DYNAMIC POSITIONING CONFERENCE
October 10-11, 2017

RISK / TESTING SESSION

(Dynamic Positioning System (DPS) Risk Analysis Using Probabilistic Risk Assessment (PRA))

By (Eric B. Thigpen (SAIC), Michael A. Stewart (NASA), Roger L. Boyer (NASA), Pete Fougere (Consultant))

Abstract

The National Aeronautics and Space Administration (NASA) Safety & Mission Assurance (S&MA) directorate at the Johnson Space Center (JSC) has applied its knowledge and experience with Probabilistic Risk Assessment (PRA) to projects in industries ranging from spacecraft to nuclear power plants. PRA is a comprehensive and structured process for analyzing risk in complex engineered systems and/or processes. The PRA process enables the user to identify potential risk contributors such as, hardware and software failure, human error, and external events. Recent developments in the oil and gas industry have presented opportunities for NASA to lend their PRA expertise to both ongoing and developmental projects within the industry. This paper provides an overview of the PRA process and demonstrates how this process was applied in estimating the probability that a Mobile Offshore Drilling Unit (MODU) operating in the Gulf of Mexico and equipped with a generically configured Dynamic Positioning System (DPS) loses location and needs to initiate an emergency disconnect. The PRA described in this paper is intended to be generic such that the vessel meets the general requirements of an International Maritime Organization (IMO) Maritime Safety Committee (MSC)/Circ. 645 Class 3 dynamically positioned vessel. The results of this analysis are not intended to be applied to any specific drilling vessel, although provisions were made to allow the analysis to be configured to a specific vessel if required.

Abbreviation / Definition

Dynamically Positioned (DP) Vessel/Mobile Offshore Drilling Unit (MODU) - A vessel which automatically maintains it position and heading by means of thruster force.

Dynamic Positioning System (DPS) - The complete installation necessary for dynamically positioning a vessel. The DPS is comprised of three primary sub-systems; the power subsystem, the thruster subsystem, and the control subsystem.

DP Control System - All control components and systems, hardware and software necessary to dynamically position a vessel. In this analysis, the control system is comprised of sensors of various types, position reference systems, network processors, and Human Machine Interface (HMI).

Emergency Disconnect – The Blowout Preventer (BOP) and the Lower Marine Riser Package (LMRP) is designed to be able to separate. The BOP control system has a single button automated control sequence that will shear the drilling pipe, close the BOP, and release the LMRP.

Probabilistic Risk Assessment Model End States – These are the logical outcomes of a loss position by the vessel due to failure of the DPS. All of these end states are assumed to result in the initiation of an emergency disconnect. Each end state is defined in a manner consistent with industry understanding regarding the cause of loss of position.

> Drift-Off - This end state occurs when a DPS failure causes the vessel to lose station and begin drifting within the nominal operation region (green operation area). If no recovery is possible the vessel may drift to a point off station where the initiation of an emergency disconnect must be declared.
>
> Drive-off - This end state results when the DPS, due to system degradation, fails to maintain position and there is an unplanned movement of the vessel. Failure of DP personnel to recognize the degraded state of the DPS and take recovery action will require the proactive initiation of the initiation of an emergency disconnect. Drive-off may also be initiated as a result of erroneous actions on the part of the Dynamic Positioning Operator when attempting to reposition the vessel within the green operation area.
>
> Push-off - This end state describes a condition where extreme weather prevents the vessel, operating with a fully functioning DPS, from maintaining position in the nominal operation range resulting in a forced emergency disconnect.

Well Operations – This term is meant to capture all activities that could occur at the well site including drilling, completion, and interventions.

Worst Case Failure (WCF) – Failure of the DPS that has the greatest effect on station keeping capability. For this analysis, WCF refers to the loss of a single DPS redundancy group (e.g. a pair of thrusters, a pair of diesel generators).

Introduction

The NASA S&MA directorate at the JSC has applied its knowledge and experience with PRA to projects in industries ranging from spacecraft to nuclear power plants. Recently, NASA was contracted by an outside interest in the oil and gas industry to apply the PRA methodology to calculate the probability that

a MODU operating in the Gulf of Mexico and equipped with a generically configured DPS loses location and needs to initiate an emergency disconnect.

