Modeling the Risk of U.S. Offshore Oil & Gas Exploration-Well Drilling, Commercial Nuclear Plants, and Human Spaceflight

Roger L. Boyer[a], Robert B. Cross[a*], Forrest E. Shanks[b], Michael Worden[b], and Robert Youngblood[c]

[a] NASA Johnson Space Center, Houston, U.S.A.
[b] Bureau of Safety and Environmental Enforcement, Houston, USA
[c] Idaho National Laboratory, Idaho Falls, USA

Abstract: Probabilistic Risk Assessment (PRA) has been applied in different industries for many years. Each industry and technology area presents varying challenges and priorities, and the risk models therefore need to be somewhat different. This paper compares aspects of risk modeling of offshore drilling, nuclear plant operation, and human spaceflight. Risk models in all three technology areas have certain high-level similarities: (1) they employ redundancy and diversity in their means to prevent or mitigate risk, including a mix of active and passive systems designed to respond to off-normal evolutions; (2) they are affected by human reliability; (3) their models require consideration of coupling between scenario structure and scenario phenomenology. But in examining the models in more detail, one sees important differences in methodology and emphasis.

For purposes of comparison, this paper discusses aspects of a risk model of an offshore drilling operation in the U.S. Gulf of Mexico, focusing on where such a development differs in important ways from models of commercial U.S. nuclear plants and models developed for human spaceflight.

Keywords: PRA, Offshore Oil and Gas, Launch Vehicles, Nuclear Power.

1. INTRODUCTION

Many of the essential ideas of risk analysis were articulated long ago (for example, by Farmer [1] and Garrick [2] among others, working in the 1960's), certainly well before Three Mile Island (1979) [3, 4], Challenger (1986) [5], Piper Alpha (1988) [6], Columbia (2003) [7], or Macondo (2010) [8] had occurred; but each of those events occasioned a step change in the level of detail and the technical sophistication of regulatory oversight in their respective domains. This was accompanied by increased use of risk analysis in each domain, carried out not only in response to regulatory oversight, but also simply to improve facility risk management [9].

Each industry and technology area presents varying challenges and priorities, and the Probabilistic Risk Assessment (PRA) models therefore need to be somewhat different. This paper compares risk modeling of offshore drilling, nuclear plant operation, and human spaceflight. Risk management practices in all three technology areas have certain high-level similarities: (1) they employ redundancy and diversity in their means to prevent or mitigate risk, including a mix of active and passive systems designed to respond to off-normal evolutions; (2) they are affected by human reliability; (3) their models require consideration of coupling between scenario structure and scenario phenomenology. However, in examining the models in more detail, one sees important differences in emphasis, stemming from each technology's particular challenges.

2. NUCLEAR POWER RISK BACKGROUND [10]

Immediately after World War II, the consequences of nuclear detonations were still fresh in people's minds; correspondingly, steps to protect the health and safety of the public from reactor accidents were being considered well before the commercial nuclear power industry really got started, and those steps were being taken at the federal level. It was arguably a first-of-a-kind development of a regulatory

* Robert.cross-1@nasa.gov

approach to oversight of high-hazard facilities ("hazard" being distinguished from "risk:" the facilities are high-*hazard* by virtue of having large source terms). Much has changed since those days, but the origin of many of the early ideas still survives in United States Nuclear Regulatory Commission (NRC) practice.

At the beginning of commercial nuclear power development, the Atomic Energy Commission (AEC) first considered remote siting of power plants to protect the public from large radiological releases, as opposed to engineered safety features. But for large commercial power reactors (as opposed to much smaller research reactors), primary reliance on distance turned out to be impractical: the distances required would be too large. A next logical step was to require functional containment in lieu of remote siting. But in time, this approach was found not to be entirely satisfactory, either; for commercial-scale light-water-reactor plants, the phenomenology of postulated severe accidents was challenging enough that it was difficult to claim convincingly that containment technology of that era could reliably contain severe-accident releases from light-water-reactor systems. Attention then turned to "emergency core cooling," on the reasoning that if severe accidents could be reliably prevented, doubts about containment performance would matter less. [10]

Throughout this evolution, much of regulatory thought was based on a worst-case reasoning process, including a tacit assumption that the "worst case" would be very serious. The idea was to be able to cope with what should have been the worst that could reasonably be foreseen, such as a large-break loss-of-coolant accident. Regulatory requirements were keyed to that thought process. License applicants had to show that their plants could cope with very challenging pipe break (loss-of-coolant) scenarios, concurrent with loss of offsite power and with the limiting single equipment failure. On top of that, even though those coping measures were intended to prevent severe core damage, plants were required to postulate significant radiological releases (intended to correspond to severe core damage) into containment, and then show that their containments would limit site boundary doses from those postulated source terms to acceptable levels. In addition to the postulated source terms, these analyses considered things like the consequences of blowdown resulting from the large pipe breaks; but they did not consider certain other key aspects of severe accident phenomenology.

