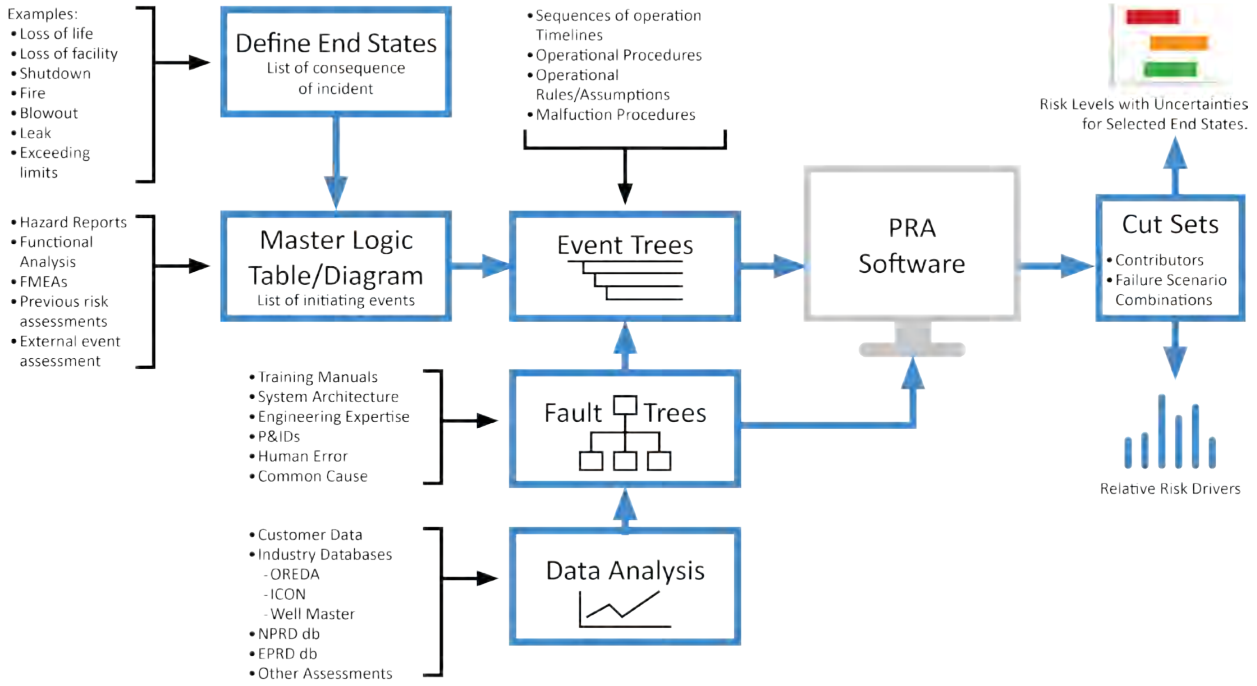


Figure 3: Major steps to perform a PRA

The initial step in developing a PRA is to determine the boundaries and focus of the analysis. First, based on the goals of the analysis and decisions to be made, what End State(s) are of interest to stakeholders? Examples may include:

- Loss of life or injury to personnel;
- Damage to the environment; and
- Damage to, or loss of, equipment or property (including facilities and public properties).

In addition to the End State(s), the boundaries of the analysis, in many cases, would define what a successful End State would be. If the goal is to evaluate the likelihood of an accident related to a well kick, the success End State may be defined as well shut-in, i.e., shutting in the well to prevent the uncontrolled flow of formation fluids. If the goal is to evaluate the likelihood of a release as a function of the magnitude of release, considerations beyond the BOP must be taken into account, such as remote operated vehicle (ROV) intervention and well capping, and success comes from killing the well rather than successfully shutting in the well with the BOP alone. Typically the goal should be based on achieving a stable state (as in the latter goal where the well has been killed) where further risk has been mitigated to ensure evaluation of the complete scenario.

