PRA Application to Offshore Drilling Critical Systems

S. Massoud (Mike) Azizi
Principal Engineer and Associate Technical Fellow
Reliability, System Safety and Specialty Engineering
Aerojet Rocketdyne – Extreme Engineering

Abstract: The nuclear and aerospace industries systems engineering approach typically incorporates Probabilistic Risk Assessment (PRA) to estimate risk using quantitative methods to determine what can go wrong, the likelihood of occurrence of such events and the probable consequences. Thus, PRA provides insight into the strengths and weaknesses of the system's design, operation and maintenance strategy. For instance, in the nuclear industry PRA is traditionally used to estimate the core damage and potential consequences relative to the reactor, facilities, power grid, environment and public. A Space Shuttle and launch vehicle operations PRA would provide an estimated risk for operations on the ground and during the launch, on-orbit, re-entry and landing phases.

Similar discipline as those applied in the nuclear and aerospace industries can also be applied to various "mission critical" onshore and offshore oil and gas drilling, exploration and production systems. This paper describes the PRA methods as they could be applied to these systems and how the outcomes of such discipline can benefit the system's design, operations and stakeholder interests.

Keywords: PRA, FMECA, Nuclear, Aerospace, Offshore Oil and Gas Drilling, Mission Critical

1. INTRODUCTION

Probabilistic Risk Assessment (PRA) methodology has been utilized in assessing the risk of accidents within various industries. The nuclear industry has been using PRA (sometimes referred to as Probabilistic Safety Analysis (PSA)), for the past four decades. NASA also used PRA to evaluate the risk of the Space Shuttle (Shuttle) accidents during various stages of the Shuttle flight. PRA methodology was also used to evaluate the consequences of radioactive nuclear material release to the environment for the launch vehicles carrying nuclear material payloads, during launch or re-entry accidents (payload nuclear safety analysis). Although the PRA methodology details vary among different applications, the ultimate objective, that is to evaluate the risk by estimating the frequency and consequences of accidents remain the same. The Oil & Gas (OIL AND GAS) industry has adopted risk management in various forms but not as extensive as the nuclear and aerospace industries.

The objective of this paper is to demonstrate some meaningful conclusions about the risk of potential oil rig accidents using the PRA methodology.

2. PRA APPLICATIONS TO NUCLEAR INDUSTRY

One of the industries that have used PRA methodology extensively is the nuclear industry. The Nuclear Regulatory Commission (NRC) mandated all US nuclear plants to perform individual plant risk evaluation [1] in 1989 as a result of the Three Mile Island (TMI) accident in 1979 (Figure 1).

> *Pursuant to 10CFR5O.54(f) the NRC issued Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities", requiring that each plant perform a systematic examination for the purpose of identifying plant specific vulnerabilities to severe accidents and to report the results to the Commission. NUREG-1335 was provided as guidance to document and submit the results of the plant specific evaluation.*

Even before the NRC mandate, many utilities took it upon themselves to complete their respective plant PRA. The NRC also established quantitative goals for each plant core damage mean frequency[2] as 1.0E-04 per reactor year (RY), and conditional containment failure probability of 1.0E-02 following core damage and release of radioactivity into the containment. Typically, a nuclear plant PRA is composed of three levels with one additional assessment for the effects of external events such as earthquake or flooding. The three PRA levels are shown in Table 1. The PRA Procedures Guide [3] provides detailed guidelines for performing the three levels of PRA and the external event analysis. The PRA Procedures Guide was derived from the Reactor Safety Study [4], developed by the US NRC in 1975. Many nuclear power plant owners used the results of the PRA to incorporate additional safety measures into their power plants, improve their operations and maintenance practices, and ultimately increase their plant availability and capacity factor [5]. Note that the US commercial nuclear plants capacity factor improved from 58% to about 90% between 1974 and 2012.

Figure 1. Three Mile Island

3. PRA APPLICATIONS TO AEROSPACE INDUSTRY

The aerospace industry has also used PRA methodology to improve launch safety for various spacecrafts. Following the Challenger accident in 1986 (Figure 2), based on the Rogers Commission recommendations [6], NASA initiated a series of risk assessment efforts in order to further improve the Space Shuttle (Shuttle) safety.

> *NASA's objective is to better understand and effectively manage risk, and thus more effectively ensure mission and programmatic success, and to achieve and maintain high safety standards at NASA. NASA intends to use risk assessment in its programs and projects to support optimal management decision making for the improvement of safety and program performance*[7].

In 1997, NASA Head Quarters (HQ) initiated HQ lead PRA effort using Quantitative Risk Assessment System (QRAS) software [7]. The application of the PRA methodology to a Shuttle environment, particularly to the potential of catastrophic Shuttle failure was addressed. The different related concerns were identified and combined to determine overall program risks. A fault tree model was used to allocate system probabilities to the subsystem level. The loss of the vehicle due to failure to contain energetic gas and debris, to maintain proper propulsion and configuration was also analyzed, along with the loss due to Orbiter, external tank failure, and landing failure or anomaly.

