MARIA VALENTINA CLAVIJO MESA

Application of Reliability, Availability and Maintainability analysis to Dynamic Positioning Systems used in offshore operations

São Paulo
2020

MARIA VALENTINA CLAVIJO MESA

Application of Reliability, Availability and Maintainability analysis to Dynamic Positioning Systems used in offshore operations

A Master Thesis submitted in fulfillment of the requirements for the degree of MASTER OF SCIENCE for the Polytechnic School of University of Sao Paulo, Brazil

São Paulo
2020

MARIA VALENTINA CLAVIJO MESA

Application of Reliability, Availability and Maintainability analysis to Dynamic Positioning Systems used in offshore operations

Corrected Version

A Master Thesis submitted in fulfillment of the requirements for the degree of MASTER OF SCIENCE for the Polytechnic School of University of Sao Paulo, Brazil

Concentration Area:
Naval Architecture and Ocean Engineering

Advisor:
Dr. Prof. Marcelo Ramos Martins

São Paulo
2020

Este exemplar foi revisado e corrigido em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 14 de fevereiro de 2020

Assinatura do autor: M. Valentina Clavijo M.

Assinatura do orientador: _____

Catalogação-na-publicação

Clavijo Mesa, Maria Valentina
Application of Reliability, Availability and Maintainability analysis to Dynamic Positioning Systems used in offshore operations / M. V. Clavijo Mesa -- versão corr. -- São Paulo, 2020.
215 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia Naval e Oceânica.

1.Reliability 2.Availability 3.Maintainability 4.Dynamic Positioning Systems I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia Naval e Oceânica II.t.

To my sister Camila

Acknowledgements

First and foremost, I would like to thank God Almighty for providing me this opportunity and granting me the capability to proceed successfully. Without his blessings, this achievement would not have been possible.

At the very outset, I would like to express my deep thanks to my research supervisor, Professor Marcelo Ramos Martins, my cordial thanks for grooming me as a master student, your warm encouragement, patience, guidance, charisma and critical comments were essential for the success of this research and to my formation as a future researcher.

I owe my gratitude to Professor Adriana Miralles Schleder for her friendship, empathy, vision and valuable help during the research. She has taught me the methodology to carry out the research works as clearly as possible.

I would like to express my deepest appreciation to all my friends at LabRisco, for their unwavering support, collegiality and hospitality. Every result described in this thesis was accomplished with the help and support of fellow lab mates and collaborators.

I am also grateful to dear Vilma Guerra and dear Lânia Camilo de Oliveira who helped me so much in the execution of all procedures required during this period.

To CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) and FUSP (Fundação de Apoio à Universidade de São Paulo), for the financial support.

My acknowledgement would be incomplete without thanking the biggest source of my strength, my family. The blessings of my parents, Diana and Hugo; and the love and care of my sister, Camila, cousins and uncles, have all made a tremendous contribution in helping me reach this stage in my life. I thank them all for their utmost moral support, love and care in all the aspects of my life. They all kept me going.

Abstract

Nowadays, Dynamically Positioned (DP) units are responsible for most of offshore oil exploitation operations, including drilling and maintenance campaigns. Due to the larger congestion of the oil fields, keep the vessel position, despite the environmental forces, is a critical issue.

This study aims to propose a methodology and apply it for a RAM analysis (Reliability, Availability & Maintainability) of DP System of two different generations (DP class 2 and DP class 3) in order to obtain accurate information that allows subsequently define their restriction diagrams.

The DP system, including various subsystems, DP classes and applications, are introduced and discussed. In addition, the necessary concept and techniques to analyze the Reliability, Availability and Maintainability of DP system are explained.

In the reliability analysis, two interest events (free drift and controlled drift) are evaluated for different operation times (12, 9, 6 and 3 months); and, as expected, the DP3 system is more reliable than DP2 system in all scenarios. Regarding maintainability, the Monte Carlo Simulation exposed that in more than 90% of the free drift, the maintenance teams of the DP systems under study are able to recover the positioning of the units in the first 6 hours; while the recovery times lower than 3 hours, represent 43% of simulated free drifts. The asymptotic availability analysis of DP2 and DP3 systems shows availability greater than 0.9998 even for operational times greater than 15 years. The study concludes with an evaluation of the impact of the uncertainty in the failure rates of critical components of DP systems and the use of a non-parametric method for the design of probability density function of repair times.

Finally, it is suggested that future studies take into consideration the impact of human factors in the DP system RAM analysis.

Keywords: reliability, dynamic positioning, repair times, failure rates, uncertainty.

Resumo

Atualmente, as unidades dinamicamente posicionadas (unidades DP) são responsáveis pela maioria das operações de exploração de petróleo offshore, incluindo campanhas de perfuração e manutenção. Devido ao maior congestionamento dos campos de petróleo, manter a posição do navio, apesar das forças ambientais, é uma questão crítica.

Este estudo tem como objetivo propor uma metodologia e aplicá-la a uma análise RAM (Confiabilidade, Disponibilidade e Manutenibilidade) do Sistema DP de duas diferentes gerações (DP classe 2 e DP classe 3) para obter informações precisas que permitam posteriormente definir seus diagramas de restrição.

O sistema DP, incluindo seus subsistemas, classes e aplicação na indústria offshore, é apresentado e discutido. Além disso, os conceitos e as técnicas necessárias para analisar a confiabilidade, manutenibilidade, e disponibilidade do sistema DP são explicados.

Na análise de confiabilidade, dois eventos de interesse (deriva livre e deriva controlada) são avaliados para diferentes tempos operacionais (12, 9, 6 e 3 meses); e como esperado, o sistema DP3 é mais confiável do que o sistema DP2 em todos os cenários. Em relação à manutenibilidade, a Simulação por Monte Carlo mostrou que em mais de 90% das derivas livre, as equipes de manutenção dos sistemas DP em estudo conseguem recuperar o posicionamento das unidades nas primeiras 6 horas; enquanto os tempos de recuperação inferiores a 3 horas, representam 43% das derivas simuladas. A análise de disponibilidade assintótica dos sistemas DP mostra uma disponibilidade superior a 0,9998, mesmo para períodos operacionais superiores a 15 anos. O estudo é concluído com uma avaliação do impacto da incerteza nas taxas de falha dos componentes críticos dos sistemas DP e a aplicação de um método não paramétrico para o desenho da função de densidade de probabilidade dos tempos de reparo.

Finalmente, sugere-se que estudos futuros levem em consideração o impacto dos fatores humanos na análise RAM dos sistemas DP.

Palavras chaves: confiabilidade, posicionamento dinâmico, tempos de reparo, taxas de falha, incerteza.

Resumen

Actualmente las unidades posicionadas dinámicamente (unidades DP) son responsables por la mayoría de las operaciones de exploración de petróleo en alta mar, incluidas las campañas de perforación y mantenimiento. Sin embargo, mantener la posición del barco en estos ambientes es un tema crítico, debido a la creciente congestión en los campos petroleros y el impacto de las fuerzas ambientales en la operación.

Este estudio propone la estructuración y aplicación de una metodología para desarrollar un análisis RAM (Reliability, Availablity and Maintainability) del sistema DP de dos generaciones diferentes (DP clase 2 y DP clase 3) con el fin de obtener información precisa que permitirá posteriormente definir sus diagramas de restricción.

El texto presenta y discute el sistema DP, incluidos sus subsistemas, clases y aplicaciones en la industria offshore. Además se explican los conceptos y las técnicas necesarias para analizar la confiabilidad, mantenibilidad y disponibilidad de un sistema.

En el análisis de confiabilidad se evalúan dos eventos de interés (deriva libre y deriva controlada), para diferentes tiempos operacionales (12, 9, 6 y 3 meses); y como era esperado, el sistema DP3 es más confiable que el sistema DP2 en todos los escenarios operativos evaluados. En cuanto a la capacidad de mantenimiento, la Simulación de Monte Carlo mostró que en más del 90% de las derivas libres, el equipo de mantenimiento de los sistemas DP en análisis consiguieron recuperar el posicionamiento de las unidades en las primeras 6 horas; mientras que los tiempos de recuperación de menos de 3 horas representaron el 43% de las derivas simuladas. El análisis de disponibilidad asintótica de los sistemas DP concluyó en una disponibilidad superior a 0.9999, incluso para periodos operativos mayores de 15 años. Finalmente, el estudio concluye con una evaluación del impacto de la incertidumbre sobre las tasas de falla de los componentes críticos de los sistemas DP y la aplicación de un método no paramétrico para el diseño de la función de densidad de probabilidad para los tiempos de recuperación de la unidad.

Para estudios futuros se sugiere considerar el impacto del factor humano en el análisis RAM de los sistemas DP.

Palabras claves: confiabilidad, posicionamiento dinámico, tiempos de reparo, tasas de falla, incertidumbre.

List of figures

List of tables

Abbreviations

ABS	American Bureau of Shipping
AC	Alternating Current
ACU	Aquamaster Control Unit
AGP	Advanced Generator Protection
AMISE	Asymptotic Mean Integrated Square Error
CB	Circuit Breaker
DC	Direct Current
DCU	Drive Control Unit
DGPS	Differential Global Positioning System
DP	Dynamic Positioning
DPO	Dynamic Positioning Officer
DPS	Dynamic Positioning System
DNV	Det Norske Veritas
EPRI	Electric Power Research Institute
ERAS	Engineered-systems Reliability Analysis Software
FMEA	Failure Modes and Effects Analysis
FS	Field Station
FT	Fault Tree
FTA	Fault Tree Analysis
FW	Fresh Water
HV	High Voltage
IJS	Independent Joystick System
IMO	International Maritime Organization
INL	Idaho National Laboratory
KDE	Kernel Density Estimation
LabRisco	Analysis, Evaluation and Risk Management Laboratory
LV	Low Voltage
MRU	Motion Reference Unit
MTS	Marine Technology Society
NIOT	National Institute of Oceanic Technology of India
NRC	Nuclear Regulatory Commission

NSWC	Naval Surface Warfare Center
OREDA	Offshore and Onshore Reliability Data
PDF	Probability Density Function
PMS	Power Management System
PMF	Probability Mass Function
PRS	Position Reference System
RAW	Risk-Achievement Worth
RBD	Reliability Block Diagram
RexCU	Rexpeller Control Unit
ROT	Rule of Thumb
RRW	Risk-Reduction Worth
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SIPLINK	Siemens Power Link
STBD	Starboard
SW	Sea Water
TMCC	Thruster Motor Control Center
UPS	Uninterruptible Power Supply
USP	University of São Paulo
VFD	Variable Frequency Drive
VRS	Vertical Reference Sensor

Contents

1. INTRODUCTION

Due to the high demand for hydrocarbons as the major source of energy, the oil and gas industry has expanded beyond the shore. Subsequently, exploration and production in the offshore oil and gas industry has moved into deeper waters (Lehmköster, 2014). The challenging environment of deep waters has required the adoption of more modern and advanced technology and equipment. One of the significant problems has been maintaining the vessel or floating platform's position for carrying out operations. This has made operations either unfeasible or very costly because of the costs of hiring the anchor handling vessels (Rappini, S., Pallaoro, A., & Heringer, 2003). The Dynamic Positioning (DP) system has, therefore, been introduced as one of the modern technologies used to solve the positioning problems of deep-water vessels/platforms.

The DP ships or DP semisubmersible platforms can be defined as vessels that must keep their position by computer-assisted thrusters that are constantly opposed to the environmental forces (IMO, 1994). DP systems comprise three subsystems: power, thruster and control.

- Power subsystem means all components necessary to supply the DP system with power; and for this, the power subsystem includes prime movers with necessary auxiliary systems, generators, switchboards, distributing system and power management system, if applicable.

- Thruster subsystem means all components necessary to supply the DP system with thrust force and direction; this subsystem includes thrusters with drive units and necessary auxiliary systems, main propellers and rudders if they are under the control of the DP system, thruster control electronics and manual thruster controls.

- Control subsystem means all components, hardware and software necessary to dynamically position the vessel, so this subsystem includes computer system, joystick system, position reference system, sensor system, operators' panels, associated cable and cable routing.

Additionally, the International Maritime Organization – IMO also established in 1994 that DP systems may be assigned with different classification notations depending on the degree of redundancy built into the subsystems. The DP classes are DPS-1, DPS-2 and DPS-3.

In this context, redundancy is the ability of a component or system to maintain or restore its function, when a single failure has occurred. Redundancy can be achieved for instance by installation of multiple components, systems or alternative means of performing a function (IMO, 1994).

However, despite the success of DP units, there are risks involved in their operations. Failure of power subsystem can cause a blackout (i.e., the DP system ceases to function properly leading the unit to drift); or failure of the control subsystem can lead the unit to drive off. The elapsed time to recover control of the unit may vary from some minutes to a few hours (Oliveira, Vardaro, Pallaoro, Jacob, & Vieira, 2004).

Since DP units have been operating in congested areas, with crescent proximity to production facilities, the consequence of a failure in the DP system may occasionally result in a collision with other field equipment, causing material, personnel and environmental damage that can be catastrophic (Rodriguez, 2012). In this scenario, it is essential to ensure that the risks associated with operations are at tolerable levels.

One of the methodologies used to guarantee operations at tolerable levels is the application of a Polar Restriction Diagram (PRD or DRs), which incorporates criteria to determine minimum “safe” distances between dynamically positioned (DP) units and any obstacle such as floating production systems (Oliveira et al., 2004).

These diagrams are centered in the DP units; the restriction area, where no obstacle can be present, is determined by calculating “safe” distances for a series of directions of the environmental forces. But, for the elaboration of DRs, the random variables involved must be considered, such as the expected interval between blackouts, average duration of a blackout, direction and distance of drift; and from the RAM (Reliability, Availability and Maintainability) analysis it is possible to estimate the probability of occurrence of blackout,

blackout duration and collision (Oliveira et al., 2004), to finally make decisions that reduce the risk of the operation.

Currently, there are few studies that present a quantitative evaluation of DP systems failures, although, the information about the DP system is essential to guarantee operations at tolerable risk levels; Hauff (2014) develops an analysis of the incidents related to the loss of position of the systems; Ebrahimi (2010) and Ferreira (2016) perform reliability calculations of some elements that make up the DP system; while Vedachalam and Ramadass (2017) present the Mean Time To Failure (MTTF) of the main components of power, propulsion and control subsystems for a vessel equipped with DP2.

Considering the issues mentioned above and that the required information about the DP system for calculating the blackout probability is not currently available, the objective of this research is to propose the application of RAM analysis to DP systems used in offshore operations, in order to define their DRs with greater accuracy, thus avoiding unnecessary exposure to the risks associated with the operation or, at the other extreme, considering more restrictive DR than necessary compromising the viability of the operation. If the DR is defined by considering overestimated collision probability, it will be more difficult to find a location for the probe to be allocated and drilling because the marine environment is increasingly restricted, compromising the technical and/or economic viability of the operation.

According to Oliveira et al. (2004), studies of technical and economic feasibility take into account DRs for the determination of the minimal distances between wells and offshore units, and for this, the more conservative DRs than necessary result in a greater distance from the wells to the production units, substantially increasing the cost of equipment and operations.

For this purpose, the research is based on the conceptual principles exposed by Modarres, Kaminskiy and Krivtsov (2009), which refer to reliability as a probabilistic connotation, that is the ability of an item (a product or a system) to operate under designated operating conditions for a designated period of time or number of cycles, while availability is the probability that an item, when used under stated conditions in an specified support environment (i.e., number of spare parts, personnel, diagnosis equipment, procedures, etc.),

will be operational at a given time. However, the conceptual principle for maintainability is presented by Ebeling (1997), which establishes that maintainability is the probability that a failed equipment or system can be restored or repaired to its normal operable state within a given timeframe, when maintenance is performed according to specified procedures.

Furthermore, the study applies different methods as function diagram that consider the system components according to the functional configuration and not just the physical; block diagrams that give a pictorial representation of the reliability structure; methods based on Boolean logic (Fault Tree – FT, Success Tree – ST, Event Tree - ET) that calculate the probability of top event; Monte Carlo Simulation that uses random sampling and statistical modeling to estimate mathematical functions (a probability distribution) for any factor that has inherent uncertainty and Kernel Density Estimator, which allows estimating the probability density function of a random variable when a parametric method is not adequate.

The objectives and structure of this thesis are shown below.

1.1 Objective

The main goal of this study is to propose a methodology and apply it for a RAM analysis (Reliability, Availability & Maintainability analysis) of Dynamic Positioning System (DP system) of two different DP generations (DP class 2 and DP class 3) to define their restriction diagrams.

This thesis intends to identify the most significant subsystem and machinery in a DP system from a generic configuration for the three classes of DP systems stipulated by international guidelines.

The main components and their possibilities of failure for two case studies are also a target of this thesis, and this is achieved from the qualitative analysis of DP class 2 and DP class 3.

In addition, the study provides the quantitative evaluation of the reliability, availability and maintainability of each DP system analyzed; techniques such as fault trees, block diagrams, Monte Carlo simulation and functional trees are also exposed.

Finally, the study provides possible improvements in the operation of DP systems and crucial information for future risk analysis involving DP drilling units. This provides a helpful foundation for decision-making.

It is worth noting that the scope of study does not consider the analysis of human reliability for DP system operation.

1.2 Thesis organization

The thesis is organized in six chapters, including this Introduction. Particularly in this section, a brief explanation of the thesis structure, focusing on the following five chapters is presented.

In Chapter 2, a review of concepts relevant to the development of this work is presented in three sections. In the first section, the DP system is introduced in general terms, followed by the second section with the concepts of reliability, maintainability and availability. The third section describes the techniques used for quantification of Reliability, Availability or Maintainability.

In Chapter 3, the DP system is exposed in detail with consideration of its history, different subsystems, components, and their operational aspects. The chapter also covers the varying DP classes, the corresponding requirements, and redundancy in different classification societies.

Chapter 4 presents the two case studies (two DP configurations of different generations). One refers to the operational structure of a semisubmersible platform DP2 and the other relates to a vessel DP3, both used in RAM analysis.

Chapter 5 concerns the RAM analysis. This section explores in detail the methodology used in the analysis and presents the results obtained in the evaluation of reliability, maintainability and availability of each DP unit.

Finally, in Chapter 6, methodological conclusions (related to the techniques and methods used in the study) and practical conclusions (related to the design and structure of DP systems) are drawn.

2. BACKGROUND

This chapter will present the theoretical concepts used during the development of this study. It starts with a brief introduction of the dynamic positioning system because the operational structure and configurations classes of the DP system will be detailed during Chapter 3. Subsequently, the fundamental concepts of reliability, maintainability and availability will be discussed, in order to establish the theoretical basis to understand the techniques normally used in RAM analysis. At the end of the chapter, the techniques commonly used to analyze the reliability, availability and maintainability of a system are exposed.

2.1 General aspects of DP systems

A DP vessel is a unit that automatically maintains its position (fixed location or predetermined track) exclusively by means of thruster force and includes components such as power, thrusters and control subsystems. The maritime industry accepts the definitions of DP system reliability as specified by the Maritime Safety Committee (MSC) of the IMO. MSC Circular 645 *Guidelines for Vessels with Dynamic Positioning Systems* specifies a DP system and DP system reliability, as follows:

> *A DP system consists of components and systems acting together to achieve a sufficiently reliable position-keeping capability. The necessary reliability is determined by the consequence of a loss of position-keeping capability* (IMO, 1994).

IMO specifies three levels of equipment class redundancy, defined by the worst-case requirement for any particular operation or a measurable level of reliability. However, IMO recommends that the vessel owner and client agree on the level of redundancy that will meet the anticipated risk. Alternately, coastal states or federal administrations may require a particular equipment redundancy class for a particular operation. The equipment classes, as defined by IMO, are as follows:

- Equipment Class 1: loss of position may occur after the loss of a single component.

- Equipment Class 2: loss of position is not to occur in the event of a single fault in any active component or system. Single-failure criteria include the following:

    - Any active component or system (i.e., generator, thruster, switchboard, or remote-controlled valve).
    - Any normally static component (i.e., cable, pipe or manual valve) that is not properly documented with respect to its protection and reliability.
    - Any reasonably probable single inadvertent act.

- Equipment Class 3: same as Equipment Class 2, except a single failure is further defined as follows:

    - Items included in Equipment Class 2 and any normally static components are assumed to fail.
    - All components are in a watertight compartment, from fire or flooding.
    - All components in any one-fire subdivision from fire or flooding.

It is worth noting that MSC Circular 645 defines no specific reliability or operating criterion. Equipment redundancy does not necessarily provide the necessary reliability. In addition, the IMO DP equipment class specifically avoids defining operating models, allowing the vessel owner, client, and coastal authorities to assess which level of equipment redundancy (IMO DP equipment class) best achieves the desired reliability requirements for any given operation.

Nevertheless, this chapter only seeks to present a brief introduction of the system because in Chapter 3 the history, operational structure and difference between the classes of DP systems according international standards and guidelines will be detailed.

2.2 Reliability analysis

Reliability has many connotations. In general, it refers to the ability of an item (a product or a system) to perform its function under designated operating conditions for a designated period of time or number of cycles (Modarres, Kaminskiy, & Krivtsov, 2009). The ability of an item to perform its function is normally designated through a probability (the probabilistic connotation).

The probabilistic treatment of an item reliability, according to the definition above, can be summarized by

$$R(t) = Pr(T \geq T' | C_1, C_2, \dots C_n) \tag{2.1}$$

where T' is the designated period of time or number of cycles for the item's operation (e.g., mission time) when time or cycle of application is the aggregated agent of failure and is the strength, endurance limit, or performance requirements when stress-strength, damage-tolerance or performance-requirements models are used.

T is the time to failure or cycle to failure when time or application cycle is the agent of failure and is the stress, amount of damage, or performance of the item when stress-strength, damage-tolerance, or performance-requirement models are used. R(t) is the reliability of the item at time or application cycle t after which the mission is completed, and $C_1, C_2, \dots C_n$ are the designated conditions, such as environmental conditions.

Simply put, if we are dealing with time as the agent of failure, then often, in practice $C_1, C_2, \dots C_n$ are implicitly considered in the reliability probabilistic analysis, and thus Eq. (2.1) reduces to

$$R(t) = Pr(T \geq t) \tag{2.2}$$

According to Puttlitz and Stalter (2004), reliability is the probability that a given system will perform without failure under a given set of operating conditions for a stated period, given it was operating at the initial instant. Figure 1 represents the reliability, which is measured as a probability that changes with time.

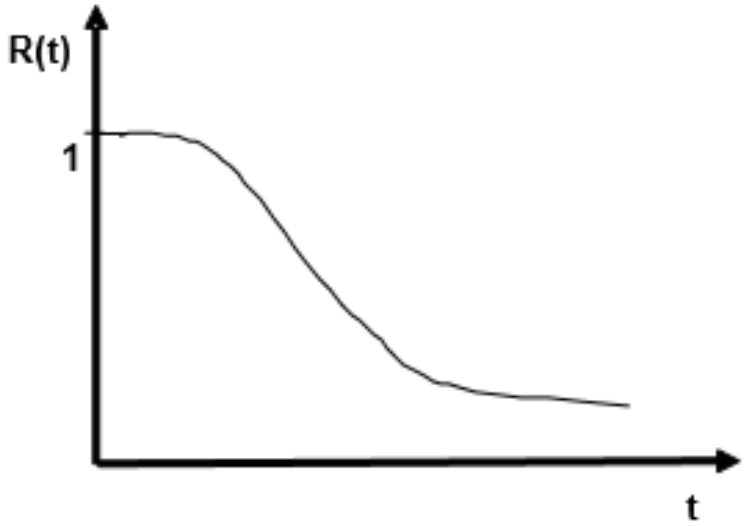


Figure 1 - Reliability representation
Source: Schleder (2015)

Notice that reliability decreases with time, in the sense that as the task duration increases, there is a greater probability of failure (unreliability).

Unreliability F(t), a measure of failure, is denoted as the probability that the system will fail by time t:

$$F(t) = P(T \leq t) \qquad for\ t \geq 0 \tag{2.3}$$

or

$$F(t) = 1 - R(t) \tag{2.4}$$

In other words, F(t) is the failure distribution function. If the time-to-failure random variable T has a density function f(t), then

$$R(t) = \int_t^{\infty} f(s)ds \tag{2.5}$$

or, equivalently,

$$f(t) = -\frac{d}{dt}[R(t)] \tag{2.6}$$

The density function can be mathematically described in terms of T:

$$\lim_{\Delta t \to 0} P(t < T \leq t + \Delta t) \tag{2.7}$$

This can be interpreted as the probability that the failure time T will occur between the operating time t and the next interval of operation, t+Δt.

Knowing that

$$P(t < T \leq t + \Delta t) = R(t) - R(t + \Delta t) \tag{2.8}$$

And

$$P(t < T \leq t + \Delta t | T \geq t) = \frac{R(t) - R(t+\Delta t)}{R(t)} \tag{2.9}$$

Then the conditional probability of failure per unit of time is

$$\frac{R(t) - R(t+\Delta t)}{R(t) * \Delta t} \tag{2.10}$$

It is possible to obtain the failure rate or hazard rate $h(t)$, as next discussed.

Before mathematically detailing the failure rate, consider a new and successfully tested system that operates well when put into service at time $t = 0$. The system becomes less likely to remain successful as time interval increases. The probability of success for an infinite time interval, of course is zero.

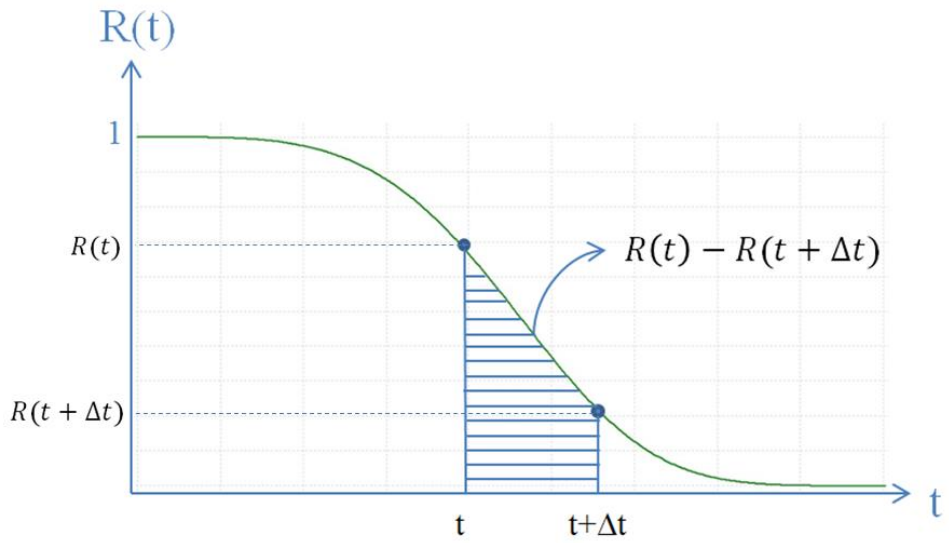


Figure 2 - System reliability for different period time

So

$$h(t) = \lim_{\Delta t \to 0} \frac{R(t) - R(t+\Delta t)}{R(t) * \Delta t} = \lim_{\Delta t \to 0} \frac{-[R(t+\Delta t) - R(t)]}{\Delta t} * \frac{1}{R(t)} \tag{2.11}$$

Where

$$h(t) = \frac{-dR(t)}{dt} * \frac{1}{R(t)} = \frac{f(t)}{R(t)} \tag{2.12}$$

Since $$h(t) = \frac{-dR(t)}{dt} * \frac{1}{R(t)} \tag{2.13}$$

$$h(t)dt = \frac{-dR(t)}{R(t)}$$

Reliability can be obtained as a function of failure rate or hazard rate $h(t)$, that is the conditional pdf (probability density function) of the component time to failure, given the component has survived to time t. Eq. (2.14) shows this relation

$$\ln R(t) = -\int_0^t h(t)dt \tag{2.14}$$

$$R(t) = e^{-\int_0^t h(t)dt}$$

The failure rate is an important function in reliability analysis since it shows changes in the probability of failure over the lifetime of a component. In practice, $h(t)$ often exhibits a bathtub shape that is the well-known "Bathtub curve", and which, over the years, has become widely accepted by the reliability community. Figure 3 shows the bathtub curve.

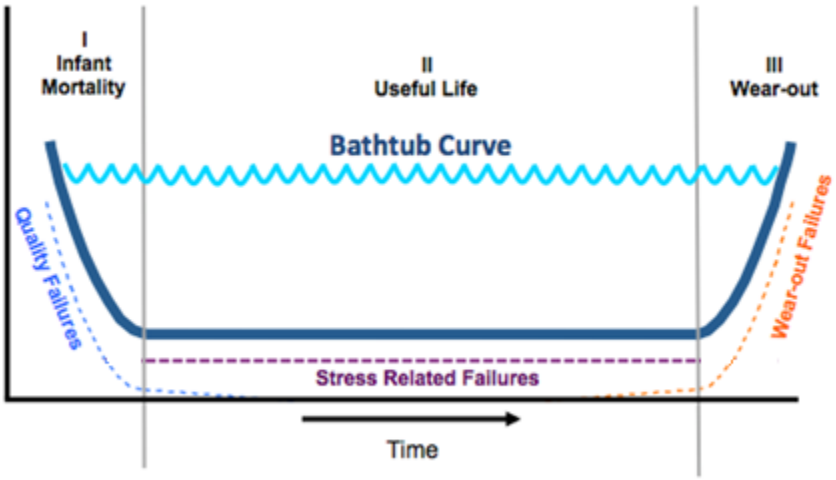


Figure 3 - Bathtub curve
Source: ARR (2015)

Generally, a bathtub curve can be divided into three regions, a decreasing failure rate (DFR), constant failure rate (CFR) and an increasing failure rate (IFR).

Zone 1 in Figure 3 is the infant mortality period and is characterized by an initially high failure rate. This is normally the result of poor design, the use of substandard components, or lack of adequate controls in the manufacturing process. When these mistakes are not caught by quality control inspections, an early failure is likely to result (O'Connor, 1981).

Zone 2, the useful life period, is distinguished by an essentially constant failure rate. This is the period dominated by chance failures. Chance failures are those failures that result from strictly random or chance causes. They cannot be eliminated by either lengthy burn-in periods or good preventive maintenance practice. Equipment is designed to operate under certain conditions and up to certain stress levels. When these stress levels are exceeded due to random unforeseen or unknown events, a chance failure will occur; however, some chance faults may occur even when the equipment is operating under design conditions.

While reliability theory and practice is concerned with all three type of failures, its primary concern is with chance failures, since they occur during the useful life period of the equipment. Figure 3 is somewhat deceiving, since Zone 2 is usually of much greater length than Zones 1 or 3. The time when a chance failure will occur cannot be predicted; however,

the likelihood or probability that one will occur during a given period within the useful life can be evaluated by analyzing the equipment design. If the probability of chance failure is too great, either design changes must be introduced for the operating environment made less severe (Bazovsky, 1999).

This CFR period is the basis for application of most reliability engineering design methods. Since it is constant, the exponential distribution of time to failure is applicable and is the basis for the design and prediction procedures as MIL-HDBK-217 (1991).

Zone 3, the wear-out period, is characterized by an increasing failure rate as a result of equipment deterioration due to age or use. For example: mechanical components, such as transmission bearings, will eventually wear-out and fail, regardless of how well they are made. Early failures can be postponed and the useful life of equipment extended by good design and maintenance practice. The only way to prevent failure due to wear-out is to replace or repair the deteriorating component before it fails.

Different statistical distributions can use to characterize each zone. For example, the infant mortality period might be represented by gamma or Weibull distributions while the useful life period by the exponential, and the wear-out period by gamma or normal distributions (Birolini, 2007).

In short, the goal of reliability analysis is to improve an item performance and for this the analyst could study reliability engineering problems or estimate and reduce the failure rate; but another way to improve item performance is to improve maintainability.

Figure 4 shows the conceptual hierarchy for improving performance proposed by Modarres, Kaminskiy and Krivstov (2009); the maintainability analysis is detailed in the next section.

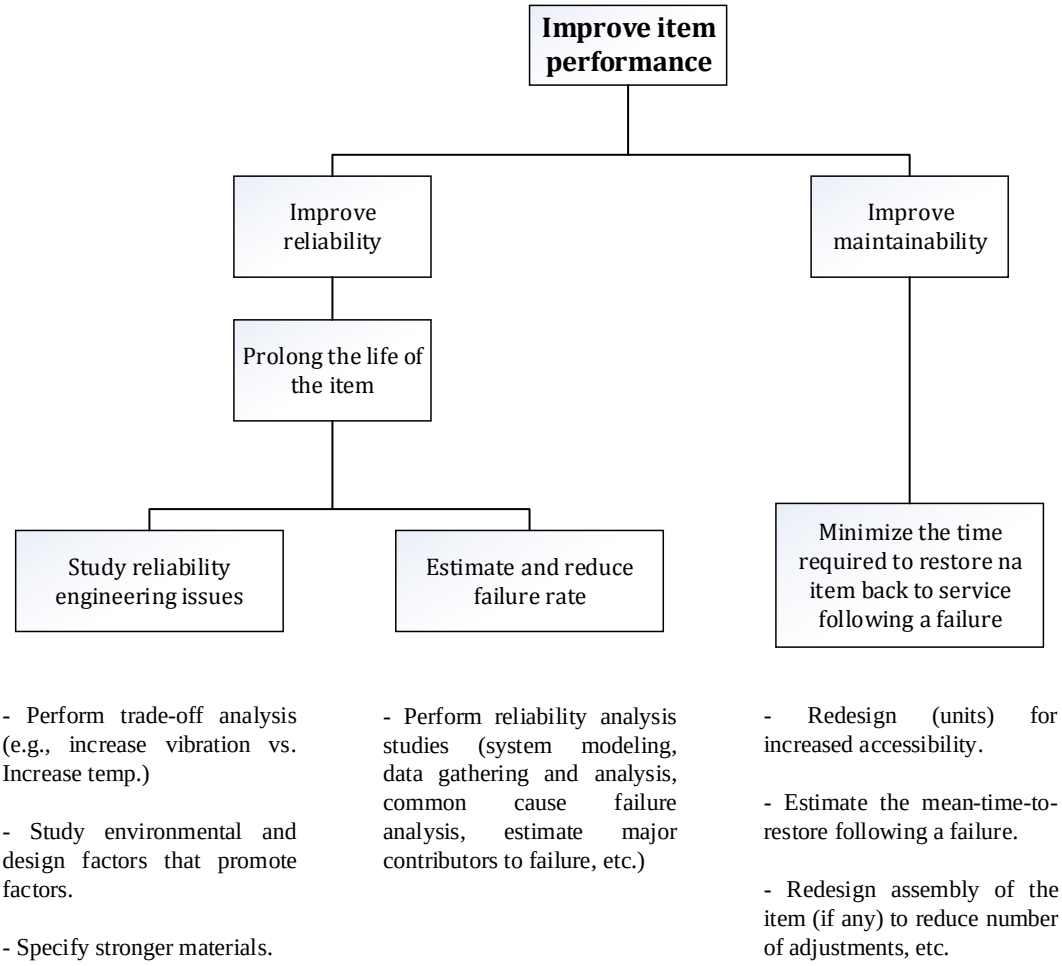


Figure 4 - Conceptual hierarchy for improving performance
Source: Modarres, Kaminskiy and Krivtsov (2009)

2.3 Maintainability analysis

When a system fails to perform satisfactorily, repair is normally carried out to locate and correct the fault. The system is restored to operational effectiveness by making an adjustment or by replacing a component.