The Initiating Events present a challenge that could lead to the End State(s) of interest. Initiating Events are found through structured, qualitative processes (including HAZID's and HAZOP's) that will produce an exhaustive list. A Master Logic Diagram (MLD), as shown in Figure 4, is often used to document the results of Initiating Event identification.

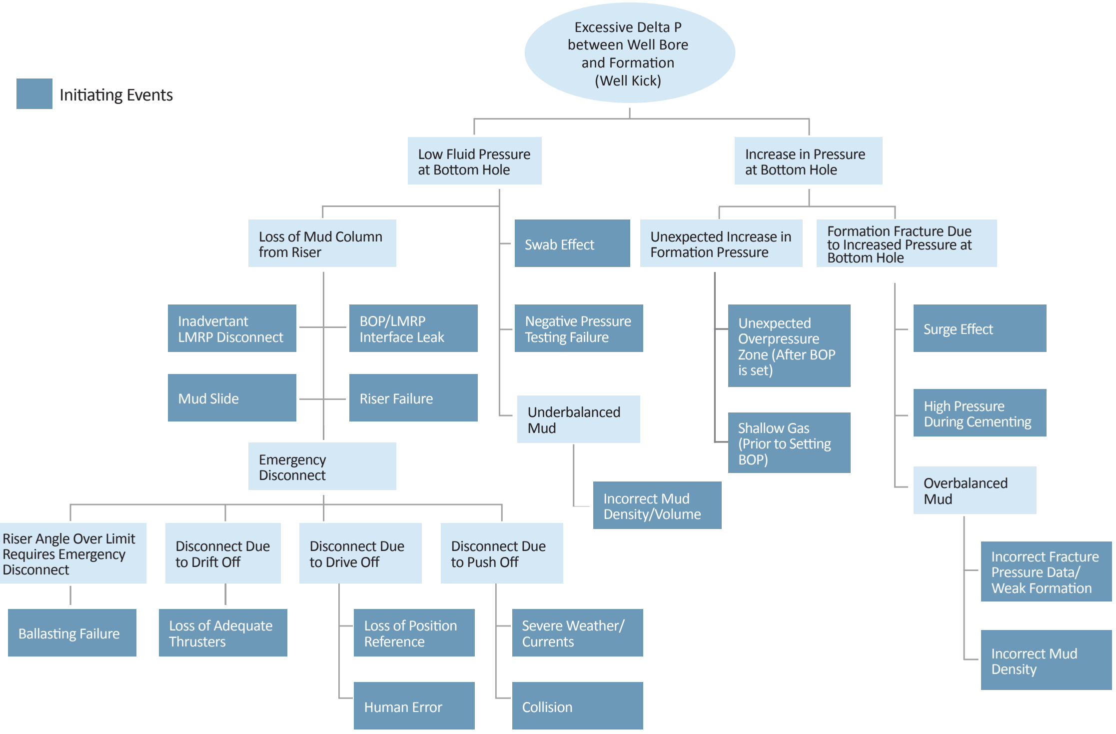


Figure 4: Notional Master Logic Diagram for a Well Kick While Drilling

Once the Initiating Events are identified, each Initiating Event is evaluated by stepping through the required actions following the Initiating Event to a stable outcome. The required events may or may not occur due to equipment failure, human interaction failure, or some other external factor (e.g., severe weather). Failures may require contingency actions, which again may either succeed or fail, and so on until a stable state is attained (e.g., well killed). If the consequence is negative (release), it may be possible to break down the scenarios into different levels of consequence, such as large/small release. Following all possible paths of action is the first step toward building individual scenarios.