Probabilistic Risk Assessment Overview

PRA is a comprehensive, structured, and disciplined approach to identifying and analyzing risk in engineered systems and/or processes [1]. It attempts to quantify rare event probabilities of failures and takes into account all possible events or influences that could reasonably affect the system or process being studied. In general, PRA is a process that seeks answers to three basic questions:

1. What kinds of events or scenarios can occur (i.e., what can go wrong)?

2. What are the likelihoods and associated uncertainties of the events or scenarios?

3. What consequences could result from these events or scenarios (e.g., LOC)?

A methodical approach to the development of a PRA is crucial to ensure that the analysis and results accurately represent the system or process being analyzed. Figure 1 provides a visual representation of the process observed by NASA in the development of a typical PRA. For additional information about the practice and application of PRA the authors encourage the reader to consult the Probabilistic Risk Assessment Procedures Guide for Offshore Applications [2]. All PRA modeling for this analysis is performed using the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) PRA tool [3].

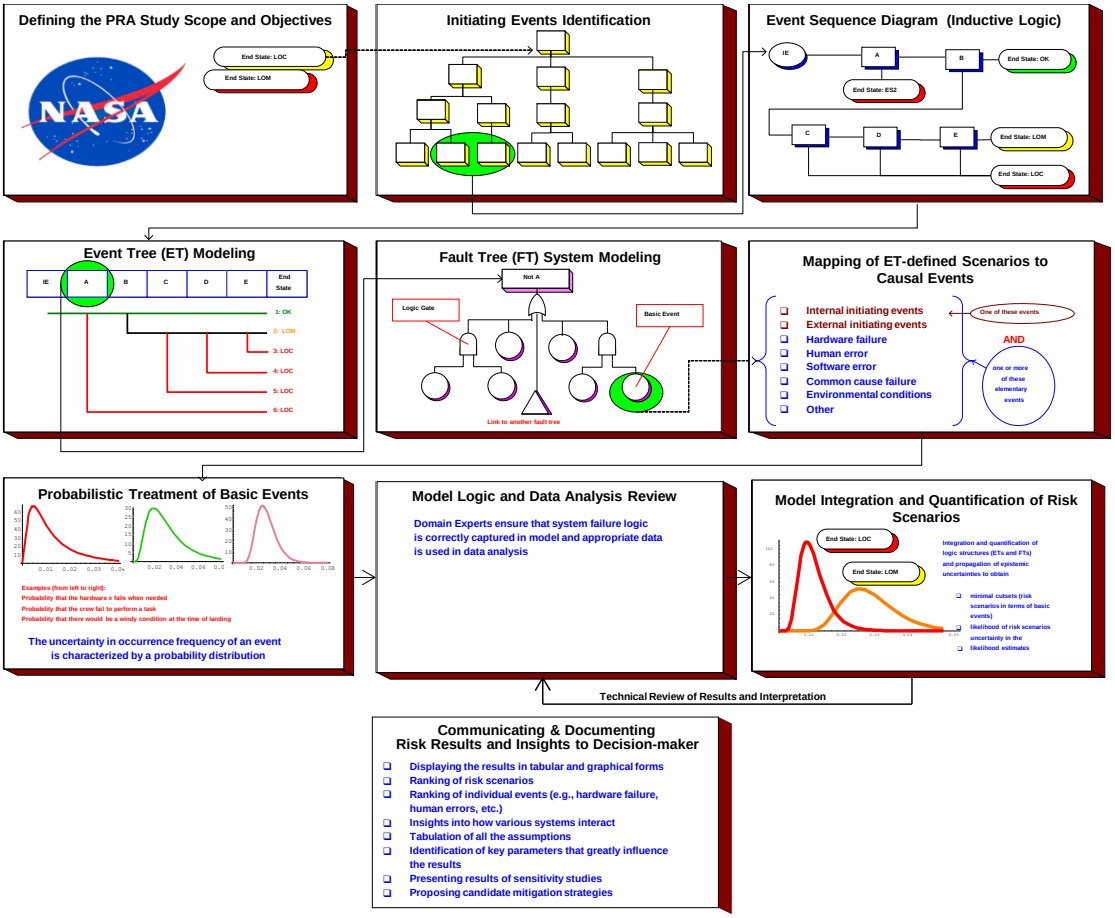

Figure 1: PRA Development Process

It is important to remember that each PRA is unique and that the steps shown in Figure 1 may be observed in more or less detail depending on the system or process being modeled. In some cases the process may be tailored in such a way that certain steps are combined or omitted; however, this should only be done when the PRA practitioner possesses a level of experience to ensure that the omission will not adversely impact the development of the analysis or the accuracy of the results.