Maintainability is defined as the probability that a failed system will be restored to specified conditions within a given period of time when maintenance is performed according to prescribed procedures and resources. In other words, maintainability is the probability of isolating and repairing a fault in a system within a given time.

Maintainability engineers must work with system designers to ensure that the system product can be efficiently and cost effectively maintained by the customer. This function requires the analysis of part removal, replacement, tear-down and build-up of the product in order to determine the required time to carry out the operation, the necessary skill, the type of support equipment and the documentation (Pham, 2006).

Figure 5 shows a typical (though simplified) history of a repairable system. Notice that it spends some of its life up and running, and the remainder down being repair. Maintainability is the study of the down times.

Observe that the down times are all different, and so are also distributed and it is generally impossible to tell in advance how long a repair will take. So statistics is involved in the study and definition of maintainability.

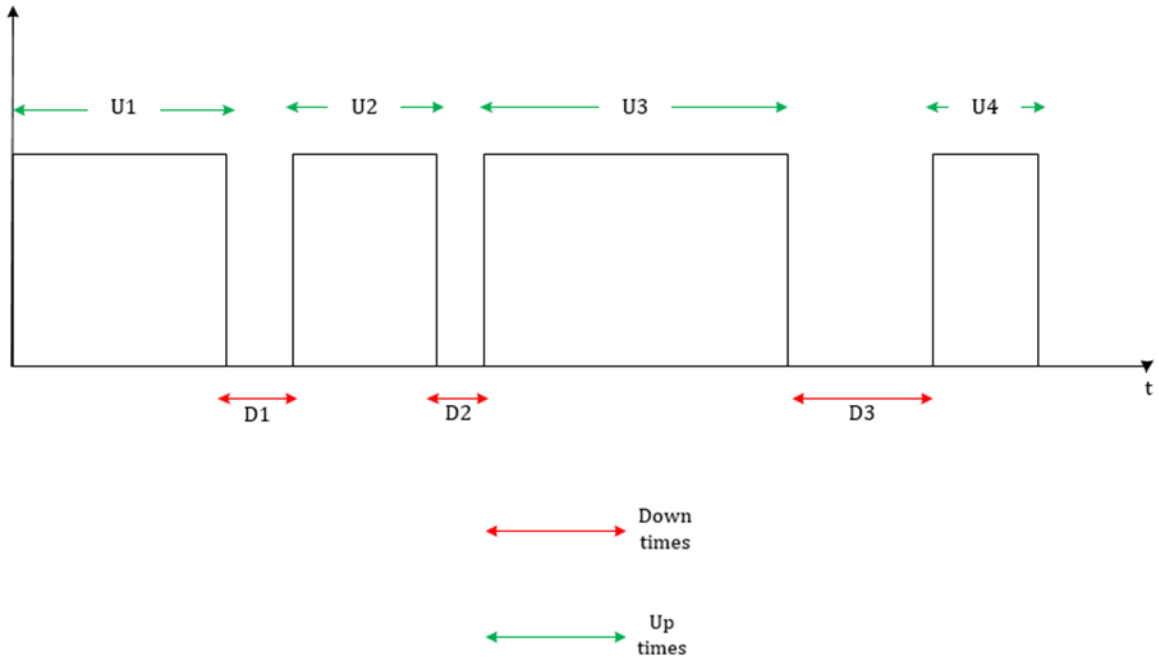


Figure 5 - History of a repairable system

In order to quantify maintainability, the repair time distribution must first be defined. Generally, repair times can be treated as random variables because repeated repair actions will result in different repair times due to unpredictable actions as delays, differences in technician experience of maintenance team, availability of repair parts, etc. This is partly a result of different failure modes or the failure of different components and parts, and the

variation in skill levels, experience and training on the part of the maintenance personnel (Ebeling, 1997).

To quantify repair times, let T be the continuous random variable representing the time to repair a failed unit, having a pdf of repair $m(t)$. Then the cumulative distribution function is

$$Pr\{T \leq t\} = M(t) = \int_0^t m(t')dt' \tag{2.15}$$

Eq. (2.15) is the probability that a repair will accomplishes within time t. The mean time to repair is given by

$$MTTR = \int_0^\infty tm(t)dt = \int_0^\infty [1 - M(t)]dt \tag{2.16}$$

2.4 Availability analysis

Reliability is a measure that requires system success for an entire mission time. No failures or repairs are allowed. Space missions and aircraft flights are examples of systems where failures or repairs are not allowed. Availability is a measure that allows for a system to repair when failure occurs (Pham, 2006).

The availability of a system is defined as the probability that a system is performing its required function at a given point in time or over a stated period of time when operated and maintained in a prescribed manner (Komal, Sharma, & Kumar, 2010). Mathematically,

$$A = \left(\frac{System\ up\ time}{System\ up\ time + System\ down\ time}\right) = \left(\frac{MTTF}{MTTF + MTTR}\right) \tag{2.17}$$

where MTTF is Mean Time To Failure and MTTR is Mean Time To Repair.

The implication of this formula is that a high availability can be obtained either by increasing the MTTF, and hence the reliability, or improving the maintainability by decreasing the MTTR (Leitch, 1995).

However, Amari (2007) assure that the steady state availability is the most important measure of repairable systems, and according to Bahri, Ghribi and Bacha (2009), the steady

state availability of the system, also called the long run or asymptotic availability is the limit of the availability function as time tends to infinity. In other words, the steady state availability is a stabilizing point where the system availability is roughly a constant value.

In short, availability is a measure of success used primarily for repairable systems. For non-repairable systems, availability, $A(t)$, equals reliability, $R(t)$. In reparable systems, $A(t)$, will be equal to or greater than $R(t)$.

2.5 Analysis techniques

With the purpose of clarifying the Reliability, Maintainability and Availability analysis process, the analytical and analysis support techniques, traditionally applied will be presented here, emphasizing the advantages and disadvantages of each one.

The first techniques presented, functional diagram and functional tree, support the analysis, since they aim to provide an initial understanding of the system to be studied. It is followed by the presentation of the block diagram method, which allows the understanding of the relations between subsystems or components, and presents alternatives to model the redundancy of the components. The fault tree is other technique presented that allows the representation of causes of undesired events in the system studied. It is worth noting that the block diagram method and the fault trees are usually applied for reliability analysis, since they allow a view of the arrangement and operation of the system and later calculation of the reliability value.

The Monte Carlo Simulation technique is presented as a proposal to evaluate the system availability and maintainability considering the components repair times and failure times, as well as an alternative to evaluate the impact of the uncertainty in the basic events of the fault trees.

Finally, the Kernel Density Estimation is presented as a technique nonparametric for estimating the probability density function of data based in the histograms.

2.5.1 Functional Diagram and Functional Tree

The Functional Diagram and the Functional Tree are tools that facilitate the understanding of the system, which is fundamental for an adequate reliability analysis. Usually, the Functional Diagram is the most popular to describe the system (Kang, 2010).

It is necessary to know the behavior and the interactions among the components of the system so that it is possible to effectively evaluate the possible failures.

The Functional Diagram shows the system components, their links and their location in relation to the others. Figure 6 shows the representation of a Functional Diagram, where each component is allocated according to its physical position in relation to the others and lines represent connections between these components.

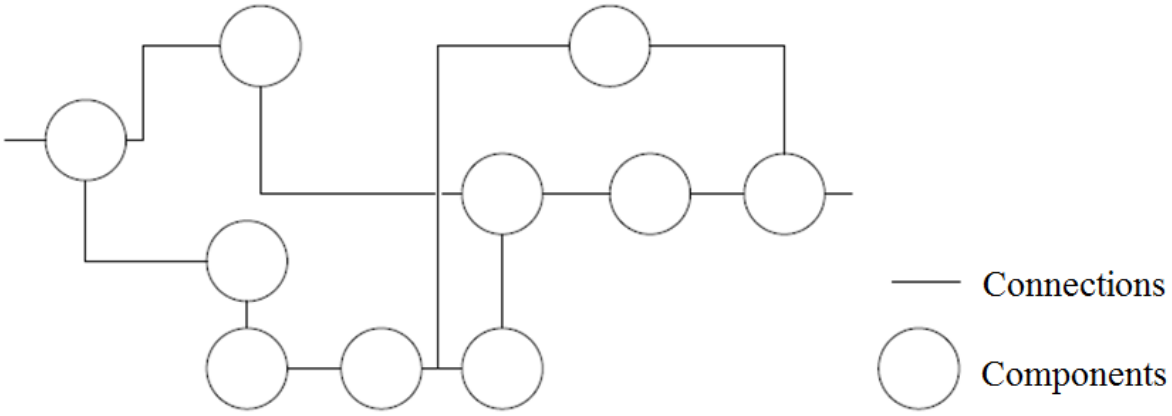


Figure 6 - Functional Diagram
Source: Schleder (2015)

In the functional tree, the relations between the different levels of the system are represented; it starts with the top event that represents the system function to be analyzed and goes on to detail how the system will perform this function. Thus, how the system and its subsystems will perform the main function is represented by the downward direction of the tree, while the cause of existence of each subsystem is represented by the upward direction. Figure 7 represents a functional tree.

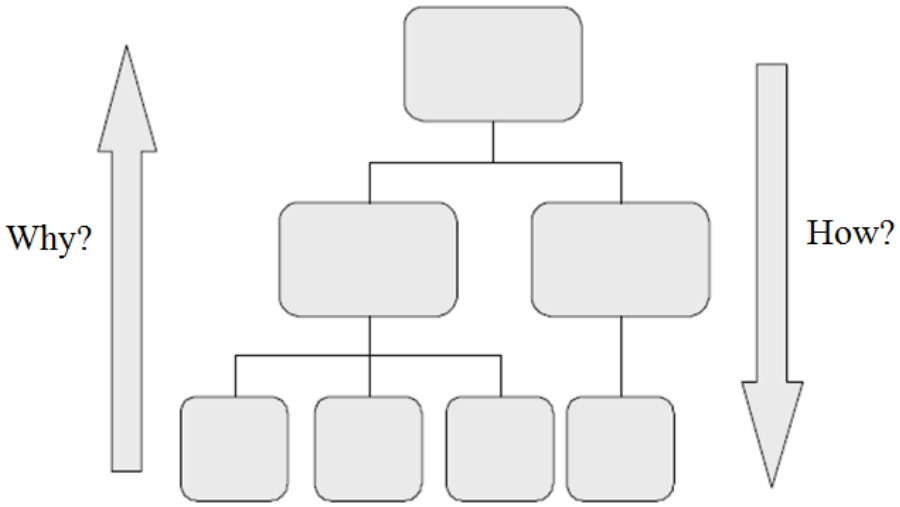


Figure 7 - Representation of the construction of a functional tree
Source: Natacci, Martins and Souza (2009)

2.5.2 Reliability Block Diagrams

A reliability block diagram (RBD) is a technique used to perform the system reliability and availability analyses on large and complex systems using block diagrams to show network relationships. The structure of the reliability block diagram defines the logical interaction of system components that are required to sustain system operation.

According to Leitch (1995), a reliability block diagram is a graphical representation of the components of the system and how the system reliability depends on the reliability of its component parts and the manner in which they are connected; the RBD can quantify the system reliability.

In the remainder of this section, the system reliability for several types of functional configurations is discussed.

2.5.2.1 Series System

Series systems are those in which all the components must function for the system to function. Figure 8 shows the reliability block diagram of a series system consisting of N blocks.

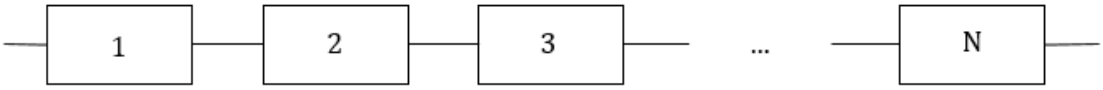


Figure 8 - Series system reliability block diagram

The reliability of the system in Figure 8 is the probability that all N units succeed during its intended mission time *t*. Thus, probabilistically, the system reliability $R_s(t)$ for independent units is obtained from

$$R_s(t) = R_1(t) \cdot R_2(t) \cdot R_3(t) \dots R_N(t) = \prod_{i=1}^{N} R_i(t) \tag{2.18}$$

where $R_i(t)$ represents the reliability of the ith block.

By *independent* is meant that knowing whether some of the components are functioning or failed does not make any more or any less likely that the remainders are in a similar state. A common reason for lack of independence is common cause or common mode failures.

2.5.2.2 Parallel Systems

In a parallel configuration, the system failure occurs only when all units' failure at the same time. Accordingly, success of only one unit would be sufficient to guarantee the success of the system. Figure 9 shows a parallel system consisting of N units.

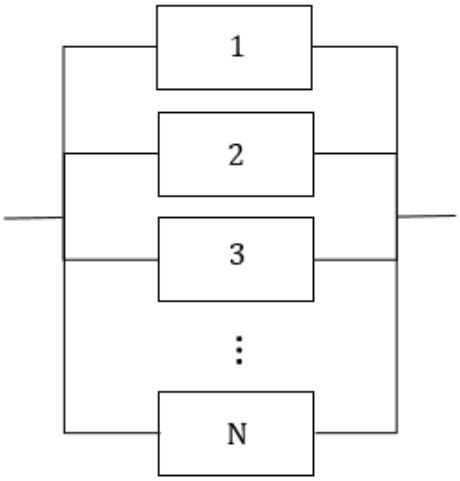


Figure 9 - Parallel system reliability block diagram

For a set of *N* independent units, the failure probability can be evaluated by,

$$F_s(t) = F_1(t) \cdot F_2(t) \cdot F_3(t) \dots F_N(t) = \prod_{i=1}^{N} F_i(t) \quad (2.19)$$

Since $R_s(t) = 1 - F_i(t)$, then

$$R_s(t) = 1 - F_s(t) = 1 - \prod_{i=1}^{N} [1 - R_i(t)] \quad (2.20)$$

It is worth noting that the redundancy may be *active or passive*, i.e. the redundant items may be switched on when the system is being used, as in the case of a multiengine aircraft that can fly if some of its engines fail, or they may be left until needed, as with a spare tire on a car. The latter case is often call standby and it is discussed in the next section.

Redundancy is also classify on a K-out-of-N basis. In this type of system, any combination of K working units out of N independent units guarantees the success of the system. For simplicity, assuming that all units are identical (which, by the way, is often the case), the binomial distribution can represent the probability that the system functions:

$$R_s(t) = \sum_{r=K}^{N} \binom{N}{r} [R(t)]^r [1 - R(t)]^{N-r} = 1 - \sum_{r=0}^{N-r} \binom{N}{r} [R(t)]^r [1 - R(t)]^{N-r} \quad (2.21)$$

2.5.2.3 Standby Redundant Systems

A system is called a standby redundant system when some of its units remain idle until they are called for service by a sensing and switching device. For simplicity, consider a situation where only one unit operates actively, while the others are in standby, as shown in Figure 10.

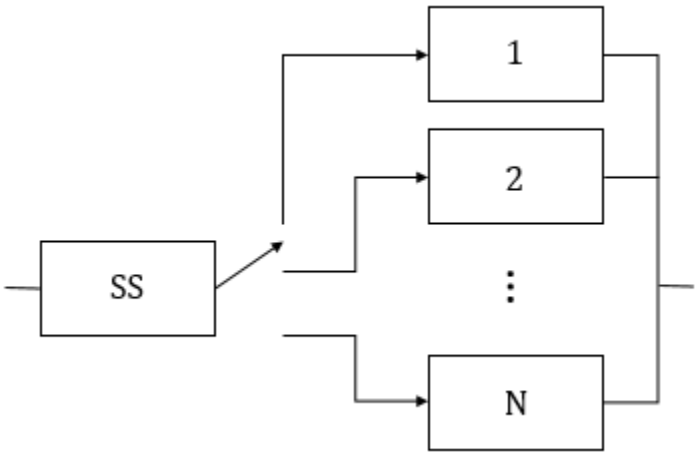


Figure 10 - Standby redundant system reliability block diagram

In this configuration, Unit 1 operates constantly until it fails. The sensing and switching device recognizes a unit failure in the system and switches to another unit. This process continues until all standby units have failed, in which case the system is considered failed. Since Units 2 to-N do not operate constantly (as in the case of active parallel systems), we would expect them to fail at a much slower rate. This is because the failure rate for components is usually higher when the components are operating than when they are idle or dormant.

System reliability is totally dependent on the reliability of the sensing and switching device. The reliability of a redundant standby system is the reliability of Unit 1 over the mission time t (i.e., the probability that it succeeds the whole mission time) plus the probability that Unit 1 fails at time t_1 prior to t and the probability that the sensing and switching unit does not fail by t_1 and the probability that standby Unit 2 does not fail by t_1 (in the standby mode) and the probability that standby Unit 2 successfully functions for the remainder of the mission in an active operation mode, and so on.

Mathematically, the reliability function for a two-unit standby device according to this definition can be obtained as

$$R_s(t) = R_1(t) + \int_0^t f_1(t_1)dt_1 \cdot R_{ss}(t_1) \cdot R'_2(t_1) \cdot R_2(t - t_1) \quad (2.22)$$

where $f_1(t)$ is the pdf for the time to failure of Unit 1, $R_{ss}(t_1)$ is the reliability of the sensing and switching device at time t_1, $R'_2(t_1)$ is the reliability of Unit 2 in the standby mode of operation at time t_1, and $R_2(t-t_1)$ is the reliability of Unit 2 as a function of time t after it started to operate at time t_1.

2.5.2.4 Load-Sharing Systems

A load-sharing system refers to a parallel system whose units equally share the system function. For example, if a set of two identical parallel pumps delivers x gpm of water to a reservoir, each pump delivers $\frac{x}{2}$ gpm. If a minimum of x gpm is required at all times, and one of the pumps fails at a given time,t_0, then the other pump speed should be increased to provide x gpm alone.

According to Modarres, Kaminskiy and Krivtsov (2009), load-sharing system reliability models can be divided into two groups: time-independent models and time-dependent models. In this section, the modeling considering the dependence of time is present, as done in the previous sections.

To illustrate the basic ideas associated with this kind of model, consider a simple parallel system composed by two identical components that share a load (i.e., each component carries half the load) and that the time-to-failure distribution for both components in this operating conditions is $f_h(s,t)$, where *s* denotes the component subject to load (stress); when one component fails (i.e., one component carries the full load), the time-to-failure distribution of the surviving pump in the new operating conditions is $f_f(2s,t)$. Also assume that the corresponding reliability functions during full-load and half-load operation are $R_f(2s,t)$ and $R_h(s,t)$, respectively. The system will succeed if both components carry half the load, or if component 1 fails at time t_0 and component 2 carriers a full load thereafter, or if component 2 fails at time to failure and component 1 carries the full load thereafter. Accordingly, as presented by Kapur and Lamberson (2009), the system reliability function $R_s(t)$ can be obtained from:

$$R_s(t) = [R_h(s,t)]^2 + 2\int_0^t f_h(s,t_1).R_h(s,t_1).R_f(2s,t-t_1)dt_1 \quad (2.23)$$

In Eq. (2.23), the first term shows the contribution from both components working successfully, with each carrying a half load; the second term represents the two equal probabilities that component 1 fails first and component 2 takes the full load at time t_0 or vice versa.

If there are switching or control mechanisms involved to shift the total load to the no failed component when one component fails, then, similar to Eq. (2.22), the reliability of the switching mechanism can be incorporated into Eq. (2.23).

2.5.2.5 Complex Systems

Most practical systems are neither a parallel nor a series configuration, but exhibit some hybrid combination of the two. These systems are often referred to as parallel-series systems. Figure 11 shows an example of such a system.

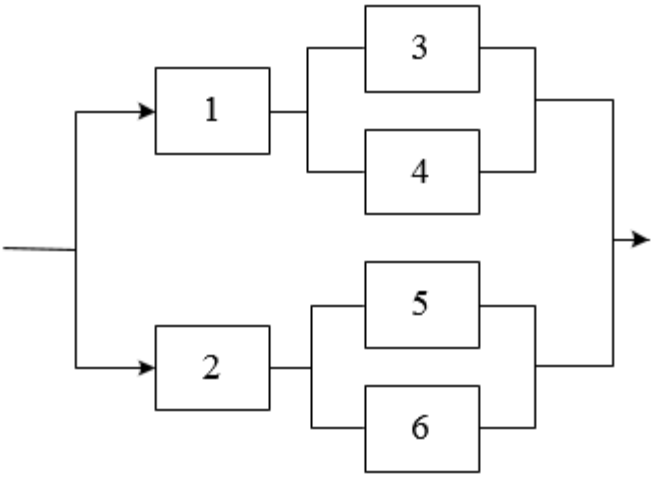


Figure 11 - Complex parallel-series system

A parallel-series system can be analyzed by dividing it into its basic parallel and series modules and then determining the reliability function for each module separately. The process can be continued until a reliability function for the whole system is determined.

For example, following with the system represented in Figure 11, the reliability of the system can be represented by a system with two items in parallel, X and Y, with item X consisting of items 1 and T in series and Y by items 2 and V also in series. In turn, item T consists of items 3 and 4 in parallel, and item V of items 5 and 6, also in parallel (see Figure 12).

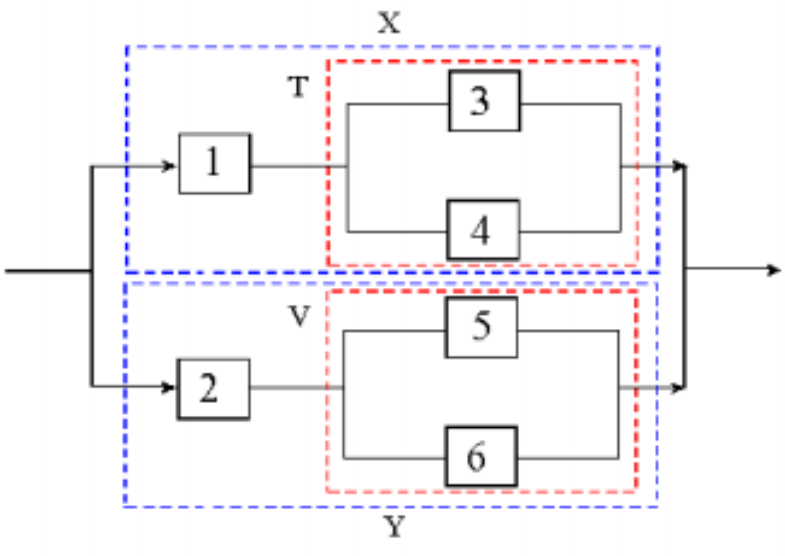


Figure 12 - Example of parallel-series system
Source: Martins (2013)

In this way, the reliability of the system shown in Figure 12 can be modeled by:

$$R_s = 1 - [(1 - R_X) \cdot (1 - R_Y)] = R_X + R_Y - R_X R_Y$$
$$R_X = R_1 \cdot R_T = R_1 \cdot (R_3 + R_4 - R_3 R_4) \quad (2.24)$$
$$R_Y = R_2 \cdot R_V = R_2 \cdot (R_5 + R_6 - R_5 R_6)$$

Another type of complex system is one that is neither series nor parallel alone, nor parallel-series. Figure 12 shows an example of such a system.

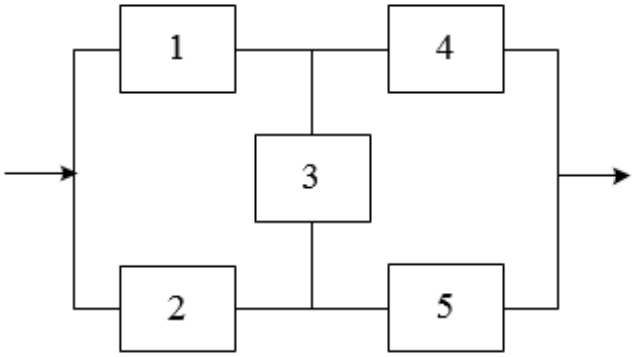


Figure 13 - Complex nonparallel-series system

For an analysis of all types of complex systems, Shooman (1990) describes several analytical methods for complex systems. These are the inspection method, event space method, path-tracing method, and decomposition method. These methods are good only when there are not many units in the system. In the following, we discuss the decomposition method.

The decomposition method relies on the conditional probability concept to decompose the system. The reliability of a system is equal to the reliability of the system given a chosen unit works multiplied by the reliability of the unit plus the reliability of the system given the unit has failed multiplied by the unreliability of the failed unit. For example, using Unit 3 in Figure 13,

$$R_s = R_s(t|unit\ 3\ work) \cdot R_3(t) + R_s(t|unit\ 3\ fail)[1 - R_3(t)] \quad (2.25)$$

For the calculation of $R_s(t|\text{unit 3 work})$ and $R_s(t|\text{unit 3 fail})$, the block diagrams shown respectively in Figure 14 (a) and (b) are used. If the system presents a greater complexity, the same strategy can be recursively used.

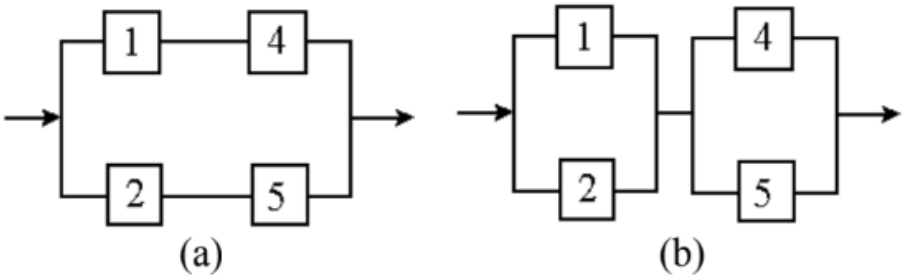


Figure 14 - Example of system decomposition with a complex configuration
Source: Martins (2013)

2.5.3 Fault Tree

Fault Tree Analysis (FTA) is a technique used in the analysis of complex systems that has been around for many years (Leitch, 1995). Bell Telephone Laboratories developed the concept in 1962 for the US Air Force for use with the Minuteman system. It was later adopted and extensively applied by the Boeing Company (NASA, 2002).

It is worth noting that the FT analysis suppose that the fault events are independents, that is, whether some of the components are functioning or failed does not make any more or any less likely that the remainders are in a similar state.

According to Lewis (1996), Fault Tree Diagrams are logic diagrams that display the state of system (top event) in terms of the states of its components (basic events). Like RBDs, Fault Tree Diagrams are a graphical design technique, and as such provide an alternative methodology to RBDs.

In other words, the Fault Tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired events. The faults can be events that are associated with component hardware failures, human errors, software errors, or any other pertinent events, which can lead to undesired event. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event, the top event of the fault tree.

It is important to understand that a fault tree is not a model of all possible system failures or all possible cause for system failure. A fault tree is tailored to its top event that corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event (Schenkelberg, 2014). Moreover, these faults are not exhaustive – they cover only the faults that are assessed to be realistic by the analyst.

It is also important to point out that a fault tree is not in itself a quantitative model. It is a qualitative model that can be quantitatively evaluated and often is. This qualitative aspect, of course, is true of virtually all varieties of system models. The fact that a fault tree is a particularly convenient model to quantify does not change the qualitative nature of the model itself (NASA, 2002).

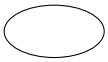
2.5.3.1 The Fault Tree Approach

Intrinsic to a fault tree is the concept that an outcome is a binary event i.e., to either success or failure. To understand the symbology of fault tree (the FT is fundamentally a logic tree), consider Figure 15.

In essence, there are three types of symbols: events, gates and transfers. Basic events, undeveloped events, conditions events, and external events are sometimes referred to as primary events. When postulating events in the fault tree, it is important to include not only the undesired component states (e.g., applicable failure mode), but also the time when they occur (Modarres et al., 2009).

The gates show the relationships of events needed for the occurrence of a “higher” event. The “higher” event is the output of the gate; the “lower” events are the “inputs” to the gate. The gate symbol denotes the type of relationship of the input events required for the output event (see Figure 15).

Primary Event Symbols

Event	Symbol	Description
Basic event		A basic event requiring no further development
Conditioning event		Specific conditions or restrictions that apply to any logic gate (used primary with PRIORITY AND and INHIBIT gate)
Undeveloped event		An event which is not further developed either because it is of insufficient consequence or because information is unavailable
External event		An event which is normally expected to occur

Intermediate Event Symbols

Event	Symbol	Description
Intermediate event		An event that occurs because of one or more antecedent causes acting through logic gates

Gate Symbols

Name of gate	Symbol	Description
AND		Output occurs if all of the input events occur
OR		Output occurs if at least one of the input events occur
NOT OR		Output occurs if at least one of the input events does not occur
NOT AND		Output occurs if all of the input events do not occur
k/N		Output occurs if k of the possible N input events occur
PRIORITY AND		Output occurs if all of the input events occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)

Transfer Symbols

Event	Symbol	Description
Transfer in		Indicates that the tree is developed further at the occurrence of the corresponding TRASNFER OUT (e.g., on another page)
Transfer out		Indicates that this portion of the tree must be attached at the corresponding TRASNFER IN

Figure 15 - Primary event, gate and transfer symbols used in logic trees
Source: Modarres, Kaminskiy and Krivtsov (2009)

To better understand the fault tree concept, consider the pumping system shown in Figure 16. Sufficient water is delivered from the water source T_1 when one of the two pumps, P_1 or P_2, works. All the valves V_1 through V_4 are normally open. The sensing and control system S senses the demand for the pumping system and automatically starts both P_1 and P_2. (If one of the two pumps fails to start or fails during operation, the mission is still considered successful if the other pump functions properly).

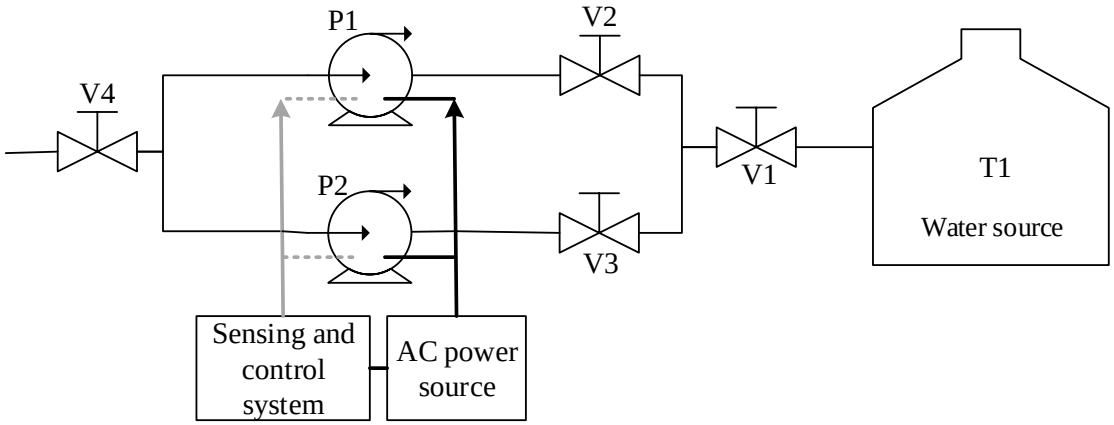


Figure 16 - Example of pumping system

The two pumps and the sensing and control system use the same AC power source. Assume the water content in T_1 is sufficient and available, there are no human error, and no failure in the pipe connections is considered important.

The system mission is to deliver sufficient water when needed. Therefore, the top event of the fault tree for this system should be “no water is delivered when needed”. Figure 17 shows the fault tree for this example.

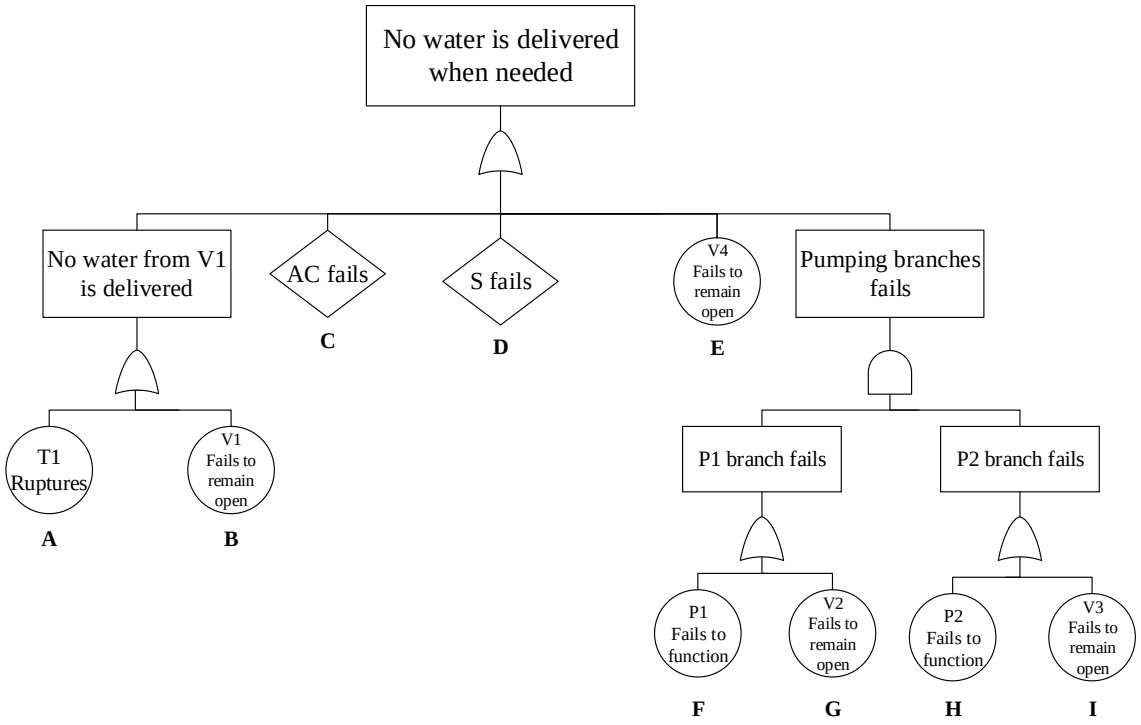


Figure 17 - Fault tree for the pumping system in Figure 16

2.5.3.2 Qualitative Evaluations of a Fault Tree

Qualitative evaluations basically transform the FT logic into logically equivalent forms that provide more focused information. The principal qualitative results that are obtained are the Minimal Cut Sets of the top event. A Cut Set is a combination of basic events that causes the top event. A Minimal Cut Set is the smallest combination of basic events that results in the top event. The basic events are the bottom events of the fault tree. Hence, Minimal Cut Sets relate the top event directly to the basic events causes. The set of Minimal Cut Sets for the top event represents all the ways that the basic event can cause the top event. A more descriptive name for a Minimal Cut Set may be “minimal failure set”. The set of Minimal Cut Sets can be obtained not only for the top event, but for any of the intermediate events (e.g. gate events) in the FT (NASA, 2002).