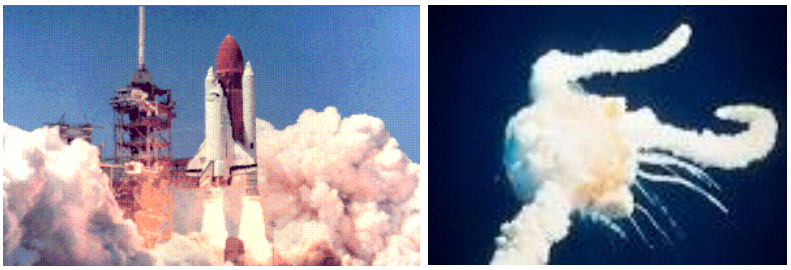


Figure 2. Space Shuttle Challenger

Although the Shuttle PRA did not set quantitative target goals, the Orbiter and other Shuttle systems such as the Space Shuttle Main Engines (SSME) failure probability were calculated and documented. Considering that there were two failures among 135 Shuttle flights, failure history resulted in historical failure frequency of 2/135 or 1.48E-02 per flight. NASA used the PRA results for risk informed flight decisions and to improve Shuttle systems reliability and safety [8].

Other risk assessments such as the Multi Mission Radioisotope Thermoelectric Power System (MMRTG) nuclear safety analysis (Figure 3) and Cassini PRA (Figure 4) provided valuable insight

into accident scenarios and potential environmental, health and safety consequences following the launch pad and in-flight catastrophic failure, or in case of re-entry back to earth atmosphere.

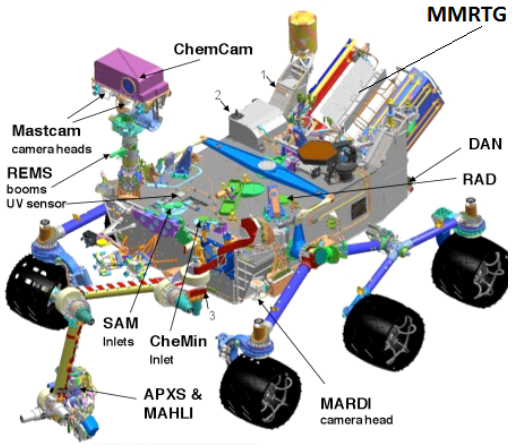


Figure 3. Mars Science Lab (Curiosity Rover) with MMRTG Power System

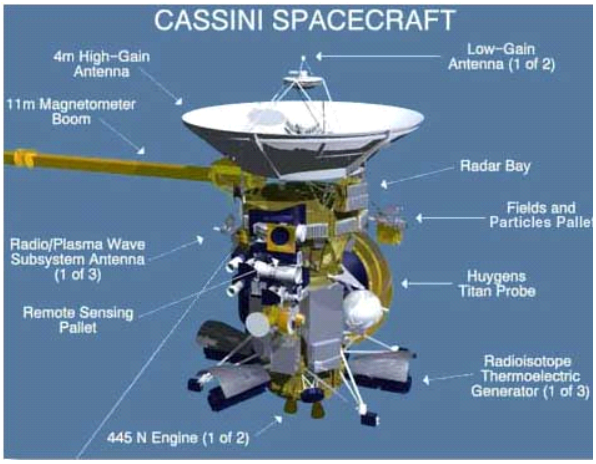


Figure 4. Cassini Spacecraft with Radioisotope Thermoelectric Generator (RTG) Power System

4. GENERAL PRA METHODOLOGY

In general, PRA methodology is composed of two distinct stages, systems analysis and consequence analysis. Each of these stages can be further broken down into various tasks depending on the system to be analyzed.

The systems analysis provides insight into the plant (power plant/rig/vehicle, etc.) configuration and interaction, components success criteria, list of potential initiating events, and the sequence of event progression resulting in various consequences, depending on potential mitigating systems behaviour.

The plant system/subsystem configuration and interaction is a process where all the plant functions, systems, subsystems, components and operational modes are identified. This step can be divided into two major tasks:

1. **Plant familiarization-** This step includes reviewing the system specs, plant layout drawings, emergency procedures, training procedures, plant walk downs, and interviewing the operations/ maintenance staff. As part of plant familiarization, the analyst also identifies plant operational modes, system/component functions and success criteria for each mode. From a reliability perspective, failure rate database generation is also initiated where plant specific or generic data for individual components are collected and analyzed using the industry generic failure rate databases or plant internal databases.
2. **Accident initiation identification-** Once the plant functions, systems and subsystems configuration and interactions are identified, the focus will be shifted to the potential plant accidents. A Master Logic Diagram (MLD) will be developed identifying the potential plant accidents and the accident initiators (initiating events). This stage will also include estimating a probability of occurrence for each initiating event. This probability can be derived by using the failure rate database or through generic industry estimates.

Development of functional and systemic event trees- Each initiating event will affect a series of functions within the plant. These functions could either help mitigate the consequences of the initiating event, have exacerbating effect or are considered as part of plant's frontline safety measure. The collective functions success or failure will generate a list of sequence of events that will each result in a specific consequence. Functional Event trees (Figure 5) will set the stage for developing more complex Systemic Event Trees (Figure 6). The next step is to expand the plant functions into the

systems within the function (systemic event tree analysis). Each event tree therefore is expanded to utilize the system interaction within each sequence. Fault tree analysis is typically used at this stage to identify contributors to each system failure. By quantifying each fault tree a list of "dominant contributors" is identified. The dominant list of contributors to each system failure (minimal cutsets) is then used within the sequence of events to develop each consequence list of minimal cutsets, or the dominant contributors to that consequence.