Event trees are tools used to develop specific accident sequences leading to the End State(s) and are used, in conjunction with fault trees, to quantify the frequency of each End State. One event tree is developed for each Initiating Event or group of Initiating Events. The graphical event tree starts with the Initiating Event that is followed by a number of pivotal events determined through the accident progression/critical function assessment for each Initiating Event. Each of the pivotal events have a potential success or failure path and are usually ordered in time sequence of the response to the Initiating Event. Each path on the event tree represents a sequence of successful and failed events used to identify and quantify individual scenarios. The end of each sequence results in a stable state, which may be a successful mitigation of the event, or a consequence of interest. An example event tree is shown in Figure 5.

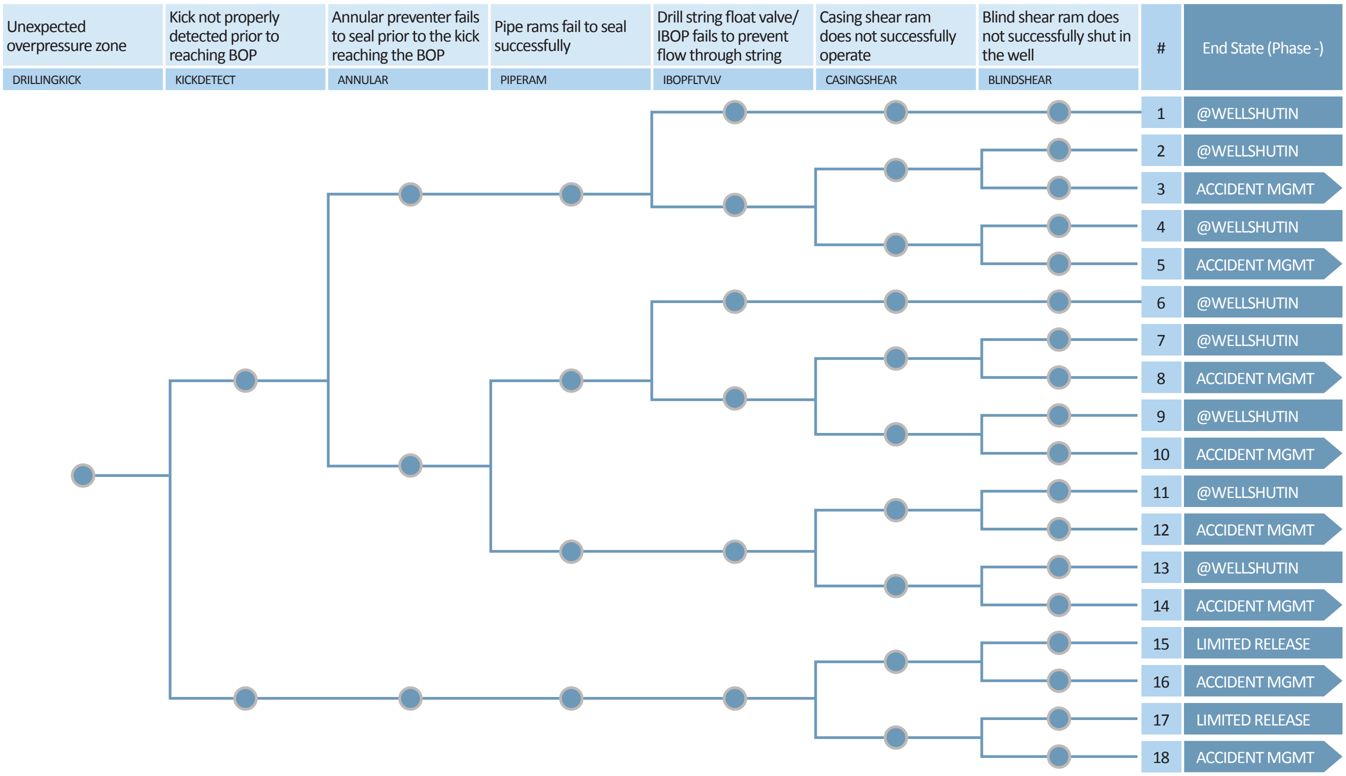


Figure 5: Example Event Tree for Response to an Unexpected Overpressure Zone While Drilling