The above way of thinking about safety is what most people nowadays call "deterministic" analysis. Specific postulated challenges to safety, such as "Loss of Coolant Accidents" (LOCAs), were analyzed according to specific protocols. The protocols required assumptions of particular conditions like single active failures, and licensees were (and are) required to demonstrate analytically a level of system performance implied by the satisfaction of acceptance criteria on key performance metrics (e.g. peak cladding temperature), despite the rigors of the challenges imposed. These analyses were meant to show that the prospect of serious radiological release was extremely remote. Many of the essential requirements of that era survive in today's practice; today's technical specifications and today's training are formulated as if the concerns of that era are the right things to focus on. But the bias towards limiting cases has proven to be suboptimal.

In the early 1970's, the AEC was asked to analyze the risks of nuclear power plants, and as a result, the WASH-1400 [11] study was initiated. Many of the tools and ideas that were used in WASH-1400 already existed, but WASH-1400 is generally agreed to be the first plant-scale analysis of its kind; in order to analyze risk, WASH-1400 had to develop detailed logic (fault tree) models of many plant systems, tie them together in fairly involved event trees in order to develop a scenario set, analyze plant phenomenology of those scenarios, quantify scenario frequencies, and interpret the results.

WASH-1400 showed numerous things, among them:

- Core damage was significantly more likely than some people had supposed, but the radiological consequences of core damage would almost certainly be less than most people had supposed.
- The analysis showed that sequences initiated by events such as transients and small LOCAs – events that are more frequent than large LOCA, and that pose different challenges to safety systems – contribute more to core damage frequency than does large LOCA.

- The reliability of post-trip decay heat removal is not necessarily in proportion to the frequency with which it is challenged.
- Some hazards had been overlooked in the deterministic analysis, including interfacing systems LOCA.

In response to this, beginning even before the accident at Three Mile Island and accelerating thereafter, PRA has played an increasing role in regulatory decision-making. Some changes to regulatory requirements were driven by PRA considerations, and PRA played an important role in generic issue resolution and in implementation of new requirements.

In 1986, the Commission issued its Safety Goal Policy Statement [discussed in 12], which:

> … expressed the Commission's policy regarding the acceptable level of radiological risk from nuclear power plant operation as follows:
>
> > *Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.*
> >
> > *Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.*
>
> The following quantitative objectives are used in determining achievement of the above safety goals:
>
> > *The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.*
> >
> > *The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.*
>
> This policy statement was not a regulation, but influenced various regulatory actions, primarily the development of the Regulatory Analysis Guidelines used in backfit analyses and the guidance developed for risk-informing reactor regulatory activities. …

In the late 1980's, all commercial reactor licensees were required [13] to perform "Individual Plant Examinations" (IPEs); among the purposes of doing this was to support resolution of the generic issue on post-trip decay heat removal reliability. In 1995, the NRC's PRA Policy Statement [14] included the following:

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.

Today, PRA is, in effect, a requirement for new plants (cf. 10 CFR Part 52 [15], and Chapter 19 of NUREG-0800 [16], the Standard Review Plan), and the technical basis for many licensing actions entails PRA analysis of proposed changes (see Regulatory Guide 1.174 [17]). Plant PRAs also inform many risk management actions as well, such as management of the plant configuration from a Maintenance Rule [18] point of view.

3. HUMAN SPACEFLIGHT RISK BACKGROUND

Human spaceflight has been a source of inspiration since Yuri Gagarin made the first human trip to space in April of 1961. The high visibility and national importance, not to mention the astronaut's lives, made launch vehicle reliability a high priority. For the U.S. space program in the 1960's, the approach to achieving high reliability revolved around testing, both at the system/component level and at the integrated-systems level. The Redstone and Atlas launch vehicles had numerous flights before Alan

Shepard and John Glenn rode them on the first human spaceflight missions for the U.S. After the Apollo program, with the space race to the moon won and the increasing cost of spaceflight, a new approach to managing risk was necessary.

With development of the Space Shuttle, extensive testing on individual systems and components (e.g. Space Shuttle Main Engines (SSMEs)) was performed, but testing the integrated system prior to humans being on board was found to be cost-prohibitive, so other means were required to evaluate and try to manage risk. Two techniques from System Safety practice [19] were used: Failure Modes and Effects Analysis (FMEA) / Critical Items List (CIL), and "hazard analyses," which are both qualitative in nature. These methodologies were exhaustively employed and complemented each other. The FMEA/CIL analyses were done for each component/subcomponent, and the results indicated whether the item/failure mode was:

- Criticality 1 – Loss of life or vehicle
- Criticality 2 – Loss of mission

Each criticality 1 item was evaluated for its detectability, test and inspection requirements, and other pertinent information to ensure that the risk from the failure mode was mitigated.