Consequence Analysis- Following the completion of initial systemic analysis and sequence quantification, the consequences are grouped based on their severity and time to effect. The list of each sequence cutset for specific consequence is analyzed to find out potential for reduction in consequence severity by modifications with the system design, operations, human interface, maintenance, etc. Finally uncertainty analysis is performed on each list of sequence cutsets and the results are evaluated for further improvements.

Nuclear Plant Level II PRA- As explained earlier, in a nuclear plant PRA, once the consequences of the initiating events are identified and analyzed, the impact of each core damage scenario is used to develop the containment behaviour model (Level II PRA). At this stage, the containment systems response ands its structural integrity is analyzed following the breach of the reactor vessel and release of fission products and gases into the containment atmosphere. Containment event trees followed by containment systems fault trees determine the sequence of events leading to containment failure including radioactive dispersion and identification of source terms. Various software codes have been developed to model the radioactive material and gases released to the containment following the core damage. These codes identify potential source terms and release fractions into the containment.

Nuclear Plant Level III PRA- For a nuclear power plant, Level III PRA models post containment failure scenarios and radionuclide release to the offsite environment. Software codes have been developed to estimate human fatality and the environmental damage due to the radioactive "plume" movement and dispersion and the consequential radionuclide fallout in its path.

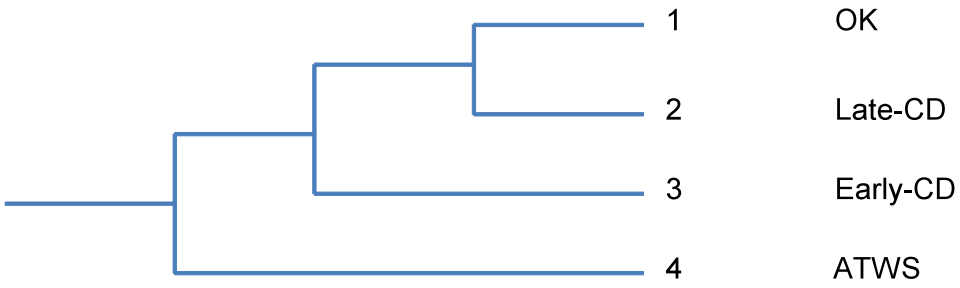
External Events Analysis- The effect of external events to plant performance is an extra series of assessment used by many nuclear reactor owners to determine the reactor response and consequences of such events. External events can be considered at any level of PRA depending on the objectives and the scope of study. Typically, the external event analysis addresses the influence of design and construction errors and human errors due to operator action or inaction.

Space Shuttle PRA- While NASA's Space Shuttle PRA (SPRA) used similar methodology as a level I nuclear plant PRA, there were some differences between the two analyses. The SPRA was the most comprehensive and peer-reviewed NASA PRA that was intended to be used as a risk management tool and provided insights into the significant risks of Space Shuttle flight. As with any PRA of a large, complex, and engineered system, the SPRA was developed for a defined scope; and engineering judgment was used to make assumptions where necessary. The following were primary limitations and observations regarding the SPRA scope.
– Did not include mission-specific on-orbit operations (e.g., extravehicular activity).
– Did not include all flight rules, and therefore all pre-planned operational procedures.
– Did not encompass ground operations (e.g., tanking, scrub turnaround, ground tracking, crew egress, etc.). Note that in some cases, ground-induced failures were incorporated in defined failure rate functions. However, ground processing was not explicitly modeled.

The Shuttle was a very reliable vehicle in comparison with other launch systems. Much of the risk posed by Shuttle operations was related to fundamental aspects of the spacecraft design and the environments in which it operated. The SPRA initially utilized QRAS as the analysis tool where "Event Sequence Diagram" was used instead of event trees; however NASA analysts later converted their method of analysis to event tree/ fault tree analysis using SAPHIRE code.

Functional Event Tree Example

Initiating Event	Reactor Trip	Short Term Core Cooling	Long Term Core Cooling	SEQ #	State
IE	RX-TR	ST-CC	LT-CC		

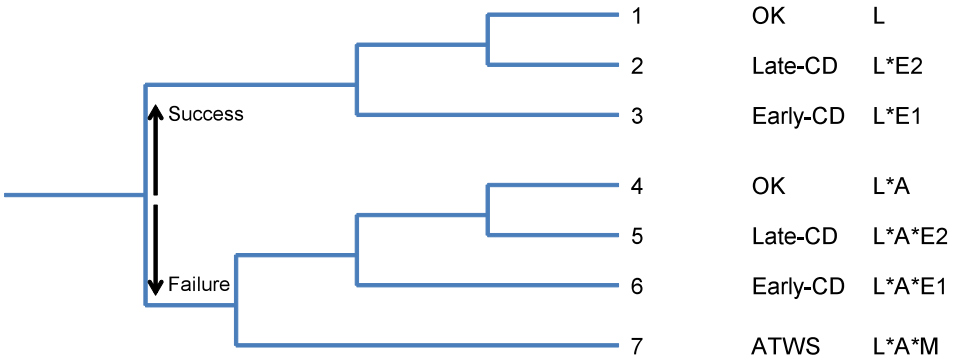


IE = Initiating Event
RX-TR = Reactor Trip
ST-CC = Short Term Core Cooling
ATWS = Anticipated Transient Without Scram
LT-CC = Long Term Core Cooling
SEQ = Sequence
CD = Core Damage