With the event sequences and their corresponding end states illustrated in the event trees, each pivotal event is further developed to a level where it may be quantified. This typically involves development of fault trees, which are models that start with a "Top Event," that is, a failure or condition matching the pivotal event in the event tree, and develop ways in which that event can happen, expressed in terms of "basic events." There can be many basic events (the lowest level in the fault tree) and combinations of basic events that can cause the Top Event. The Top Event model may be composed of numerous basic events which include component failures, human actions, environmental conditions, etc. The basic event level contains probabilistic data used for quantification. An example of a fault tree is shown in Figure 6.

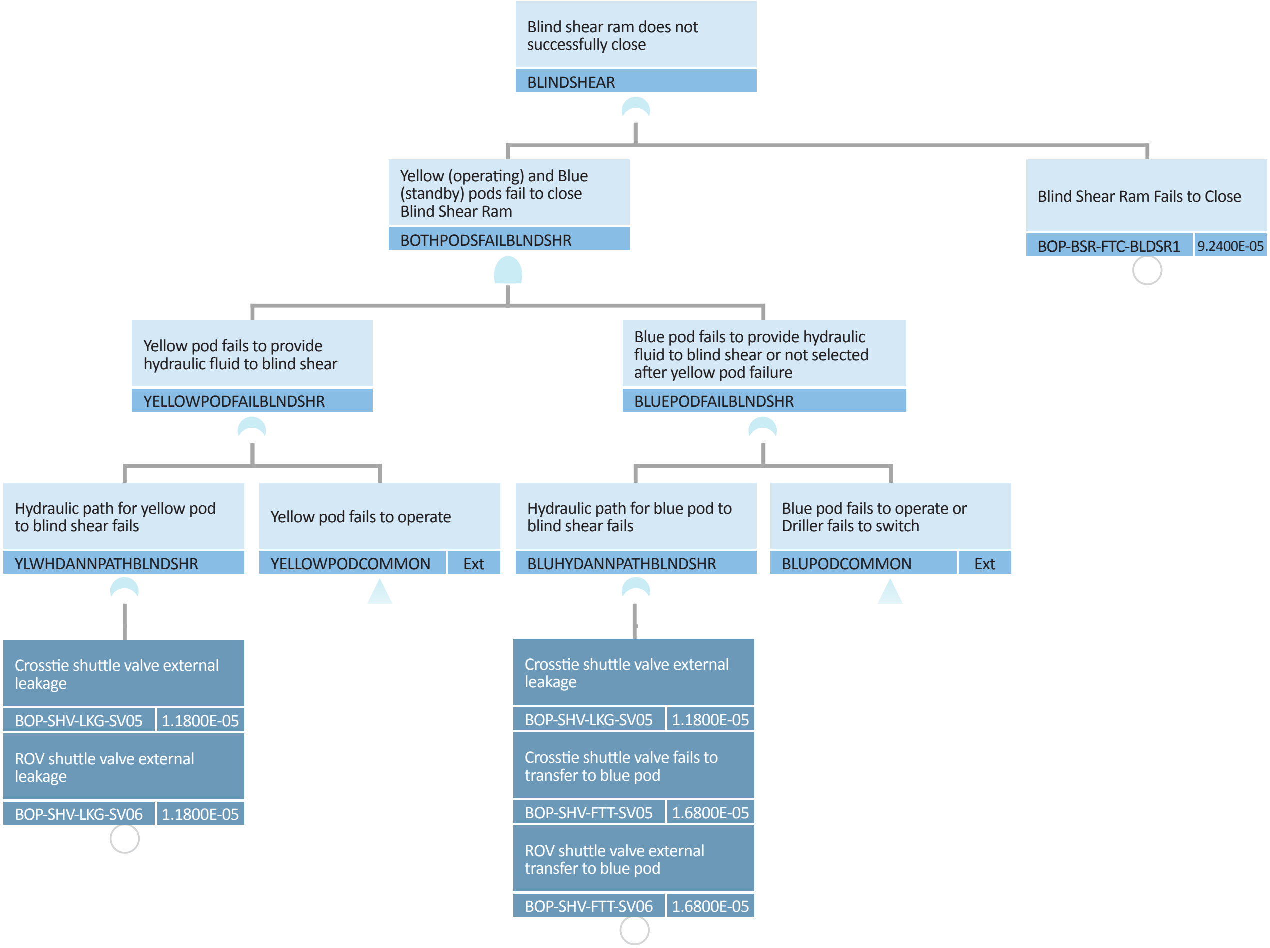


Figure 6: Example Fault Tree for failure of the Blind Shear Ram to Successfully Close

Quantification requires the development of data to populate the logic model and considers not only component failure rates but also human reliability, common cause failure, and external conditions, such as weather, to fully quantify the scenarios.

Component failure rates are the bulk of what is needed for a typical PRA model. The preferred source of information is significant facility-specific data. In many cases, however, only limited or partial data is available from a specific facility. In this case, surrogate data is commonly used to determine a mean value with an uncertainty distribution that accounts for a diverse set of operations and maintenance conditions. If limited facility-specific data is available, it can be combined with surrogate data to establish a more informed distribution. Surrogate failure rates are available from a variety of sources, such as the Offshore and Onshore Reliability Data (OREDA)[1] organization.

Critical human actions are often required in the identification and mitigation of accidents. Methods such as Technique for Human Error Rate Prediction (THERP)[2] and Cognitive Reliability Error Analysis Method (CREAM)[3] were developed to estimate the probability of human errors for specific tasks. NASA has used both methods, and results have compared quite well with empirical data. The methods generally use performance shaping factors, such as those shown in Table 2, to estimate the probability of failure (p_f).

Adequacy of Organization
Working Conditions
Adequacy of Man Machine Interface
