Probabilistic Risk Analysis (PRA) of a Mobile Offshore Drilling Unit (MODU) Dynamic Positioning System (DPS)

Eric B. Thigpen*[a], Roger L. Boyer[b], Michael A. Stewart[b]
[a]SAIC, Houston, Texas
[b]NASA Johnson Space Center, Houston, Texas

Abstract: Probabilistic Risk Assessment (PRA) has been utilized by NASA in a variety of space oriented projects. It has served as one of the primary risk identification and ranking tools. 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. As a result, NASA has entered into an agreement with Anadarko Petroleum Company (APC) to collaboratively develop PRAs for different aspects of the subsea drilling and completion process of well development. This paper documents how PRA was applied to estimate the probability that a Mobile Offshore Drilling Unit (MODU) equipped with a generically configured Dynamic Positioning System (DPS) loses location and needs to initiate an emergency disconnect. Since this project was in essence a pilot project, 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.

Keywords: DPS, PRA, DPO, Emergency Disconnect

1. INTRODUCTION

The National Aeronautics & Space Administration (NASA) Safety & Mission Assurance (S&MA) directorate at the Johnson Space Center (JSC) has applied its knowledge and experience of Probabilistic Risk Assessment (PRA) to space oriented projects in the past. However, the personnel in the NASA S&MA directorate come from a variety of backgrounds and have applied their knowledge of PRA to projects in industries ranging from nuclear power to the chemical processing industry. 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 Mobile Offshore Drilling Unit (MODU) operating in the Gulf of Mexico (GoM) and equipped with a generically configured Dynamic Positioning System (DPS) loses station and needs to initiate an emergency disconnect from the well on which subsea operations are being conducted. The analysis assumed that well operations would be carried out using a generic sixth generation Class 3 MODU. All PRA modeling for this analysis is performed in accordance with standard NASA practices [1] using the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) PRA tool [2].

The DPS is an active system that maintains vessel location and heading during well operations, such as drilling and completion. The DPS uses data about the ship's position and operating environment to ensure that it maintains a designated position and heading inside a designated region, typically referred to as the green operation area. In addition to the green operation area, watch circles (yellow and red) are designated by the Dynamic Positioning Officer (DPO) based on specific weather or well operations that may be planned. The watch circles have increasing radii (red being the outermost) with the origin at the surface position above the well head. The radii are calculated based on the water depth, vessel operation, environment, subsea equipment characteristics and the time required to disconnect. If the vessel moves beyond the red watch circle, there is an increased likelihood of damage to equipment (e.g. the riser, Blowout

* eric.b.thigpen@nasa.gov

Preventer (BOP), etc.) and, potentially Loss of Containment (LOC). In order to prevent potentially catastrophic mishaps including LOC, the vessel's position within the operations envelope is monitored. If the vessel position cannot be maintained, an emergency disconnect is initiated.

2. VESSEL CLASSIFICATION

The DP Class definitions were developed by the International Maritime Organization (IMO) in its Maritime Safety Committee (MSC)/Circ. 645 [3]. A vessel normally obtains a DP class notation which is issued by Marine Classification Societies as an additional notation to main vessel class. Example class notations are DYNPOS-AUTRO and DPS3 per Det Norske Veritas Germanischer Lloyd (DNV GL), and DPS-3 per the American Bureau of Shipping (ABS). The DP classifications indicate Worst Case Failure (WCF) design goals. A listing of the various class notations and their requirements as well as a corresponding list of classification societies in Table 1.