Figure 5. Sample Functional Event Tree for a Nuclear Reactor Loss of Coolant Accident (LOCA)

Systemic Event Tree Example

Initiating Event	Reactor Trip		Short Term Core Cooling	Long Term Core Cooling	SEQ #	State	Logic
LOCA (L)	Auto (A)	Manual (M)	ECI (E1)	ECR (E2)			



LOCA = Loss Of Coolant Accident

Figure 6. Sample Systemic Event Tree for a Nuclear Reactor Loss of Coolant Accident (LOCA)

5. PRA APPLICATIONS TO OIL AND GAS INDUSTRY

The oil and gas industry also adopted risk management in various forms since the early 1970s. The terms QRA (Quantitative Risk Assessment), PSA and PRA are used synonymously in various occasions by different analyses to identify the risk assessment methods. Note that while the nuclear industry tends to require that the frequency of a given radiological release and associated doses are less than defined levels, on an offshore platform however, where only workers are exposed, the emphasis is more on the individual risk to personnel. The 2010 Macondo accident demonstrated that the consequences of a catastrophic offshore drilling rig failure will not only affect the rig workers but could potentially have severe impact on the environment and the regional economy. Most of the oil and gas industry, specifically the offshore drilling and production risk analysis, have been limited to Failure Modes, Effects and Criticality Analysis (FMECA) and HAZOP and Hazard Analysis to understand the risks associated with the rig and the subsea systems. These assessments were useful to identify the many risks inherent in the design and operating environment of the systems, and the assessment results could be used to inform recommendations for improving the design and operational risk controls. However, the qualitative nature of these assessments can lead to inconsistency and imprecision in risk characterization that make risk prioritization difficult and risk aggregation impossible. For these reasons, it is not historically feasible to derive a robust rig surface and subsea systems reliability estimate or to accurately prioritize top risk contributors. Such insight is crucial to improving the reliability of these systems. Although there have been guidelines published by various organizations (e.g., OLF [9] and API [10]) no structured PRA approach, such as the ones used in the nuclear industry, or by NASA has been recommended or implemented for the oil and gas industry. As mentioned above, the qualitative analyses such as FMECA or hazard analysis where single point contributors to the system design and operation failure were identified has been the norm for performing risk management. A detailed analysis, such as a nuclear plant level I PRA however, can point to various scenarios leading to catastrophic failures with different levels of severity. Further, the consequences of those failures need to be assessed similar to a nuclear plant level III PRA, where the potential damage to onboard and/or subsea systems could result in loss of life and property, and environmental catastrophe. Table 1 illustrates how an offshore rig PRA might equate to a nuclear plant or aerospace type PRA analysis.

In order to develop a meaningful quantitative assessment, it may be necessary to establish a target frequency of occurrence for a specific catastrophic failure scenario such as “fire/explosion on board the rig due to uncontrolled blow out” or “Release of hydrocarbon to the environment beyond XYZ gallons per unit time”, etc. This approach will establish a target similar to the core damage frequency (1.0E-04/RY) established by the US NRC for the commercial nuclear reactors. The quantitative target will help the analyst evaluate and compare the results of his assessment against a target value. This evaluation could lead into modifications in system design, operation or maintenance activities that could potentially reduce the consequence frequency to the target goal.

Table 1: Comparison of PRA activities among different industries

PRA Level	Nuclear	Aerospace	Offshore Oil	Notes
1	• Systems Analysis • Core Damage Frequency Evaluation • Consequence Analysis • Uncertainty Analysis	• Space Shuttle Systems Analysis • Calculate Probability of Loss of Vehicle • Calculate Probability of Loss of Crew • Uncertainty Analysis	• Rig systems Failure Analysis • Subsea Systems Failure Analysis • Hydrocarbon Release Frequency Evaluation • Consequence Analysis • Uncertainty Analysis	1. Plant/vehicle/rig operational mode should be clearly identified 2. Human Reliability and Data Analysis are integrated part of systems analysis 3. Quantitative risk target is industry specific
2	• Containment Analysis • Containment Failure modeling and Probability • Uncertainty Analysis	NA	NA	Containment failure modelling includes fission product release into containment
3	• Radionuclide release modeling • Source Term calculations • Human fatality estimates • Environmental Damage estimates • Uncertainty Analysis	• Nuclear Safety Analysis for Space Nuclear Power Systems (Cassini, MMRTG) • Radionuclide Release Modeling • Source Term Calculations • Human fatality estimates • Environmental Damage estimates • Uncertainty Analysis	• Hydrocarbon Release Modeling • Environmental Damage Estimates • Uncertainty Analysis	Severity of hydrocarbon release to be determined by the regulators
External Events	• Earthquake • Flood • Fire • Wind • Sabotage • Aircraft Impact	NA	• Earthquake • Hurricane • Object/ iceberg/ vessel impact • Sabotage • Aircraft Impact	