Procedures/Plans
Number of Goals
Available Time
Time of Day
Training and Preparation
Crew Collaboration

Table 2: Typical Performance Shaping Factors for Human Reliability Analysis

Other data may be required for events that are not component or human-based, such as weather conditions when analyzing a dynamic positioning system (DPS). In this case, certain combinations of thrusters must be available depending on what weather conditions are being experienced; so, not only is the likelihood of the thrusters being available necessary but also the probability of certain weather conditions is necessary to establish an accurate portrayal of the risk of a drift-off or push-off.

In addition to event probability data, engineering analysis may be required to establish success criteria for systems or events. As in the DPS example above, the PRA must have information related to what constitutes success for a system and under what conditions. Wind speed, wave height, and current data may be required to determine the thruster combinations that are required to maintain adequate positioning during drilling operations.

---

[1] OREDA. Offshore and Onshore Reliability Data 6th Edition. 2015.

[2] Swain, Alan D., and Henry E. Guttmann. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report No. NUREG/CR-1278; SAND-80-0200. Sandia National Labs., Albuquerque, New Mexico (USA), 1983.

[3] Hollnagel, Erik. CREAM. Elsevier, 1998.

Summary

PRA is an advanced risk analysis technique that overcomes many of the limitations of qualitative techniques. In general, the choice of techniques in a given decision analysis needs to be made based on the magnitude of consequences associated with the decision and the complexity involved in analyzing the possible outcomes. In a situation with high consequence, complexity, and uncertainty, it is unlikely that a qualitative model result will be robust enough to address all of these consequences.

The results of the PRA will be a list of risks that can be ranked by their expected frequency of occurrence. The results may also be grouped in various ways to provide insights that might otherwise be hidden when addressing individual scenarios.

In addition to the risk rankings provided by PRA, the analysis also provides a measure of uncertainty around both the inputs and results. Failure rates and probabilities are inherently uncertain, so providing a range on events and results can help to inform users of the true state of knowledge regarding the results.