For large PRAs involving more than one PRA analyst, consistency becomes a major attribute in developing a PRA. A PRA of a drill ship or oil rig involves many subsystems and substantial data needs. Having a close knit team working to the same guidelines and periodically communicating common methods and lessons learned helps to make the PRA consistent and the results relative for risk ranking the major contributors.

Communicating the results of the PRA to the domain or subject matter experts (SME) as well as to the decision makers provides feedback as to what the SME needs to know about their system/component and what the decision makers need to know to make risk-informed decisions. The risk results can be shown at several levels, such as overall Drill Ship, DPS level, and component level, and from different views, such as a Pareto chart ranking the various risk contributors and the top risk scenarios from the PRA.

Documentation is also a major part of a PRA. While developing the PRA, information is fresh in the minds of the analysts. However, as time progresses and analysts move on to other projects, what was

well known (e.g. assumptions, data sources, system references, etc.) becomes vague or lost. As with most PRAs and engineering analyses, changes or updates may be required, thus an understanding of the original basis is needed before changes can be made. It is important to document ground rules and assumptions made in the original assessment in a report to help those who are picking up where others left off.

Dynamic Positioning System Overview

During well operations in the GoM, the MODU must maintain location within a designated radius nominally centered on the wellhead to which the vessel is currently attached. If the vessel moves beyond this radius to the extent that impending damage to equipment or uncontrolled leakage of hydrocarbons presents a significant risk, the vessel will be forced to initiate an emergency disconnect of the LMRP from the BOP attached to the wellhead. A reliable DPS is required to ensure that the vessel location is maintained within the designated operating radius and well operations are conducted successfully. In this report, failure of the DPS is defined as a loss or degradation of the DPS such that the drilling vessel cannot maintain location and an emergency disconnect must be initiated.

The MODU modeled in this PRA is intended to be generic such that the vessel meets the general requirements of an IMO MSC/Circ. 645 [3] Class 3 dynamically positioned vessel. This analysis is not intended to be applied to any specific drilling vessel. The DPS for the Class 3 MODU was assumed to have six thrusters, three forward and three aft (see Figure 2).