Hazard analyses is the second methodology used for the Space Shuttle in order to identify and control hazards. Hazards deemed "catastrophic" are of primary importance; they are hazards that may cause a loss of life or permanent disabling injury or a loss of the vehicle. Identified hazards are eliminated or controlled by some combination of the following steps, in order of preference: [20]

- Hazard elimination
- Design to minimize hazards
- Incorporate safety devices
- Provide caution and warning devices
- Develop special procedures

In 1981, the Space Shuttle became the first crewed launch vehicle that did not have any test flights of the integrated vehicle prior to being crewed. In 1986, the Challenger disaster occurred, and caused the National Aeronautics and Space Administration (NASA) to review its safety program. During this time, PRA was introduced to NASA through a limited study on the Auxiliary Power Units (APUs) [21]. The study was limited in scope, and performed as a proof of concept to evaluate benefits available from PRA. The first full-scope PRA of the integrated vehicle was completed in 1995 [22] followed by NASA developing its own PRA capabilities and models. Because the Space Shuttle was a mature system, the PRA was used to provide input on Space Shuttle upgrades and operational events.

NASA's approach today for assessing launch vehicle risk has multiple tiers depending on the launch payload. In general, the value of the payload drives the approach to ensuring the reliability of the launch vehicle. The launch vehicle risk for satellites and other science payloads are mostly evaluated through NASA's Launch Service Provider (LSP) program, which matches payloads to launch vehicles in order to maximize success of the mission. For human spaceflight, and for some science payloads containing nuclear material, the full scope of risk management techniques are required to be performed, including FMEA/CILs, hazard analysis, and PRA. The Constellation Program, which was to be the successor to the Space Shuttle, was the first program to include PRA requirements. These requirements started with limits on both Loss of Crew (LOC) probabilities per mission and Loss of Mission (LOM) probabilities per mission. The requirements have evolved to a threshold and goal philosophy that includes a maximum level of risk for a program to proceed, and a goal that drives additional mitigation to the extent that technology exists and it is not cost prohibitive.

One other consideration for launch vehicle risk not directly managed by NASA for its launches is the risk to the public and property. Range safety is managed by the Air Force through the use of probabilistic methods that evaluate:

- The probability of launch vehicle failure
- The probability of the type of trajectory the launch vehicle will be on and when it fails
- The inventory of hazardous material and projected characteristics of debris

NASA provides inputs [23] for these values and the Air Force performs a probabilistic analysis to estimate the number of expected casualties (E_c). The outcome of the analysis may cause a shrinking of the flight corridor, which defines an acceptable flight path that, if violated, will require the range safety officer to destroy the vehicle, and may also cause limitations on the number of launch observers in some higher-risk areas.

4. OFFSHORE OIL AND GAS WELL DRILLING RISK BACKGROUND

Offshore oil and gas exploration in the U.S. began in California in 1896 when it was found that the Summerland oilfield extended to the Pacific Ocean. Since then, many thousands of wells have been drilled offshore, in very shallow water to depths exceeding 10,000 feet. Most of the wells have been drilled in the Gulf of Mexico with an overall excellent safety and environmental record; however, like nuclear power and human spaceflight, significant accidents have occurred, and managing the risk from offshore drilling has become increasingly important with the new technologies being used and the more extreme environments being explored.

Until recently, modern offshore drilling in the U.S. has primarily depended on a qualitative approach to identifying and managing risk. A variety of tools is routinely used in this area including Hazard Identification (HAZID), Hazard and Operability studies (HAZOPs), Failure Modes and Effects Analyses (FMEAs), and Bowtie Diagrams.[†] HAZIDs and HAZOPs are performed in a group setting where a facilitator leads a technically diverse group of experts through an exercise to identify hazards related to equipment design of a given system in a given operating mode. The design intent in each operating mode needs to have been specified in sufficient detail to support a sensible discussion of system behavior: in particular, nominal values need to have been specified for all important system parameters. The HAZOP discussion is then cued to analyze the system considering "deviations" of key parameters in one node at a time, based on applying "guide words" (e.g., "high," "low") to each parameter (e.g., "flow") characterizing each node (e.g., high flow in node 32, low flow in node 32). For each such deviation, the group brainstorms possible causes and possible consequences of each cause, and then may consider other factors relevant to the decision context, including possible recommendations for design changes. This discussion implicitly addresses classes of scenarios, identifying them in terms of physical behaviours, many of which could be caused by any of several different component states (good or failed), and some of which could arise even if no components are nominally "failed."