Deepwater Horizon Accident (Figure 7) may have been prevented had a PRA been completed and the results implemented into the design, maintenance and normal and emergency operations procedures. Reviewing the sequence of events from the various incident investigation teams demonstrate that following an initiating event (Hydrocarbon leakage through annulus cement barrier), a series of events resulted in loss of the rig and human life and release of millions of barrels of oil into the Gulf of Mexico (Figure 8).

> *The team did not identify any single action or inaction that caused this accident. Rather, a complex and interlinked series of mechanical failures, human judgements, engineering design, operational implementation and team interfaces came together to allow the initiation and escalation of the accident…*[11]

Figure 7. Deepwater Horizon Accident

A review of the sequence of events following the leakage of hydrocarbon through the bottom casing annulus cement barrier is reflected in the event tree illustrated in Figure 9. As illustrated in this event tree, a series of events occurred following the initial failure of the cement barrier resulting in on-board fire and explosion that caused loss of life, the rig and release of millions of barrels of oil into the Gulf [14]. Had these scenarios been modelled and systemic event trees and related fault trees been developed and the results applied to the design, operation and maintenance and emergency procedures, the likelihood of such catastrophe would have been dramatically minimized. The above event tree is only based on a single initiating event. Many other functional and systemic event trees could be modelled for other potential initiating events. A structured PRA would facilitate such effort.

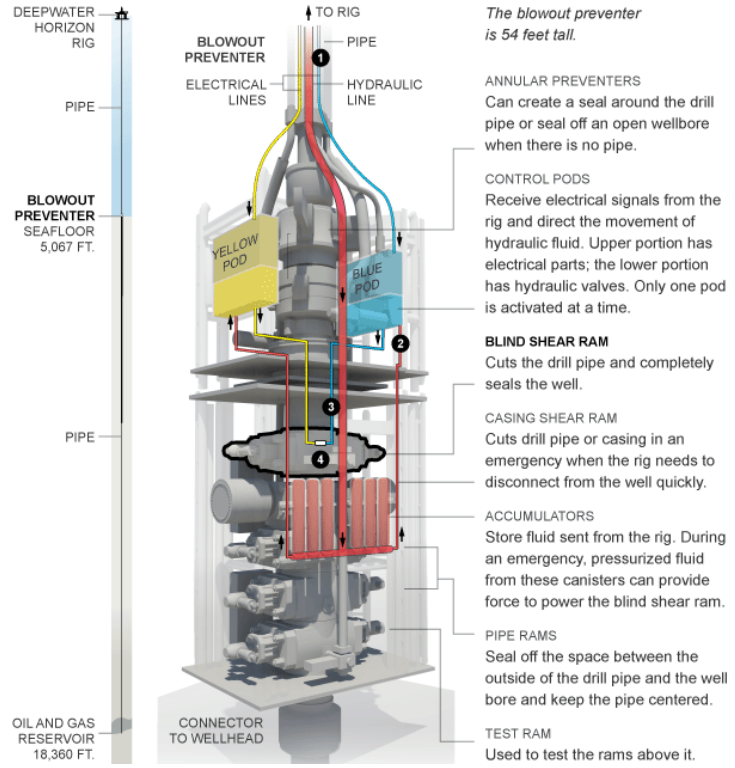
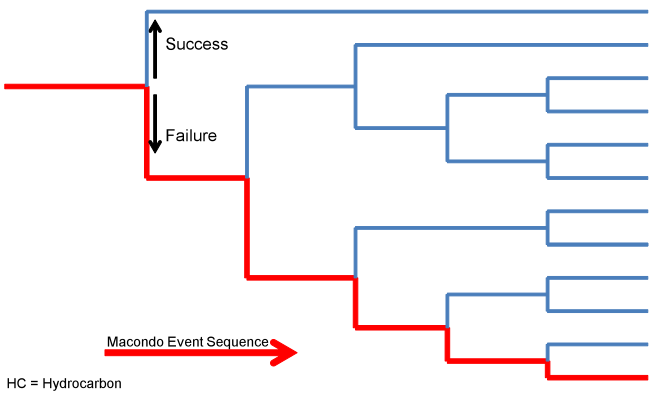


Figure 8. Deepwater Horizon Operational Mode and Blowout Preventer

Deepwater Horizon Sample Functional Event Tree

Hydro-carbon leakage through annulus cement barrier	Well Integrity	Well Hydrostatic Control	Well flow Control	Hydro-carbon Release Control	The BOP Emergency Function	SEQ #	State	Logic
Leak (L)	WI (W)	WHSC (H)	WFC (F)	HCRC (R)	BOPEF (B)			