Table 1: Vessel Classifications by Classification Society

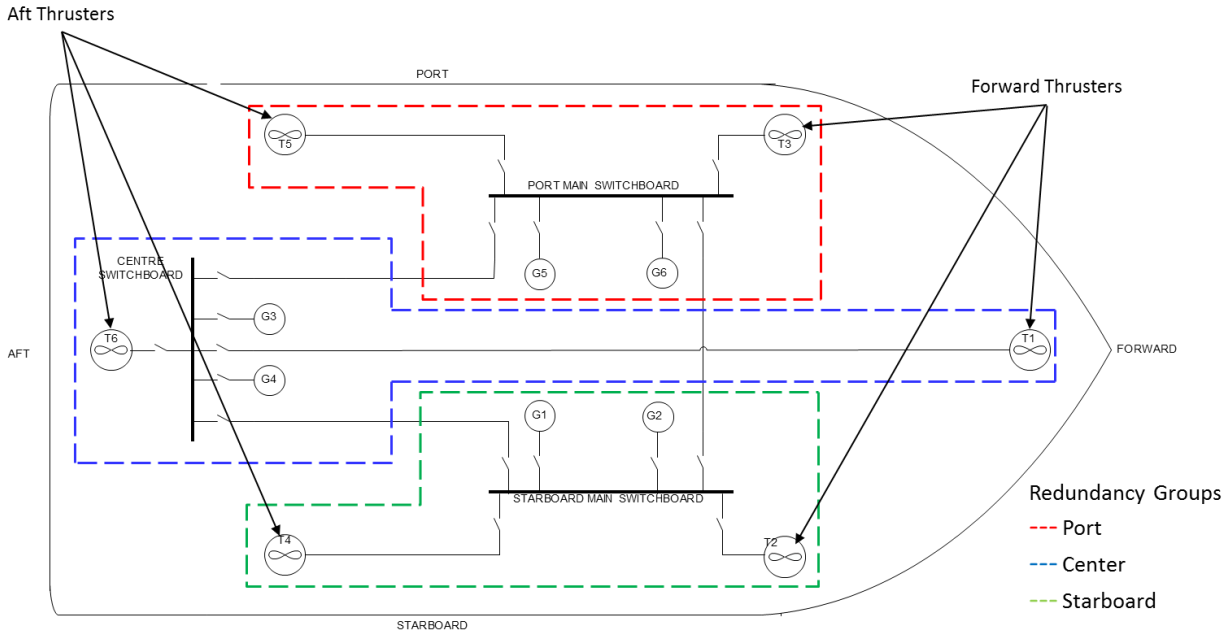
Description	IMO Equip. Class	LR Equip. Class	DNV GL Equip. Class	ABS Equip. Class	NK Equip. Class	BV Equip. Class
Manual position control and automatic heading control under specified maximum environmental conditions	-	DP(CM)	-	DPS-0	-	
Automatic and manual position and heading control under specified maximum environmental conditions	Class 1	DP(AM)	DP 1	DPS-1	DPS A	DYNAPOS AM/AT
Automatic and manual position and heading control under specified maximum environmental conditions, during and following any single fault excluding loss of a compartment. (Two independent computer systems).	Class 2	DP(AA)	DP 2	DPS-2	DPS B	DYNAPOS AM/AT R
Automatic and manual position and heading control under specified maximum environmental conditions, during and following any single fault including loss of a compartment due to fire or flood. (At least two independent computer systems with a separate backup system separated by A60 class division).	Class 3	DP(AAA)	DP 3	DPS-3	DPS C	DYNAPOS AM/AT RS

3. DPS SYSTEM

Since the DPS approximated in this analysis was considered generic, actual schematics and drawings for specific systems and components were not used. Instead a general system architecture was established by consulting with a subject matter expert. As a result, general insights from this study may be broadly applicable to Class 3 vessels; however, caution should be taken when evaluating the risks associated with specific DPS architectures.

Fundamentally, the DPS is comprised of three basic subsystems: the power generation system, the thrusters, and the control system. For this analysis, the emergency shutdown system was also incorporated into the models because loss of location due to a power blackout caused by a spurious trip of this system has been seen in the field. From the perspective of vessel propulsion, it was agreed that the vessel would utilize six thrusters: three forward and three aft. The thrusters would be arranged in three redundancy groups: port, center, and starboard. Figure 1 provides an illustration of the thruster arrangement and the layout of the redundancy groups.