Technical details of FMEA vary from application to application, but they are generally the same as described in [19].

Bowtie analysis results in a graphical representation of a class of scenarios that helps decision-makers reason appropriately.

- The middle of the bowtie represents a hazardous condition that results when control of a facility is lost (for example, an underbalanced condition).
- The left hand side develops causes that can lead to the hazardous condition and the controls in place to prevent its occurrence.
- The controls (including physical barriers) are placed between the cause and hazard showing the

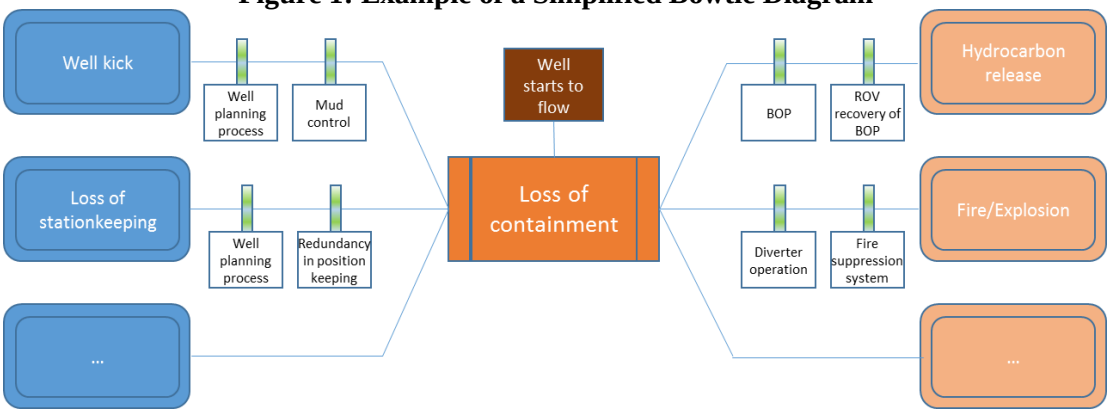
[†] References to these techniques are provided in [24].

failures that must occur for the hazard to occur.

- The right-hand side portrays scenarios ensuing from the occurrence of the hazardous condition, culminating in consequences on the far right. The scenarios on the right are specified in terms of the functions (including physical barriers) that limit or mitigate the consequences potentially resulting from the hazard.
- Each complete left-to-right path through a bowtie is a representation of a hazardous scenario to be considered.

A simple example of a bowtie diagram is shown in Figure 1.

Figure 1: Example of a Simplified Bowtie Diagram



The *Deepwater Horizon* incident in 2010, [8] offshore of Louisiana, resulted in a review of offshore drilling risk management processes by the Bureau of Safety and Environmental Enforcement (BSEE). As part of this effort, BSEE became interested in exploring whether PRA may be useful in identifying and managing risks, particularly for evaluating new technologies, operations in higher-risk environments, and proposed alternative means of compliance for existing regulations. BSEE and NASA formed a five-year collaborative agreement to pursue this effort starting in 2016 [25, 26].

While this paper focuses on the U.S offshore industry, specifically drilling, where some limited PRA studies have been done (e.g. [27]), it is recognized that in other parts of the world PRA techniques have been applied in the offshore oil & gas industry since the Piper Alpha event in 1988 [6].

5. OFFSHORE OIL AND GAS EXPLORATION WELL DRILLING BASICS

Since U.S. offshore oil and gas drilling technology is relatively new to some PRA practitioners in the U.S., a discussion of some of the basics involved in drilling an offshore exploration well is in order.

An offshore well may be located in just a few feet of water, or at depths greater than 10,000 feet. The water depth will influence the type of rig used to drill the well. A jackup (self-elevating) rig, one that has legs fixed in the seafloor while drilling, is used for shallow water wells (generally less than 400 feet). Semisubmersibles and drillships are used for deeper water, and maintain position by mooring to the seafloor if they are operating in shallow water, or by dynamic positioning if they are working in deeper water.

A well is spud (begun) by jetting a new hole with conductor pipe to a depth of hundreds of feet. The conductor pipe is large (36” to 42”) and thick (2” +/-) and its primary propose is to provide a structural conductor to provide support for lateral forces and support wellhead loads vertically until additional casings are installed. After the conductor is in place, a smaller drill bit is run through it to the bottom of the hole and drilling of the “surface” hole begins. When the surface hole is drilled to its designed depth, the bit is pulled out of the hole and surface casing is run to the bottom of the hole and cemented in place. The surface casing supports the high-pressure wellhead which is part of the surface casing.