SEQ #	State	Logic
1	OK, No Leak Thru Shoe Track	L
2	Leak detected, WHSC applied	L*W
3	Failure of WFC, HC flow up thru riser	L*W*F
4	HCRC failure, late release overboard	L*W*F*R
5	Initial Blowout, controlled BOPEF	L*W*F*R
6	BOPEF failure, late loss of rig	L*W*F*R*B
7	OK, BOP prevents HC release	L*W*H
8	Partial release, early fire/exp. overboard	L*W*H*B
9	Early blowout, cntl'd by HCRC and BOPEF	L*W*H*F
10	Early blowout, failed BOPEF, HC release	L*W*H*F*B
11	Early blowout, cntl'd BOPEF	L*W*H*F*R
12	Early blowout, fire explosion, loss of rig	L*W*H*F*R*B

Figure 9. Deepwater Horizon Sample Functional Event tree

6. DATA

One of the concerns with many oil companies and their drilling contractors is data management and utilization of the operational and maintenance data in the rig and sub sea systems risk assessment. The nuclear industry resolved this issue with the help of the Institute of Nuclear Power Operations (INPO). INPO was established by the nuclear power industry in December 1979. The main mission of INPO is:

> *To promote the highest levels of safety and reliability – to promote excellence – in the operation of commercial nuclear power plants* [11]

The three main objectives of INPO operations are:

- Establishing performance objectives, criteria and guidelines for the nuclear power industry
- Conducting regular detailed evaluations of nuclear power plants
- Providing assistance to help nuclear power plants continually improve their performance

One of the areas that INPO has been able to drastically help the nuclear industry was with nuclear power plants data management. The Nuclear Plant Reliability Data System (NPRDS) was introduced in the middle-70s, it allows the nuclear industry to compare component performance, analyze failures and find nuclear plants with similar equipment. INPO took over NPRDS management in 1982, and has made a number of enhancements to improve its usefulness and reliability. NPRDS is now called Equipment Performance and Information Exchange (EPIX) since 1997. EPIX is a computer database of engineering and failure data on components installed in U.S. nuclear plants. EPIX is the only industry wide component database currently available to all utilities. In addition to the nuclear industry, the NRC also uses INPO EPIX database as well.

> *EPIX is maintained by INPO and provides an industry-wide database of information on Maintenance Rule components at all US nuclear power plants. NRC staffs access the EPIX database through the INPO website. EPIX data are used in NRC's Reliability and Availability Data System (RADS), Integrated Data Collection and Coding System, and Common Cause Failure Database to estimate probabilistic risk assessment (PRA) parameters. EPIX data are also used to update NRC Standardized Plant Analysis Risk (SPAR) models and to assist in developing and implementing the Mitigating System Performance Index (MSPI).* [12]

One of the best organizations in the oil & gas industry whose mission is similar to INPO is the American Petroleum Institute (API),

> *The American Petroleum Institute (API) is the only national trade association that represents all aspects of America's oil and natural gas industry. Our more than 550 corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry. They are producers, refiners, suppliers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry.* [13]

Although API mission is broader than INPO, the focus of both organizations is to improve their respective industry safety and reliability. API has generated safety related document such as API-17N in order to standardize safety and reliability methodology approach. API has also established other safety branches such as Center for Offshore Safety (COS) whose focus is "promoting the highest levels of safety and environmental protection for offshore drilling, completions and production operations in deepwater Gulf of Mexico". Therefore it is possible that API can develop a similar database as INPO's EPIX where the oil and gas companies and their contractors and operators can benefit from it. This however is a decision to be made by API and its members.

7. PRA MANAGEMENT

PRA management can be viewed from two aspects, from a regulatory aspect, and from the user/ industry aspect. The regulator uses PRA to align its regulations and guidelines to the industry according to the risk drivers and how they are managed by the industry. The user/ industry use PRA as a risk management tool to evaluate and the strength and weaknesses within its plant/ system and make appropriate modifications into its design, operation, maintenance, inspection, etc.
One of the methods for managing PRA is to utilize "Risk-informed" approach to system design and operation. PRA may not have all the answers, but when the risk-informed and the deterministic approaches are blended together, there is a likelihood of getting closer to the right answer. Risk-informed approach refers to incorporating insights from the plant's probabilistic risk assessment (PRA) into a process that also considers equipment reliability and test/maintenance history to establish surveillance test frequencies. Figure 10 illustrates a block diagram depicting concept through interfaces among PRA, reliability and safety analysis methods that could ultimately enhance the design, operation and maintenance.