Figure 1: Thruster Layout



4. POWER GENERATION SYSTEM

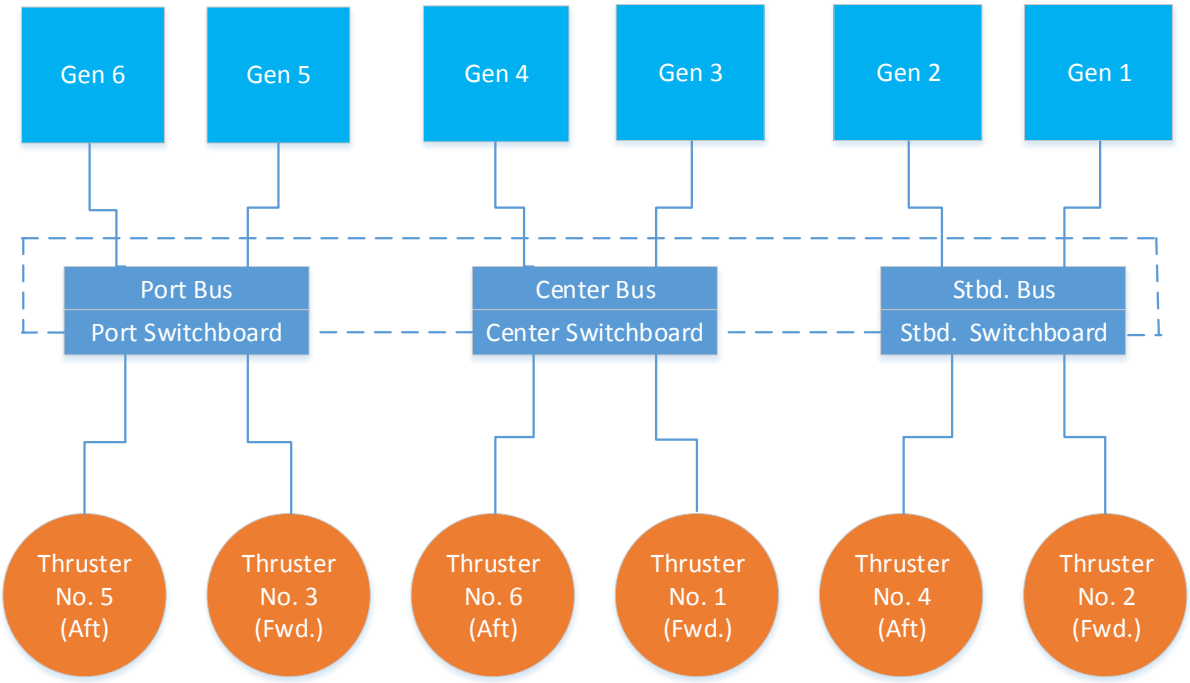
The thrusters are powered by six diesel generators: two per redundancy group. Both generators in a redundancy group are connected through a switchboard that will allow them to be isolated, either individually or as a group, in the event of a failure. Figure 2 shows the arrangement of the generators and thrusters.

Each of the diesel generator redundancy groups is supplied by an independent fuel system. Each fuel system is equipped with redundant fuel pumps, a back-up or emergency pump, several fuel filters, and a heat exchanger for fuel cooling. The emergency pump is not used during normal station keeping operations; therefore, it is not captured in the models.

Each diesel generator redundancy group is also equipped with a cooling system. The cooling system is comprised of both a fresh water and sea water cooling system. The fresh water cooling system provides

cooling to the power generation components. The sea water cooling system provides cooling to the fresh water system. The fresh water system provides direct cooling via heat exchangers to the generators, the diesel engines that power them, and the thrusters. Each fresh water cooling system has redundant pumps, various heat exchangers to provide cooling to specific system components, and temperature regulating valves.

Figure 2: Power Generation System



5. CONTROL SYSTEM

The DP control system controls the diesel generators and thrusters to maintain position and heading. It also includes operator stations that provide information to the DPO about system condition, vessel performance, the operating environment, and provides for entry of operator commands. The Class 3 vessel is equipped with redundant differential global positioning systems (DGPS) and Hydroacoustic Position Reference (HPR) systems that establish the position of the vessel. These systems satisfy class requirements for three position references. The DP control system includes redundant Gyro Compasses (Gyros), Vertical Reference Sensors (VRSs), and wind sensors to provide information about the environment and the vessel to assist with maintaining position and heading.

The control system has a primary system and a back-up system that provides station keeping capability in the event of a primary failure. All of the information gathered from the sensing portion of the control system is fed into a triple redundant primary processor, or Dynamic Position Controller (DPC), hence the DPC-3 designation, and based on the DPO's vessel location requirements, the DPC will send direction and speed commands to the thrusters to ensure that the vessel maintains position and heading. In the event that the control system is operating on the back-up control system, a single processor (noted as DPC-1) is used to perform control. The power generation system will also respond as necessary to meet the requirements of the thrusters. The primary control system computers can be controlled from any one of three DP Operating Stations (DPOS). The back-up control system is operated from its own single DPOS. There is also an independent joystick control to allow the DPO to manually maintain position and heading. It is

important to note that the joystick is not frequently used and may be difficult to use so there exists the possibility for human error.