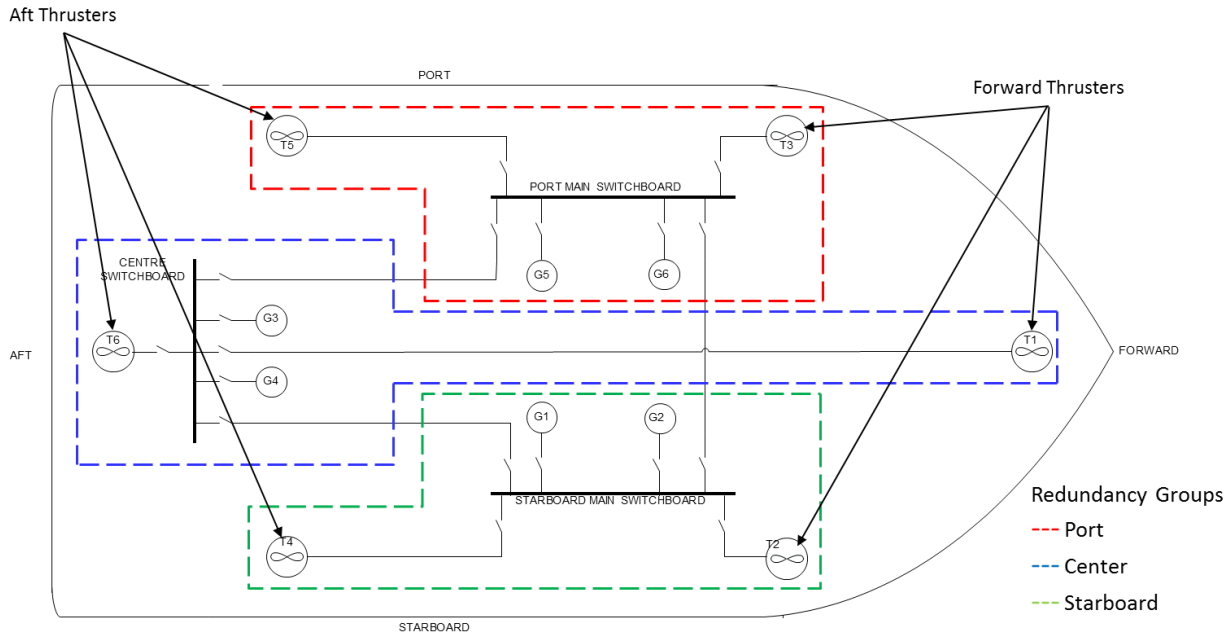

Figure 2: Thruster Layout

The MODU is also assumed to be equipped with six diesel generators arranged in three redundancy groups which are isolated from one another in separate compartments on the MODU. The three redundancy groups, two generators and thrusters per group, provide a level of robustness against single point failures. The arrangement of the diesel generator redundancy groups and the thrusters powered by them respectively are shown in Figure 3. All modeled operations are open bus, so bus ties are not shown.

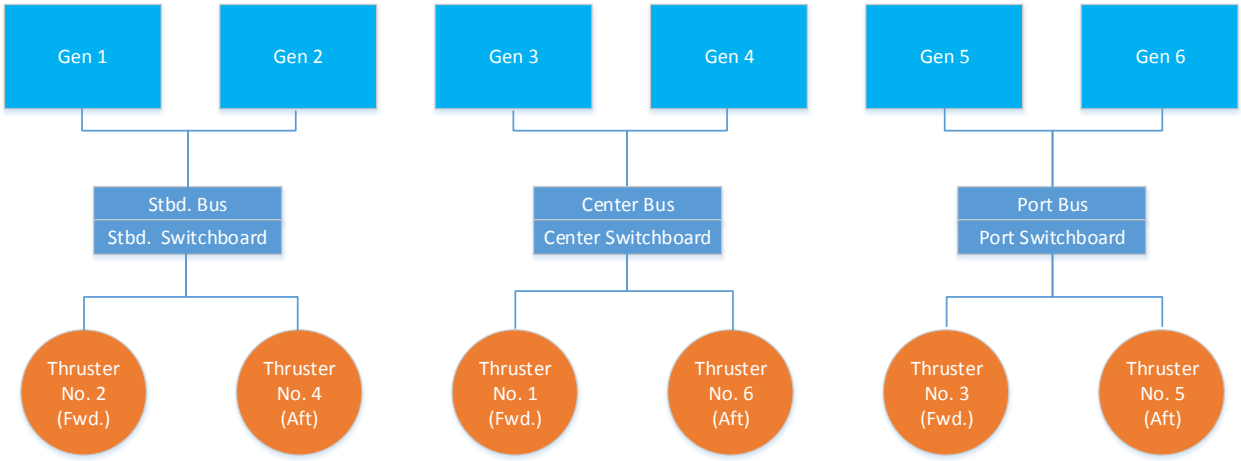

Figure 3: Power Generation/Thruster Architecture

Support systems for the diesel generators and thrusters, such as the fuel system and cooling systems are also captured in this PRA although they are not shown here.

The DP control system, as modeled for this analysis, is comprised of a variety of sensors that monitor various aspects of the environment in which the MODU is operating. These inputs are read and processed by the DPS computers and outputs are sent to the power generation system and thrusters that allow the vessel to maintain location within the specified operating radius. The control system incorporates a high level of redundancy and there is also functional overlap to increase the robustness of the design. A block representation of the control system modeled in this PRA is shown if Figure 4.