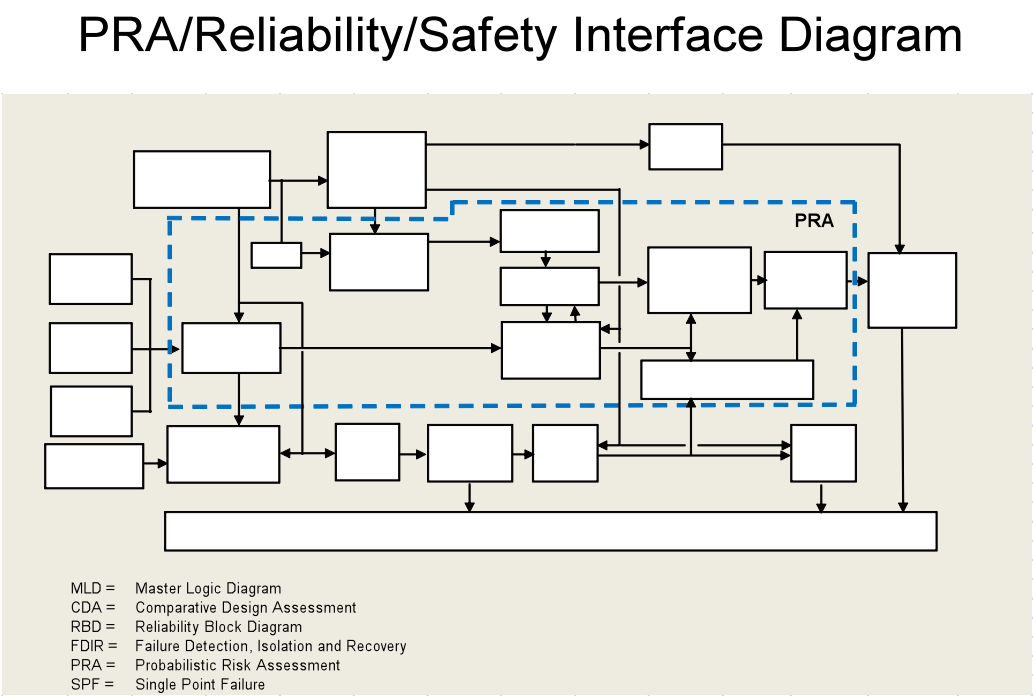


Figure 10. PRA, reliability and system safety assessments enhance the "Risk-Informed" Approach

Another important approach to PRA management is to utilize "Defense-in-Depth". Defense-in-depth is an approach to designing and operating facilities that prevents and mitigates accidents that could result in severe consequences. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense-in-depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures. The principle of defense-in-depth is that layered safety mechanisms increase safety of the system as a whole. If a failure causes one safety mechanism to fail, other mechanisms may still provide the necessary safety measure to protect the system.

7.1. PRA management in nuclear industry

The nuclear industry started applying PRA methodology to the commercial nuclear plants following the development of the Reactor Safety Study (Wash-1400) [4].

- Wash-1400 forced the NRC to consider many issues and eventually start making changes to its regulatory system.

- NRC utilizes PRA to quantify a risk metric (e.g., core damage frequency, core damage probability, large early release frequency) for the assessed plant configuration which typically includes comparison against nominal plant configuration

- NRC PRA management takes measures to avoid risk-significant configurations, acquire better understanding of the risk level of a particular plant configuration, and/or limit the duration and frequency of such configurations that cannot be avoided
- Many plant owners have developed their respective plant PRA as "Living PRA", where plant operational, maintenance and emergency historical data are fed back into the PRA analysis to reevaluate the accident consequences. In many instances, the plant design, operations and maintenance modifications resulted from PRA analysis has also been incorporated into the plant's technical specifications (Tech Specs), Emergency Operations Manuals and maintenance procedures.

7.2. PRA management in Aerospace industry and NASA

Space Shuttle Program (SSP) initiated the development of the SPRA to provide a useful risk management tool for identifying strengths and possible weaknesses in the Shuttle design and operation. The SPRA model is a typical PRA model in that it is based on fault trees and event trees populated with failure rate and probability data. However, it is unique because of the dynamic nature of the mission and environment it models.

The assessment included representatives from a variety of organizations including almost 200 engineers, astronauts, instructors, analysts, and managers contributed to the SPRA. The SPRA methodology was peer reviewed by an independent panel of PRA experts outside NASA. Additionally, the SPRA model logic and failure data were reviewed by each of the project offices within the SSP and the NASA Engineering and Safety Council reviewed specific topics.

The SPRA is only one part of the risk-informed decision-making process. Operational constraints, qualitative risk assessments, budgetary considerations, etc., are also integral parts of the program decision-making process.

> *The SPRA is intended to be used as a risk management tool. The SPRA provides insights into the significant risks of Space Shuttle flight. The SPRA model results produced the following insights: The calculated overall mean estimate for Loss of Crew and Vehicle (LOCV) highly agrees with flight history. As described earlier, the historical LOCV probability is 1 in 65, which corresponds well with the SPRA risk estimate of 1 in 85. The decrease over the previously reported probability, 1 in 67, is mainly due to return-to-flight improvements, which were not reflected in the previous model. An estimated 82% of Shuttle LOCV calculated risk is realized during ascent and entry. This estimation represents a small fraction of overall mission duration and may be the result of the current ground rule to not include mission-specific on-orbit activities. Most of the ascent and entry risk is related to the inherent design and operating environment of the Shuttle, and therefore would be difficult to improve without significant design changes. However, the results emphasize the contribution of ascent debris and Micro Meteorite and Orbital Debris (MMOD) to the overall mission risk.* [15]

The Department of Energy (DOE) used an assessment similar to nuclear plants level III PRA (offsite release of radioactivity and its consequences) to evaluate the risk of potential nuclear payload accidents during launch or reentry. DOE has primary responsibility for developing Safety Analysis Report (SAR) for the radioactive plutonium loaded into the General Purpose Heat Sink (GPHS) that fuelled the Radioisotope Thermoelectric Generator (RTG) used in several NASA missions. DOE assigned responsibility for SAR to Sandia National Laboratories. SAR documents risk assessment of plutonium-based fuel contained in multi-mission radioisotope thermoelectric generator (MMRTG) that powers the Curiosity rover. SAR is essential document for launch approval by the Office of the President of the United States.