Following the example of Figure 16, the Minimal Cut Sets for the pumping system are presented in Figure 18.

The Minimal Cut Set analysis for the pumping system example has shown that with a single failure of T1 (rupture), sensing and control system, AC power, V1 or V4 (fails to remain open), the top event can occur, while the single failure of P1, P2, V2 or V3 does not result in the undesired event "No water is delivered when needed", because these components will only generate the occurrence of the top event in case of combined failures.

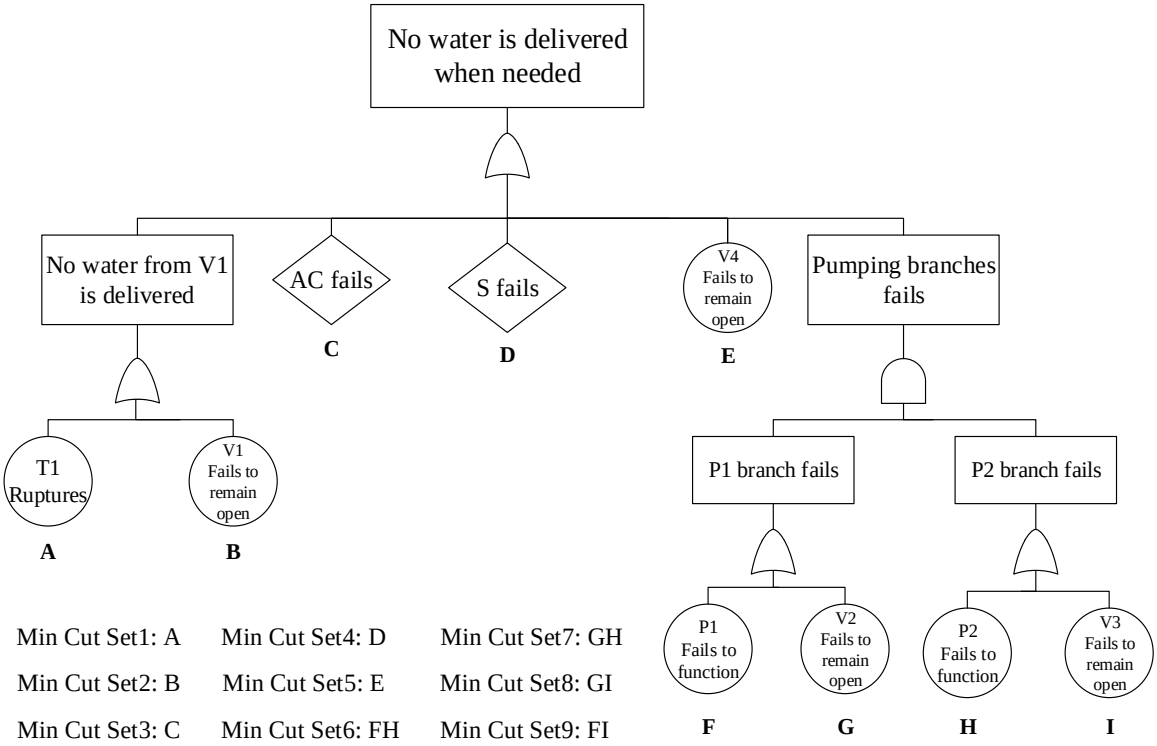


Figure 18 - Minimal Cut Sets of the Fault tree for the pumping system (example)

Knowing the Minimal Cut Sets for a particular fault tree can provide valuable insight concerning potential weak points of complex systems, even when it is not possible to calculate the probability that either a particular cut set or the top event will occur. According to Lewis (1996), in the cut-set interpretation, there are three qualitative considerations, in particular, which may be very useful: the ranking of the Minimal Cut Sets by the number of primary failures required, the importance of particular component failures to the occurrence of the Minimal Cut Sets, and the susceptibility of a particular cut set to common-mode failures.

Minimal cut sets are normally categorized as singlets, doublets, triplets, and so on, according to the number of primary failures in the cut set. Emphasis is then put on eliminating cut sets corresponding to small numbers of failures, for ordinarily these may be expected to make the largest contributions to system failure. In fact, the common design criterion, that no single component failure should cause system failure is equivalent to saying that all singles must be removed from the fault tree for which the top event is system failure.

Note that if component failure probabilities are small and independent, then provided that they are of the same order of magnitude, doublets will occur much less frequently than singles, triplets much less frequently than doublets, and so on.

A second application of cut set information is in assessing qualitatively the importance of a particular component. Suppose that it is desired to evaluate the effect on the system of improving the reliability of a particular component, or conversely, to ask whether, if a particular component fails, the system-wide effect will be considerable. If the component appears in one or more of the lower-order cut sets (singlets or doublets), its reliability is likely to have a pronounced effect. On the other hand, if it appears only in minimal cut sets requiring several independent failures; its importance to system failure is likely to be small.

These arguments can rank minimal cut sets and component importance, assuming that the primary failures are independent. If they are not, that is, if they are susceptible to common-mode failures, the ranking of cut-set importance may be changed. For example, if in a minimal cut set with six failures, five of them can occur as the result of a common cause, the probability of the cut set occurring is more comparable to that of a doublet.

Additionally, with the Minimal Cut Sets determined the probability data may be used for the primary failures and proceed with quantitative analysis. In the next section, this analysis is detailed.

2.5.3.3 Quantitative Evaluations of a Fault Tree

As previously commented, the evaluation of a fault tree proceeds in two steps. First, a logical expression is constructed for the top event in terms of combinations (i.e., unions and intersections) of the basic events. This is referred to as qualitative analysis. Second, this expression is used to give the probability of the top event in terms of the probabilities of the primary events. This is alluded to as quantitative analysis. Thus, knowing the probabilities of the primary events, it is possible to calculate the probability of the top event (Lewis, 1996).

According to NASA (2002), an FT can be thought of as a pictorial representation of Boolean relationships among fault events that cause the top event occurrence. In fact, an FT can always be translated into an equivalent set of Boolean equations. Thus, an understanding of the rules of Boolean algebra contributes materially toward the construction and simplification of FTs. Once an FT has been drawn, it can be evaluated to yield its qualitative and quantitative characteristics. These characteristics cannot be obtained from the FT per se, but they can be obtained from the equivalent Boolean equations.

The rules of Boolean algebra are presented in Appendix A along with a short discussion of each rule.

One of the main purposes of representing an FT in terms of Boolean equations is that these equations can then be used to determine the fault tree associated Minimal Cut Sets. Once the Minimal Cut Sets are obtained, the quantification of the FT is quite straightforward.

Any FT will consist of a finite number of Minimal Cut Sets that are unique for that top event. One-component Minimal Cut Sets, if there are any, represent those single failures that will cause the top event occurrence. Two-component Minimal Cut Sets represent the double failures that together will cause the top event occurrence. For an n-component Minimal Cut Sets, all n components in the cut set must fail in order for the top event occurrence.

The minimal cut set expression for the top event can be written in the general form,

$$T = C_1 + C_2 + C_3 + \cdots + C_k \tag{2.26}$$

Where T is the top event and C_i is i-th minimal cut set. Each Minimal Cut Set consists of a combination of specific component failures, and hence the general n-component minimal cut can be express as

$$C_i = X_1 \cdot X_2 \cdot \ldots \cdot X_n \tag{2.27}$$

where X_1, X_2,X_3, etc., are basic component failures in the tree.

In general terms, knowing the Minimal Cut Sets, it is possible to calculate the probability that the top event, T, occurs in a mission time, t

$$P(T) = P(C_1 \cup C_2 \cup \ldots \cup C_n) \tag{2.28}$$

Note that in cases where Minimal Cut Sets are mutually exclusive, the intersection is zero and Eq. (2.28) can result in

$$P(T) = \sum_{i=1}^{n} P(C_i) \tag{2.29}$$

However, in general, the development of Eq. (2.28) results in the fact that the probability of the top event will be given by the sum of the probability of the individual Minimal Cut Sets, minus the sum of the probability of all possible pairs, plus the sum of the probabilities of all possible combinations of three cut sets, minus the probabilities of all possible combinations of four cut sets, plus the probability of intersection of all five minimal cut sets, and so on (U.S.NRC., 2011a). Mathematically:

$$P(T) = \sum_{i=1}^{n} P(C_i) - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} P\left(C_i \cap C_j\right) + \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} P\left(C_i \cap C_j \cap C_k\right) - \cdots$$

The number of terms in this expression grows considerably as the number of Minimal Cut Sets in a FT increases. For large FTs, to get the Minimal Cut Sets can be a formidable job even for powerful mainframe computers (Modarres et al., 2009). In this sense,

computational processing can be very costly and, depending on the number of Minimal Cut Sets, become even impracticable.

In the case where the probability of occurrence of each Minimal Cut Sets is small, the terms that involve their combination tend to contribute little to the probability of occurrence of the top event, since the product of numbers much smaller than 1 results in a number of order of magnitude even closer to zero. Thus, the bounding result can also use as an approximation of the true top event value. This is often called the rare event approximation. The expression of the probability of top event results in:

$$P(T) \simeq \sum_{i=1}^{n} P(C_i) \tag{2.30}$$

Another possible approximation to the probability of union of the Minimal Cut Sets for the FT is the Minimal Cut Set Upper Bound. The equation for this method is:

$$P(T) = 1 - \prod_{i=1}^{n} [1 - P(C_i)] \tag{2.31}$$

Barlow and Proschan (1981) showed that Eq. (2.31) gives an upper bound on the exact probability of the top event. This expression is exact for the case in which Minimal Cut Sets do not have basic events common to each other, that is, in cases where cut sets are mutually exclusive. Otherwise, as emphasized, the approximation will be conservative and will represent only an upper limit of the top event probability. In Appendix B the possible overestimation of top event probability, though an example that uses the Minimal Cut Set Upper Bound expression is discussed.

In short, in qualitative analysis, information about the logical structure of the tree is used to locate weak points and evaluate and improve system design, and the quantitative evaluations of an FT consists on the determination of top event probabilities and basic event importance (assuming that the basic events are independent). Uncertainties in any quantified result can also be determined. Fault trees are typically quantified by calculating the probability of each Minimal Cut Set and by summing all the cut set probabilities. The cut sets are then sorted by probability. The cut sets that contribute significantly to the top event probability are called the dominant cut sets. While the probability of the top event is the

primary focus in the analysis, the probability of any intermediate event in the fault tree can also be determined.

In addition to the identification of dominant cut sets, importance of the events in the FT are some of the most useful information that can be obtained from FT quantification. Quantified importance allows actions and resources to be prioritized according to the importance of the events causing the top event.

In the case where the reader wishes to develop the technique of the FTA, some references are recommended as Leitch (1995), Lewis (1996), NASA (2002) and Modarres, Kaminskiy and Krivtsov (2009).

2.5.4 Monte Carlo Simulation

Some systems are too complex to be analyzed easily by analytic methods. In cases like these, Monte Carlo Simulation is frequently used, as it is very versatile, and can be used to examine different maintenance policies, design solutions, spares holdings, and many other parameters that affect reliability, availability, maintainability or other measures of effectiveness (Leitch, 1995).

According to Mooney (1997), Monte Carlo Simulation is a mathematical technique that generates random numbers from random variables for modeling risk or uncertainty of a certain system; in other words, Monte Carlo Simulation is a probabilistic method suitable for modeling risk or uncertainty in a system.

The method is used extensively in a wide variety of fields, such as physical sciences, computational biology, statistics, artificial intelligence and quantitative finance.

The principle behind Monte Carlo Simulation is that the behavior of a statistic in random samples can be assessed by the empirical process of actually drawing many random samples and observing their behavior. The strategy for doing this is to create an artificial

"world", or pseudo-population, which resembles the real world in all relevant respects. This pseudo-population consists of mathematical procedures for generating sets of numbers that resemble samples of data drawn from the true population. The pseudo-population is used to conduct multiple trials of the statistical procedures of interest to investigate how that procedure behaves across samples.

In the next sections, an overview of the Monte Carlo Simulation history is presented, followed by a general description of the method.

2.5.4.1 The Monte Carlo Simulation Approach

During the wartime period, the first electronic computer ENIAC was developed at the University of Pennsylvania. It was used for the calculation of thermonuclear problems in the Manhattan Project. After the war, Stan Ulam, who was well versed with statistical sampling techniques, has an idea to use ENIAC's miraculous ability for this technique. He discussed with John von Neumann. In 1947, von Neumann showed a detailed outline of a possible statistical approach to solving the problem of neutron diffusion in fissionable material (Matsuoka Takeshi, 2013). Additionally, von Neumann conceived the algorithm for generating uniformly distributed pseudo-random numbers. This was the starting of the Monte Carlo Simulation. The method was named after the Monte Carlo Casino, a famous casino where many people, including Ulam's uncle, would often gamble away their money (Metropolis, 1987).

The simulation is treated as a series of real experiments, and statistical inference is used to estimate the confidence intervals for the performance. As an example, consider component failure phenomenon. Start with a sound state of a component and observe it for a certain time duration t. The component will be in sound or failed state at time t with the aid of random events in a computer model. Repeat this observation many times and collect the events the component is in the sound state. The fraction of the number of sound states over the total observation number gives the success probability of a component at time t, and this probability is the reliability R(t) of this component. The numerical value of the success

probability is easily obtained, and the success probability reflects an assigned failure model, which is used in the generation of random events.

The Monte Carlo simulation allows us to consider various aspects of system characteristics, which cannot be easily captured by analytical methods, such as K-out-of-N success criteria, redundancies, phased mission, stand-by condition, aging effects, repair and maintenance for components.

Differently from a physical experiment, Monte Carlo Simulation performs random sampling and conducts a large number of experiments in a computer. Then the statistical characteristics of the experiments (model outputs) are observed, and conclusions on the model output are drawn based on the statistical experiments. In each experiment, the possible values of the input random variable $X = (X_1, X_2, \dots, X_n)$ are sampled (generated) according to the performance function $Y = g(X)$ at the samples of input random variables. With a number of experiments carried out in this manner, a set of samples of output variable Y are available for the statistical analysis, which estimates the characteristics of the output variable Y.

The outline of Monte Carlo Simulation is depicted in Figure 19. Three steps are required in the simulation process: Step 1 – sampling on random input variables X, Step 2 – evaluating model output Y, and Step 3 – statistical analysis on model output. These steps are discussed in the following sections.

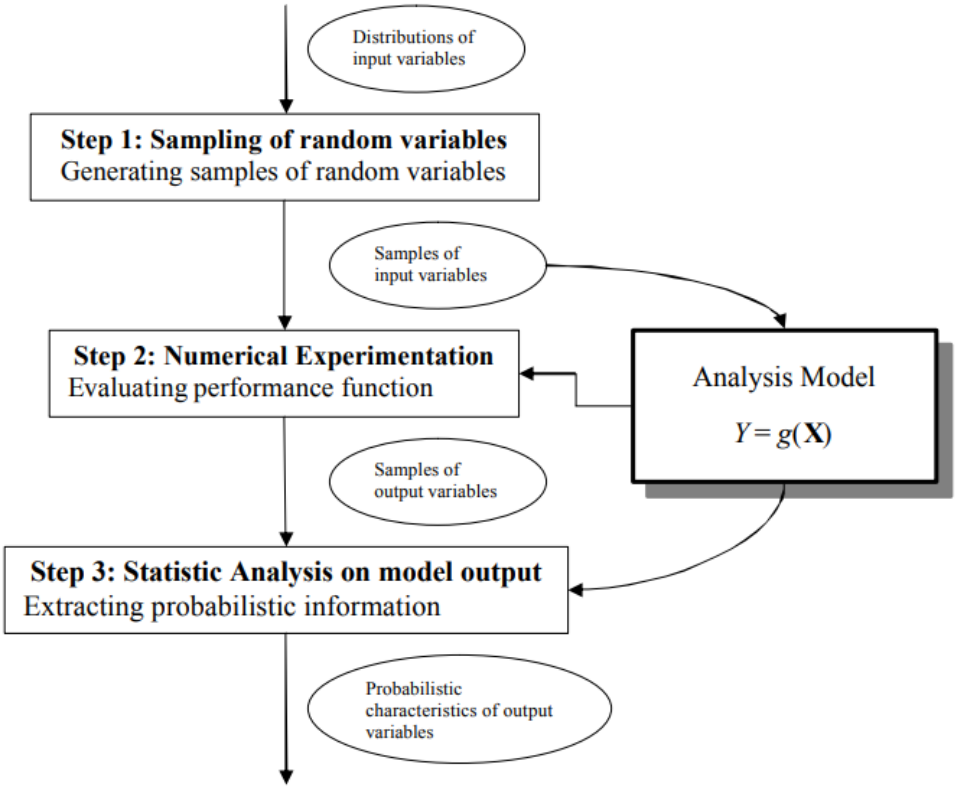


Figure 19 - Monte Carlo Simulation
Source: Siddall (1983)

2.5.4.2 ***Sampling on input random variables***

The purpose of sampling on the input random variables $X = (X_1, X_2, \dots, X_n)$ is to generate samples that represent distributions of the input variable from their *cdfs* (cumulative density functions) $F_{x_i}(x_i)(i = 1,2, \dots, n)$. The samples of the random variables will then be used as inputs to the simulation experiments. Two steps are involved for this purpose: Step A – generating random variables that are uniformly distributed between 0 and 1, and Step B – transforming the values of the uniform variable obtained from Step A to the values of random variables that follow the given distributions $F_{x_i}(x_i)(i = 1,2, \dots, n)$.

Step A – Generating random variables that are uniformly distributed between 0 and 1

The importance of uniformly distributed numbers over the continuous range [0,1] is that they can be transformed into real values that follow any distributions of interest. In the early times of simulations, random numbers were generated by mechanical ways, such as

drawing balls, throwing dice, as the same way as many of today's lottery drawings. Now any modern computers can generate uniformly distributed random variables between 0 and 1. There are a number of arithmetic random generators developed for the computer-based random generation. Random variables generated this way are called *pseudo random numbers*(Siddall, 1983). A random-generator produces a sequence of uniform numbers between 0 and 1. The length of the sequence before repeating itself is machine and algorithm dependent.

To study the pseudo random numbers, some references are recommend as Siddall (1983), Mooney (1997) and Zio (2013).

Step B – Transforming [0,1] uniform variable into random variables that follow a given distribution

The task is to transform the samples of [0,1] uniform variables, $z = (z_1, z_2, \dots, z_N)$, where N is the number of samples, generated from Step A, into values of random variable X_i that follow a given distribution $F_{x_i}(x_i)$. There are several methods for such a transformation. The simple and direct transformation is the inverse transformation method (Siddall, 1983). By this method, the random variable is given by

$$x_i = F_{x_i}^{-1}(z_i)\ , i = 1,2, \dots, N \tag{2.32}$$

Where $F_{x_i}^{-1}$ is the inverse of the cdf of the random variable X_i.

The transformation is demonstrated in Figure 20.

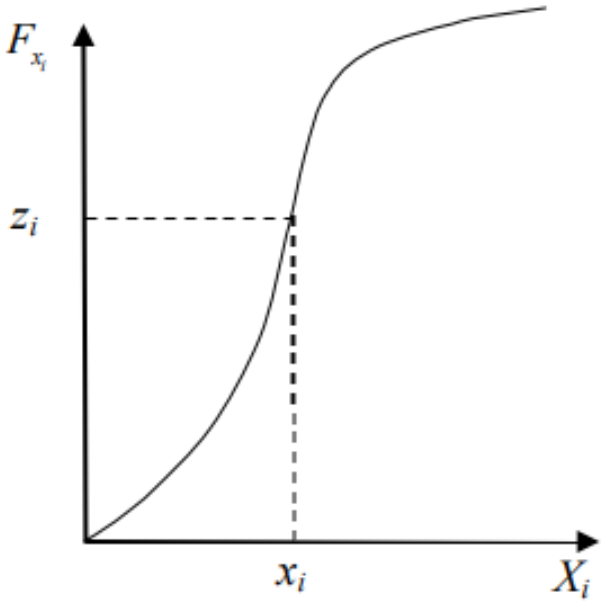


Figure 20 - The Inverse Transformation Method
Source: Siddall (1983)

For example, if X is normally distributed with $N(\mu_X, \sigma_X)$, since

$$z = F_X(x) = \phi\left(\frac{x - \mu_X}{\sigma_X}\right)$$

Then

$$x = \mu_X + \sigma_X \phi^{-1}(z)$$

Mooney (1997) and Zio (2013) present the inverse transformation method in detail.

2.5.4.3 Numerical Experimentation

Suppose that N samples of each random variable are generated, then all the samples of random variables constitute N sets of input, $x_i = (x_{i1}, x_{i2}, \dots, x_{in})$, $i = 1,2, \dots, N$, to the model $Y = g(X)$. Solving the problem N times deterministically yields N samples points of the output Y.

$$y_i = g(x_i), \quad i = 1,2, \dots N \tag{2.33}$$

2.5.4.4 Extraction of probabilistic information of output variables

After N samples of output Y have been obtained, statistical analysis can be carried out to estimate the characteristics of the output Y, such as the mean, variance, reliability, the probability of failure, *pdf* and *cdf*. The associated equations are given below:

The mean

$$\bar{Y} = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{2.34}$$

The variance

$$\sigma_Y^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y_i - \bar{Y})^2 \tag{2.35}$$

If the failure is defined by the event $g \leq 0$, the probability of failure is then calculated by

$$P_f = P\{g \leq 0\} = \frac{N_f}{N} \tag{3.36}$$

where N_f is the number of samples that have the performance function less than or equal to zero, i.e. g≤0.

The reliability is then estimated by

$$R = P\{g > 0\} = 1 - p_f = \frac{N-N_f}{N} \tag{2.37}$$

2.5.5 **Kernel Density Estimation (KDE)**

In probability theory, a continuous random variable is a variable whose value is obtained by measuring, for example, height of students in class, time it takes to get to school or distance traveled between classes, while a discrete random variable is a variable whose value is obtained by counting, for example, number of students present, number of red marbles in a jar or students' grade level.

For a discrete random variable, $P(X = x)$ is called the probability mass function (pmf); for continuous random variables, the probability that X takes on any particular value x is zero. That is, finding $P(X = x)$ for a continuous random variable X is not going to work. Instead, it is need to find the probability that X falls in some interval (a,b), that is, one needs to find $P(a < X < b)$, and for this, a probability density function (pdf) is used (Perez, 2014).

Figure 21 illustrates the difference between a probability mass function of a discrete random variable (a) and a probability density function of a continuous random variable (b).

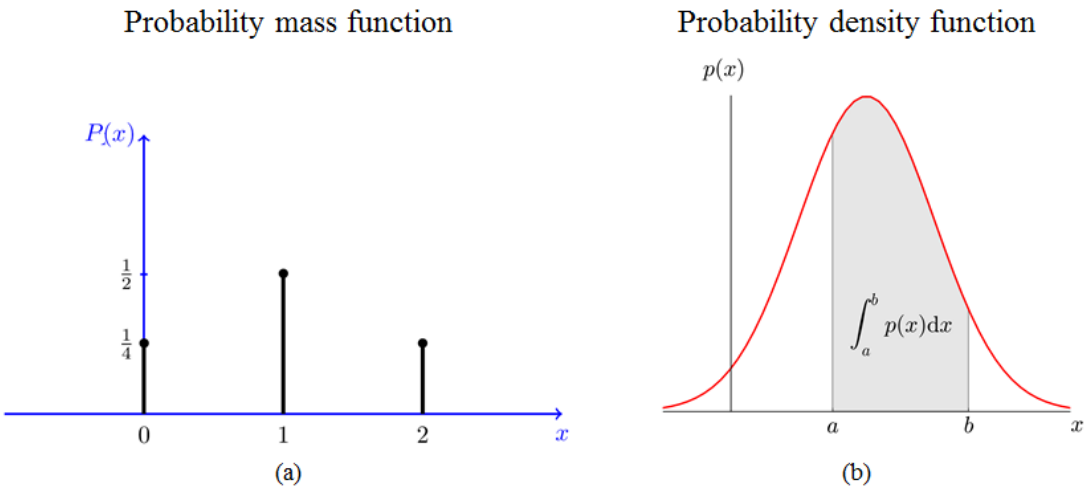


Figure 21 - Probability mass function and Probability density function
Source: Eberly College of Science (2014)

It is worth noting that the ‘pd’ in pdf stands for “probability density”, not probability. Density means probability per unit value of the random variable and it can easily exceed 1. What has to be true is that the integral over the entire space of pdf must be exactly 1 (Nakano, 2013).

In statistics, the Kernel Density Estimation (KDE) is a non-parametric way to estimate the pdf f(x) of a random variable X. KDE is a fundamental data smoothing problem where inferences about the population are made based on a finite data sample (Chouaib, 2015).

KDE belongs to a class of estimators called non-parametric density estimators because it provides a simple way of finding structure in data sets without imposing any parametric model. That is, in comparison to parametric estimators where the estimator has a fixed functional form (structure) and the parameters of this function are the only information that is necessary to be stored, non-parametric estimators have no fixed structure and depend upon all the data points to reach an estimate. To understand KDE it is necessary to understand histograms.

A histogram is the simplest non-parametric density estimator and the one that is mostly frequently encountered, Silverman (1986). To construct a histogram, the interval covered by the data values is divided into equal sub-intervals, known as `bins'. Every time a data value falls into a particular sub-interval, then a block, of size equal to 1 by the bandwidth is placed on top of it. When a histogram is constructed, it is necessary to consider these two main points: the width of the bins (the bandwidth) and the end points of the bins. For example, if breaks are chosen at 0 and 0.5 and a bandwidth of 0.5, the histogram looks like this

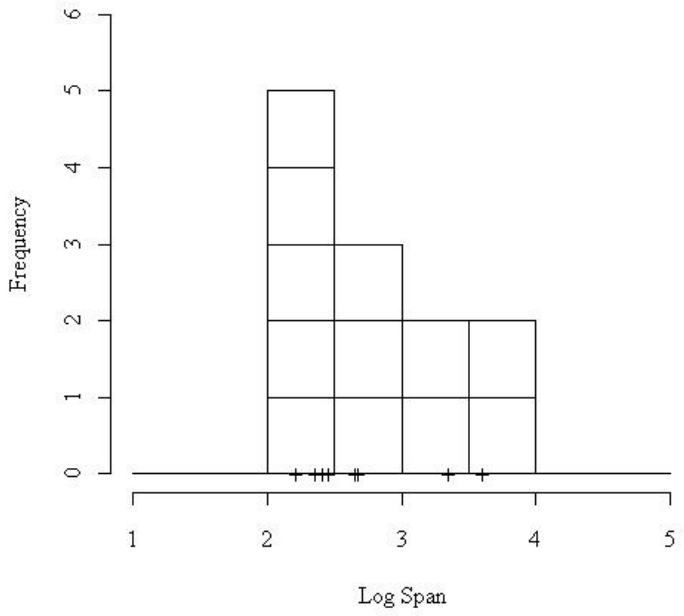


Figure 22 - Histogram with breaks at 0 and 0.5, bandwidth=0.5
Source: Doung (2001)

The data represent wingspans of aircraft built in from 1956 - 1984. (The complete dataset can be found in (Kafadar, Bowman, & Azzalini, 1999)). For the histogram construction a subset is used, namely observations 2, 22, 42, 62, 82, 102, 122, 142, 162, 182, 202 and 222. Crosses on the x-axis represent the data points. This density appears unimodal and skewed to the right, according to this histogram.

The choice of end points has a particularly marked effect of the shape of a histogram. For example, if the same bandwidth is used but with the end points shifted up to 0.25 and 0.75, then the histogram will look like the one displayed in Figure 23.

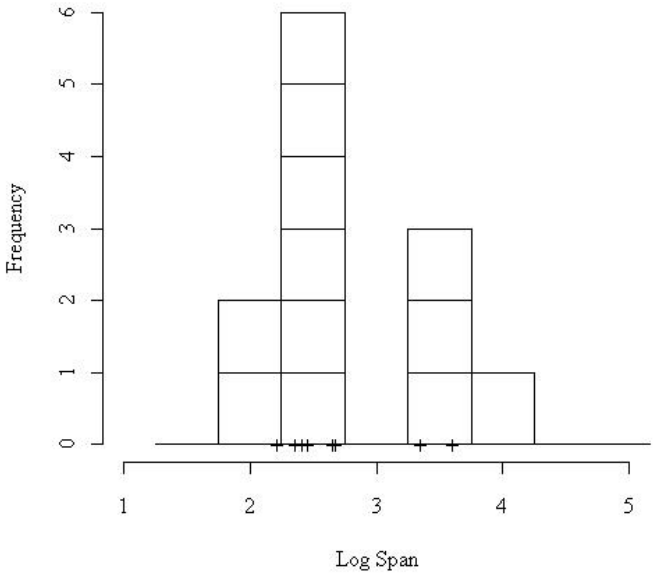


Figure 23 - Histogram with breaks at 0.25 and 0.75, bandwidth=0.5
Source: Doung (2001)

Now, the estimated density has a completely different shape - it now appears to be bimodal. These two examples are intended to show the properties of histograms. That is, the histograms are:

- Not smooth
- Depend on end points of bins
- Depend on width of bins

However, the first two examples can alleviate by using kernel density estimators (Hwang, Lay, & Lippman, 1994). To remove the dependence on the end points of the bins, each block is centered on each data point rather than fixing the end points of the blocks.

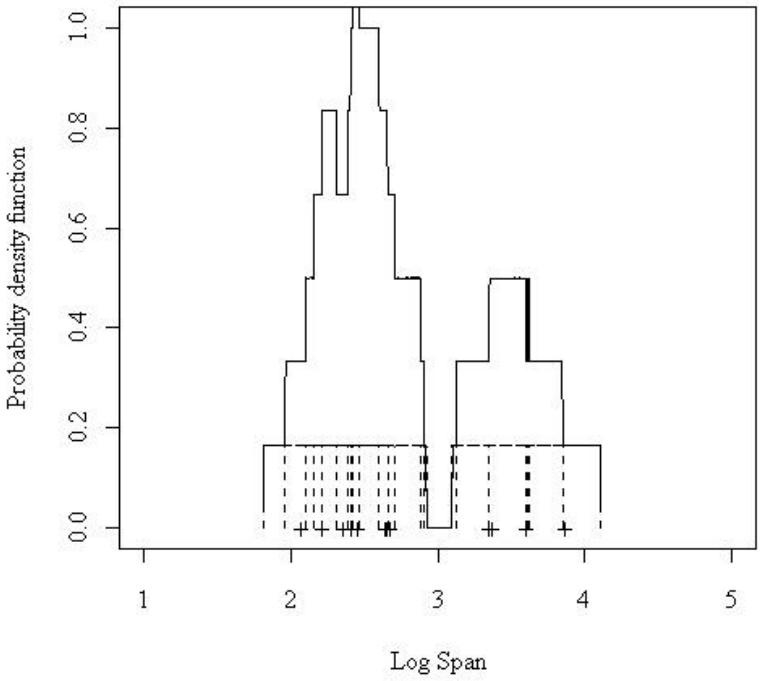


Figure 24 - Histogram with blocks centered over data points
Source: Doung (2001)

In the `histogram' of Figure 24, a block of width 1 and height 1/12 is placed (the dotted boxes) as there are 12 data points, and then they are added up (Wand & Jones, 1995). This density estimate (the solid curve) is less blocky than either of the histograms, as some of the finer structure is starting to extract. It suggests that the density is bimodal.

The estimated density at any point x will be:

$$\hat{f}(x) = \frac{1}{nb}\sum_{i=1}^{n} K\left(\frac{x-x_i}{b}\right) \tag{2.38}$$

Where K denotes the "kernel function", x_i the data points, n the number of data points and b the so-called bandwidth.

It is worth noting that even though the most widely used Kernel is Gaussian of zero mean and unit variance, there are various choices among Kernels as shown in the table below (Conlen, 2014).

Table 1 - Kernel functions

Kernel	$\boldsymbol{K(u)}$
Uniform	$\frac{1}{2} \quad to \quad \lvert u\rvert \leq 1$
Triangle	$(1-\lvert u\rvert) \quad to \quad \lvert u\rvert \leq 1$
Epanechnikov	$\frac{3}{4}(1-u^2) \quad to \quad \lvert u\rvert \leq 1$
Biweight	$\frac{15}{16}(1-u^2)^2 \quad to \quad \lvert u\rvert \leq 1$
Triweight	$\frac{35}{32}(1-u^2)^3 \quad to \quad \lvert u\rvert \leq 1$
Tricube	$\frac{70}{81}(1-u^3)^3 \quad to \quad \lvert u\rvert \leq 1$
Gaussian	$\frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}u^2}$
Cosine	$\frac{\pi}{4}\cos\left(\frac{\pi}{2}u\right) \quad to \quad \lvert u\rvert \leq 1$

Source: Chouaib (2015)

When working with Kernel estimator two choices must be made: the Kernel function K and the smoothing parameter or bandwidth h. According to Chouaib (2015) and Xu, Yan and Xu (2015) the choice of K is a problem of less importance, because K is not very sensitive to the shape of estimator, and different functions that produce good results can be used

The Kernel used in Figure 24 is known as box kernel density estimate - it is still discontinuous, as a discontinuous kernel has been used. If a smooth kernel is used for the building block, then it will have a smooth density estimate. Thus, the first problem with histograms can be eliminated. Unfortunately, the dependence on the bandwidth still cannot be removed (which is the equivalent to a histogram bandwidth).

It is important to choose the most appropriate bandwidth since a value that is too small or too large is not useful. If a normal (Gaussian) kernel is used with bandwidth or standard deviation of 0.1 (which has area 1/12 under each curve) then the kernel density estimate is said to be under smoothed as the bandwidth is too small in Figure 25. It appears that there are four modes in this density - some of these are surely artifices of the data.