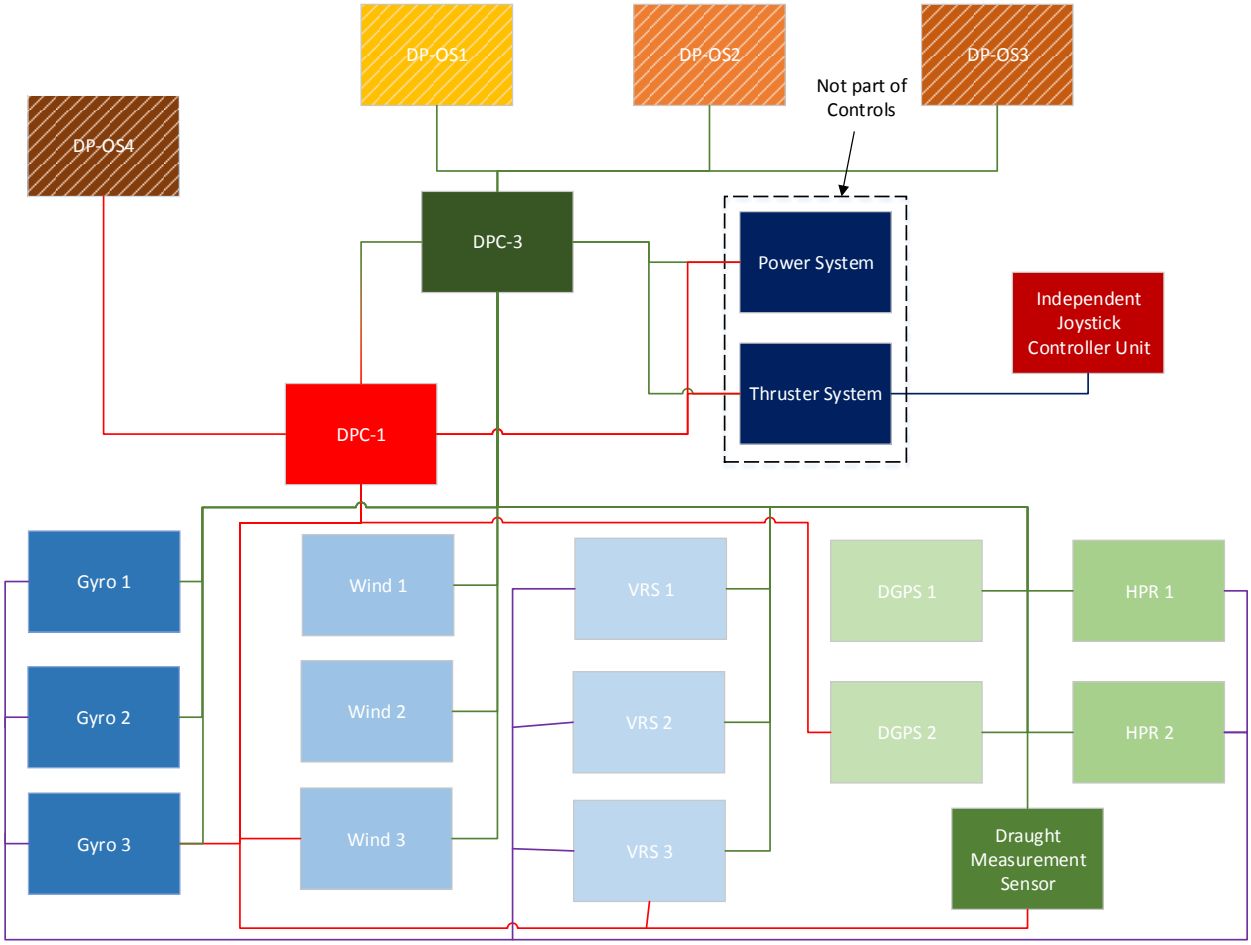

Figure 4: DPS Control System

Scope and Objectives

The first step in proceeding with the DPS PRA was to define the scope and objectives. With regard to the analysis scope, the DPS PRA is intended to address only failures of the DPS that can result in a loss of location. The DPS is assumed to consist only of the systems and components discussed previously. Failures associated with other shipboard equipment or drilling hardware are beyond the scope of this analysis, although human error as it pertains to operation of the DPS is included. The fundamental objective of this analysis is to determine the risk of the DP vessel losing location during well operations. Of equal importance in this analysis is to determine which elements of the DPS are the principal contributors to this overall risk and their relative risk ranking.