7.3. How should PRA be managed in OIL AND GAS industry?

As discussed above, PRA management should be viewed from the regulators and the industry point of view. The regulatory agency mission is to protect the public health, safety and environment by providing necessary regulations and oversight to the industry. This mission is accomplished by promoting the security of life, property, and the natural environment primarily through the development of cost effective regulatory guidelines for the design, construction, and operational maintenance of oil and gas facilities. The oil and gas regulatory agency mission statement should be similar to what the NRC mission statement is for the nuclear industry:

> *The Nuclear Regulatory Commission regulates the civilian uses of nuclear materials in the United States to protect public health and safety, the environment, and the common defense and security. The mission is accomplished through licensing of nuclear facilities and the possession, use and disposal of nuclear materials; the development and implementation of requirements governing licensed activities; and inspection and enforcement activities to assure compliance with these requirements. It is not connected in any way with defense matters or nuclear weapons.* [16]

The oil and gas regulatory agency will further interact with other regulators such as EPA, Department of Transportation (DOT) US Coast Guard (USCG), etc. to ensure coordination in application of regulatory guidelines. The regulatory agency further works with industry and its representatives to assure implementation of PRA methodology and verification of incorporation of the findings into the drilling and production design, operation and maintenance. This agency will set specific quantitative targets for catastrophic events such as loss of the rig due to fire, explosion or release of hydrocarbon to the environment, etc.

From a management prospective, PRA provides a proactive approach in improving the systems design, operations and maintenance. The industry integrators such as the American Petroleum Institute (API) may want to use the results of the PRA to provide guidelines on standardization of certain critical practices that may help improve efficiency and reduce cost without jeopardizing operational or personnel safety. The insurance industry involved will be able to utilize the PRA results in their risk assessment profile and develop a more risk informed rate structure for their clients.

8. CONCLUSION

Probabilistic Risk Assessment (PRA) has been used by different industries to estimate potential risk to the plants, vehicles and facilities. The PRA analysis is used by the commercial nuclear and aerospace industries to improve systems design, operation and maintenance, and reduce the probability of severe accidents and the potential consequences associated with those accidents.

The offshore oil and gas exploration and production industry can benefit tremendously from PRA application. Regulatory agencies should establish quantitative requirements for the consequences such as “fire/explosion on board the rig due to uncontrolled blow out” or “Release of hydrocarbon to the environment. The agencies can use similar strategies to that of the INPO to provide databases to the industry as reference to reduce uncertainties in quantitative analysis and facilitate identification of hard to find spares.

Currently the oil and gas industry uses FMECA as a standard risk management tool. While FMECA analysis may identify some single point contributors to system failure, it is unable to establish scenarios where multiple independent failures could result into an undesired event. A major advantage to performing PRA is to make the facility owner aware of potential scenarios involving multiple failures leading to a catastrophic event. In that case, the owner and operator can utilize measures such as defense-in-depth to help minimize the probability of such undesirable events.

References

1) NUREG 1334, “Individual Plant Examination”, August 1989
2) NUREG/BR-0058, “Regulatory Analysis Guidelines of the US Nuclear Regulatory Commission”, September 2004
3) NUREG/CR 2300, “PRA Procedures Guide”, January 1983
4) NUREG 75/014 (WASH-1400), “Reactor Safety Study”, October 1975
5) Nuclear News, “US Capacity Factors”, Pages 30-34, May 2013 issue
6) House Report 99-1016, “Investigation of the Challenger Accident”, 99th Congress, 2d Session, October 29, 1986
7) Yohon Lo, “Space Shuttle main Engine PRA”, July 11, 2011
8) Michael Stamatelatos et.al., “Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners”, December 2011
9) Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, 1/2/2001
10) American Petroleum Institute (API) “Subsea Production System Reliability and Technical Risk Management, First Edition”, 3/1/2009
11) Institute of Nuclear Power Operations “Mission Statement”, INPO Website, http://www.inpo.info/AboutUs.htm
12) NRC Memorandum, “Summary of Equipment Performance and Information Exchange (EPIX) Ad Hoc Working Group Meeting” August 4, 2005
13) American Petroleum Institute “Mission Statement”, API Website, http://www.api.org/globalitems/globalheaderpages/about-api/api-overview
14) BP Internal Incident Investigation team Report, “Deepwater Horizon Accident Investigation Report”, September 8, 2010
15) Teri L. Hamlin, et. al, “2009 Space Shuttle Probabilistic Risk Assessment Overview”, 2009
16) Nuclear Regulatory Commission “Mission Statement”, NRC Website, http://www.nrc.gov/about-nrc.html