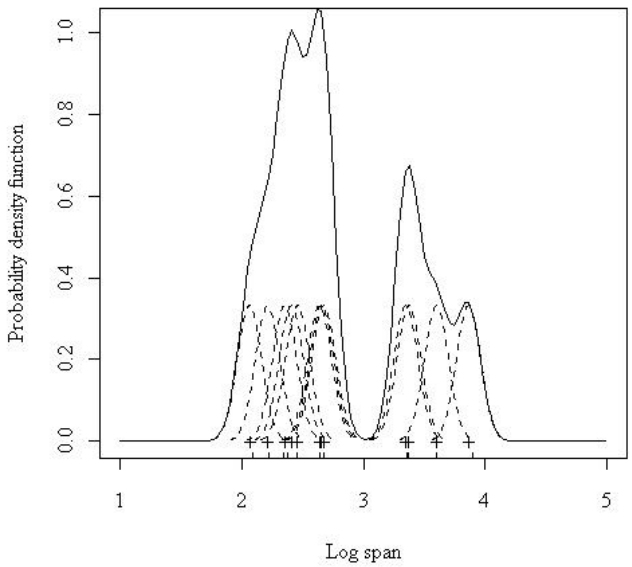


Figure 25 – Under smoothed
Source: Doung (2001)

We can try to eliminate these artifices by increasing the bandwidth of the normal kernels to 0.5. Then, a much flatter estimate with only one mode is obtained. This situation is said to be over smoothed as a too large bandwidth was chosen and have obscured most of the structure of the data.

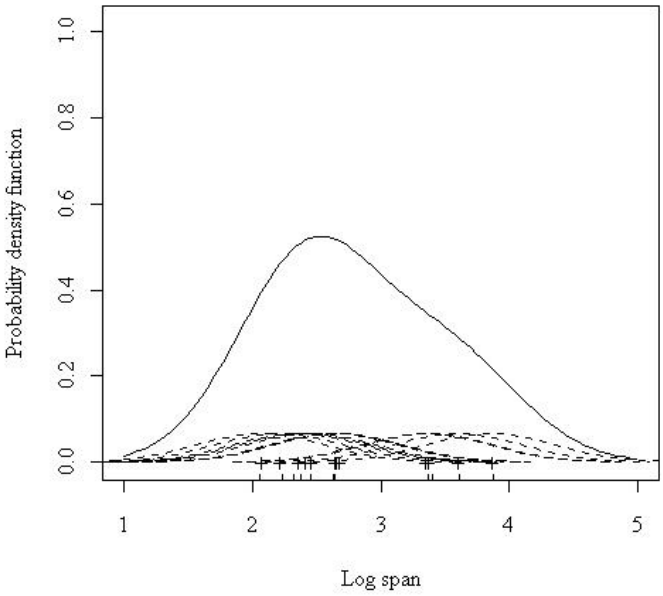


Figure 26 - Over smoothed
Source: Doung (2001)

So how does the optimal bandwidth is chosen? A common way is the use of the bandwidth that minimizes the optimality criterion (which is a function of the optimal bandwidth)

$$\text{AMISE} = \text{Asymptotic Mean Integrated Squared Error} \tag{2.39}$$

So then

$$\text{Optimal bandwidth} = \text{Arg min AMISE} \tag{2.40}$$

i.e. the optimal bandwidth is the **arg**ument that **min**imizes the AMISE.

In general, the AMISE still depends on the true underlying density (which is not known) and so it is necessary to estimate the AMISE from the data as well. This means that the chosen bandwidth is an estimate of an asymptotic approximation. It now sounds as if it is too far away from the true optimal value but it turns out that this particular choice of bandwidth recovers all the important features whilst maintaining smoothness.

A very simple formula for the bandwidth when using the rectangular kernel is:

$$b = 1.843sn^{-\frac{1}{5}} \tag{2.41}$$

Where s denotes the standard deviation of the data and n the sample size. If the normal kernel is used, then replace 1.843 by 1.059 (this is known as *Rule-of-Thumb*).

The formula is more robust if s is replaced by the robust estimate:

$$\min\left(s, \frac{interquartile\ range}{1.34}\right) \tag{2.42}$$

It is worth noting that the interquartile range is a measure of variability, based on dividing a data set into quartiles. Quartiles divide a rank-ordered data set into four equal parts. The values that divide each part are called the first, second and third quartiles; and they are denoted by Q1, Q2 and Q3, respectively.

Q1 is the "middle" value in the first half of the rank-ordered data set. Q2 is the median value in the set. Q3 is the "middle" value in the second half on the rank-ordered data set. The interquartile range is equal to Q3 minus Q1.

Regarding, the aircraft example, it can be concluded that the optimal value of the bandwidth for the dataset is about 0.25. From the optimally smoothed kernel density estimate, there are two modes. As these are the log of aircraft wingspan, it means that there were a group of smaller, lighter planes built, and these are clustered around 2.5 (which is about 12 m), whereas the larger planes, maybe using jet engines as the ones used on a commercial scale from about the 1960s, are grouped around 3.5 (about 33 m).

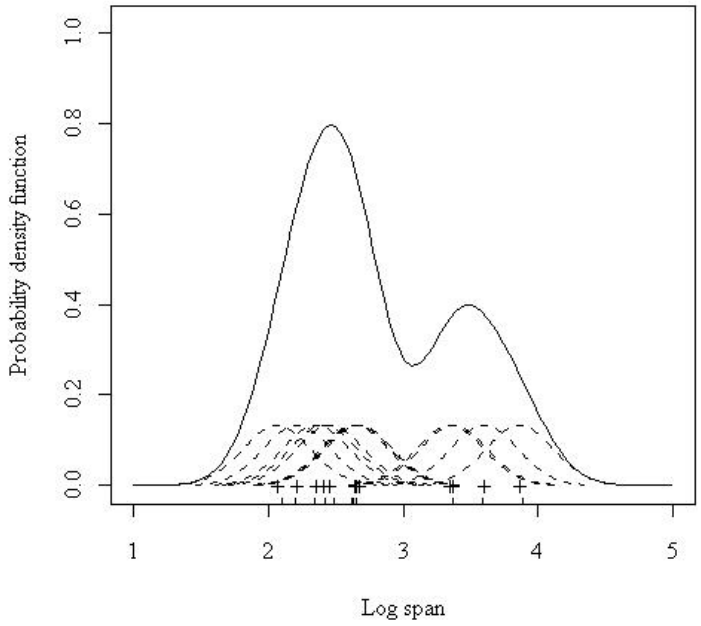


Figure 27 - Optimally Smoothed
Source: Doung (2001)

The properties of kernel density estimators are, as compared to histograms:

- Smooth
- No end points
- Depend on bandwidth

In short, it is worth noting that there are also rules based on over smoothed b, difference based b and others briefed by Jansseen et al (1995). Bhaveshkumar (2015) argues that a bandwidth selection rule that achieves precise bandwidth parameter at low computation is still open for research, and Schindler (2011) suggests that although the simplest *Rule-of-Thumb* is not the optimal bandwidth selector, this rule is used either as a very fast reasonably good estimator or as a first estimator in multistage bandwidth selectors.

In the case where the reader wishes to study more literature reviews about KDE and Bandwidth selection, some references are recommended as Sheather (1986), Silverman (1986), Park and Marron (1990), Park and Turlach (1992), Wand and Jones (1995), Jones, Marron and Sheather (1996) and Chouaib (2015).

3. DYNAMIC POSITIONING SYSTEM

Undoubtedly, the high demand for hydrocarbons has led humankind to increase exploration and production of oil and gas; and for many years, offshore natural gas and oil production was restricted to shallow waters such as the North Sea or coastal areas around the US. However, as many older deposits have become exhausted, companies have increasingly moved into deep waters (Lehmköster, 2014). Considering that the deeper waters represents harsher environment that requires special facilities for exploration and production, the *Dynamic Positioning System* has been introduced as the solution to maintain the position of offshore floating structures (Rasoulzadeh, 2015).

A dynamically positioned vessel (DP vessel) can be defined as "*a unit or vessel which automatically maintains its position (fixed location or predetermined track) exclusively by means of thruster force*" (IMO, 1994).

In this section, the DP systems history, different subsystems, components, and their operational aspects will be presented in detail. The chapter also covers the varying DP classes, the corresponding requirements, and redundancy in different classification societies.

3.1 History of DP system in the offshore industry

In 1961, the idea for mounting thrusters on vessels for position keeping was proposed by Willard Bascom. The vessel was called "CUSS 1 – Continental, Union, Superior and Shell oil companies" (shown in Figure 28), which was an exploration floating drill ship. The team of Bascom wanted to see if she could hold her position enough to do drilling without an anchor. In the meantime, Bill Bates who was the marine division manager of Shell and had worked in the CUSS 1 project, convinced Shell to build a small drilling ship with a position maintaining system (MTS, 2007). The vessel was name "Eureka" (shown in Figure 29).

Figure 28 - The “CUSS 1” Vessel
Source: Dynamic Positioning Committee (2012)

“CUSS 1” was equipped with four rotating thrusters, one at each corner. The direction and engine speed were manually controlled in addition to measuring the heading that had been controlled by compass. The test of CUSS 1 was done in Mach 1961 and was successful. She did drilling in 11,000 feet depth of water, and she could hold her position in a radius of 180 meters. The distance was measured by sighting inside the preassigned buoy ring (Dynamic Positioning Committee, 2012).

Figure 29 - The “Eureka” Vessel
Source: Dynamic Positioning Committee (2012)

The “Eureka” constructing ended up with two steerable thrusters that had 200 horsepower’s and electrically driven. In this case, the speed and direction of thrusters had been manually adjusted. However, the position could be checked on an oscilloscope by a dot in addition to visual sighting. The “Eureka” moved out from shipyard to the Gulf of Mexico in May 1961 for the first operation. Although, the first manual position test was not successful, however, when the system turned to the automatic, she could hold her position and start drilling operations (Dynamic Positioning Committee, 2012).

The popularity of the DP system was dramatically increased after good establishment in 1970 as the number of DP vessels reached 65 in 1980 and 150 in 1985. Nowadays, the exact number of DP vessels in the world is not known, however, professionals guess over 2000 DP vessels worldwide are in operation (Dynamic Positioning Committee, 2012).

3.2 Operational modes of a DP system

Since a vessel in the marine and offshore environment is exposed to different external forces, namely waves, current and wind, she needs to have a system to keep her correct position for properly doing her operation. Furthermore, each and every floating vessel has six degrees of freedom. Three of these are rotational including *pitch, roll and yaw* motions in addition to three translational, which are *heave, surge and sway* motions. Only the surge, sway, and yaw are the concerns for the DP system as the surge and sway are related to the vessel position, and yaw is associated with the vessel heading (Rasoulzadeh, 2015).

For both position and heading, a set point is predetermined regarding the vessel operation. In addition, the real value of vessel position is measured by position references while gyrocompasses record the real value of vessel heading. The deviation between the set point and measured value for both position and heading is called error or offset that must be minimized as much as possible by the DP system. The environmental forces and relevant vessel motions can be seen in Figure 30.

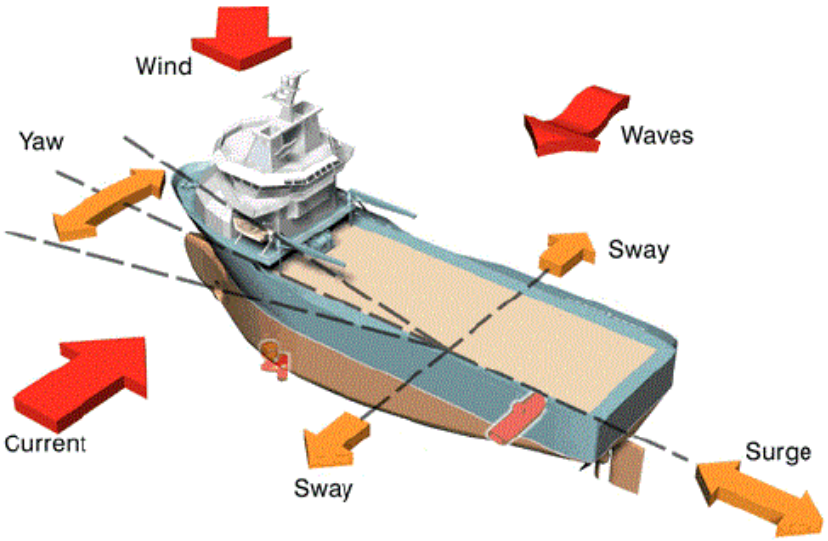


Figure 30 - Basic external forces and relevant vessels motions
Source: Dynamic Positioning Committee (2012)

A dynamic positioning system includes all equipment and components that support the automatic vessel position maintaining and correcting. For automatic position correction by DP system, a computational facility must be utilized for processing and doing calculations. The computer program in a DP system is a mathematical model of the vessel that contains some vessel characteristics such as positions and capacities of thrusters. Moreover, the data, which is collected by wind sensors, position reference sensors, motion sensors and gyrocompass, is sent to the computer and will be merged and analyzed with the default information of software. The outcome of the computational program is the determination of direction, angle, and amount of power that thrusters shall produce for maintaining or correcting the vessel position.

In addition to keeping the pre-assigned position and heading, a DP system should be capable of adjusting the position and heading with respect to the new data that are given by DP Operator (DPO). The DPO can also tune the speed of vessel during correction action. This operational aspects and Functional Diagram of DP system are detailed in section 3.3.

3.2.1 DP based on PID regulator

This DP system is only able to correct the position of a vessel when some deviation has actually happened. In other words, the system is not smart enough to predict some external forces, which can cause vessel movement. Thus, PID regulator can only correct the errors between the actual position/heading and the predetermined one (Holvik, 1998).

3.2.2 DP based on Model control

This system is more robust against external loads and system parameters changes than the previous one. It can predict the amount of deviation that is going to happen. The possible deviation can be prevented from occurring by providing the proper thruster power, angle, and direction. It means that the model-based control DP system tries to keep and maintain the position in advance rather than correcting an occurred deviation. The prediction of position/heading deviation can be done since the vessel sensors continuously read and record wind, wave, and current data. Those data is given to the computer as an input to process and calculate the thruster action, which must be taken before the vessel deviates (Holvik, 1998).

Further, there is another capability for the model control DP system called *dead reckoning* (DR) mode or memory. This system can hold the vessel in a position in case of losing all the reference systems. Because of receiving the last data that is available in the system memory, keeping the position is possible when the reference systems are deteriorate. It should be noted that the duration of position keeping in case of failure of the reference system is short (5-15 minutes) depending on environmental conditions and external forces. However, the DR system helps DPO by taking the right action and for not being a rush to change the system operation from automatic to manual (IMCA, 2007).

3.3 Typical configuration of DP System

The DP systems comprise three subsystems: power, thruster and control; additionally, there is a set of auxiliary subsystems that support the operation of these main subsystems. The general structures of each subsystem and generic configuration for DP systems are presented below; they follow the structures established by international standards and guidelines (IMO, 1994), (MTS, 2012), (ABS, 2013) and (DNV, 2013).

Power subsystem means all components and systems necessary to supply the DP system with power. The power subsystem includes:

- Generators and movers with necessary auxiliary subsystems; the purpose of mover-generators is to convert kinetic energy from the motor into electrical energy in the form of alternating current and voltage.

- Power Management System – PMS; this system is designed to control and monitor the electric power production and consumption on-board a vessel (MTS, 2012). The PMS is mainly responsible for the automatic start-up or shutdown of the generators, tripping of non-essential consumers and share load between generators (D. Ferreira, 2016). It should be noted that PMS is not a requirement for all classes of DP systems.

- Switchboards; the switchboard refers to a large single panel, assembly of panels, a structural frame or assembly of structural frames, on which buses, switches, protective and other control devices may be mounted. The main role of the switchboard is to allow the incoming electric power to be divided into smaller independent circuits according to their current requirements. The circuit breakers as well as over current protection devices for each of the sections are selected according to the load current (Coast, 2012) and (IEM, 2017). The main components of the switchboard are:
    - Circuit breakers that serve to protect equipment in case of overload. The circuit breaker protects the generators and thrusters.
    - Control and monitoring devices such as synchronizers, protection relays, power transformers, and others.
    - Bus tiebreakers (high voltage bus bar interconnects circuit breakers) are programmed to open and isolate the fault, restricting the effect to the faulty bus.
    - Panels or frames to hold devices such as switches, circuit indicators and other devices that allow the delivery of power and circuits controlling (Schonek, 2017).

- A bus bar is a breaker that can be closed to connect two separate systems together (the bus bar connects the switchboards). It should be noted that the bus bar is not a requirement for all classes of DP systems.

- Distribution system:

  - Emergency switchboard, which shall ensure the power supply to critical components of the control subsystem and the thruster subsystem, for a predetermined period in the event of failure of the main switchboard.
  - Emergency generator and motor, responsible for power supply to the emergency switchboard solely.
  - Cabling and cable routing, cabling is used to carry electrical current between electronic devices and cable routing is designed to route and manage copper data cables, fiber optic cables and power cables within the switchboard (PANDUIT, 2014).

The structure of power subsystem is shown in Figure 31. As previously mentioned, the PMS and bus bar are not presented as minimum requirements for all classes of DP systems and for this reason, they are marked with discontinuous lines in Figure 31.

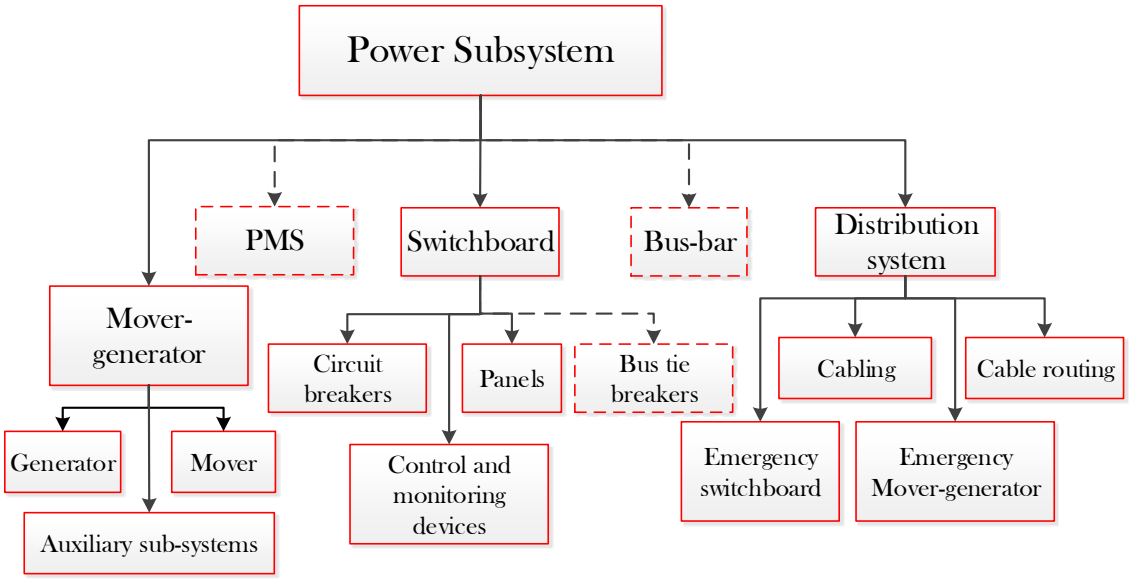


Figure 31 - General structure of a power subsystem in DP system

Thruster subsystem means all components and systems necessary to supply the DP system with thrust force and direction. The thruster subsystem includes:

- Thruster with drive units and necessary auxiliary subsystems. The required amount of thrusters is not specified in the structure below because the international standards consulted only state that thrusters must ensure adequate thrust in longitudinal and lateral directions, and provide yawing moment for heading control, but do not establish neither type nor quantity of thrusters. In general, three types of thrusters are common in the offshore industry: conventional, tunnel or azimuth thruster.

- Main propellers and rudders (if these are under the control of the DP system).

- Thruster control electronics, whose purpose is the constant monitoring of the operational parameters of the thruster.

- Manual thruster controls; this system is to be independent of the DP control systems so that it will be operational if the automatic control systems fail. The system is to provide an individual lever for each thruster and to be located at the main DP control station. This system also includes the emergency stop buttons, that is, an emergency stop facility for each thruster is provided at the main DP control station, and the emergency stop facility is to be arranged to shut down each thruster individually. The emergency stop activation buttons are to be placed in a dedicated mimic representing the thruster location and which is consistent with the vessel axis and layout, or they may be arranged together with the corresponding thruster levers if these are arranged in accordance with the physical thruster layout. Since an accidental operation of the emergency stop buttons can occur, a protective cover is to be mounted (ABS, 2013).

- Cabling and cable routing: cabling is used to carry electrical current between devices and cable routing is designed to route and manage copper data cables, fiber optic cables and power cables within electronic components.

The Figure 32 show the structure of the thruster subsystem.

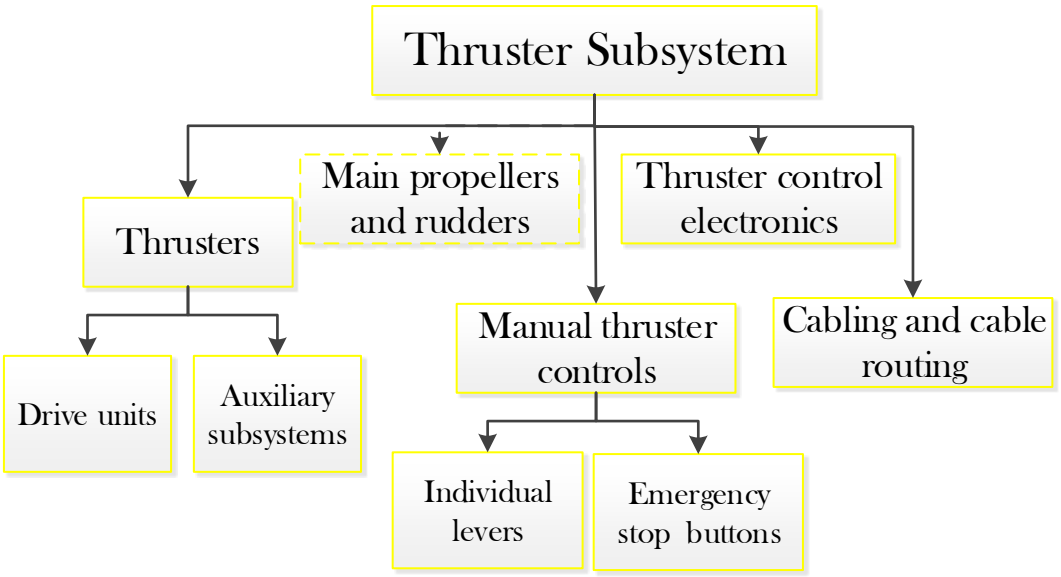


Figure 32 - General structure of a thruster subsystem in DP system

Control subsystem means all components and systems, hardware and software necessary to dynamically position the vessel. The DP control subsystem consists of the following:

- Position reference system - PRS; all hardware, software and sensors that supply information necessary to give position reference. They may vary due to the nature of the principle used to obtain the positioning data, i.e. they may be hydro acoustic (USBL, SSBL), satellite (DGPS, GLONASS), laser (Fan beam, CyScan), mechanical (Taut wire) or radar (Artemis, RADius, RadaScan). Regardless of the principle of data collection, the PRS has an alarm subsystem (visual and audible) in common, which indicates the operational status of the DP and software that stores and processes all information.

- Uninterruptible Power Supply Systems – UPS; used as filters between the power system and the control system in order to absorb current peaks (Rappini, S., Pallaoro, A., & Heringer, 2003). However, its main function is to provide battery backup power to the DP system, and for this purpose, the UPS is to be capable of supplying power for a minimum of 30 minutes after failure of the main power supply.

- Computer system consisting of a highly complex software composed of a series of estimation and control algorithms, a joystick lever that centralizes the manual position control and automatic heading control, an interface (a transfer point at which information is exchanged), a peripheral (a device performing an auxiliary function in the system, e.g., printer, data storage device) and a display system (or operator panel).

- Cabling and cable routing, cabling is the connection between computer networks, and cable routing is designed to route and manage copper data cables, fiber optic cables and power cables within the main components (computers, IJS, PRS, etc.).

- Environment sensors; a system comprising devices that measure vessel heading (such as gyrocompasses), vessel motions (such as Motion Reference Unit – MRU, also called Vertical Reference Sensor - VRS), and wind speed and direction.

- Independent Joystick System – IJS; the DP vessel must have a manual position control system independent of the control computers of control subsystems and it cannot rely on common cabling. The system is to be arranged such that it will be operational if the main controllers of control subsystem fail. The system provides one joystick for manual control of the vessel position and provided with the arrangements for automatic heading control, that is, when using the IJS control the operator has limited modes available and tends to be controlling most of the vessel axes using manual commands from the joystick and heading selection control; however some aspects of the thruster control may be under automatic control e.g. control of heading (LLC, 2009). As the IJS must be able to operate as a simple DP system, it has similar equipment to the control computers, but it is important to emphasize that the IJS presents three basic differences in relation to the control computers; First, the IJS has an independent cabling connection for each driver (it does not share the connection of the control computers); second, the IJS software is simpler, because while the control systems software must incorporate the "judges", that is, self-diagnosis and decision-making, the IJS software is not equipped with these algorithms, keeping only the coordinates pre-established by the operator. And third, if the vessel position

has to be controlled from the IJS, it will be necessary to disconnect the well, because the IJS only operates with the PID regulator principle.

Figure 33 shows the structure of the control subsystem.

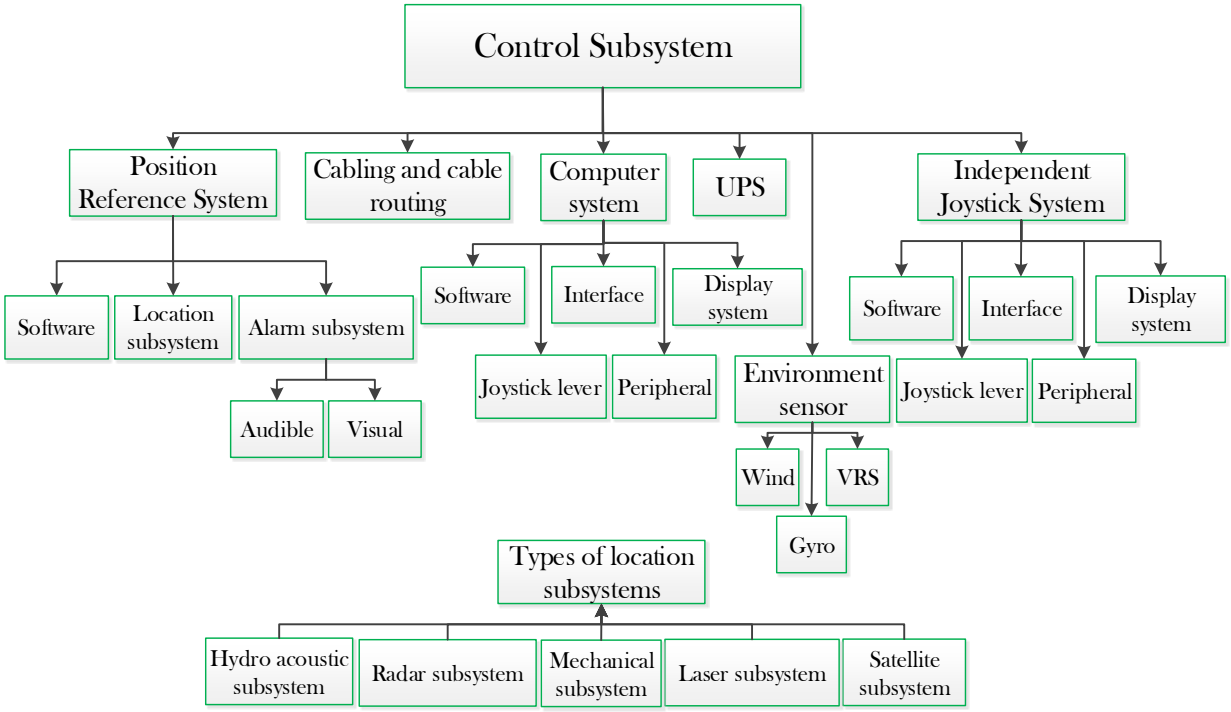


Figure 33 - General structure of a DP control subsystem in DP system

Finally, the standards state that the design of the auxiliary subsystems, which support the operations of the main subsystems (power, thruster and control), must comply with the requirements of the vessel mandatory classification notations. Therefore, the auxiliary subsystems are considered in this study. Figure 34 shows the structure of the auxiliary subsystems.

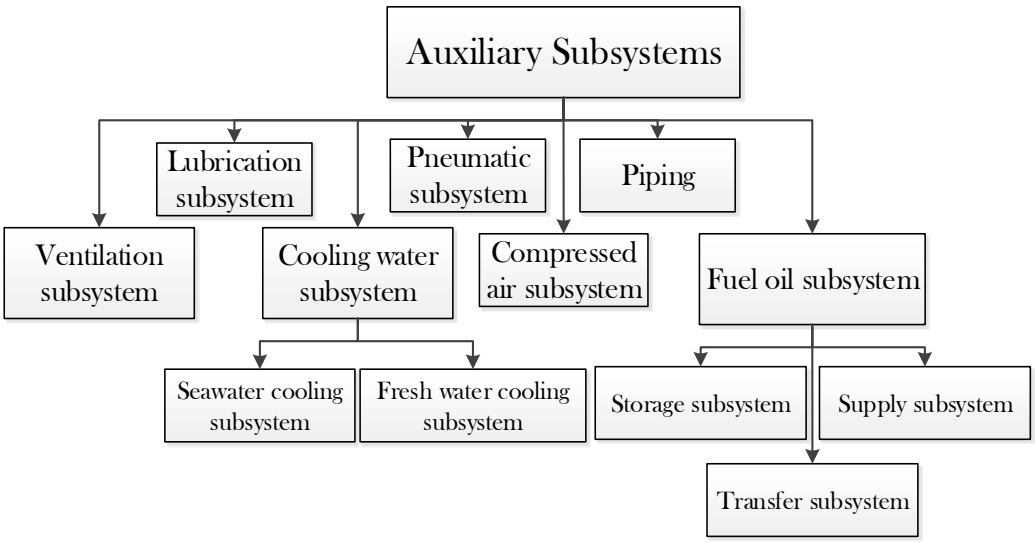


Figure 34 - General structure of auxiliary subsystems in DP system

Each auxiliary subsystem has a specific function:

- Ventilation (High Volume Air Conditioning - HVAC): the purpose of this subsystem is keeping the temperature controlled in the spaces containing equipment essential to DP. Thus, each engine room has supply fans responsible for supplying the combustion air for the engines and the required air for heat mission, while the thruster columns are ventilated by supply and exhaust fans, and refrigerators to improve compartments cooling.

- Lubrication: this subsystem fulfills two main functions; it is responsible for the maintenance and renewal of the oil between the internal bearings of the engines (in the mover-generators) and must ensure the circulation of the oil in the thrusters in order to assist their driving.

  Figure 35 shows the main components of the lubrication oil subsystem in a motor-generator.

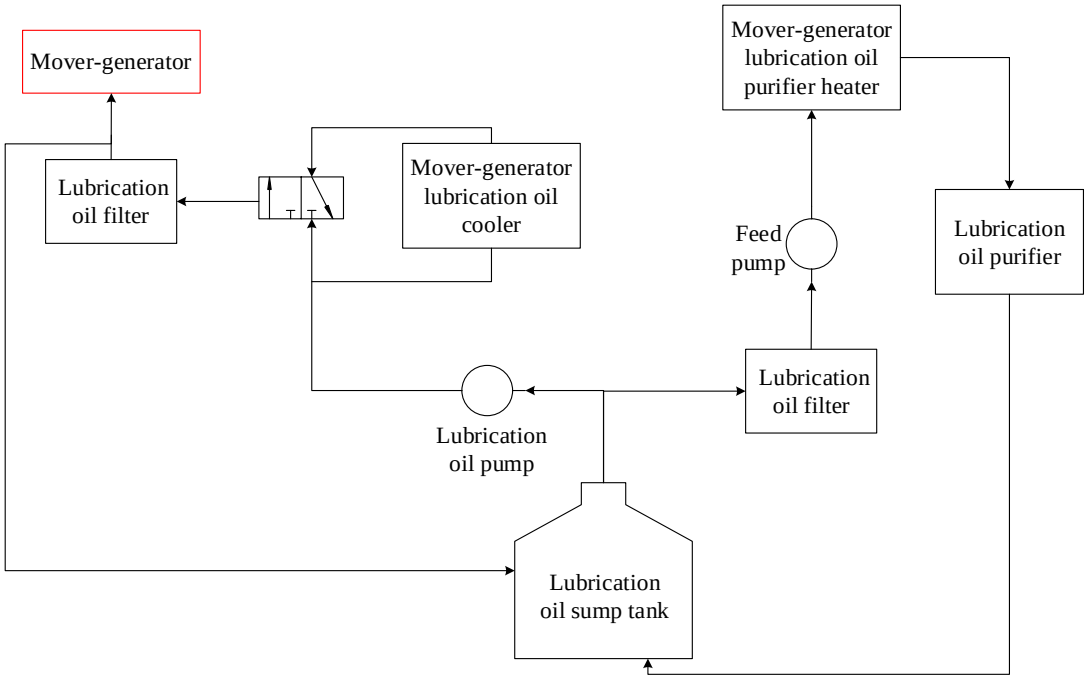


Figure 35 - Lubrication oil subsystem diagram for a mover-generator

A lubrication oil pump draws the oil from the lubrication oil sump tank and supplies pre-lubrication oil to an engine when it starts. But during normal operation a lubrication oil pump draws lubrication oil from the sump tank; and depending upon the temperature of lubrication oil, part of the oil passes through the 3-way valve into the lubrication oil cooler and the cooled oil enters through the 2nd port of the 3-way valve and enters the engine through a filter for lubricating the engine parts. Lubrication oil supplied to mover-generator returns to the tank itself after being used and purified by the lubrication oil purifier. The purified lubrication oil is stored in the sump tank attached to the engine casing.

Figure 36 shows the main components of the lubrication oil subsystem in a thruster.