Figure 3 is a representation of primary control system that shows the major components included in the PRA models. It should be reiterated that this DPS, including the control system, is a generic configuration. Other systems might have different configurations or different levels of control.

Figure 3: Primary Control System

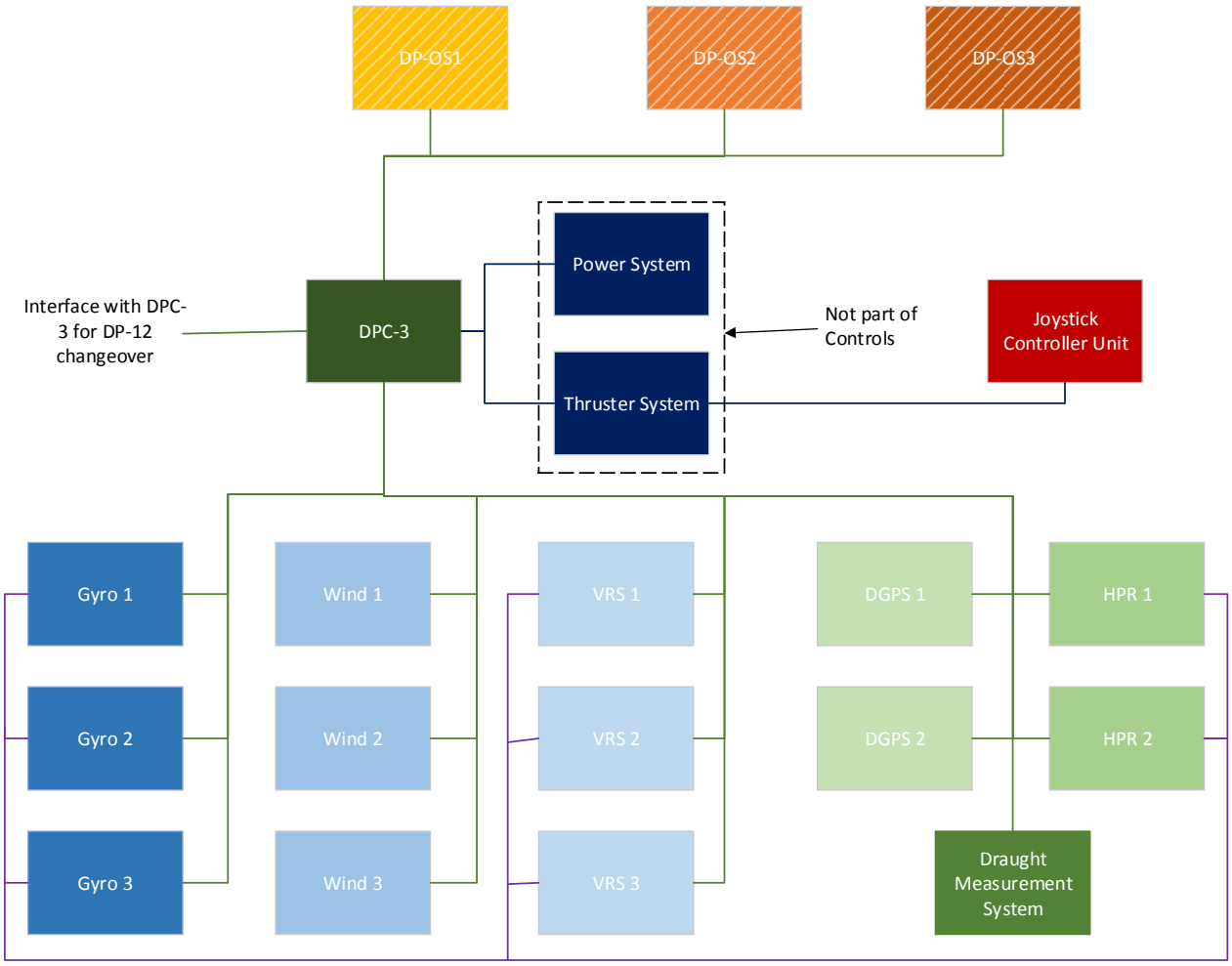
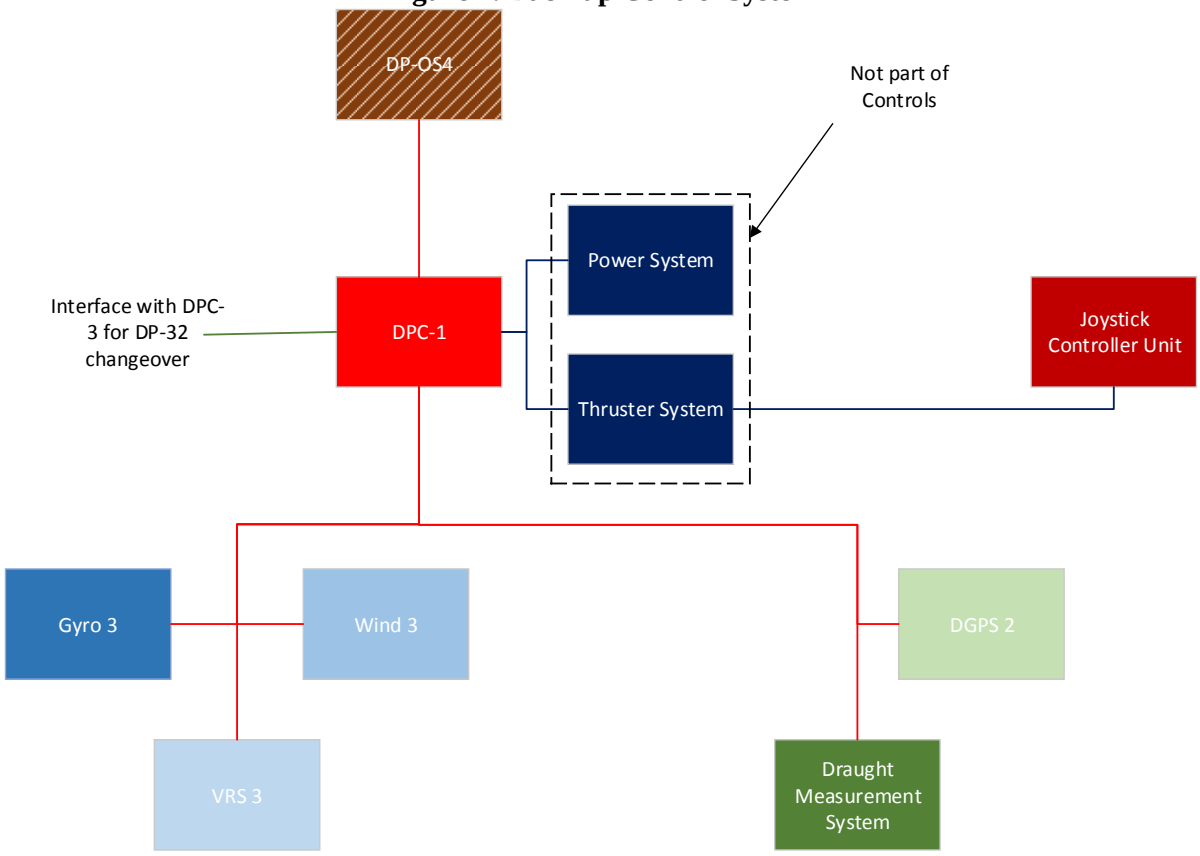