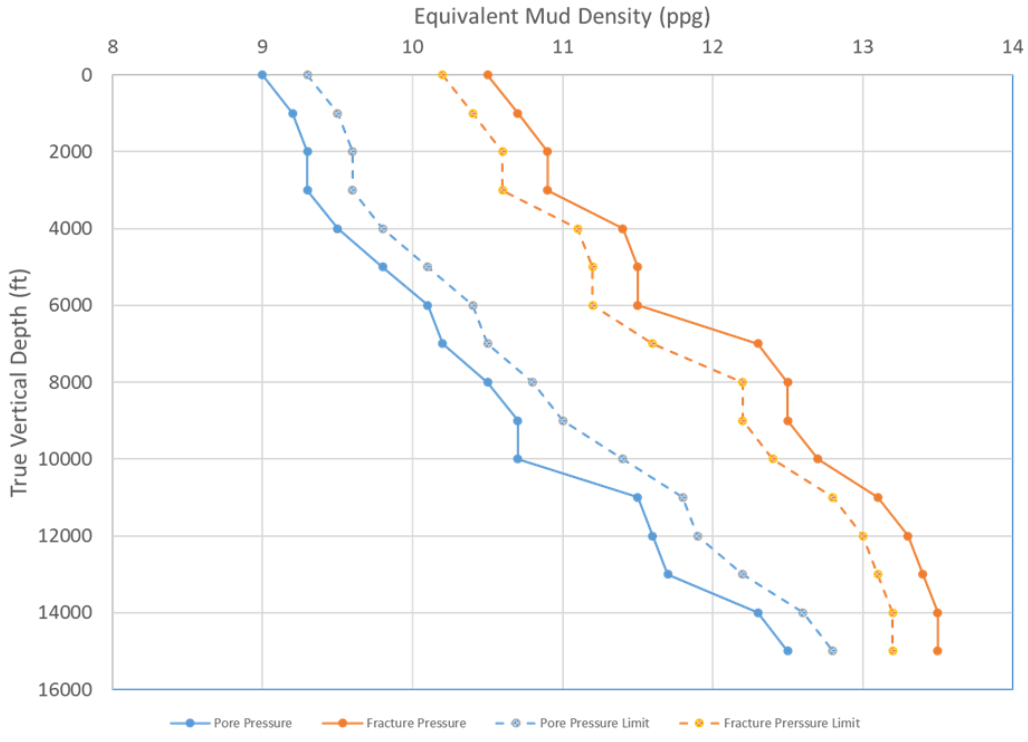
Casing is a metal pipe used to prevent an influx to the well; the cement provides a barrier by filling while the annulus between the casing and the formation.

Next, the blowout preventer (BOP) is lowered and latched to the wellhead. The BOP is attached to the rig by the riser, which is a series of pipe segments with external buoyancy to reduce the in-water weight. Prior to the BOP being latched up, when drilling fluid (mud) is pumped down the drill pipe to the bit, it returns up the hole and onto the seafloor; with the BOP installed, the drilling fluid for the remaining hole sections returns up the inside of the casing, through the BOP and riser to the rig. There, it is run through the mud system to remove the cuttings (small pieces of the formation), get conditioned and pumped back down the drill pipe to repeat the process.

The process of drilling new hole and running pipe (casing or liner) continues until the well has reached the target hydrocarbon reservoir. The setting depth of each casing interval is determined by the geologic conditions. Each casing interval must be smaller in diameter to the previous one to fit inside it. Since there is a physical limit as to the number of pipes that can be run inside each other and still leave the innermost pipe a large enough diameter to be able to complete the well for production, extending each casing segment as far as possible allows deeper wells, but again, geologic conditions must be factored into the well design.

Throughout the process, control of the well must be maintained so that no hydrocarbons are released. The primary means of well control is keeping a hydrostatic overbalanced pressure on the well so that formation fluids cannot enter the well. This is accomplished by adjusting the density of the drilling mud based on the geologic conditions anticipated. Two key parameters are of interest: the pore and the fracture pressure versus depth. The hydrostatic pressure due to the mud column in the well must be above the pore pressure of the formation to prevent an influx, but also must not be so high as to fracture the formation, which can also lead to a loss of well control and a hydrocarbon influx. An example of pore pressure and fracture gradient versus depth is shown in Figure 2, and shows how the values can vary with depth. This type of plot aids the well design team choosing the depths at which to set each casing segment.