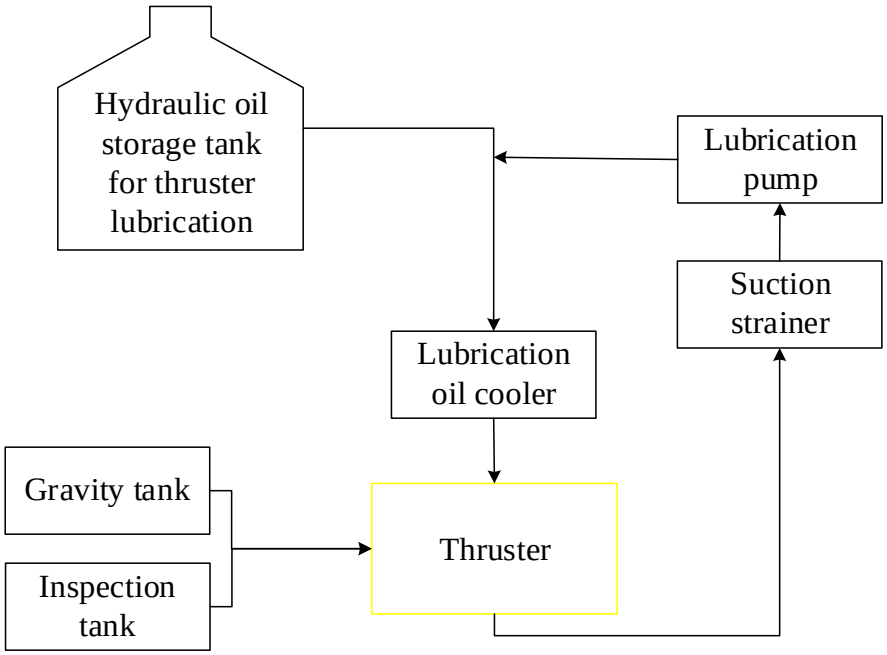


Figure 36 - Lubrication oil subsystem diagram for a thruster

The thrusters have lubrication units, in these units a pump provides power to circulate oil from inside thruster to the lubrication oil cooler; the suctions trainer is like a filter and removes impurities of the oil. The lubrication oil cooler makes oil temperature down in order to maintain setting temperature of oil inside thruster. The lubrication oil subsystem in the thrusters has two tanks in order to help with the lubrication oil supply. These tanks are the gravity tank and the inspection tank. The gravity tank serves two major functions. The first is that the gravity tank complements fluctuations of oil in a thruster, which is caused by expansion or contraction due to temperature. The other is to provide oil to the steering seal and the shaft seal. The inspection tank provides oil to seal and checks seal conditions.

- Cooling water subsystem: responsible for controlling the high temperatures in the mover-generators and the thrusters. The cooling water subsystem consists of seawater (SW) and fresh water-cooling subsystem (FW). FW cooling subsystem takes heat from mover-generators, auxiliary equipment, and thrusters; and SW cooling subsystem removes heat from the FW cooling subsystem overboard.

Figure 37 and Figure 38 show the general operation of the refrigeration subsystem in a motor-generator and a thruster, respectively.

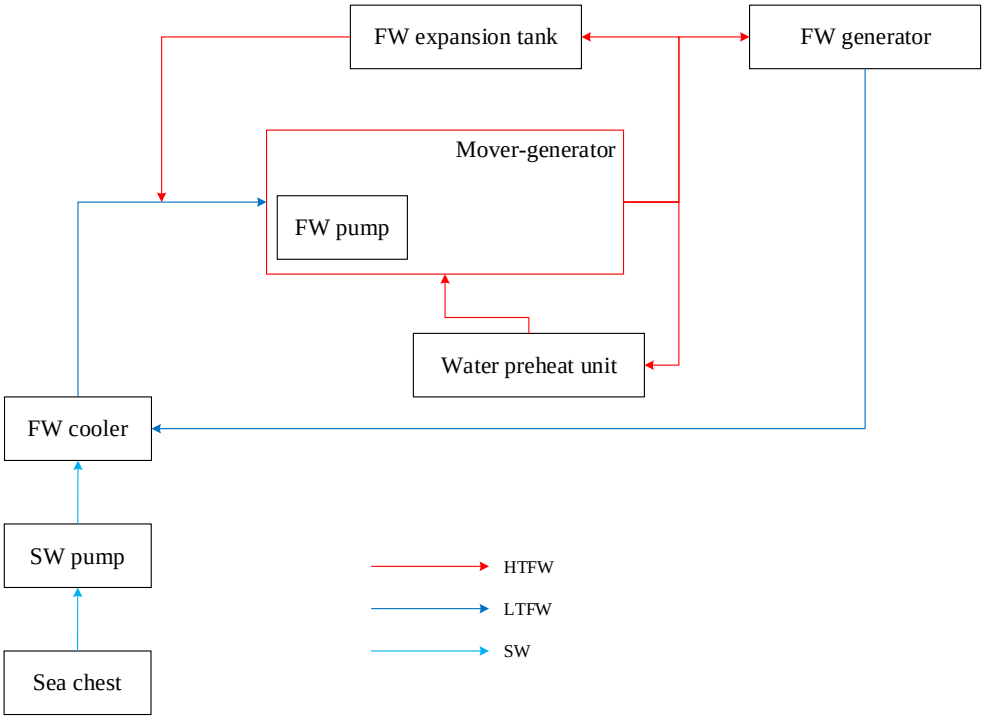


Figure 37 - Cooling water subsystems diagram for a mover-generator

The SW subsystem consists of sea chest, cooling seawater pump and fresh water cooler. The cooling seawater pump supplies SW into FW coolers, and the outlet from the coolers is discharged directly overboard.

The FW subsystem consists of a fresh water expansion tank, FW pumps and a water preheat unit. The expansion tank supplies fresh water with static pressure and serves as a buffer for thermal expansion. The used cooling water goes to the FW cooler, where a pneumatic 3-way temperature control valve controls the water in the coolers to maintain the set point temperature of the loop.

The FW cooling subsystem in the engine rooms is divided into low temperature (LTFW) cooling and high temperature (HTFW) cooling.

The LT cooling water is circulated through consumers by LTFW pumps; these pumps provide LT cooling water to the mover-generator inside. After cooling by LT cooling water, the mover-generator discharges high temperature water. This high temperature cooling water goes to a preheater unit and a fresh water generator. The fresh water generator uses this thermal energy to generate fresh water from seawater.

With respect to the thruster cooling subsystem, there are pumps that raise seawater from a bottom and transfer it to cooler. The cooler is a heat exchanger and exchanges heat between SW and FW. After heat exchanging, SW is directly discharged overboard.

At the outlet of the FW cooler, an actuated 3-way control valve recirculates the water in it to maintain the temperature at 36 ºC. Finally, a pump transfers cooling water to thruster components.

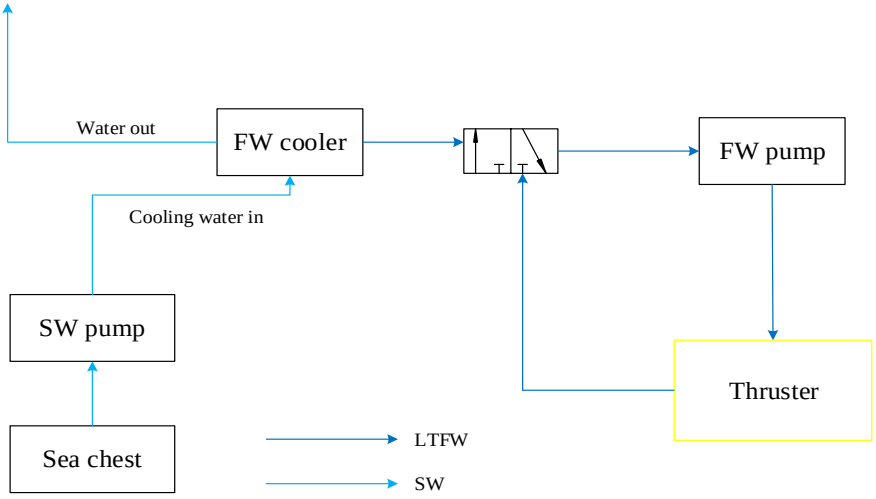


Figure 38 - Cooling water subsystems diagram for a thruster

- Pneumatic subsystem: it is an auxiliary system of the thrusters. Commonly, the shaft brake system of thrusters is a pneumatic system that uses compressed air to engage the shaft brakes.

  In order to clarify the function of the pneumatic subsystem, Figure 39 shows an example of the brake system in an azimuth thruster.

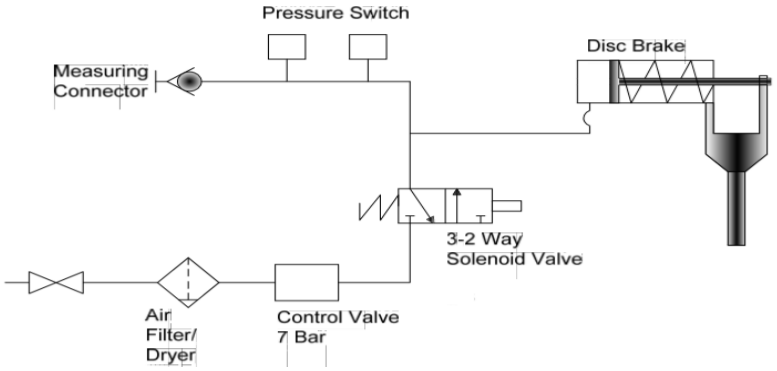


Figure 39 - Pneumatic diagram of the shaft brake system

The shaft brake system is a pneumatic system that uses compressed air to engage the shaft brakes (air on/spring off with pressure switches used to determine if brake is applicable). The control valve in the pneumatic shaft brake system limits the pressure in the system to 7 bar. When the thruster must be stopped, the 3-2 way solenoid valve is activated to allow compressed air to engage the shaft brakes.

- Fuel oil subsystem: responsible for supplying fuel to the mover-generators. This subsystem can divide into "storage", "purification" and "supply". The storage subsystem allows segregation of fuel using fuel oil storage tank and transfers pumps. The purification subsystem consists of pumps, purifiers, filters and service tanks, while the supply subsystem is composed of supply pumps, fuel oil coolers and suction filters. Figure 40 shows the components and the fuel flow between each of the subsystems.

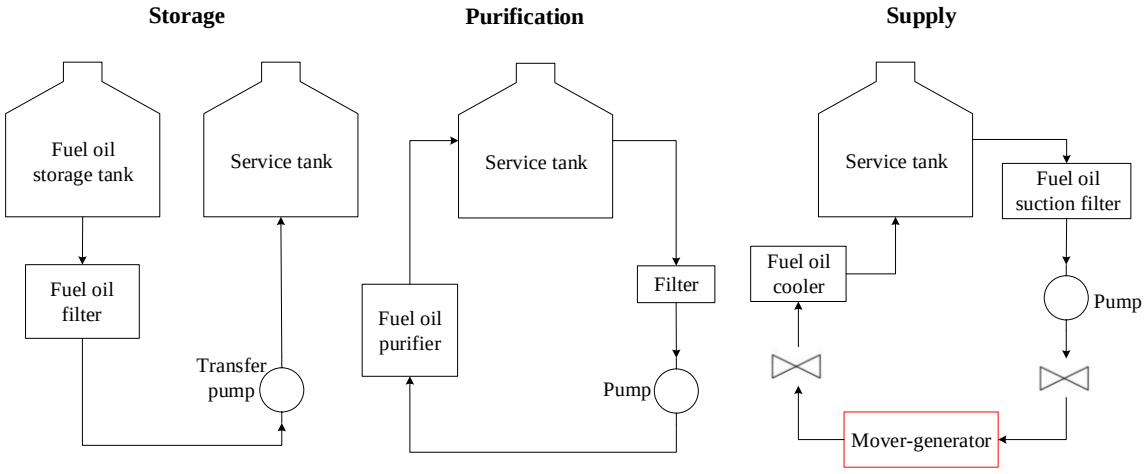


Figure 40 - Fuel oil subsystem diagram for a mover-generator

- Compressed air subsystem: this subsystem supplies air to the engines of the mover-generators. The major purpose of starting air is to generate driving force when engine starts and also provides engine control air and jet assist air to mover-generators.

- Piping: This item refers to the set of ducts and pipes between the different subsystems.

Figure 41 shows the general configuration of the main subsystems in a DP vessel and the three main subsystems described above [power (red), thruster (yellow) and control (green)]. Notice that the auxiliary subsystems do not appear in this figure, since its operation is to support the main components (mover-generators and thrusters), because the purpose here is to show only a general configuration.

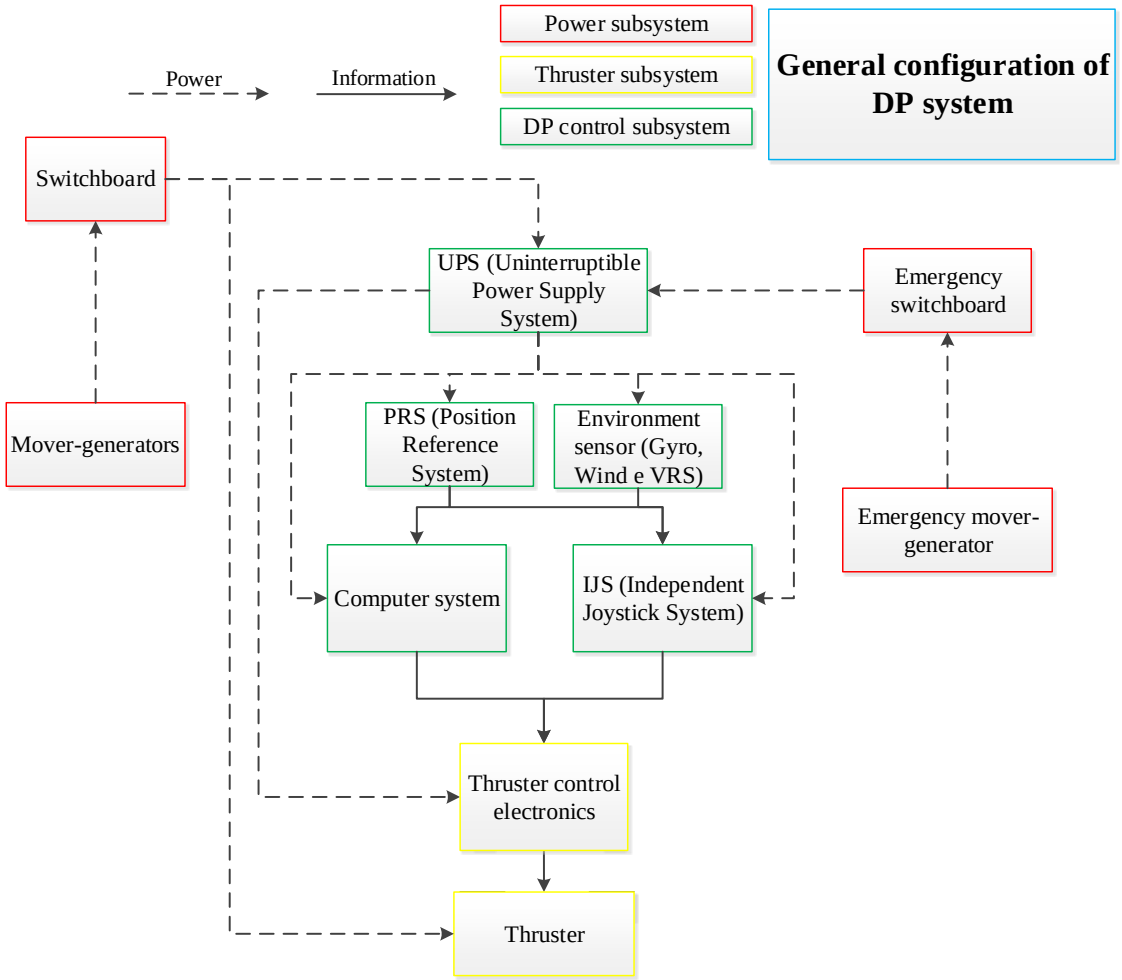


Figure 41 - General configuration of DP system

As can be seen from Figure 41, the DP system power is produced in mover-generators and then arrives at the switchboard, where it is redirected to the control and the thruster subsystems.

In order to supply power to the control subsystem equipment, the switchboard filters power through UPSs to absorb current spikes (Rappini, S., Pallaoro, A., & Heringer, 2003). In the event that the mover-generators fail, an emergency power source will provide power to the UPSs in order to maintain control of vital components.

However, it should be noted that the emergency mover-generator (the reserve mover-generator) would not have sufficient power for running the thrusters (Rasoulzadeh, 2015). This is due to high power consumption of thrusters.

In relation to the flow of information, the control computers receive information from two sources: the environment sensors (Gyro, Wind and VRS) and PRS. The computer processes all the information and sends signals to the electronic controls of the thruster subsystem.

The DP vessels should have an alternative manual control of the thrusters for the case where all control computers fail; to ensure this, there is an IJS, which is directly connected to the electronic controls of the thruster subsystem, and the UPS powers it. Additionally, as previously commented, the IJS receives information from some of the environment sensors and PRS.

Finally, once the information and power are transmitted to the electronic controls of the thruster subsystem, these equipment send the information to the thrusters in order to reach the directions and commands previously established, and to obtain control of the vessel position.

3.4 Classification of DP systems

The DP systems may be assigned with different classification notations depending on the degree of redundancy built into the subsystems. The DP classes are DPS-1, DPS-2 and

DPS-3. For the DPS-1, loss of position may occur in the event of a single fault (IMO, 1994). Figure 42 shows the typical configuration of DPS-1.

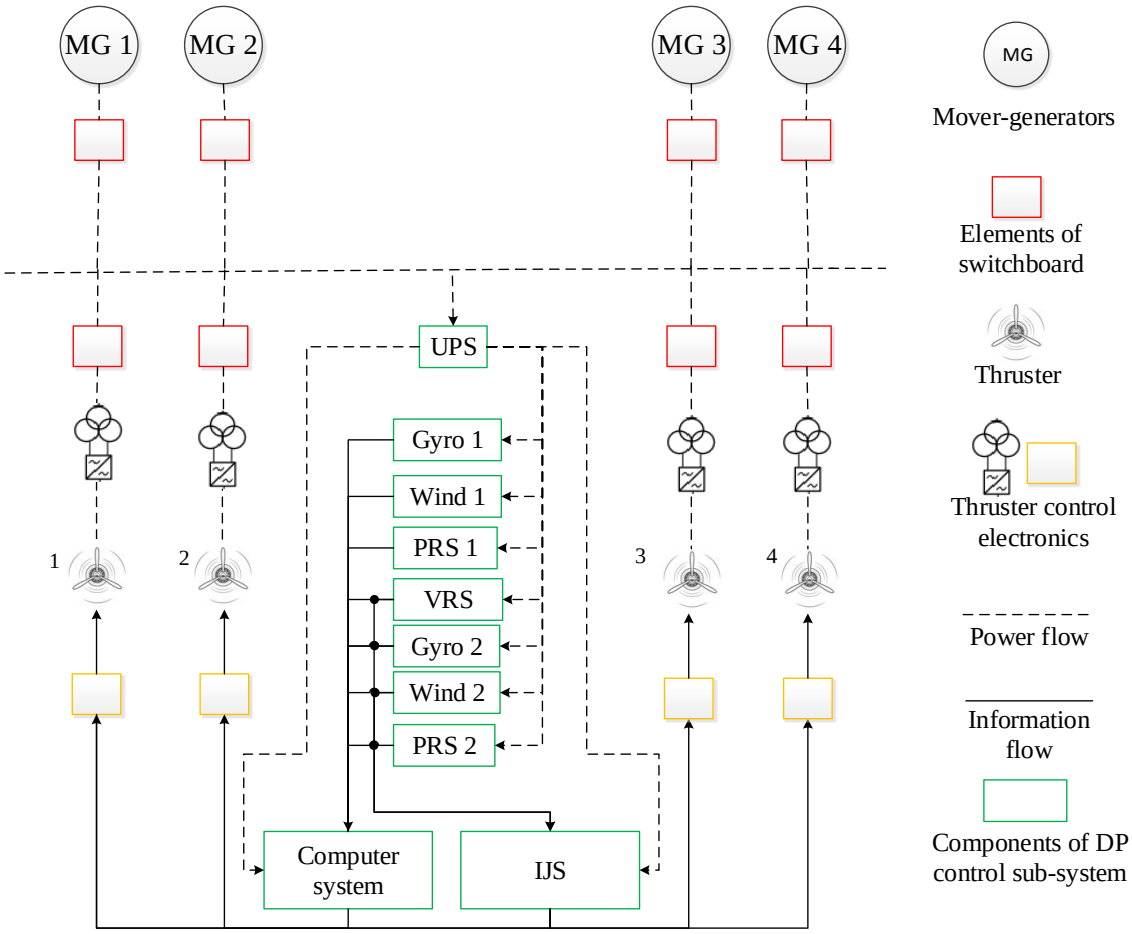


Figure 42 - Typical configuration of DPS-1

Figure 42 is a representation of the minimum requirements for DPS-1 recommended by international standards and guidelines; thus, the IJS needs the information from part of the sensors in order to allow it to operate as an independent DP system if required. However, it is important to mention that not all sensors will send information to the IJS (some will send information only to the computer system).

The following requirement is not represented in Figure 42 in order to better synthesize the information. However, it is worth noting that the ABS (2013) guide recommends that in DP vessels each UPS should have a main power supply and a backup supply from the emergency switchboard.

For the DP systems class 2, a loss of position is not to occur in the event of a single fault in any active component or subsystem (mover-generators, thrusters, switchboards, remote controlled valves, etc.) (IMO, 1994). Figure 43 exposes the typical configuration of DPS-2.

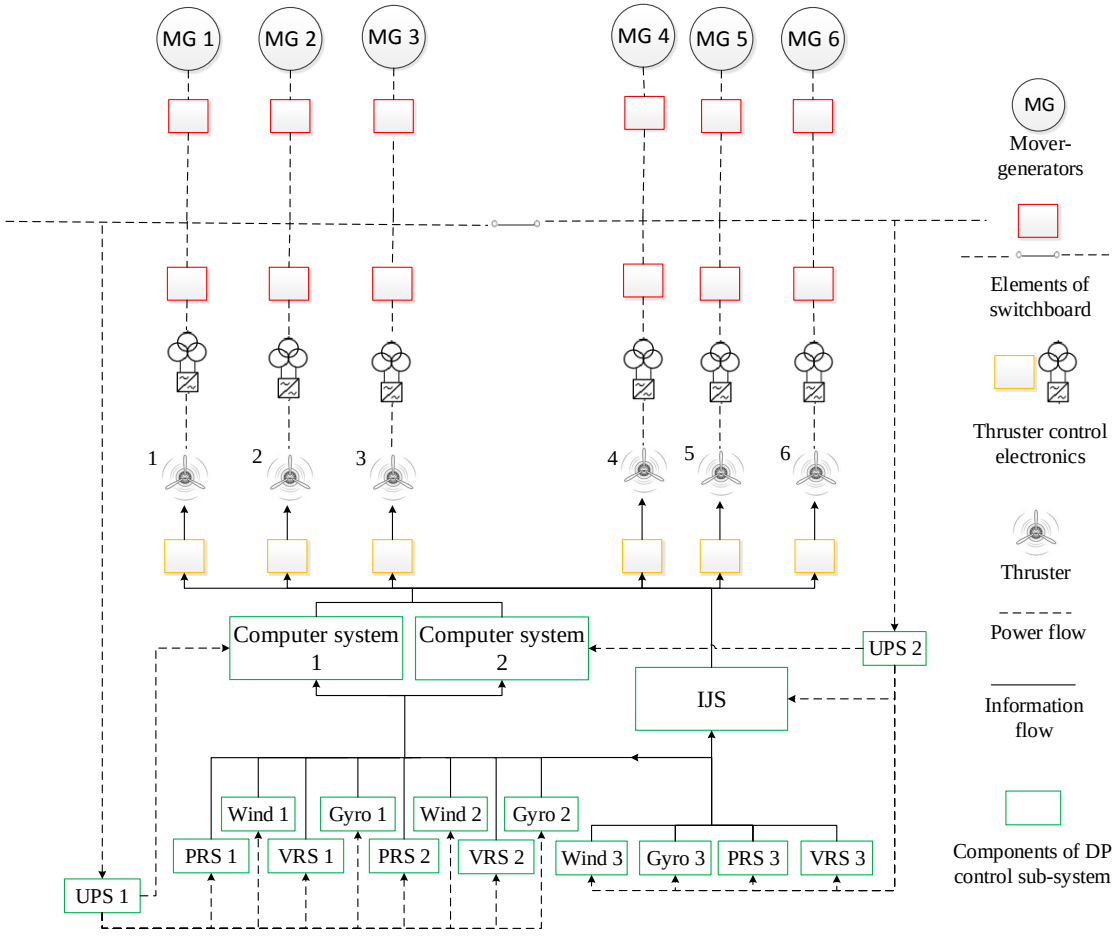


Figure 43 - Typical configuration of DPS-2

Figure 43 has been elaborated considering the minimum requirements for DPS-2 recommended by (IMO, 1994), (ABS, 2013) and (DNV, 2013). As this figure is a generic representation, the diagram indicates that the IJS is powered by one of the UPSs, which in this case was identified as UPS2, even so, it does not have to be this one in particular that provides energy for it; the same is valid for the representation of the third sensors (Wind3, PRS3, VRS3 and Gyro3), which only represents that some sensors are going to send information to the computer systems and the IJS.

In addition, the ABS (2013) guide recommends that DP vessels must have an emergency switchboard to provide power to the UPSs in case of failure of the main switchboards. This requirement is not represented in Figure 43.

The minimum required number of each of the items for the DP system class 2 is shown in Table 2.

Table 2 - The minimum required number of each of the items for DPS-2

DPS-2		
Subsystem	**Item**	**Quantity**
Power subsystem	Mover-generators	Redundant*
	Switchboard	1
	Bus-tie breaker	1
	PMS	Yes
Thruster subsystem	Rudders	Redundant*
	Thrusters	Redundant*
	Single lever for each thruster at main DP-control center	Yes
DP control subsystem	Gyro	3
	Wind	3
	UPS	2
	VRS	3
	PRS	3
	IJS	Yes
	Computer system: number of control computers	2
	Consequence analyzer	Yes

* The IMO (1994), ABS (2013) and DNV (2013) guidelines recommend redundancy but do not specify the exact amount of components.

In general, the DPS-1 and DPS-2 are similar; but a DPS-2 presents redundancy, i.e. redundancy means ability of a component or system to maintain or restore its function, when a single failure has occurred. Redundancy can be achieved, for instance, by installation of multiple components, systems or alternative means of performing a function (IMO, 1994).

The differences between the power subsystem DPS-1 and DPS-2 are: the DPS-2 presents redundancy in its mover-generators and the switchboards has a bus-tie breaker, while the DPS-1 switchboards do not have this element. Also, IMO (1994) states that for

DPS-2 vessels, the power subsystem must have a PMS, which is not a minimum requirement in DPS-1 vessels.

In a DPS-2 the bus can operate open or closed (MTS, 2012) and (DNV, 2013); closed bus often describes an operational configuration where all or most sections and all or most switchboards are connected together, that is, the bus-tie breakers between switchboards are closed. The alternative to closed bus is open bus, sometimes called split bus or split ring. Closed bus is also called joined bus, tied bus or closed-ring (ABS, 2013).

The main advantage of operating with the closed buses is that this gives a higher average load on the mover-generators, making it possible to save fuel and attenuate the effects of carbonization on the movers. In the event of a fault when operating with closed buses, the bus tiebreakers are programmed to open and isolate the fault, restricting the effects alongside the faulty electrical circuit. This type of configuration requires a more sophisticated protection system in order to ensure that even severe failures do not cause a total blackout. The advantage of operating with the open buses is that even severe failures in the system do not cause a total blackout of the unit, since the operation takes place through sections of the electric circuit completely isolated / insulated. In general, this setting is recommended for operations with higher degrees of criticality. The circuit breakers responsible for connecting or isolating certain electrical circuit equipment are located inside the switchboard (D. Ferreira, 2016).

Regarding the differences of the thruster subsystems of DPS-1 and DPS-2, DNV (2013) recommends that DPS-2 shall be transverse and longitudinal thrust, and have a yawing moment after any single failure.

As for the control subsystem, the DPS-2 should have at least two UPSs and the DPS-1 should have one; the DPS-2 should have at least two control computers (each receiving the same information and operate in parallel, i.e. all controllers independently compute required information to maintain station and pass this information to the thrusters control electronics); while the DPS-1 should have one control computer. DPS-2 has an additional PRS for the DPS-1, which must comply with the diversity rule (where more than two PRS are required, at least two are to be based on different measurement techniques, i.e. the nature of the

principle used to obtain the positioning data; and each of the two are to be independent with respect to signal transmission and interfaces) (IMO, 1994); (ABS, 2013). It should be noted that all PRSs are connected to both control computers.

Another difference in the control subsystem is that the DPS-1 should have at least a VRS while the DPS-2 should have at least three. In addition, DPS-2 control computers have a program called "consequence analyzer", which is a software function that issues an alarm if the vessel is not able to keep position and heading after predefined worst-case failure should occur at current operation mode and weather conditions. Additionally, the consequence analyzer is to be able to perform calculations to verify that in the event of a single fault there will be sufficient thrust available to maintain position and heading (ABS, 2013) and (DNV, 2013).

Finally, DNV (2013) and ABS (2013) state that auxiliary subsystems of vessels with class DP2 or higher must include redundancy in main components that support the operation of thrusters and mover-generators.

For the DP systems class 3, a loss of position is not to occur in the event of a single fault either from active or static components (cables, pipes, manual valves, etc.), including complete loss of a compartment due to fire or flood (IMO, 1994).

Although the general configuration of DPS-3 is similar to that of DPS-2, the DP3 systems have an additional station, called backup control station that is to be provided in a separate compartment located and arranged such that no single fault, including a fire or flood in one compartment, will render both the main and backup control system inoperable. This room is to be separated by an A-60 class division from the main DP control station, and located with access from the main DP control station (IMO, 1994) and (ABS, 2013). The components of said station are marked in Figure 44 by the purple boxes.

“Class A-60 division” means a division formed by a bulkhead or deck that is:

I. constructed of steel or an equivalent material and suitably stiffened,
II. constructed to prevent the passage of smoke and flame after 60 minutes of exposure to a standard fire test, and

III. insulated with non-combustible materials so that, if either side is exposed to a standard fire test, after 60 minutes the average temperature on the unexposed face will not increase by more than 139°C above the initial temperature and the temperature at any point on the unexposed face, including any joint, will not increase by more than 180°C above the initial temperature (IADC, 2014).

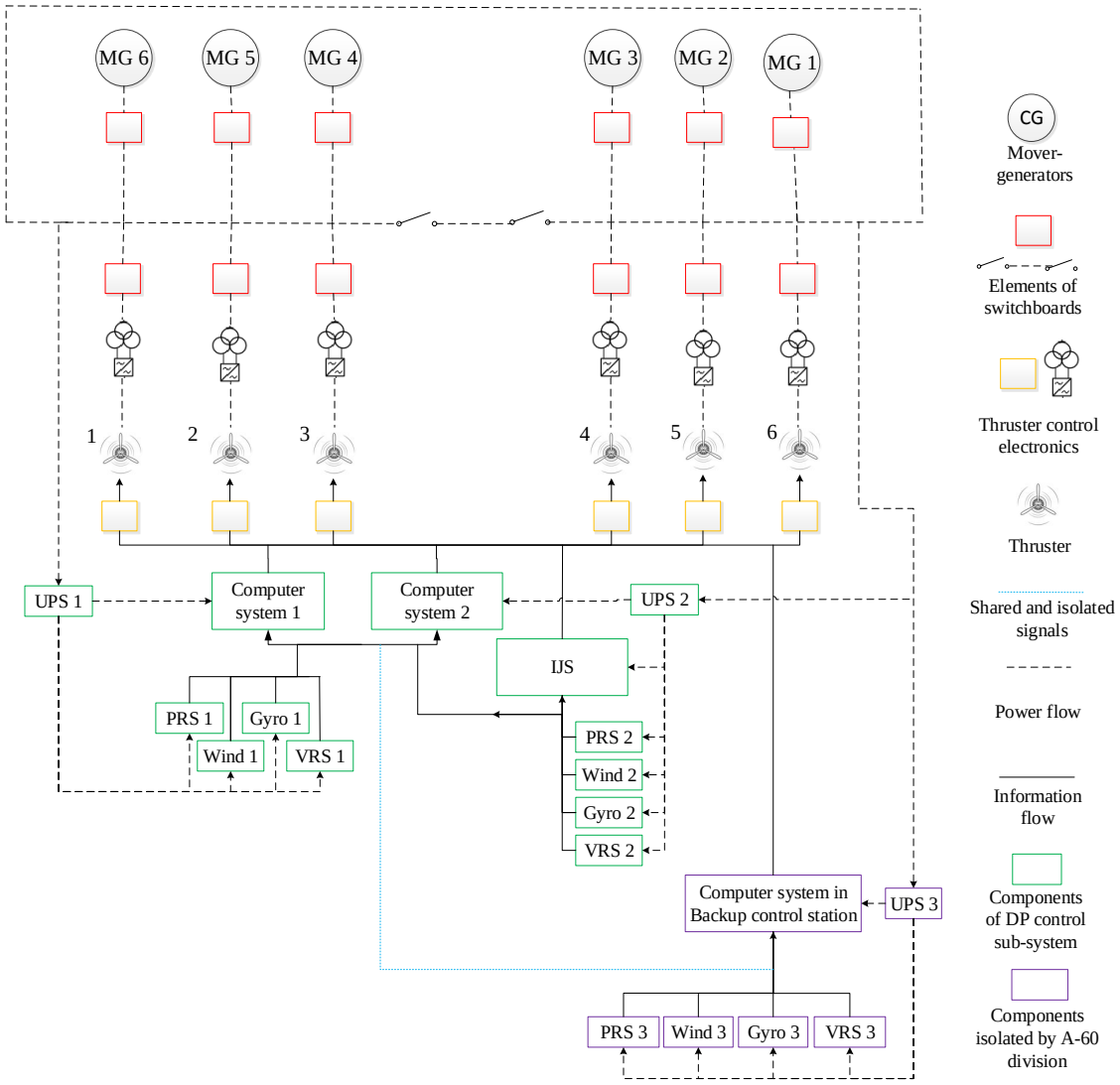


Figure 44 - Typical configuration of DPS-3

Figure 44 has been elaborated considering the minimum requirements for DPS-3 recommended by IMO (1994), ABS (2013) and DNV (2013). The standards mention that the IJS should serve as a simple control computer of control subsystem in case of a failure in the

main control computers, so the IJS needs the information coming from part of the environment sensors and PRS.

As in previous configurations (Figure 42 and Figure 43), notice that the ABS (2013) guide recommends that DP vessels must have an emergency switchboard to provide power to the UPSs in case of failure of the main switchboards, but this situation is not represented in Figure 44 in order to show the main power suppliers and synthesize the most relevant information.

The minimum required number of each of the items for which the DP system is class 3 is shown in Table 3.

Table 3 - Minimum requirements for classification notation DPS-3

DPS-3		
Subsystem	**Item**	**Quantity**
Power subsystem	Mover-generators	Redundant*
	Switchboard	2
	Bus-tie breaker	2 (open)
	PMS	1
Thruster subsystem	Rudders	Redundant
	Thrusters	Redundant
	Single lever for each thruster at main DP-control center	Yes
DP control subsystem	Gyro	2+1 in backup control station
	Wind	2+1 in backup control station
	UPS	2+1 in backup control station
	VRS	2+1 in backup control station
	PRS	2+1 in backup control station
	Computer system: number of control computers	2+1 in backup control station
	Backup Control Station	Yes
	Consequence analyzer	Yes

* The IMO (1994), ABS (2013) and DNV (2013) guidelines recommend redundancy but do not specify the exact amount of components.