Initiating Events and Success Criteria

In general, for a PRA the initiating condition precedes the scenario being analyzed. The initiating condition for these models is a fully functioning DPS. In other words, there is no initiating failure at the

outset of the failure sequence that ultimately results in a loss of location by the vessel. DPS failure, human error, and weather are treated by the analysis as causes that could compromise a fully functioning DPS.

The analysis does take into consideration the possibility that certain weather conditions will affect the level of DPS failure that the vessel can withstand and still maintain position. It is important to note that while weather systems are fairly predictable, ongoing well operations may make relocating the vessel out of the path of extreme weather impossible. In cases where the vessel must endure extreme weather, the failure criteria for the DPS are more restrictive. In other words, the DPS can withstand less failure and still be capable of maintaining location. This means that different success criteria were identified for different weather conditions.

In a normal environment with calm seas, low winds, and mild currents, the vessel requires less power or thruster control and; therefore, can withstand more thrusters or generators being inoperable whether due to failure or maintenance. Marine classification societies specify the design requirements for the various vessel classifications. Part of these classifications are the robustness of the DPS design and what level of failure the DPS must be able to withstand and still remain functional. The level of failure the DPS must be able to withstand and remain operational is defined as Worst Case Failure (WCF). For Class 3 vessels such as the one modeled in this analysis, WCF is defined as the loss of a single redundancy group or one pair of generators or thrusters as shown in Figure 2. Since the DPS must be able to maintain location with the loss of a redundancy group, it was assumed that any system failure occurring after the loss of a redundancy group would be considered failure. Therefore, the analysis assumed that the vessel could not operate with fewer than four generators or thrusters, or with the loss of their respective support systems. In higher weather conditions, such as sudden hurricanes, the MODU requires more power and thruster capability to keep station; therefore, loss of a single thruster or generator was assumed to result in a loss of location.

Event Trees

An event tree is an inductive analytical diagramming technique that employs Boolean logic to capture failure events that could result in predetermined outcomes or end states. The end states for this analysis were established by identifying the general failure modes by which the MODU could lose location. It was determined that the vessel could lose location through three separate failure modes: drift-off, drive-off, and push-off.

1. Drift-off occurs when one or more failures inhibit the DPS from maintaining vessel location and it drifts beyond the designated radius of operation.

2. Drive-off occurs when the DPS experiences operational degradation to an extent where human intervention is required. During this intervention, human error causes the thrusters to begin moving the MODU off location. As the vessel gains momentum, the risk of potential damage to subsea equipment before re-establishing position becomes unacceptably high resulting in the initiation of an emergency disconnect.

3. Push-off occurs when the weather environment exceeds the position keeping capabilities of a fully operational DPS resulting in the vessel losing location and an emergency disconnect must be initiated.

Two event trees capturing both the nominal operating environment and the extreme weather environment were constructed. The end states for each of the events sequences were assigned based on the failures

captured by each of the top events using the previous definitions of drift-off, drive-off, and push-off. The event tree constructed for the nominal operating environment is shown below in Figure 5.