Figure 2: Example Well Pore Pressure and Fracture Pressure Versus Depth



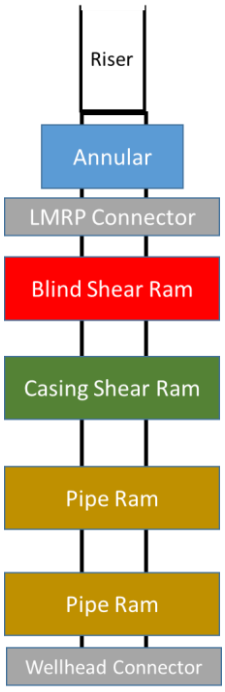
The secondary means of well control uses the BOP. In the event of an influx, the BOP has several independent means available to stop the influx from getting past it. A simplified BOP is shown in Figure 3. Several types of preventers are available, and are used alone or in combination depending on the well, influx, and BOP status. Some preventers are designed to close around drill pipe, while others are designed to close around casing or drill pipe. Of primary importance is the blind shear ram. It is capable of shearing drill pipe, if it is across the BOP, and sealing the well.

If the primary and secondary means of well control fail, hydrocarbons may get past the BOP into the riser, and up to the rig and into the environment. Remotely operated vehicles (ROVs), capping stacks, or relief wells are then needed to stop the release, and these can take a significant amount of time to implement.

6. A COMPARISON OF KEY RISK MODEL INPUTS/FEATURES

The three industries discussed all have high risks associated with them, and a need to identify and manage the risk associated with potentially hazardous events. The technologies and potential hazardous consequences associated with these industries are very diverse and require a range of specialties to adequately assess the associated risks. Of the three industries, nuclear power and human spaceflight have so far embraced the use of PRA for risk-informed decision making, while the U.S. offshore oil and gas industry is currently working with NASA to perform a proof of concept similar to what NASA did following the Challenger disaster. The remainder of this paper will compare some of the key PRA inputs/features of the offshore oil and gas modeling to those of the more established nuclear power and human spaceflight areas.

Figure 3: Simplified Blowout Preventer Stack



6.1. End States

The first step in developing a PRA model is to determine what end states (consequences) are of interest to support the decisions being made. For purposes of managing risk to the public from commercial light-water reactors, it was realized some years ago that severe accidents involving release of radionuclides from containment are useful end states to model. Core damage is an important intermediate end state; core damage does not automatically result in a hazard to the public, plant personnel, or the environment, but is an extreme consequence likely to result in a loss of the asset. To evaluate the risk to the public

and the environment, nuclear plant PRAs nowadays focus on "large early" releases of radioactive material that may affect people close to the plant before they can be evacuated. The definition of "large early" release is determined operationally.

Human spaceflight PRAs have been developed with two end states as well, Loss of Crew (LOC) and Loss of Mission (LOM). These end states are dependent on each other, but not in the way the nuclear power end states are. LOC is specific in that one or more crew members have lost their lives while on the mission. LOM is failure to meet one or more major mission objectives, which is generally defined as reaching the intended destination, staying for the intended duration, and returning the crew safely. LOC events by definition are included in LOM, since a mission objective is to return the crew safely.

As discussed in a previous subsection, risk to the public is also considered in analysis of spaceflight safety, involving different end states, but the present emphasis is on methodologies involved in LOC and LOM.

For offshore oil and gas drilling, safety and environment are paramount. While many risks may be encountered on an offshore rig, from crane accidents to rig floor mishaps, the risk with the greatest safety and environmental implications is an unmitigated release of hydrocarbons. An uncontrolled release from the formation that reaches the rig can cause a loss of life of the crew, and the often-remote locations of the rigs can make a rapid response from shore difficult. In addition, once a well has blown out, recovery can be difficult since some wells today are in 10,000 feet of water or more, and many recovery operations must be performed remotely. In short, a hydrocarbon release is an end state of interest, and modeling can be extended to address loss of life or assets through fire/explosion simulation, which is commonly done in other areas of the world such as the North Sea. Because oil and gas reservoirs can be many millions of gallons of hydrocarbons in size, once primary containment methods have failed, and the problem becomes developing a longer-term incident management approach, oil and gas drilling PRAs may find it useful to employ simulation techniques to estimate the likely size of releases. The size and location (close to shore, far offshore, etc.) of the release could have a significant effect on the environmental damage likely to occur.

6.2. Initiating Events

Over the years of industry and USNRC applications of PRA, a generic list of initiating events has been developed for each of the currently dominant plant types (boiling water reactor (BWR) and pressurized water reactor (PWR)), although individual plants may have some unique initiators, and some "generic" initiators may not apply to all plants. Initiating events are typically separated into two main classes, internal and external events. Internal events are a set of events that start within the plant systems, such as general transients that lead to a reactor trip or LOCAs. External events are those that initiate outside of plant systems, such as earthquakes and tornados. By definition, all "initiators" occurring at power should result in a reactor trip, and if a trip does not occur or other subsequent failures occur, a challenge to the integrity of the fuel may occur.