The main differences between the DPS-2 and DPS-3 power subsystems are: the DPS-3 should have at least two switchboards, while the DP2 system should have only one; and with respect to the buses, a DPS-3 must have at least two buses and bus-tie breakers should be open (MTS, 2012) and (DNV, 2013); in DPS-2 there may be only one bus that could

operate open or closed. Operating with open bus reduces overall power plant reliability but maintains the availability of thrusters during any equipment fault (Garg & Shah, 2011).

It is also necessary to have an extra control station (backup control station) in DPS-3 that has all the necessary components to operate as an alternative control station and for this reason there are three control computers fed by three independent UPSs, whereas in the DPS-2 there are only two control computers powered by two UPSs, also independent. In DPS-3 the third wind sensor, third gyrocompass and the third PRS are to be directly connected to the backup DP control station and with their signals repeated to the main DP control station with appropriate signal isolation (ABS, 2013).

Regarding auxiliary subsystems, the guidelines state that the cables for redundant equipment or systems are not to be routed together through the same compartments; and that the redundant piping subsystem (i.e., piping for fuel, cooling water, lubrication oil, hydraulic oil, etc.) should not be routed together through the same compartments.

Table 4 presents a summary of minimal requirements of different DP classes.

Table 4 - Summary of DP System requirements for each classification notation

	Equipment	Minimum Requirements for each classification notation		
		DPS-1	**DPS-2**	**DPS-3**
Power subsystem	Mover-generators	Non-redundant	Redundant	Redundant
	Switchboard	1	1 with bus-tie	2 with bus-ties, in separate compartments
	Bus-tie breaker	0	1 (open or closed)	2 (open)
	Power Management	No	Yes	Yes
Thruster subsystem	Rudders	Non-redundant	Redundant	Redundant
	Thruster	Non-redundant	Redundant	Redundant
	Single lever for each thruster at main DP-control center	Yes	Yes	Yes
Control subsystem	PRS	2	3	2+1 in backup control station
	VRS	1	3	2+1 in backup control station
	Wind	2	3	2+1 in backup control station
	Gyro	2	3	2+1 in backup control station
	UPS	1	2	2+1 in backup control station
	IJS	Yes	Yes	Yes
	Computer system: number of control computers	1	2	2+1 in backup control station
	Consequence analyzer	No	Yes	Yes
	Backup control station	No	No	Yes

Source: IMO (1994), ABS (2013) and DNV (2013)

4. CASES STUDY

Considering that the main types of oil exploration vessels are drill ships and semi-submersible vessels (Karan, 2017), two typical configurations were selected to evaluate the reliability, availability and maintainability of the DP system: a DP Class 2 drilling semi-submersible platform and a DP Class 3 drillship. Then each configuration will be detailed. However, it is worth noting that the configurations are established according to literature review and the descriptions presented in chapter 3.

4.1 Configuration for case study 1: Semi-submersible platform

The first case study is a semi-submersible platform with eight thrusters arranged in pairs at the ends of the port and starboard pontoons. The vessel has a Diesel electric propulsion system with six mover-generators providing power to variable speed, fixed pitch thrusters. Figure 45 shows the configuration of the thrusters.

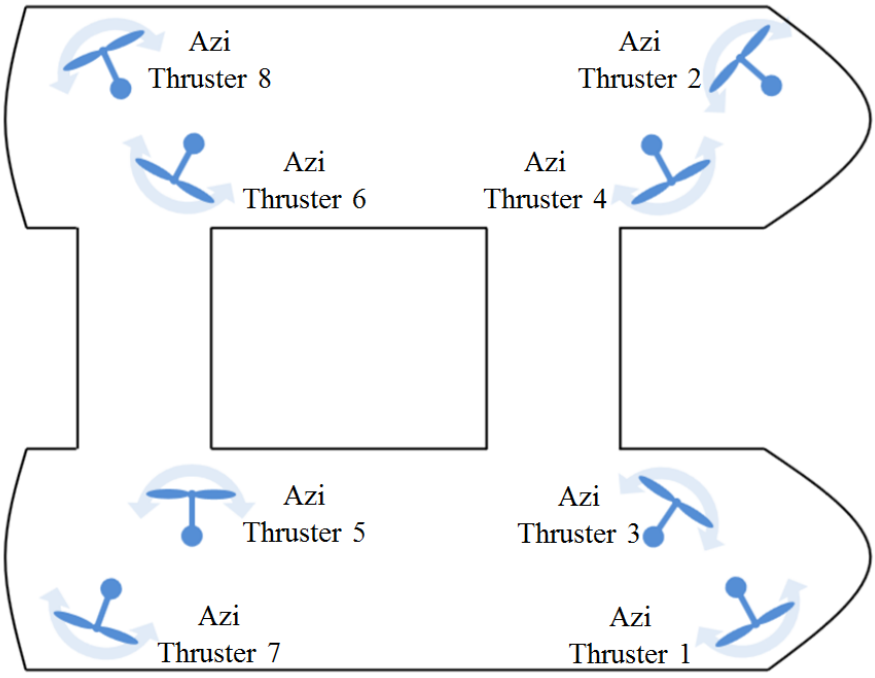


Figure 45 - Case study #1 (semi-submersible platform)
(*) Thrusters 1, 4, 6 and 7 belong to one side of the electric circuit and the thrusters 2, 3, 5 and 8 to the other side.

The semi-submersible platform operates with DP class 2, Table 5 shows the main components of the DP system.

Table 5 - DP system components for case study #1

Case study 1 (DP2)		
Subsystem	**Item**	**Quantity**
Power subsystem	Mover-generators	6 (4 online and 2 stand by)
	Switchboard HV (11kV)	2
	Bus tie breaker	2
	Circuit breaker	18
	Emergency mover-generator*	1
	Emergency switchboard*	1
	Three phase transformers**	2
	Switchboard LV (480V) **	2
	PMS	1
Thruster subsystem	Thrusters	8
	UPS***	8
	Siplink***	4 main + 4 auxiliary
	Transformer***	8
	TMCC (Thruster auxiliary supplies Motor Control Center) ***	8
	ACU (Aquamaster Control Unit) ***	8
	Field station***	8
	Manual thruster control	8
DP control subsystem	PRS	2 Hydro-Acoustic + 2DGPS
	VRS	3
	Wind	3
	Gyro	3
	UPS	3
	Computer system: number of control computers	3
	IJS	1

(*) It is worth noting that IMO (1994) and DNV (2013) do not establish as a minimum requirement of any DP system class the components identified in the table with (*), these components are associated with an additional power supply to the main switchboard and the main mover-generators. However, ABS (2013) recommends that every UPS must have a main power source (mover-generators and main switchboard) and a backup source of the emergency switchboard. As this requirement is not common to all guidelines, it has not been included in the tables of the minimum components for each DP system class (Table 4). In the case study, the platform has an emergency mover-generator that provides power exclusively to the emergency switchboard, and this switchboard acts as the second source of power for all UPSs of the DP system and equipment of auxiliary subsystems.

(**) The case study has two three phase 3.15MVA (AN), 4.095MVA (AF) 11kV/480V Dy11 transformers, responsible for converting high voltage from main switchboards (11kV) to low voltage (480V). It is important to mention that the emergency switchboard provides low voltage (480V) power.

(***) As for the thruster subsystem, as the case study has azimuthal thruster and there is no rudder required in an azimuth system (Patil, Ayare, Mahajan, & Bade, 2015); then the rudders will not be considered as DP platform components. Additionally, it has been established that the guidelines only recommend UPS for the DP control subsystem, but in the case study, it was considered that there are additional UPSs in the thruster subsystem; these UPSs are rated for 8 minutes' operation in the case of blackout, providing the power required for the electronic components of the thrusters. The thruster control electronics are the so-called Siplinks (name given by the supplier), transformers, TMCCs (Thruster auxiliary supplies Motor Control Center), ACUs (Aquamaster Control Unit) and field stations. The function of each of them is detailed below.

Therefore, the thruster control electronics (components that constant monitoring the operational parameters of the thruster) are defined as follows:

- Siplink: in simple terms, the Siplink can be described as two bi-directional AC to DC converters (called line converters) linked at their DC side. Inverter loads are then connected to the DC bus and can draw power from both line converters. This electronic component increases the reliability of the DP system because even when one 11-kV switchboard is faulty, the Siplink is able to provide the required power (Siemens, 2010). In the case study, the Siplinks are programmed to draw 50% of the total thruster load from each 11kV but they can also be programmed to share power as though the DC link was split, i.e., all power for thrusters 4, 6, 1 and 7 comes from Bus A and all power for thrusters 2, 3, 5 and 8 comes from Bus B. Therefore, in the case study 1 there are four main Siplinks (one for each pair of thrusters) and four auxiliary Siplinks (one for each pair of thrusters). Figure 46 shows the relationship between main and auxiliary Siplink (the title Auxiliary Siplink denies the importance of the lower voltage Siplink as it is responsible for controlling the main 11kV circuit breaker for the Siplink pair, pre-charging the Main Siplink and pre-magnetizing the Siplink transformers prior to connection, in addition to its primary role of supplying the thruster auxiliary pumps and fans).

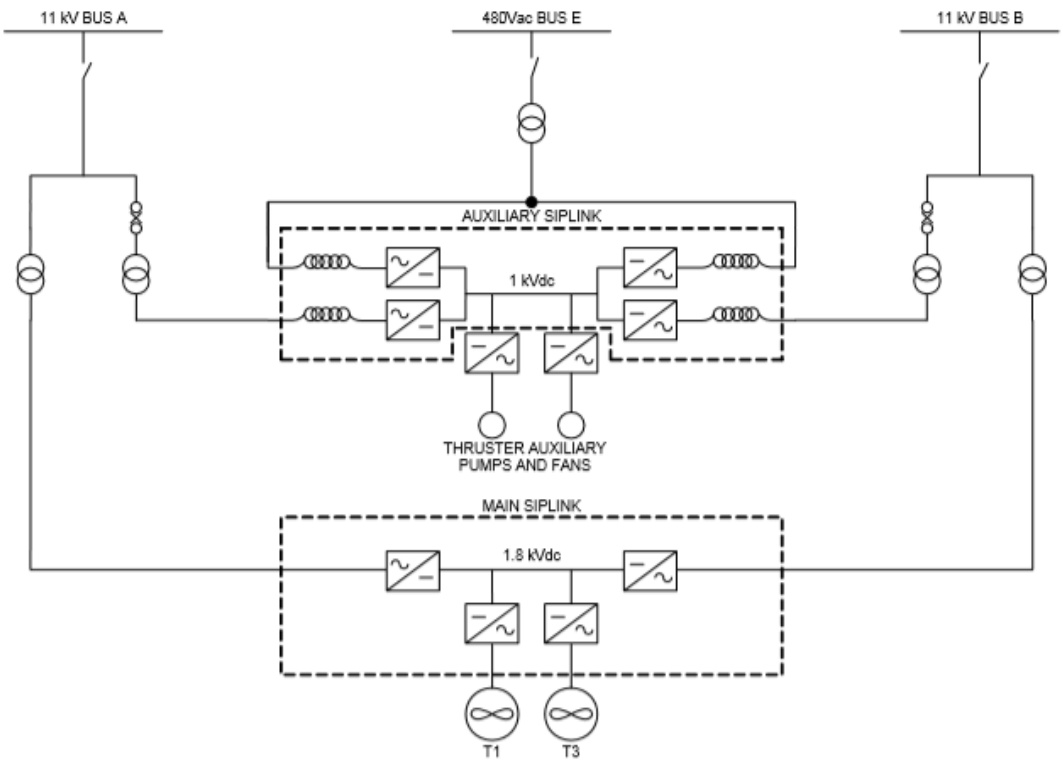


Figure 46 - Relationship between Main and Auxiliary Siplinks
Source: Cargill (2007)

- Transformers: Responsible for converting the power of the HV switchboards (1kV) in energy of 1.8kVdc to the thrusters.

- TMCC (Thruster Auxiliary Supply Motor Control Center): each thruster has its own Auxiliary MCC powered by the Auxiliary Siplink. It has a Variable Frequency Drive (VFD) that controls the operation speed of an AC motor by controlling the frequency and voltage of the power supplied to the motor. TMCCs ensure the power supply to the auxiliary components of each thruster; in the case study the Thruster MCC supplies the consumers as lube oil pump, freshwater cooling pump, exhaust and supply fan, clean power, Aquamaster (Hydraulic Power Unit), etc.

- ACU (Aquamaster Control Unit): The Aquamaster Control Unit is the interface between the control subsystem and the thruster. Its primary function is to provide closed loop control of thruster azimuth direction but it also provides a means of locally controlling the thruster. The ACU also provides the safety shut down signals

to the prime mover and monitors a number of status indicators to determine if the thruster is ready for DP.

- Field station: The thruster commands from the three control computers are compared by the "master" computer and the median command is selected to be the final output. The voting of the thruster commands is performed in the thruster control field station (Kongsberg, 2014), and then shared with the ACU.

Figure 47 shows the connection between the main electronic controls, the control subsystem and the thrusters.

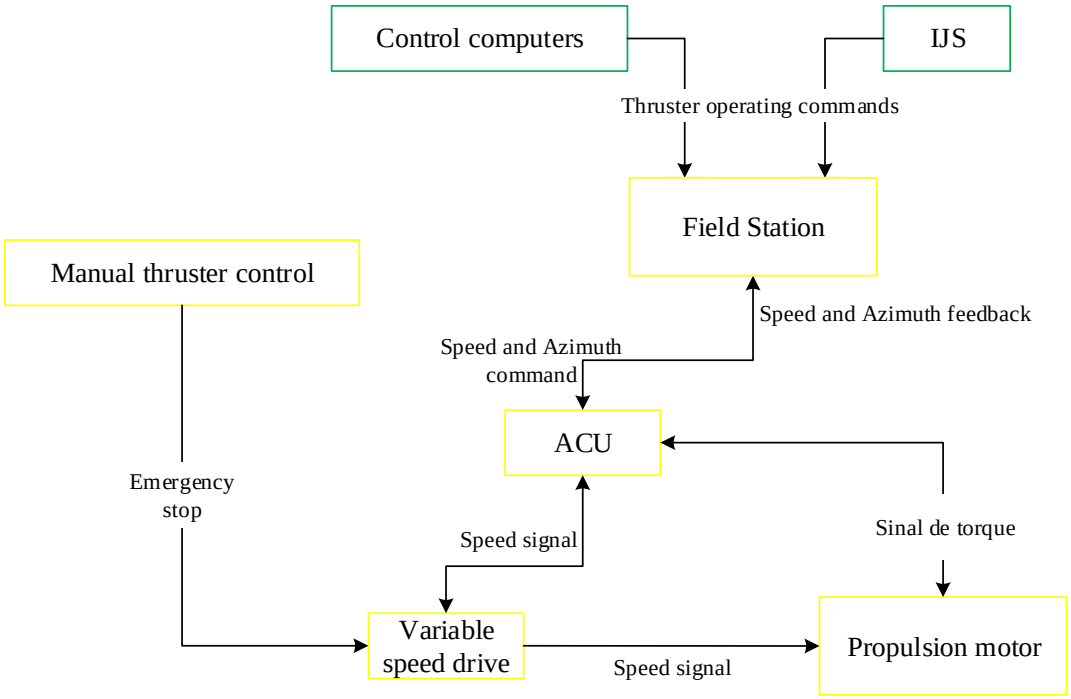


Figure 47 - Connection between the main electronic controls, the control subsystem and the thrusters

Thus, the configuration of the DP system admitted for case study #1 is presented in Figure 48.

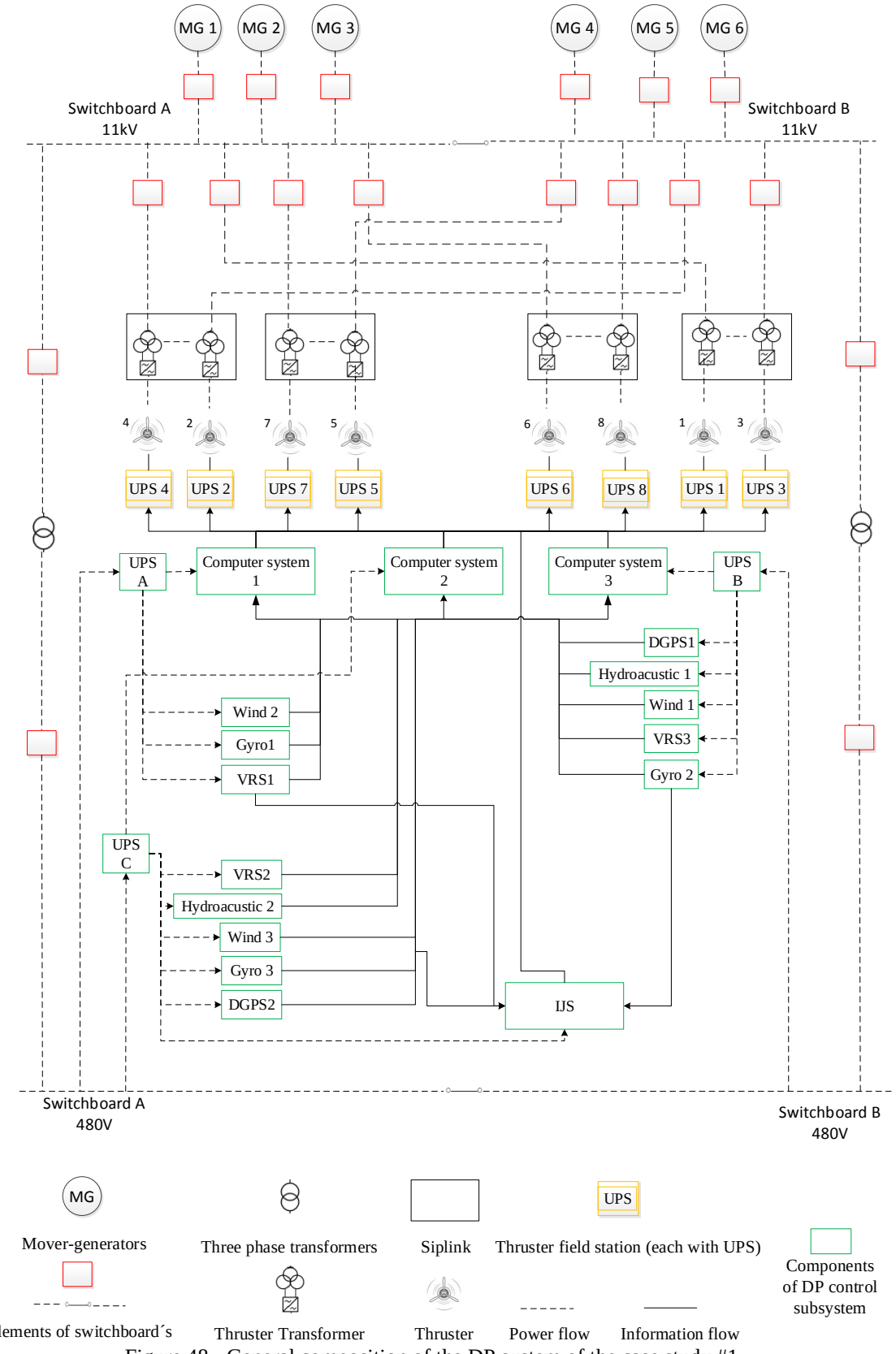


Figure 48 - General composition of the DP system of the case study #1

As can be seen in Figure 48, power is generated by six mover-generators and passes through circuit breakers before powering the main switchboard (two high voltage); such platform has two 11kV switchboard and the DP system electrical circuit is divided in two (side A and side B).

Normally, the platform operates with closed bus, that is, the two switchboard sections of high voltage are connected together (even in low-voltage switchboards); that is why the case study will develop assuming this operating condition.

The two high voltage switchboards are able to provide power to the thruster subsystem and the control subsystem. The power supplied to the thruster subsystem feeds the Siplinks of each pair of thrusters, after that the transformers decrease the voltage; and the power supplied to the control subsystem throughout three phase transformers (two) and the low voltage switchboards distribute power to the UPSs.

Table 6 shows the components that receive power through the UPSs of the control subsystem.

Table 6 - Distribution of power supplied to the control subsystem by the UPSs (DP2)

UPS A	**UPS B**	**UPS C**
Computer system 1	Computer system 3	Computer system 2
VRS 1	VRS 3	VRS 2
Wind 2	Wind 1	Wind 3
Gyro 1	Gyro 2	Gyro 3
	Hydroacustic 1	Hydroacustic 2
	DGPS 1	DGPS 2
		IJS

Finally, all environment sensors and PRSs send information to the three control computers and some repeat this information to the IJS (enabling the system to operate as a simple control computer of control subsystem). The three control computers operate in parallel, each receiving the same input from the sensors and PRSs; all controllers independently compute required information to maintain station and pass this information to the field station of the thrusters. The field stations take the median value as the commands signal and feed this torque and azimuth commands to the Aquamaster units, while the IJS in

case of being enabled as DP system, sends isolated analog signals to the field stations of the thrusters in order not to share connection with the control computers.

The emergency switchboard and its mover-generator are not shown in Figure 48, but their function is to ensure the backup supply of power (480V) for all UPSs of the DP system (UPSs of the control subsystem and the UPSs of the thruster subsystem) and equipment of auxiliary subsystems, in case of Low Voltage switchboards failure.

It is important to mention that there are three auxiliary subsystems that are critical to the operation of a DP unit: cooling water subsystem, fuel oil subsystem and lubrication subsystem. In addition to the three main subsystems (power, thruster and control), there are five other subsystems that support the operation of the DPS-2 (ventilation, compressed air, cooling water, fuel oil and lubrication). According to failure modes and effects analysis – FMEA of the case study #1, failure modes of the ventilation and compressed air subsystem will not cause any transient effect on DP positioning. However, the failure of the cooling water, fuel oil and lubrication subsystem can lead to loss of three mover-generators or four thrusters, overcoming the worst-case projected failure and consequently leading to loss of controlled propulsion (TRANSOCEAN, 2009).

Table 7 shows the quantity of the main components in these critical subsystems for case study #1.

Table 7 - Equipment of the auxiliary subsystems for case study #1

Case study 1 (DPS-2)		
Subsystem	**Item**	**Quantity**
Cooling water subsystem (thruster)	Centrifugal pump (SW)**	8 (4 forward pumps are shared with movers)*
	Cooler (FW)	8
	Centrifugal pump (FW)**	8
Cooling water subsystem (mover-generators)	Centrifugal pump (SW)**	4
	Sea chest	4
	Expansion tank (FW)	2
	Generator (FW)	2
	Cooler (FW)	2
	Circulation Pump (LTFW)	2
	Circulation pump (FW)	6
Lubrication subsystem (thruster)	Gravity tank	8
	Inspection tank	8
	Lubrication pump	8
	Duplex filter	8
	Lubrication oil cooler	8
Lubrication subsystem (mover-generators)	Sump tank	1
	Transfer pump	2
Fuel oil subsystem	Storage tank	3
	Transfer pump	2
	Service tank	2
	Pump of the purification system	4
	Purifier	4
	Oil cooler	6

(*) Pumps shared between the mover-generators and thrusters 1, 2, 3 and 4.
(**) FW and SW Pumps operate in pairs, where one operates and the other is redundant in standby.

4.2 Configuration for case study 2: Drillship

The second case study is a drillship with six thrusters arranged in pairs. The vessel has a Diesel electric propulsion system with six mover-generators. Figure 49 shows the configuration of the thrusters.

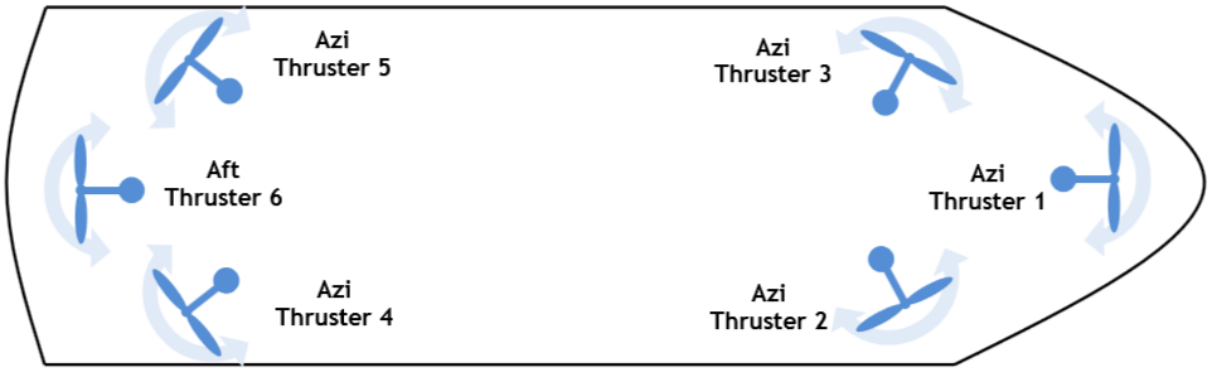


Figure 49 - Case study #2 (drillship)

(*) In order to minimize the impact of power loss, the combination of thrusters in the drillship electrical circuit ensures that in the event of failure of a switchboard the missing thrusters are not located on the same side (all in the stern, all in the bow, all in port or all on starboard): thus thrusters 1 and 5 belong to "PORT" bus, thrusters 3 and 4 to "STBD" bus and thrusters 6 and 2 to "CENT" bus of the drillship electrical circuit.

The vessel operates with DP class 3, the main components of the DP system are shown in Table 8.

Table 8 - DP system components for case study #2

Case study 2 (DP3)		
Subsystem	**Item**	**Quantity**
Power subsystem	Mover-generators	6
	Switchboard HV (11kV)	3
	Bus tie breaker*	3
	Circuit breaker	12
	Emergency mover-generator	1
	Emergency switchboard	1
	Three phase transformers	2
	Switchboard LV (440V)**	5
	PMS*	1
Thruster subsystem	Thrusters	6
	UPS***	6
	Field station***	6
	Transformer***	6
	RexCU (Rexpeller Control Unit) ***	6
	DCU (Drive Control Unit) ***	6
	Manual thruster control	6
DP control subsystem	PRS	2 Hydro-Acoustic + 4DGPS
	VRS	4
	Wind	3
	Gyro	3
	UPS	3
	Computer system: number of control computers	3
	IJS	1
	Backup control station	1

(*) According to IMO (1994), ABS (2013) and DNV (2013) vessels equipped with DP system class 3, must operate with open bus, so this operating condition will be assumed for this case study. Further, with open bus, each side of circuit electric has a PMS that operates independently (MTS, 2007), in this case study the PMS is divided in three (PMS port, PMS cent, PMS stbd).

(**) The vessel has five LV Switchboards (440V), which are divided as follows: two Forward LV switchboards (No.1 and No. 2) that receive power from the PORT HV switchboard and STBD HV switchboard, these Forward LV switchboards are responsible for powering the control subsystem UPSs. Three Aft LV switchboards (No. 3, No.4 and No. 5) that receive power from each of the HV switchboards (PORT HV switchboard supplies power to Aft LV switchboard No. 5; CENT HV switchboard supplies power to Aft LV switchboard No. 4 and STBD HV switchboard supplies power to Aft LV switchboard No. 3); these Aft LV switchboard are responsible for supplying power to the Low Voltage equipment of the mover-generators and the thrusters 4, 5 and 6.

Since thrusters 1, 2 and 3 do not have dedicated LV switchboards, they have HV panels with transformers that allow them to supply power to their low voltage equipment. Figure 50 represents the distribution of switchboards between the ship thrusters.

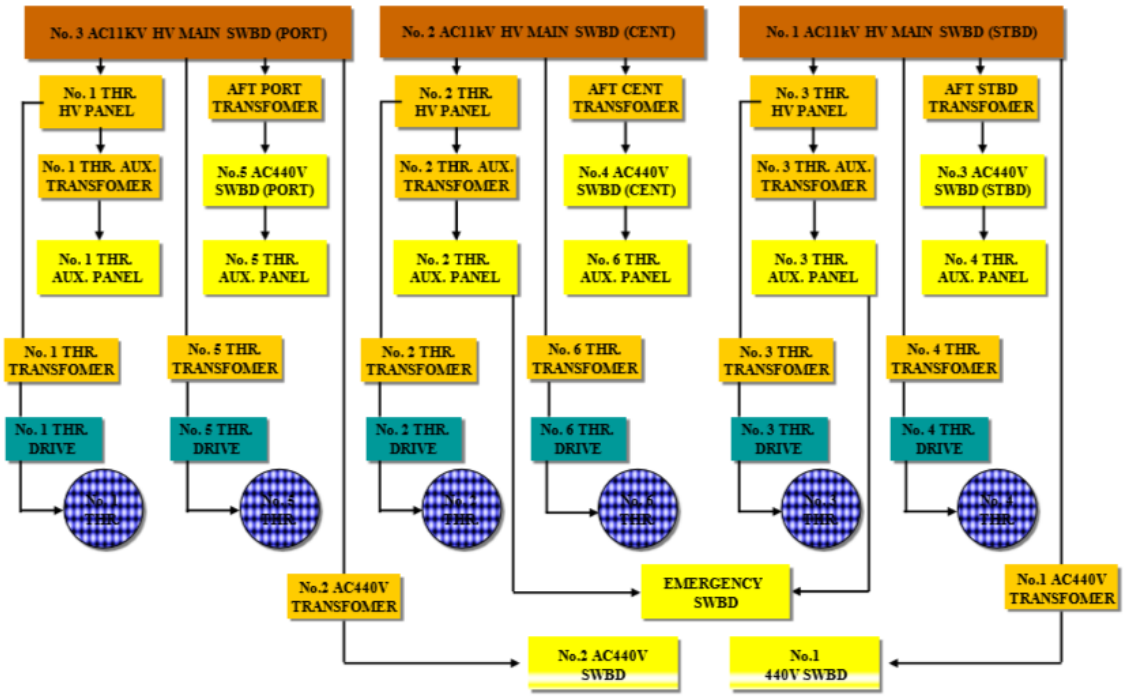


Figure 50 - LV power distribution for thrusters

(***) The guidelines do not state that the thruster subsystem should have UPS, but for the case study, it was considered that there is a UPS for each thruster, providing the power required for the thruster control electronics. The thruster control electronics are the field stations, the transformers, the RexCUs (Rexpeller Control Unit) and the DCUs (Drive Control Unit).

The thruster control electronics (components that constantly monitor the operational parameters of the thruster) are defined as follows:

- Field station: each thruster has a field station as defined in case study #1.

- Transformers: as defined in case study #1.

- RexCU (Rexpeller Control Unit): each thruster has its own thruster control units (DCU and RexCU). RexCU interfaces and control signals, which are related to thruster oil system such as not only the azimuth command or feedback but also oil temperature.

- DCU (Drive Control Unit): DCU interfaces and controls signals such as the speed command or feedback, which are related to operating thruster motor.

- VFD (Variable Frequency Drive): The variable frequency drive (VFD) controls the operation speed of an AC motor by controlling the frequency and voltage of the power supplied to the motor.

This operation of the electronic components of the thrusters is shown in Figure 51. Each thruster control system is independent of the others and consists of equipment and signals in order to control a thruster.

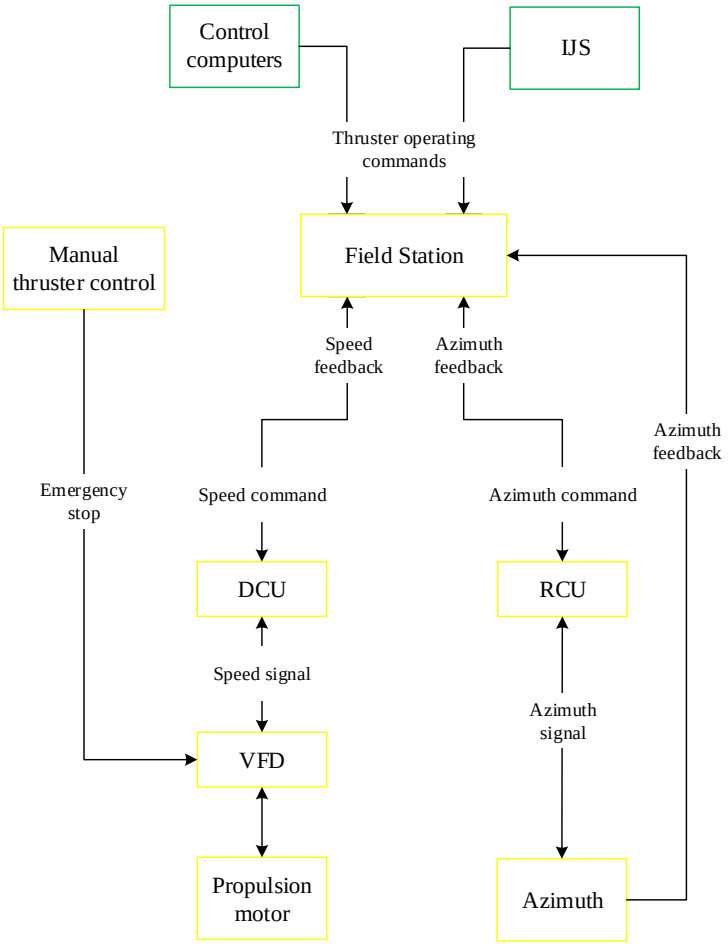


Figure 51 - Connection between the main electronic controls, the control subsystem and the thrusters

The configuration of the DP system accepted for the case study #2 is exposed in Figure 52.