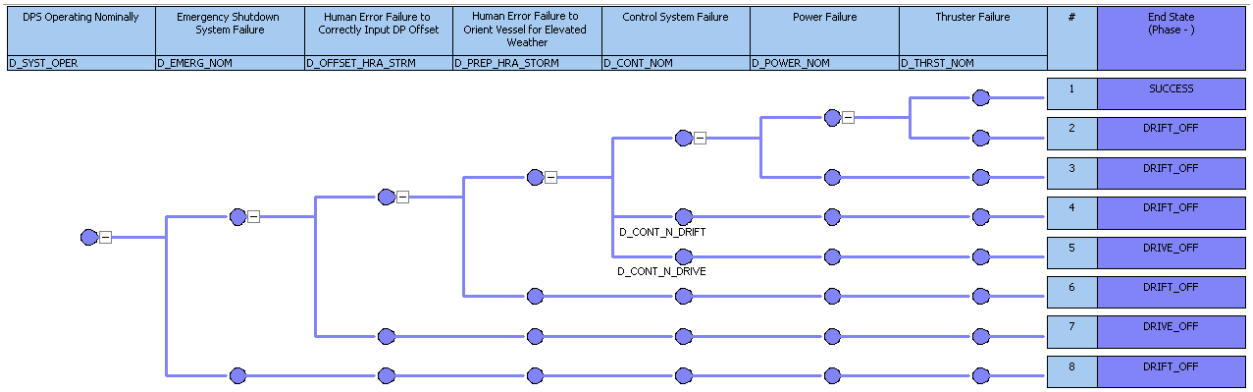

Figure 5: Nominal Operating Environment Event Tree

Fault Trees

A fault tree is a top down, deductive failure mapping approach in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. Fault trees were constructed for each top event in the event trees outlined previously. For the most part the fault tree captured hardware failures such as loss of power generation capability, or control system failures; however, human error was also incorporated using fault tree logic. A sample fault tree showing the failure logic for Generator 1 in the nominal operating environment is shown below in Figure 6.

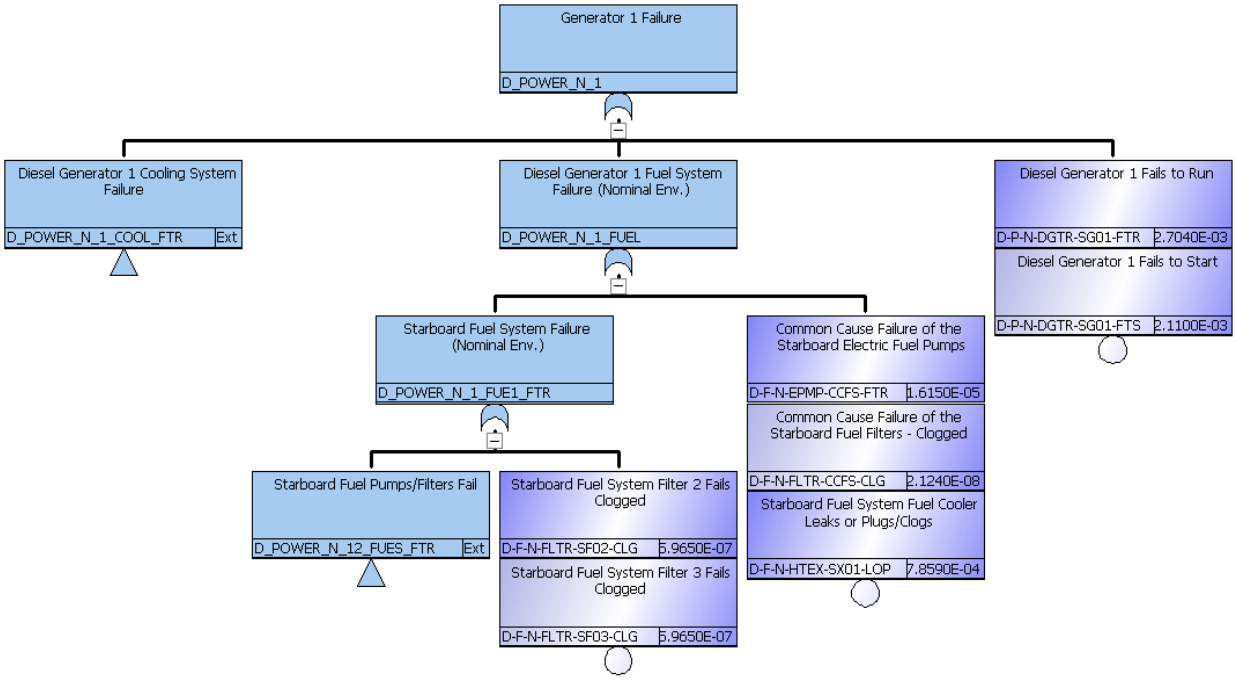

Figure 6: Generator 1 Failure in a Nominal Operating Environment

Data Development

In order to assess the failure probability of the DPS, the failure probability of its components had to be evaluated. This was done by first identifying the component failure modes and then quantitatively estimating the likelihood that the component would fail during the period of interest. Estimating the likelihood of component failure was done by gathering recorded failure data for each of the components from accepted data sources.

Oil and gas industry specific generic data was used when available, and non-industry specific generic data was used otherwise. Most published data was somewhat dated and may not have represented the most recent conditions or uses for the equipment. The data used in this study is believed to be adequate for a generic model, but design specific data should be used in the future to make the analysis applicable to a specific design. Some industry related data was made available for this analysis. However, specific information regarding the data sources and collection methods for this data were not made available so the data was used "as is". The exposure period for the time the MODU would spend on site at a particular well was assumed based historical estimates of DP operation times in the GoM. This estimate was used for all failures occurring in the nominal operating environment. Extreme weather durations were assumed to be significantly less.