For spaceflight PRA, the approach to initiating events is somewhat different from the nuclear approach. Initiating events for a launch vehicle or spacecraft equate to failures which cause an end to the mission without completing its objectives. For human spaceflight, this is failure to complete its major mission objectives or safely bring home the crew after completing its mission. Internal and external event categories still apply to the PRA, but the structure of the model is not based on classes of initiating events followed by sequences of events leading to an end state. Rather, the model is set up with the initiating event being "launch." From there, the sequence follows the events required to complete the mission and the "initiating events" correspond to failure of the required functions, such as failure of thrust on ascent, or external events such as impingement of micrometeoroids and orbital debris (MMOD). Because human spaceflight is dynamic and has distinct phases (ascent, orbit, and entry), failures in redundancy must be tracked across the phases, as they can occur during one phase and become an "initiator" in another.

For offshore oil and gas drilling, evaluating initiating events uses a combination of the nuclear power and human spaceflight approaches. An offshore exploration well is a dynamic operation with different phases of operation similar to a spaceflight, but sequences of events can depend on the initiator, as in a nuclear power plant. The main consequence of interest is a large, uncontrolled release of hydrocarbons, which poses a threat to the crew and environment. All initiating events that can lead to this consequence start with either a hydrostatic underbalance or overbalance in a well. Each well is geologically different, and the drilling mud is the primary means of well control as discussed previously.

There are many causes of initiating events that can cause the hydrostatic pressure to be too low or too high. They are generally dependent on the well operation taking place. For instance, well swabbing occurs only when the drill pipe is being removed from the well. The suction created by removing the pipe can lower the downhole pressure to below the pore pressure, causing an influx of hydrocarbons. Some initiators, such as a loss of rig position, may occur during any operation. Should the dynamic positioning system fail and the rig lose position, an emergency disconnect occurs, and the loss of the slight overbalanced hydrostatic pressure comes when the rig separates from the BOP.

In addition to what operation is occurring, timing can affect whether the initiating event can lead to a hydrocarbon release. The target hydrocarbon reservoir(s) is at a specific depth, and hydrocarbons may or may not be present prior to reaching the reservoir, so some initiating events such as a loss of position will not necessarily be challenging from a large-release perspective.

6.3 Human Error

Human performance is generally important to safety. In nuclear power and human spaceflight, initiating events leading to a reactor SCRAM or an ascent abort may call for system response that is quicker than the response time window required by humans, and therefore initial facility response is automated. However, important human actions are still required in these industries, such as control of running systems in nuclear plants after they have been automatically initiated, and lowering the landing gear as part of the normal mission timeline for the Space Shuttle.

Offshore oil and gas drilling is somewhat different in terms of human error. The initial response to a well kick is based on human action, including diagnosing that a kick has taken place to begin with. Since each well is different geologically, and well kicks have many causes, diagnosing the kick may be difficult. Kicks may be very subtle with small influxes building over hours until the mud density in the well is reduced below the pore pressure, at which point the kick can start to "snowball." Conversely, some kicks may result in rapid large volume influxes that are much easier to detect. Time is critical to detection, because once the formation fluid has gotten past the BOP and into the riser, hydrocarbons will reach the rig.

Once a kick has been detected, the driller must respond appropriately by shutting in the well. Several options are available for this, and the conditions that must be considered include what, if any, type of pipe is across the BOP. Should problems occur when shutting in the well, the driller must make a decision as to whether to close the blind shear ram. If there is pipe across the BOP at the time, and usually during a kick there is, using the blind shear ram will shear the pipe, dropping it into the well, and this can be a costly event to retrieve the sheared pipe and continue well operations. Successful response to a well kick is accomplished when the well is "killed." Killing a well is successful when the well becomes static; this may take days or even weeks, with human actions determining the methods and processes used.

Another significant area for potential human error in offshore drilling is associated with dynamically positioned rigs. A Dynamic Positioning Officer (DPO) has the responsibility for maintaining position over the well. This can be challenging if significant weather occurs. At that point the DPO must align the rig appropriately, and failure to do this can result in a situation where an emergency disconnect is required. The emergency disconnect is also a human action, and failure to perform it can lead to serious consequences.

Overall, the offshore drilling industry requires some of its most critical and time-sensitive tasks to be performed by humans, and therefore, modeling of human error is crucial in offshore drilling PRA.

7. CONCLUSION

So far, logic-model-based PRA has been found to be useful in all three industries discussed here. Each industry (commercial nuclear power, human spaceflight, exploration-well drilling) has its own issues, calling for its own emphases and its own modeling needs (e.g., human error in drilling operations), but the general principle holds that scenario-based modeling is needed to inform decisions made in managing the risks of a complex, high-stakes technology.

However, in all three domains, it is necessary to consider not only logic modeling of scenario sets, but also modeling of scenario phenomenology, including fire and explosion. Reference [24] is a work in progress, and future revisions of it will need to devote substantial attention to these areas.