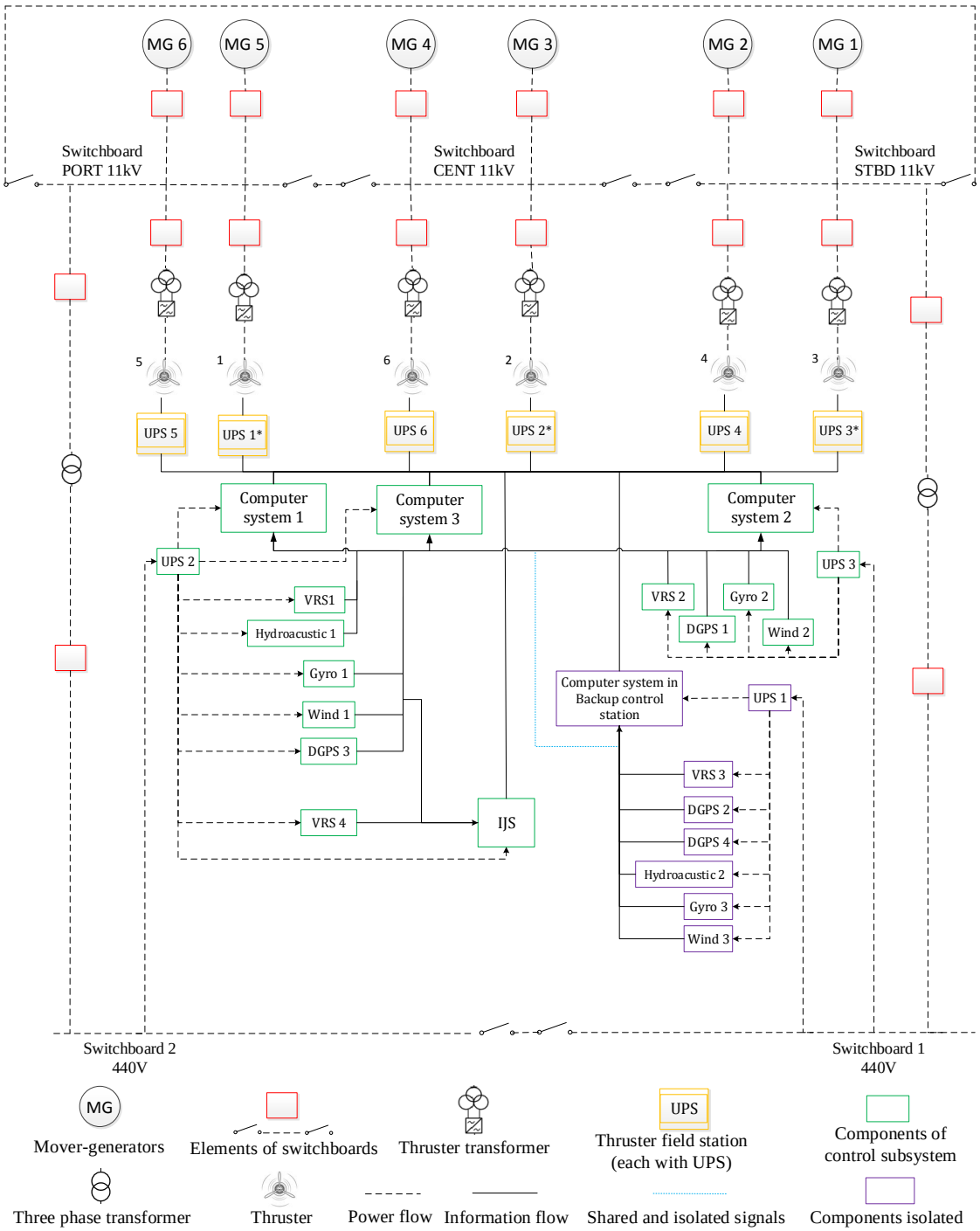


Figure 52 - General composition of the DP system for case study #2

As Figure 52 shows, the power is generated by six mover-generators and passes through circuit breakers before powering the main switchboard (three High Voltage); as such, the platform has three 11kV switchboards, the DP system electrical circuit is divided in three (port, cent and starboard).

The three high voltage switchboards provide power to the thruster subsystem while only the starboard and port switchboard provide power to the control subsystem.

The thruster transformers filter the power supplied to the thruster subsystem while two three-phase transformers that convert the high voltage (11kV) into a low voltage (440V) filter the power supplied to the control subsystem. The Low Voltage switchboards are responsible for powering all DP system UPSs.

Table 9 shows the components that receive power through the UPSs of the control subsystem.

Table 9 - Distribution of power supplied to the control subsystem by the UPSs (DP3)

UPS A [exclusive for Backup control station]	**UPS B**	**UPS C**
Computer system in Backup control station	Computer system 1	Computer system 2
VRS3	Computer system 3	VRS 2
Wind 3	VRS 1	Wind 2
Gyro 3	VRS 4	Gyro 2
Hydroacustic 2	Wind 1	DGPS 1
DGPS 2	Gyro 1	
DGPS 4	Hydroacustic 1	
	DGPS 3	
	IJS	

Finally, all environment sensors and PRSs send information to the three control computers and some repeat this information to the IJS (enabling the system to operate as a simple control computer of DP control subsystem). It is worth mentioning that the environment sensors (Wind 3, Gyro 3 and VRS 3), and the PRSs (DGPS 2 and 4, Hydroacustic 2) of the backup control station, send signals to the control computers through an isolating box.

The emergency switchboard and its mover-generator are not shown in Figure 52, but their function is to ensure the power supply (440V) for all UPSs of the DP system (UPSs of the control subsystem and the UPSs of the thruster subsystem), in case of Low Voltage switchboards failure.

It is important to mention that there are three auxiliary subsystems that are critical to the operation of a DP unit: cooling water subsystem, fuel oil subsystem and lubrication subsystem. In addition to the three main subsystems (power, thruster and control), there are five other subsystems that support the operation of the DPS-3 (ventilation, compressed air, cooling water, fuel oil and lubrication). According to failure modes and effects analysis – FMEA for case study #2, failure modes of the ventilation and compressed air subsystem will not cause any transient effect on DP positioning. However, the failure of the cooling water, fuel oil and lubrication subsystem can lead to loss of four mover-generators or four thrusters, overcoming the worst-case projected failure and consequently leading to loss of controlled propulsion (Samsung Heavy Industries, 2012).

Table 10 shows the quantity of the main components in these critical subsystems for case study #2.

Table 10 - Equipment of the auxiliary subsystems for the case study #2

Case study 2 (DPS-3)		
Subsystem	**Item**	**Quantity**
Cooling water subsystem (thruster)	Centrifugal pump (SW)**	6 (shared)* + 6
	Cooler (FW)*	6 (shared)* + 4
	Centrifugal pump (FW)**	6 (shared)* + 6
Cooling water subsystem (mover-generators)	Centrifugal pump (SW)**	6 (shared)*
	Sea chest	6
	Expansion tank (FW)	3
	Generator (FW)	3
	Cooler (FW)*	6 (shared)*
	Centrifugal pump (FW)	6
	Water preheat unit	3
	Centrifugal pump (LTFW)**	6 (shared)*
Lubrication subsystem (thruster)	Gravity tank	6
	Inspection tank	6
	Lubrication pump	12
	Duplex filter	6
	Lubrication oil cooler	6
Lubrication subsystem (mover-generators)	Sump tank	6
	Supply pump	6
Fuel oil subsystem	Storage tank	4
	Supply pump	6
	Service tank	2
	Pump of the purification system	4
	Purifier	4
	Oil cooler	6

(*) Components shared between mover-generators and thrusters 4, 5 and 6.
(**) FW and SW Pumps operate in pairs, where one operates and the other is redundant in standby.

5. RAM ANALYSIS

In this section, the methodology used to analyze Reliability, Availability and Maintainability of each cases study, as well as the main differences between the obtained results are exposed. The analysis techniques applied and the step by step of its implementation are available in Figure 53.

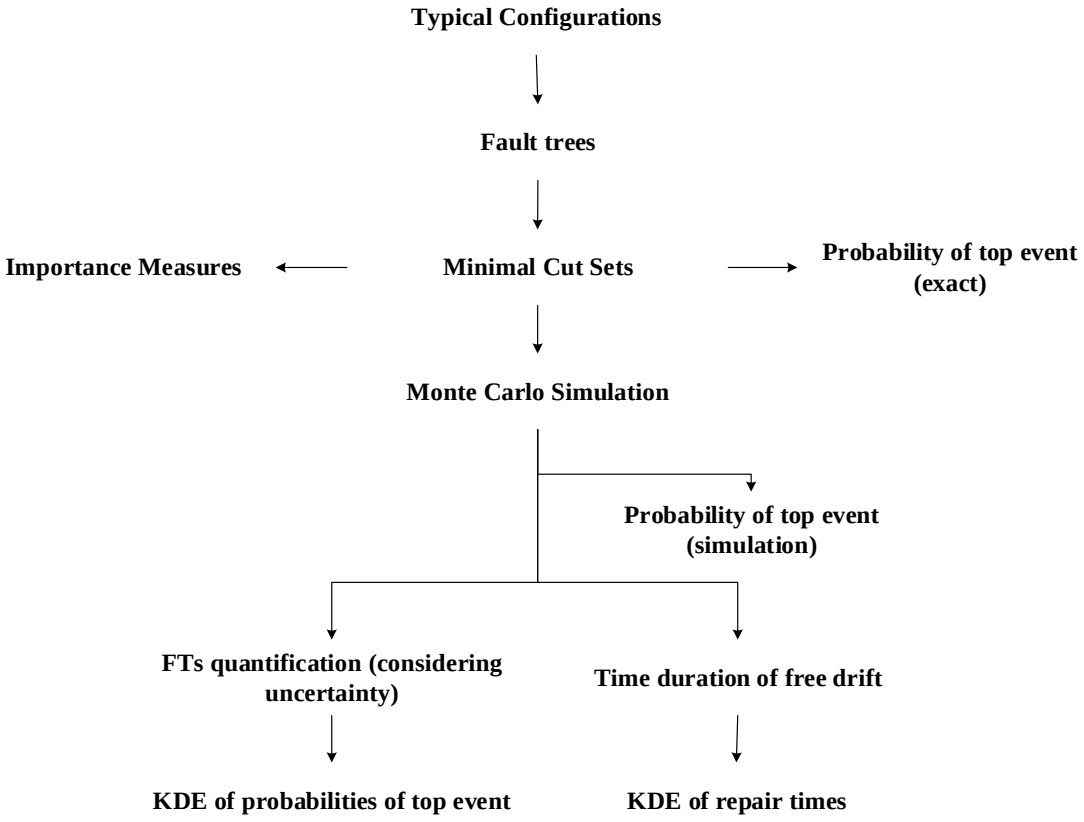


Figure 53 – Methodology

The first step is to know the main characteristics and operational structure of each DP systems in study, and for this, we applied the literature review presented in Section 3. Additionally, the analysis techniques as functional diagrams and RBD are used to represent the configurations defined in order to elaborate the model to perform the RAM analysis. This is, with these implementations are defined the typical configuration of DP2 system (semisubmersible platform) and the typical configuration of DP3 system (drillship).

From the typical configurations, the FTs of events of interest are designed (controlled drift and free drift); and before quantifying the FTs, a qualitative analysis is developed that allows identifying the minimal cut sets of each FT.

The minimal cut sets are the inputs for various analyses, for example, the reliability analysis that aims to quantify the probability of partial and total failure of each DP system is developed using the minimal cut sets of trees and considering the failure rate of equipment for operating times of 3, 6, 9 and 12 months. However, in the analysis of importance measures we also use the minimal cut sets, where it is intended to identifying the equipment criticality ratings (see Appendix C).

It is worth noting that the RAM analysis considers operational times of 3, 6, 9 and 12 months because the offshore industry got interested in these times since in the recent years the offshore activities have been evolving and, with this, reducing the operational times. For example, according to PETROBRAS (2018) in 2010, the mean construction time for offshore wells was 310 days but in 2018, this time fell to 127 days; that is, the RAM analysis is developed in order to identify changes in failure probability and in the repair times of DP systems when the operational times decrease.

To apply the Monte Carlo Simulation method, we used the minimal cut sets as inputs, and to verify that the Monte Carlo Simulation is a suitable method to model the operation of DP systems, the probability of FTs is quantified again but, this time, using simulation, the comparison between these values is presented in Appendix D.

Once the Monte Carlo Simulation has proved to be able to represent the operation of the DP systems, it will be necessary to perform maintainability and availability analysis. That is, from the repair times of the critical equipment collected in the literature, with Monte Carlo Simulation, we develop experiments and the downtimes of each DP system under study are identified.

In order to distinguish the form, the central point and the variation of the distribution of the repair times obtained via Monte Carlo Simulation histograms are drawn, and, from each histogram, the corresponding pdf is defined using KDE.

Finally, KDE is also used to define the pdf of the results obtained during the data uncertainty analysis using the built FTs that is also evaluated via the Monte Carlo Simulation method.

5.1 Reliability analysis

The first step in the evaluation of the case studies is the definition of the events of interest, that is, knowing that the main purpose of a DP system is to keep a floating vessel on a specific position by proper action of the propulsion system of the vessel (Balchen, Jenssen, Mathisen, & Saelid, 1980), it is possible to define the loss of DP system functionality as the position loss of the DP unit.

We studied two types of loss of position: free drift and controlled drift. Each of them is define below:

- Controlled drift: it occurs when the vessel loses position due to the partial loss of the main or auxiliary critical subsystems; however, some degree of maneuver is still possible to avoid a collision, considering that the DP vessel has not lost all power or thrust suppliers.

- Free drift: it occurs when the vessel loses full propulsive capacity due to the total failure of any of the main subsystems or any of the critical auxiliary subsystems.

In the following sections, the Fault Trees for each event of interest (controlled drift and free drift) regarding the configurations of case studies #1 and #2 will be presented.

5.1.1 Controlled drift for case study #1 – DP2 Semi-submersible platform

In general, there are three events that may result in a partial loss of propulsive capacity. They may lead the vessel to a controlled drift; Figure 54 presents a macro fault tree for this event. This tree will be further detailed through the development of each base event (partial

failure of power subsystem, partial failure of thruster subsystem or partial failure of control subsystem).

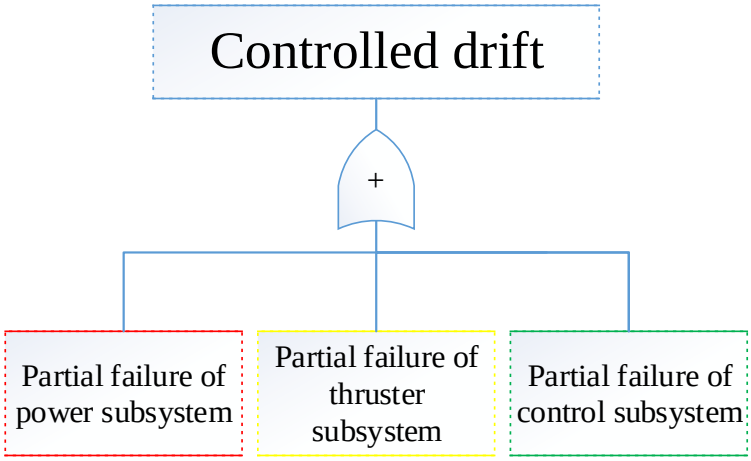


Figure 54 - Fault tree for controlled drift in case study #1

Starting from the partial failure of power subsystem, we obtained the tree of Figure 55. As discussed previously, the electric circuit of the semi-submersible platform is divided into two sections: section A and section B; thus, it is observed that the partial failure of the power subsystem occurs due to the unavailability of one side of the electric circuit (side A or side B).

It is worth noting that the gate of this tree is an “Exclusive OR”, because the partial failure event of the power subsystem will occur if exactly one side of the electric circuit becomes unavailable, if both sides of the vessel are unavailable another top event would happen, the free drift (this top event will be studied afterwards).

Provided the context, we can assume that one side of the electric circuit fails if:

I. There is a failure to generate power in the electrical circuit. This fault occurs when all the mover-generators of the electrical circuit (two mover-generators online and stand-by mover-generator) fail, either due to a mechanical fault (motor, generators, AGP or circuit breakers failure) or a failure of the auxiliary subsystems that support the operation of these mover-generators (lubrication, cooling or fuel subsystem). According to the FMEA of the platform, this situation leads the vessel to a degree of high degradation because the propulsion is limited to 50% of the installed power.

II. PMS failure: although in the case of PMS failure the switchboards can be manually activated, in the fault tree in question, a PMS failure that generates false demands on the side of the electrical circuit under study (for example, operates spuriously on one bus when there is no blackout) was considered.

III. Failure of one of the high voltage switchboards (11kV); the power subsystem is partially failed because it loses one side of the circuit electric vessel, i.e. Siplink allows all thrusters to have power, but it limits the propulsion to 50% of the installed power.

IV. Partial failure in the distribution of Low Voltage (LV) energy on one side of the electric circuit. As discussed earlier there are two 480V switchboards that receive power from the main switchboard through a three-phase transformer each; according to the FMEA of the vessel, in the event of failure of one transformer, another can supply power to the two LV switchboards. Therefore, this partial failure tree only includes on each side of the electrical circuit the failure event in which there is loss of the LV switchboard and the emergency components cannot provide 480V power on the side of the faulty electrical circuit leading. Thus, giving the vessel a controlled drift since it will lose all auxiliary subsystems of the four thrusters.

Figure 55 shows the structure of the partial failure of the power subsystem.

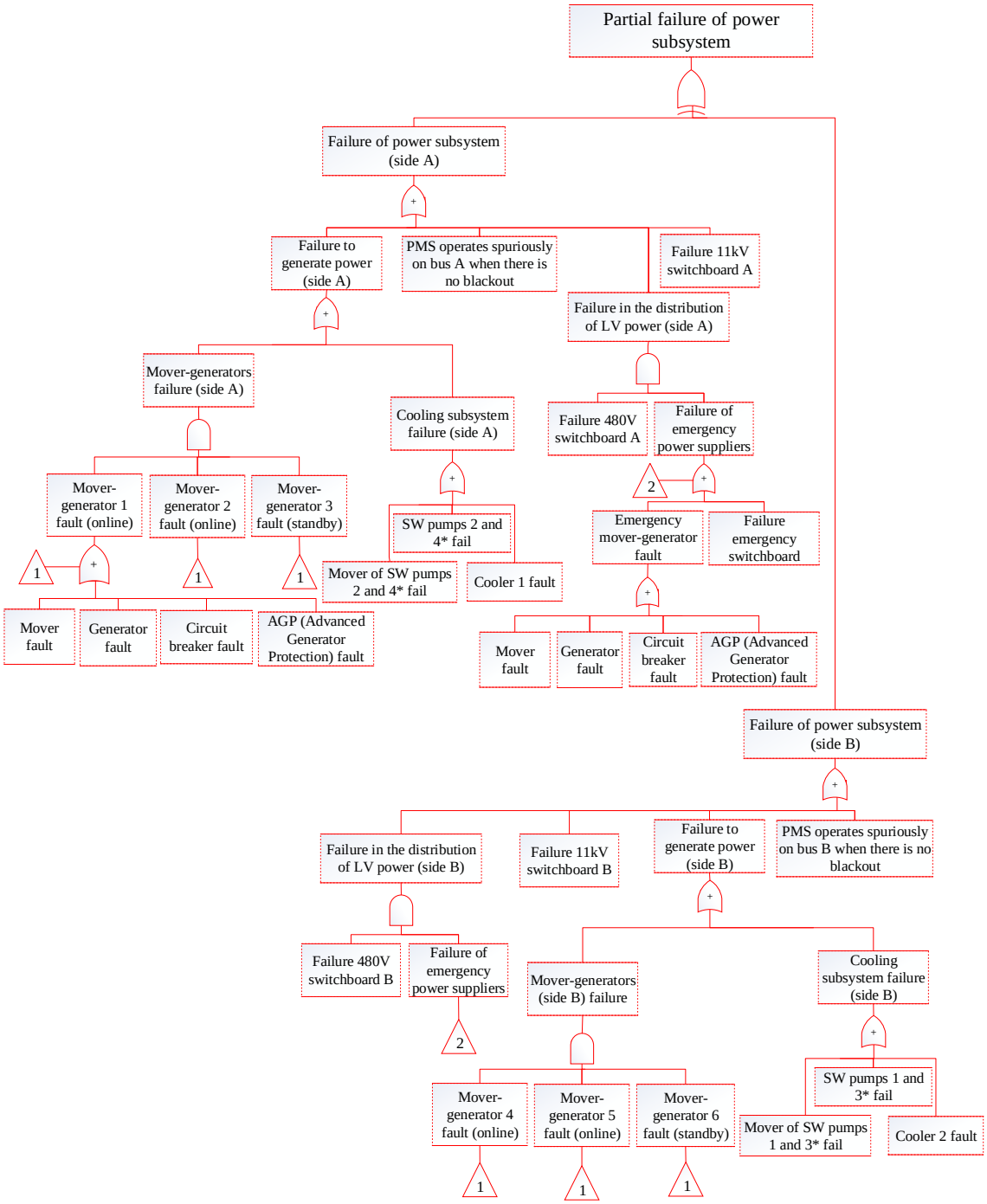


Figure 55 - Fault tree for power subsystem in case study #1 (controlled drift)
(*) Equipment that has standby redundancy.

Regarding the thruster subsystem, this generates partial propulsion loss, therefore, the occurrence of the partial drift if two or three sets of thrusters fail. According to the FMEA of vessel, the thrusters of the platform are configured in pairs as shown in Figure 48 and each pair of thrusters has components in common. The tree of Figure 56 represents both: the failure

of common components (which generates the loss of one set of thrusters) and the failure of the components that are independent for each thruster. Figure 57 shows in detail the thruster failure.

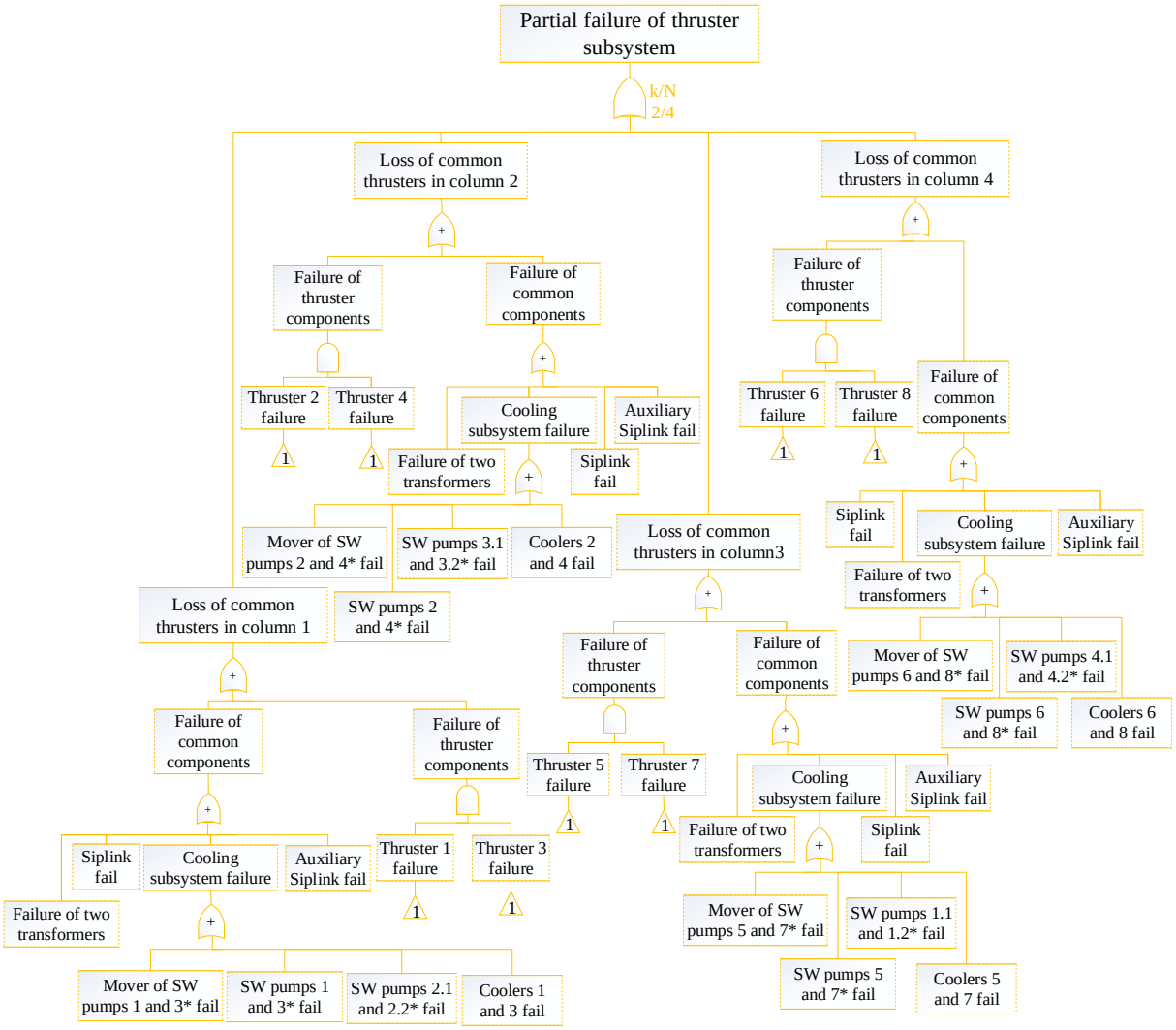


Figure 56 - Fault tree for thruster subsystem in case study #1 (controlled drift)
(*) Equipment that has standby redundancy.

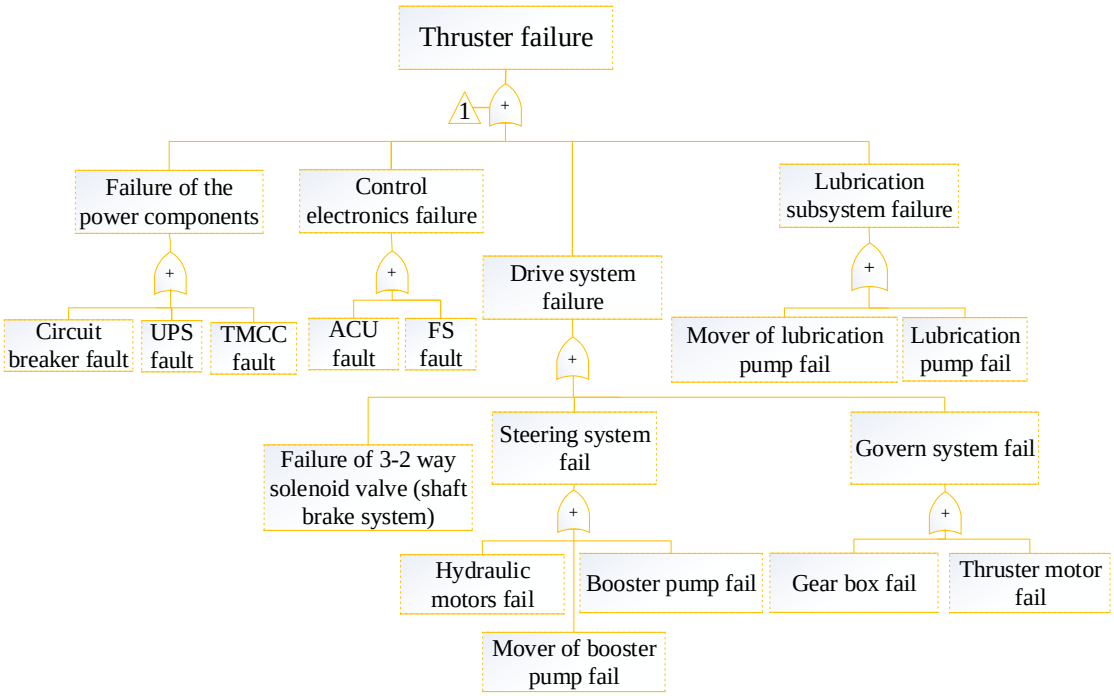


Figure 57 - Fault tree for thruster in case study #1

Another subsystem that partially fails and can cause controlled drift is the control subsystem. The partial failure of the control subsystem happens when all the control computers or the environmental sensors and PRSs that are exclusives to them fail. That is, Analyzers insured in this tree that the sensors and PRS shared with the IJS do not fail in order to have a partial and not total failure of the control subsystem. Figure 58 shows the failure tree of the control subsystem.

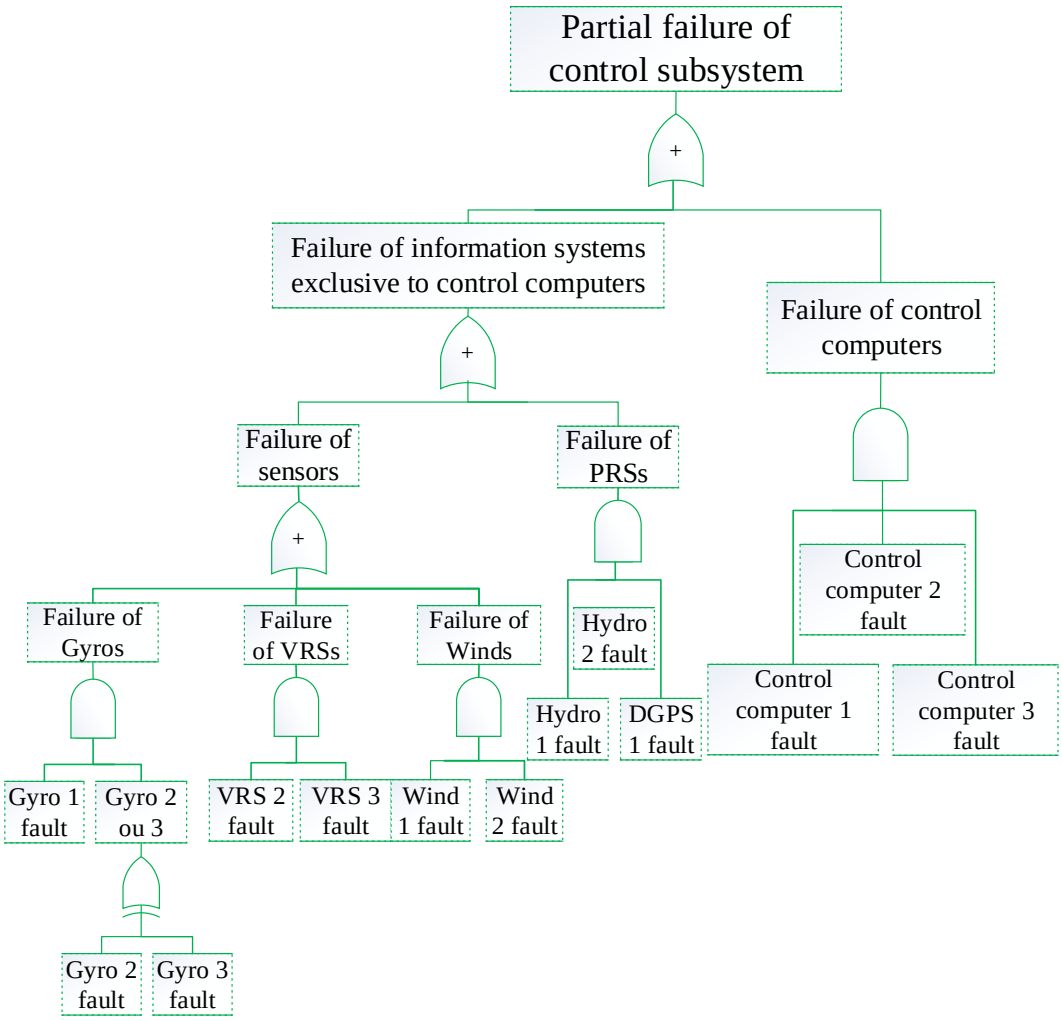


Figure 58 - Fault tree for control subsystem in case study #1 (controlled drift)

5.1.2 Free drift for case study #1 – DP2 Semi-submersible platform

Free drift resulting from the total loss of propulsion occurs when there is a total failure of one the main subsystems. Figure 59 shows a macro fault tree of this event. There will be further details about this tree through the development of each base event.

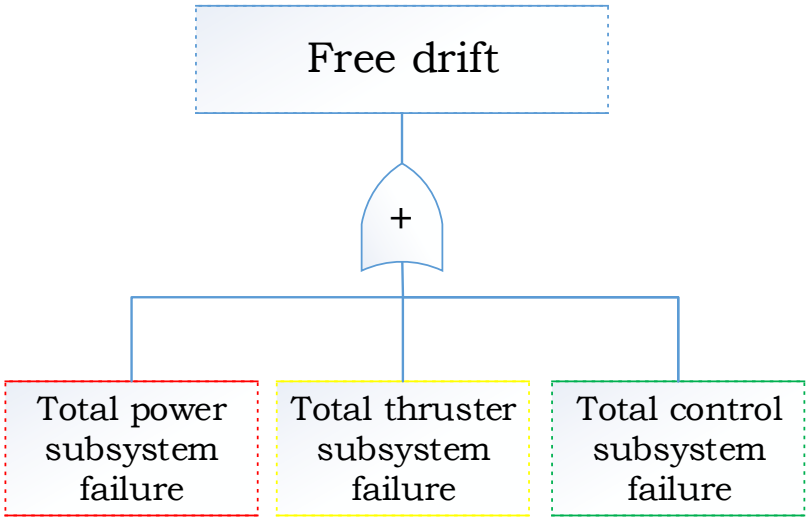


Figure 59 - Fault tree for free drift in case study #1

Regarding the failure of power subsystem, the fault tree in Figure 60 identifies that a complete failure of subsystem occurs if any of the following failures occur:

I. Total failure of fuel subsystem, which the loss of the two fuel oil transfer pumps may cause it (this subsystem was not considered in the partial failure, since if one of the pumps fails, the other will be able to supply fuel for the all mover-generators, so the failure of these pumps only could lead to a total failure).
II. Failure to generate power occurs when both sides of the electrical circuit are unavailable (side A and side B). Note that it is possible to operate some equipment of the control subsystem and electric components of the thrusters with the UPSs; but as the UPSs cannot supply the amount of power that the thrusters need, then a failure to generate power will result in the loss of the vessels because the thrusters will be lost.
III. Total failure of lubrication subsystem. This failure event occurs when two lubricating oil transfer pumps fail (as in the fuel subsystem, these pumps only cause a total loss of the power subsystem because if one fails the other can transfer lubricating oil to all the mover-generators).
IV. Total failure in the distribution of LV power, this occurs when there is loss of LV power on the sides (A and B) of the electrical circuit of the vessel. As discussed earlier, two 480V switchboards receive power from the main switchboards through a three-phase transformer each, and in case one transformer fails, the other can take

over its function. Thus, if the transformers or the two LV switchboards fail and the emergency components are not capable of supplying 480V power, the vessel will be in free drift, as it will lose power to all DP system UPSs and auxiliary equipment of thrusters.

V. Bus-bare failure, that is, HV switchboards operate with bus-bare closed, in case of bus-bare present failures like short circuit, earth fault, etc., the entire power supply of 11kV will be lost.