Weather data was required to determine frequency with which extreme weather might be present in the GoM. For this analysis extreme weather frequency was determined from weather data for a specific location. Future analyses in other locations would need more region specific weather data in order to generate more accurate results. Additionally, the weather frequency estimates along with vessel DP capability plots provided by the system expert were used to establish the extreme weather environment based on wind speed.

Human Reliability Analysis (HRA) was included in the models to capture the impact that human error could have on the overall risk. HRA describes any action or inaction taken by people that increases the likelihood of an event. It should be noted that human actions can be added to recover or improve the system performance but then the probability of failure to perform these recovery/improvements must be estimated. The term "human error" carries with it negative implications often implying that blame may be attributed to an individual. Generally, HRA does not view human error as the product of individual weaknesses but rather as the result of circumstantial and situational factors that affect human performance. These factors are commonly referred to as performance shaping factors, such as training, time available to perform the function, and experience. These factors serve to enhance or degrade human performance relative to a reference point or baseline. This PRA employed an adapted version of the Cognitive Reliability and Error Analysis Method (CREAM) [5] to estimate HRA event probabilities.

Conclusion

Aggregating the results of the DPS PRA model indicates that the MODU losing location and initiating an emergency disconnect during DP operations would be less than 5% of the time. This assumes no shutdown or refurbishment between wells; however, routine maintenance was taken into consideration in the models.

Looking into the risk of initiating an emergency disconnect as a function of the operating environment reveals that the nominal operating environment is the largest contributor to the overall risk at over 90%, because the vessel spends most of its operation time in the nominal environment. In the nominal operation mode, human error to adequately prepare and maintain vessel orientation prior to the onset of extreme weather comprises over 80% of the risk making it the largest contributor to the overall risk. The

shorter exposure time and the lower frequency of occurrence of extreme weather makes its 5% contribution to the overall risk insignificant which supports the idea that extreme weather in the GoM is not a significant contributor to the DP vessel losing position.

If the risk is broken down by end state, the drift-off end state is the largest contributor to the overall risk at over 90%. Once again, the large contribution from human error makes this end state the largest contributor to the overall risk. The risk of DPS failure due to drive-off is also largely driven by the human error contribution; however, two types of human error contribute to this end state. The first is a failure to correctly reposition the vessel within the green operation area by incorrectly entering an offset into the DPS. The second human error is an incorrect response to a degraded DPS control system.

It is clear that human error is the dominant risk contributor. For this reason, it may be prudent to focus risk reduction efforts on improving human factors, vessel specific training, ergonomics, or decision support tools or technology rather than improve hardware reliability.

The importance of the generators and thrusters to the DPS cannot be overstated; however, from a risk perspective they are relatively low contributors at less than 10% of the overall risk. The reason for this low occurrence rate is due primarily to the ability of the vessel to operate in a degraded state during nominal operations, the respective levels of redundancy within the generator and thruster subsystems, the independence of the redundancy groups, and the fact that repairs are possible during nominal operations.

When changes are made to the design and/or operation of the DPS, or any other risk sensitive system, it is important to determine the effect they have on the overall risk as other contributors will rise in the risk ranking and become the next thing to address.

References

1. ESD 10011 Rev. A, National Aeronautics and Space Administration, Cross Program Probabilistic Risk Assessment Methodology. 2014.
2. BSEE-2016-xxx, Probabilistic Risk Assessment Procedures Guide for Offshore Applications (DRAFT),https://www.bsee.gov/sites/bsee.gov/files/bsee_pra_procedures_guide_draft_10-25_for_web.pdf, October, 25, 2016,
3. Smith, C. L., and S. T. Wood. Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE): Version 8. Washington, D.C.: U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 2011.
4. IMO MSC/Circ. 645, Guidelines for Vessels with Dynamic Positioning Systems, International Maritime Organization, June 6, 1994
5. Hollnagel, Erik. Cognitive reliability and error analysis method (CREAM). Elsevier, 1998.