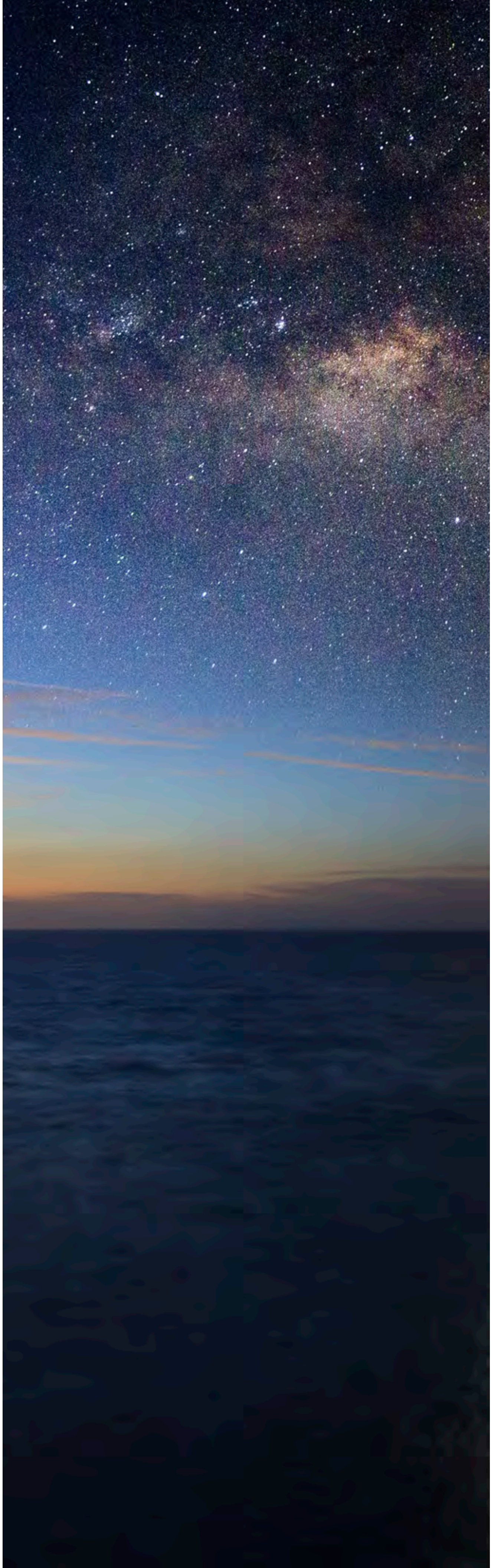
By reviewing the results in these different ways, a clear picture emerges of what the top risk scenarios are and what components/systems contribute to the risk and why. This information can then be used to identify prudent design changes, operational procedure enhancements, and to define maintenance strategies to minimize risk.

PRA Guide

BSEE and NASA have developed a draft guide for the use of Probabilistic Risk Assessment (PRA) in the offshore oil and gas industry. The draft PRA Guide is the next step in evaluating PRA as a potential risk assessment tool for operators in a less-understood offshore environment for new technologies. The document Probabilistic Risk Assessment Procedures Guide for Offshore Applications (DRAFT; October 25, 2016) is available on the BSEE website at:

https://www.bsee.gov/what-we-do/offshore-regulatory-programs/risk-assessment-analysis/probabilistic-risk-assessment-analysis

The PRA Guide is not a policy document and does not discuss regulatory requirements; rather, it discusses particular modeling techniques that have been found useful for decision-making in complex and high-hazard operations. In this draft document, certain sections of the PRA Guide are incomplete. NASA is currently working to produce an initial, “generic PRA” for a deep water drilling facility, which may be incorporated into PRA Guide revisions.



NASA Document No. JSC-SAA-NA-24402-01
May 1, 2017

Please provide comments, corrections, or suggestions to:

David Kaplan at david.i.kaplan@nasa.gov