Figure 4 shows the back-up control system. The backup system is intended to replace the primary control system if there is a fire or flood incident that disables the primary control.

Figure 4: Back-up Control System



6. MODELING APPROACH

There are many factors that can contribute to a vessel losing the ability to maintain station. Based on discussions with subject matter experts, the environment, specifically the weather, in which the vessel is operating is fundamental to maintaining location in the event of a DPS failure. The weather in the GoM can vary from benign to extremely severe. To simplify the analysis, two environments were established to represent the full range of operational conditions that the vessel will experience in the GoM; normal operating environment and extreme weather. The normal operating environment exists any time the vessel is within the green operation area and well operations are occurring. In the GoM, remaining on location during extreme weather is rare because of the established procedures for planned disconnect and evacuation in response to forecasted weather events, such as hurricanes. The extreme weather environment is meant to capture the rare occasions when the vessel may be forced to remain on location during extreme weather. The extreme weather environment also captures the case where extreme weather forces the vessel off location event though the DPS may be fully functional. An event tree was created for each vessel operating state. Fault trees were added to address the top level events in each of the event trees. The fault trees incorporated logic to address both human error and hardware failures that could result in the initiation of an emergency disconnect. The fault tree logic for hardware failures took into account the success criteria for the DPS in each state.

7. MODEL SCOPE

The over-arching objective of this analysis was to develop a model that would calculate the risk of initiating an emergency disconnect. The system architecture modeled in this analysis has been established by the system level expert based on considerable experience with Class 3 MODUs currently in operation. It should

be understood that the design of specific DPS systems for DP Class 3 vessels vary, hence different systems could have different reliability experience. The generic model developed for this analysis includes common high level equipment but does not account for detailed design features specific to individual Class 3 vessels. The model accounts for loss of control, power, and support systems, as well as human error. In general, the DPS was modeled at the system level which included all major components of a particular system.

Other events that might result in loss of position such as a full vessel blackout, collision with another vessel, loss of vessel stability, crew incapacitation, drilling or other shipboard operations mishaps are considered out of scope for this analysis because failure is dictated by factors that are outside of the DPS as defined by the analysis. Additionally phenomenological events, (e.g. fire, impact with another vessel resulting in flooding of the hull) are considered to be out of scope because it is assumed that these type events would compromise the vessel to the extent that loss of position might be a secondary concern. This analysis only includes operations when the BOP is connected to the wellhead. Other operations, such as deploying or retrieving the BOP, top-hole drilling, and running and cementing surface casing are outside of scope of this analysis because, during these phases of well development, hydrocarbons should only be present in small quantities. Losing position under any of these circumstances is not likely to result in a major release of hydrocarbons into the GoM. Components that are not part of the DPS but whose proximal location might jeopardize function in the event of a violent failure are not captured in the models for the same reason that phenomenological events are not addressed. Also standard PRA modeling practice dictates that passive components (e.g. wiring, tubing, etc.) whose failure probabilities are expected to be very low are not modeled. Given that the model was approximating a generic system, it was constructed modularly so that it could be easily modified to meet the design architecture of a specific DPS at a future date, if required.

8. 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.

As mentioned previously, the analysis does take into consideration varying weather conditions. The weather conditions will affect the level of DPS failure that the vessel can withstand and still maintain position. 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. It was assumed that all power generation equipment and the thrusters must be fully operational. In other words, any single failure in either of these systems will result in a loss of position and is considered system failure. The control system had separate failure criteria that were established by the subject matter expert.

9. DATA DEVELOPMENT

Generic data was used for all modeled components. Oil and gas industry specific generic data was used when available, and non-industry specific generic data was used otherwise. Generic data sources were limited. Most published data was also 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 on historical estimates of DP operation times in the GoM. This estimate was used for all failures occurring in the normal operating environment. Given the predominantly mild weather conditions in the GoM for most parts of the year, 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 in the GoM. Region specific weather data would be needed to analyze rigs in other locations. 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. 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, which 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) [4] to estimate HRA event probabilities.

10. RESULTS AND CONCLUSIONS

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 or less than five times during every 100 wells drilled by this generically configured MODU. This estimate assumes no shutdown or refurbishment between wells; however, routine maintenance was taken into consideration.

Looking into the risk of initiating an emergency disconnect as a function of the operating environment reveals that the normal operating environment is the largest contributor to the overall risk at over 90%, because the vessel spends most of its operation time in the normal environment. In the normal 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 normal 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 normal operations.

Acknowledgements

The authors wish to thank Anadarko Petroleum Company for their support in supplying the subject matter expertise necessary to conduct this analysis.

References

[1] JSC-BSEE-NA-24402-02, Probabilistic Risk Assessment Procedures Guide for Offshore Applications (DRAFT), https://bsee_prod.opengov.ibmcloud.com/sites/bsee.gov/files/ProbalisticRiskAssessment%20%28PRA%29/bsee_pra_procedures_guide_-_10-26-17.pdf, October, 26, 2017.

[2] 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.

[3] IMO MSC/Circ. 645, Guidelines for Vessels with Dynamic Positioning Systems, International Maritime Organization, June 6, 1994.

[4] Hollnagel, Erik. Cognitive reliability and error analysis method (CREAM). Elsevier, 1998.