Acknowledgements

Work at INL was performed for NASA's Johnson Space Center under DOE Idaho Operations Office Contract DE-AC07-05ID14517. Opinions expressed in this paper are opinions of the authors, and do not necessarily represent the views of the Johnson Space Center, BSEE, or INL.

References

[1] Farmer, F. R., Siting criteria - a new approach, Presented at IAEA Symposium on the Containment and Siting of Nuclear Power Reactors, Vienna, SM-89/34 (April 1967).
[2] Garrick, B.J., 1968. Principles of Unified Systems Safety Analysis, Nucl. Eng. And Design 13, 245-321 (North-Holland Publishing Company, 1970).
[3] USNRC, 1980 (January). Special Group Inquiry; Three Mile Island — A Report to the Commissioners and to the Public. Mitchell Rogovin, Director.
[4] Kemeny, J.G., 1979 (October). Report of the President's Commission on the Accident at Three Mile Island.
[5] Presidential Commission on the Space Shuttle Challenger Accident (Washington: Government Printing Office, June 6, 1986).
[6] Cullen, The Hon. Lord W. Douglas (1990). The public inquiry into the Piper Alpha disaster. London: H.M. Stationery Office. ISBN 0101113102.
[7] Columbia Accident Investigation Board Report, National Aeronautics and Space Administration (NASA, 2003).
[8] "Deepwater Horizon Joint Investigation Team Report," https://www.bsee.gov/newsroom/library/deepwater-horizon-reading-room/joint-investigation-team-report, September 9, 2011.
[9] Jan-Erik Vinnem, Offshore Risk Assessment: Principles, Modeling, and Applications of QRA Studies, Third Edition (Vols. 1 and 2), Springer Series in Reliability Engineering, Springer-Verlag (London, 2014).
[10] "Perspectives on Reactor Safety," NUREG/CR-6042, SAND93-0971, Revision 2, U.S. Nuclear Regulatory Commission, 2002.
[11] "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," NUREG-75/014 (WASH-1400), U.S. Nuclear Regulatory Commission, October 1975.
[12] W. D. Travers, "Modifications to the Reactor Safety Goal Policy Statement," SECY-00-0077, U.S. Nuclear Regulatory Commission memorandum, March 30, 2000.
[13] "Individual Plant Examination for Severe Accident Vulnerabilities," 10 CFR 50.54(f) (Generic Letter No. 88-20), U.S. Nuclear Regulatory Commission, November 23, 1988
[14] Probabilistic Risk Assessment (PRA) Policy Statement, 60 FR 42622, U.S. Nuclear Regulatory Commission, August 16, 1995.

[15] "Licenses, Certifications, and Approvals for Nuclear Power Plants," 10 CFR Part 52, U. S. Nuclear Regulatory Commission.
[16] "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," NUREG-0800, U. S. Nuclear Regulatory Commission, August 4, 2004.
[17] "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Revision 3," Regulatory Guide 1.174, U. S. Nuclear Regulatory Commission, January 2018.
[18] "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," 10 CFR 50.65, U. S. Nuclear Regulatory Commission.
[19] "Department of Defense Standard Practice System Safety," Department of Defense, MIL-STD-882E, February 10, 2012.
[20] "Constellation Program Hazard Analyses Methodology," CxP 70038 Baseline, 12/18/2006.
[21] Garrick, B. J., **"**Space Shuttle Probabilistic Risk Assessment, Proof-of-Concept Study, Auxiliary Power Unit and Hydraulic Power Unit Analysis Report," December 1, 1987.
[22] Fragola, J. R. et al., "Probabilistic risk assessment of the Space Shuttle. Phase 3: A study of the potential of losing the vehicle during nominal operation," February 28, 1995.
[23] Cross R., Gowan J., et al., "Development of Launch Area Risk Assessment Input Data for Ares I-X," Atmospheric Flight Mechanics Conference and Exhibit, Honolulu, Hawaii, August 18-21, 2008
[24] Probabilistic Risk Assessment Procedures Guide for Offshore Applications (DRAFT), JSC-BSEE NA-24402-02, downloadable from [25].
[25] https://www.bsee.gov/what-we-do/offshore-regulatory-programs/risk-assessment-analysis/probabilistic-risk-assessment-analysis [BSEE web page]
[26] BSEE/NASA Interagency Agreement E16PG00012, "Quantitative Risk Assessment, Engineering Test Design, and Failure Analysis." 2016
[27] Shanks E., Pruitt J., Schroeder J., "Surface BOP Reliability Issues for Deepwater Floating Drilling Rigs," IADC World Drilling 2002, Madrid, Spain, June 5-6, 2002.