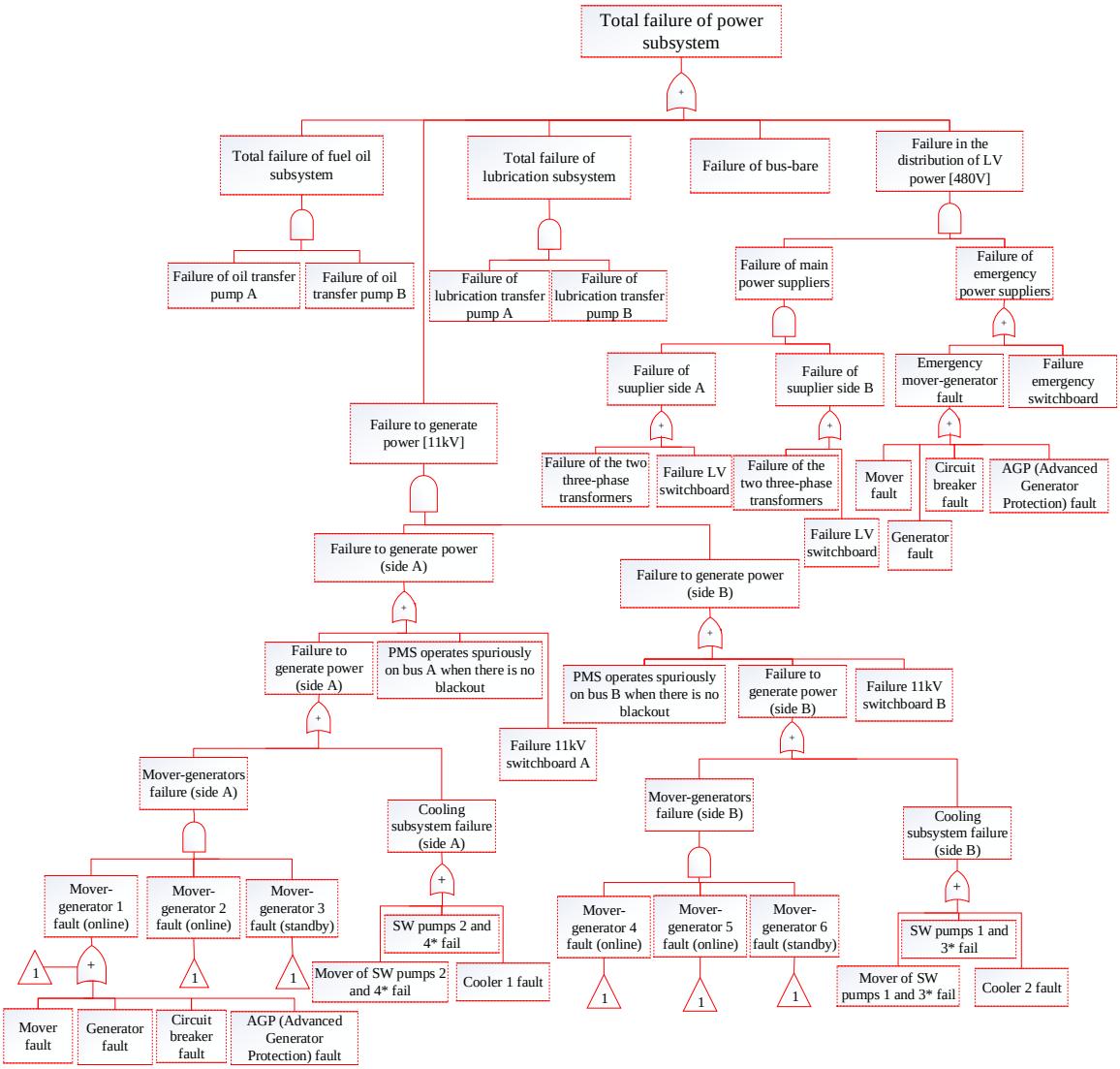


Figure 60 - Fault tree for power subsystem in case study #1 (free drift)
(*) Equipment that has standby redundancy.

In case of the thruster subsystem, free drift will occur in the event of loss of four sets of thrusters (columns of thrusters). It is important to know that possibly the platform does not have to lose all the thrusters to reach a free drift, (for example, in case of the vessel has only one or two thrusters available, depending on the environmental conditions, the vessel may already be in free drift). However, the analysis is developed considering as free drift the total loss of propulsion (no thruster operates, see Figure 61).

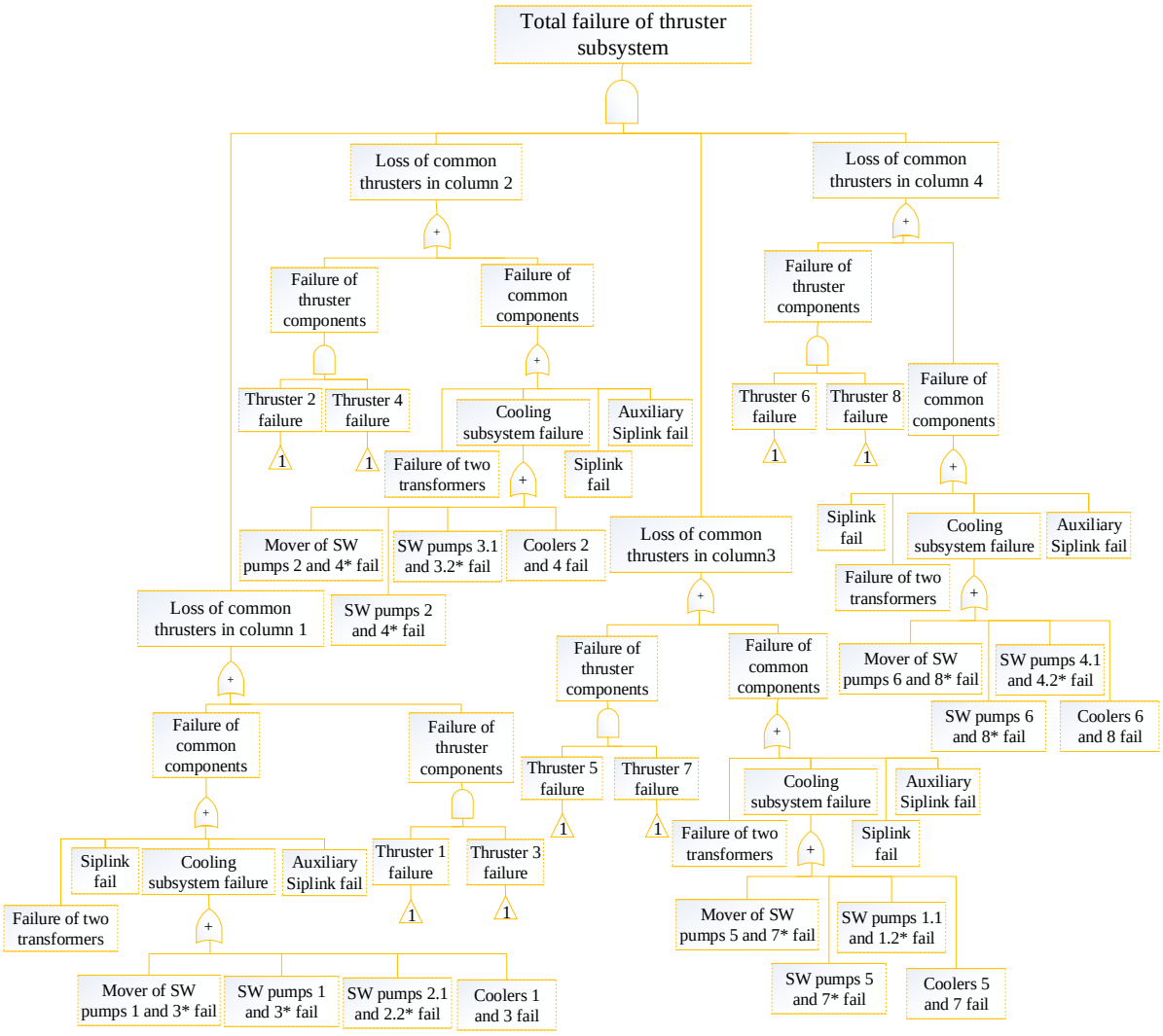


Figure 61 - Fault tree for thruster subsystem in case study #1 (free drift)
(*) Equipment that has standby redundancy.

The total failure of the control subsystem will occur when all system controllers (control computers and IJS) fail or critical UPS failures occur (see Figure 62). Following the

structure shown in Figure 48, UPS B and UPS C are critical. When they fail, the DP system loses two control computers, the IJS, some sensors (VRS2, VRS3, Wind1, Wind3, Gyro2 and Gyro3) and the four position reference systems (Hydroacoustic1, Hydroacoustic2, DGPS1 and DGSP2), while UPS A supplies power to the control computer 1 and sensors, providing redundancy for sensors but not for position reference systems. Similarly, it is noted that when UPS A operates and critical UPS fails, DP system loses control because it does not have PRS information.

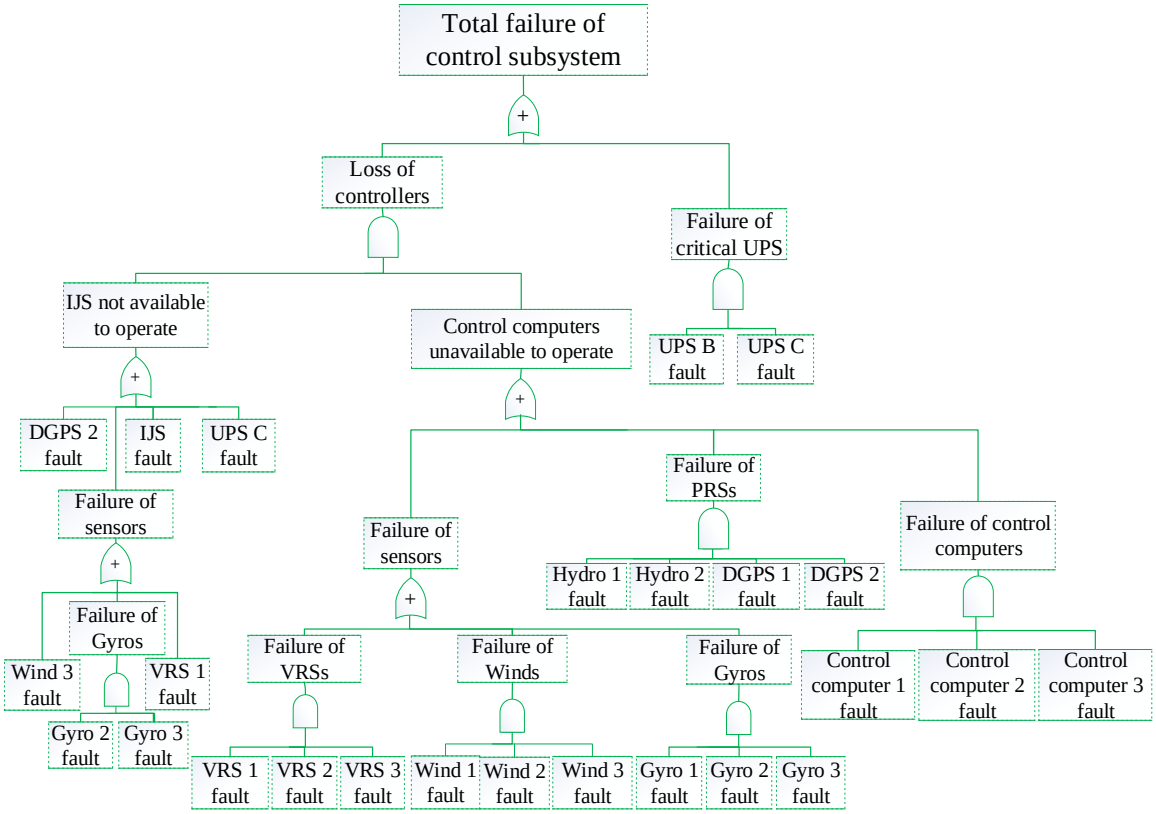


Figure 62 - Fault tree for control subsystem in case study #1 (free drift)

5.1.3 Controlled drift for case study #2 – DP3 Drillship

As in case study #1, the controlled drift of the drillship will occur when partial failure of the main subsystems (power, thruster or control) occurs. However, the overall structure changes as the drillship do not have Siplink (electronic component that ensures that all thrusters remain online even if a switchboard fails) and that the drillship operates with open

bus-bare. Thus, it was necessary to elaborate an FT where the power and thruster subsystems are evaluated independently for each electric circuit of the vessel (see Figure 63).

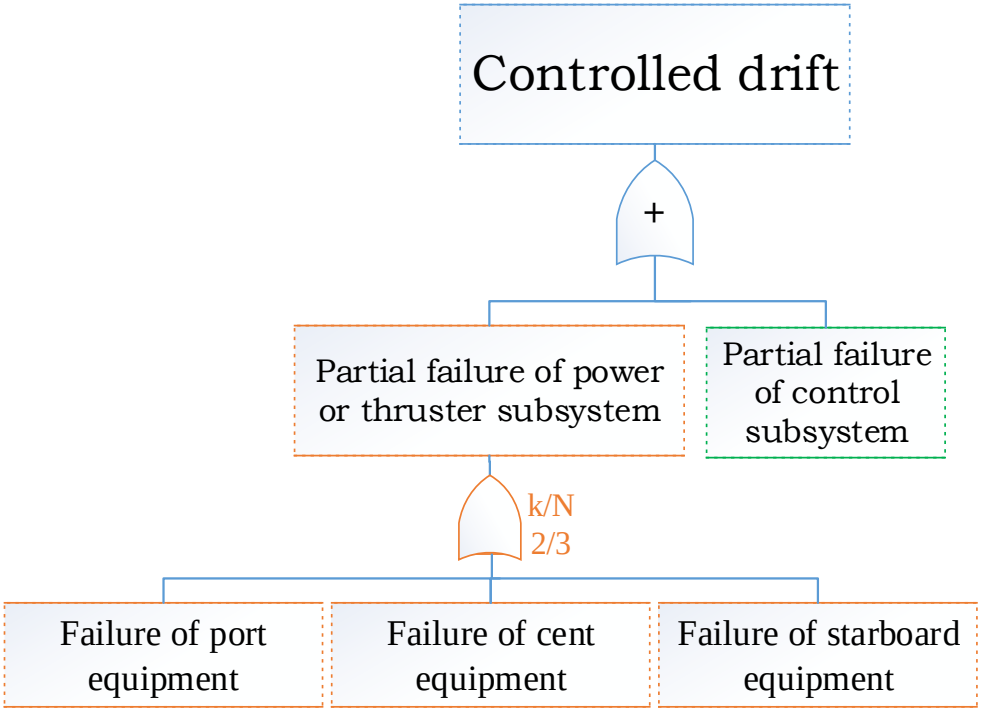


Figure 63 - Fault tree for controlled drift in case study #2

It is worth noting that in order to be a partial failure, it requires the failure of at most two of the three sides of the electric circuit of the vessels If the three sides fail, another top event would occur, the free drift (event developed afterwards in the next section).

The previously exposed structure lead the elaboration of the tree in Figure 64, which shows the events that can lead to the loss of power equipment or propulsion in the drillship port.

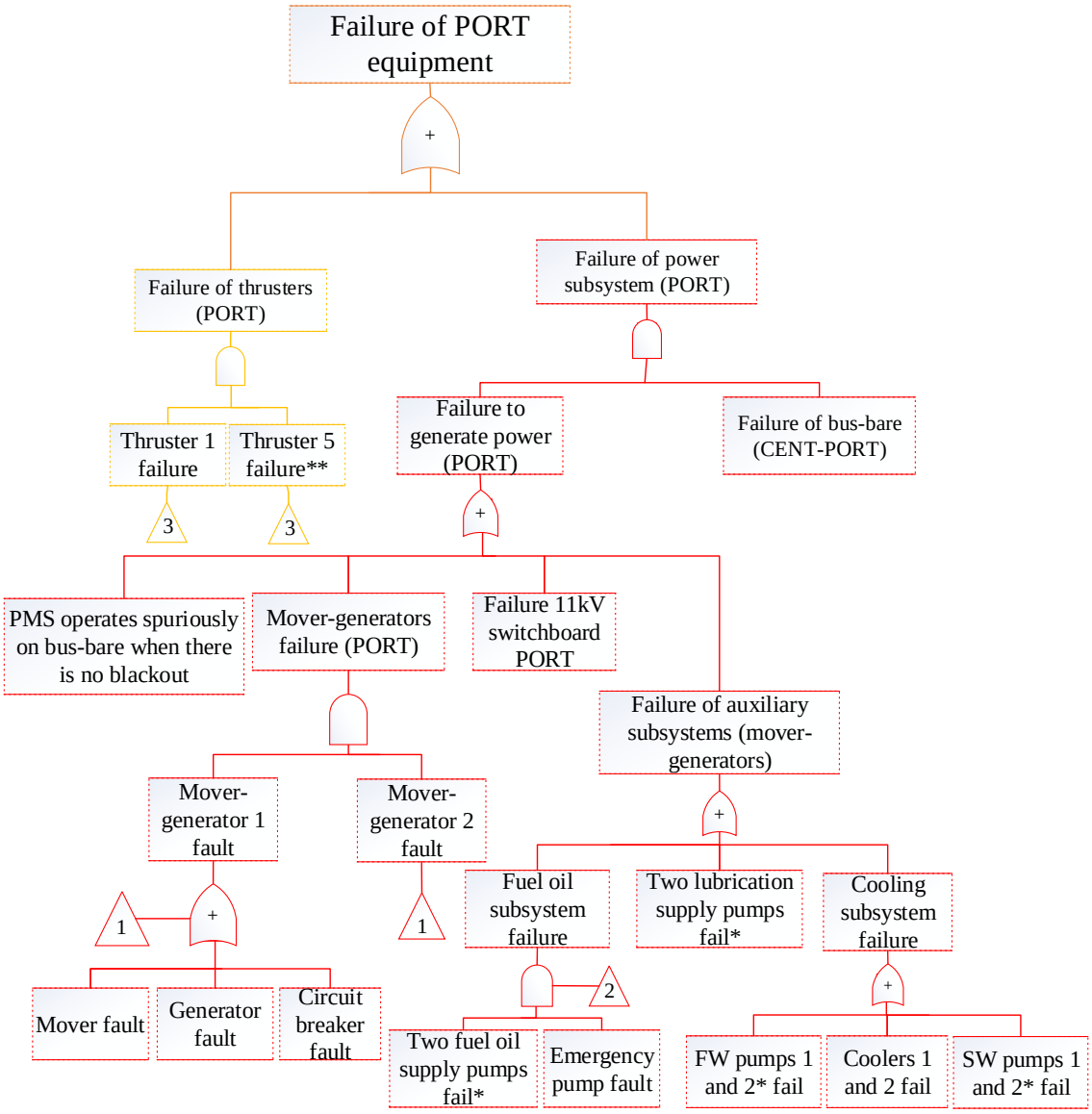


Figure 64 - Fault tree for power or thruster subsystem of PORT equipment in case study #2 (controlled drift)
(*) Equipment that has standby redundancy.
(**) The cooling subsystem of thruster 5 is shared with the mover-generators of PORT.

The PORT equipment may fail due to failure in thruster subsystem or due to loss of power (loss of PORT power generation and inability to obtain power from another vessel electric circuit due to bus bar failure). Each of these events will be detailed below.

- Failure to generate power in PORT electric circuit happens if any of the following events occur:

I. PMS failure: knowing that in case of PMS failure (no signal), the operator can activate manually the switchboards. In the fault tree in question, it was considered PMS failure that generates false demands on the side of the electrical circuit under study (for example, operates spuriously on one bus when there is no blackout).
II. Failure of mover-generators that supply power for LV switchboard 2, thrusters 1 and thruster 5.
III. Failure of the high voltage switchboard (11kV); leading to a failure in the distribution of power between the mover-generators, thrusters and transformers of LV switchboards.
IV. Failure of auxiliary subsystems of mover-generators. The failure of lubricating subsystem occurs if the two lubricating supply pumps (main and redundant) fail; the fuel oil subsystem fault occurs if two fuel supply pumps and the emergency supply pump fails; the cooling subsystem fails if any critical equipment fails.

- Failure in PORT thruster subsystem occurs when thrusters 1 and 5 fail. Figure 65 details the thruster failure.

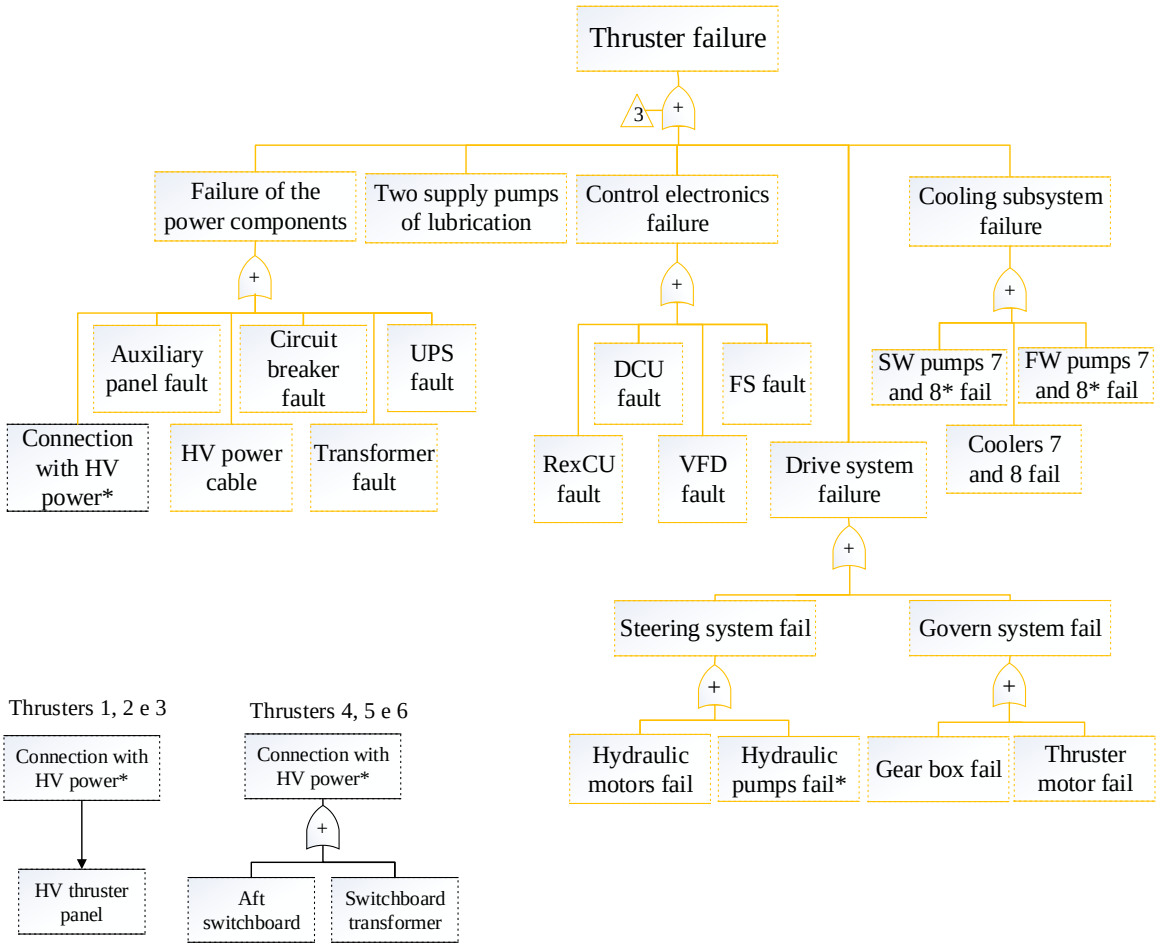


Figure 65 - Fault tree for thruster for case study #2

(*) The connection component between HV power and the thruster may be different for each thruster. As shown in Figure 50, the thrusters 1, 2 and 3 have HV panels; whereas in thrusters 4, 5 and 6 the transformers are connected directly to the HV switchboards. For the power supply to auxiliary equipment, the thrusters 1, 2 and 3 use the panel and the thrusters 4, 5 and 6 use a transformer and an LV switchboard (Aft switchboard).

The structure of FT for the power or thruster subsystem of PORT is similar to the power or thruster subsystem of CENT and STBD. Figure 66 shows the FT of Center and Figure 67 presents the FT for the Starboard equipment.

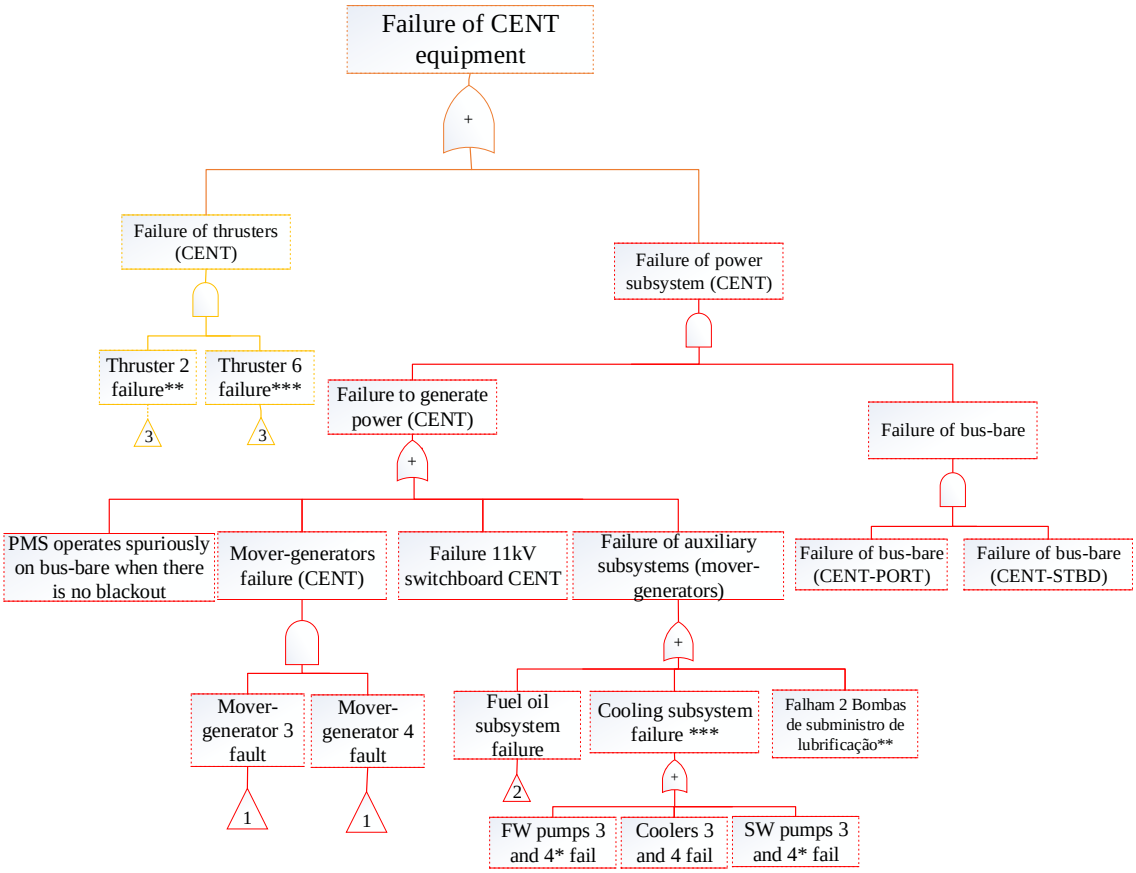


Figure 66 - Fault tree for power or thruster subsystem of CENT equipment in case study #2 (controlled drift)

(*) Equipment that has standby redundancy.

(**) Thruster 2 has three relevant characteristics: it has a HV panel, while thruster 6 does not because the transformer of thruster 6 is directly connected to the HV switchboard of the center. Thruster 2 does not have a LV switchboard for its auxiliary equipment as it does for thruster 6; and thruster 2 does not present redundancy in the cooler of the cooling subsystem (i.e. thruster 2 only have one unit of cooler).

(***) Thruster 6 shares the cooling system with the mover-generators of CENT.

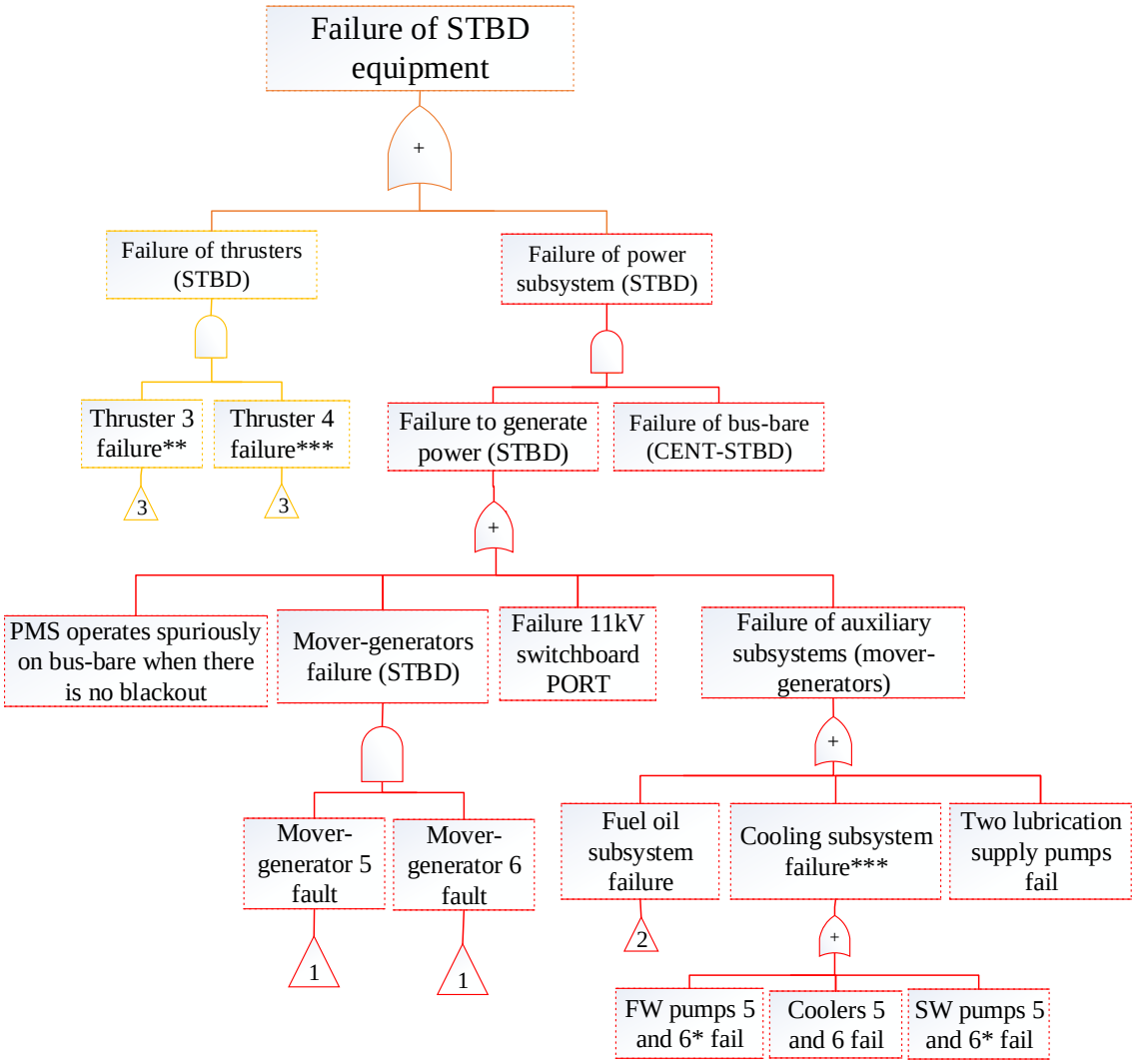


Figure 67 - Fault tree for power or thruster subsystem of STBD equipment for case study #2 (controlled drift)

(*) Equipment that has standby redundancy.

(**) Thruster 3, as well as thruster 2, have three relevant characteristics: thruster 3 has a HV panel whereas thruster 4 does not, since its the transformer is directly connected to the HV switchboard of the starboard; thruster 3 does not have a LV switchboard for its auxiliary equipment as it does for thruster 4; and thruster 2 does not present redundancy in the cooler of the cooling subsystem.

(***) Thruster 4 shares the cooling system with the mover-generators of STBD.

Finally, the partial failure of controls subsystem occurs when the control computers fail or they cannot operate due to loss of information, and the drillship loses the backup control station as well. Thus, the only way to control the vessel will be by IJS. Figure 68 shows the partial failure tree of the control subsystem.

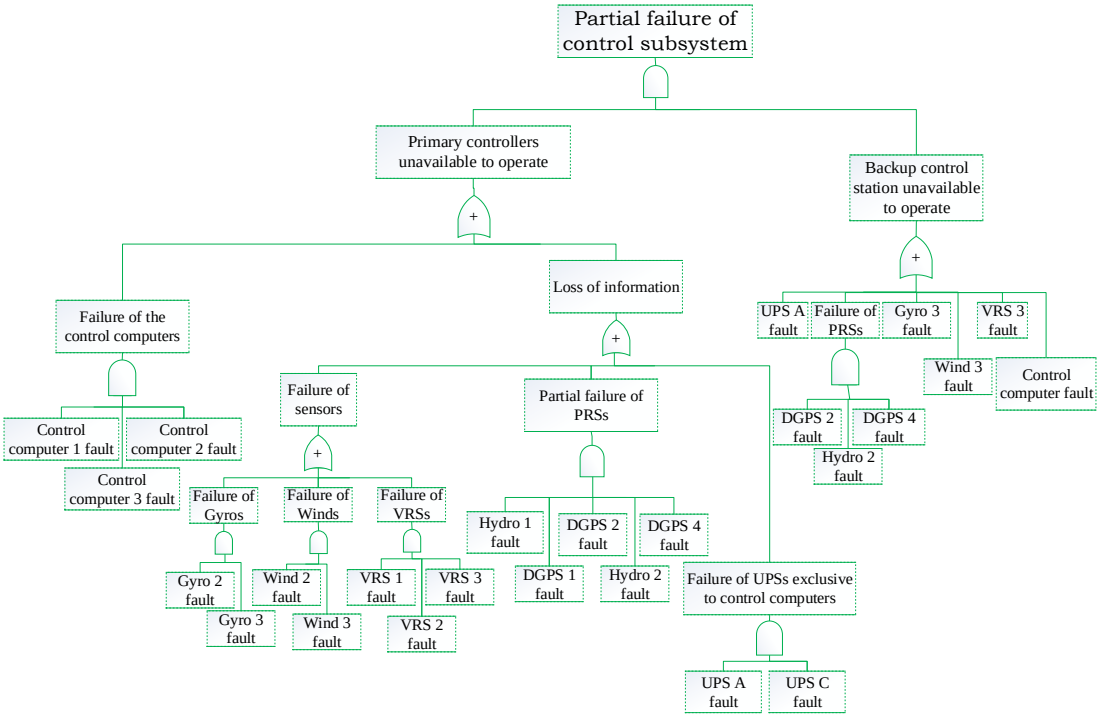


Figure 68 - Fault tree for control subsystem in case study #2 (controlled drift)

5.1.4 Free drift for case study #2 – DP3 Drillship

Free drift occurs when the drillship loses at least one of the subsystems of the DP system (power, thruster or control). Figure 69 shows the FT of this event, considering a design similar to the controlled drift event.

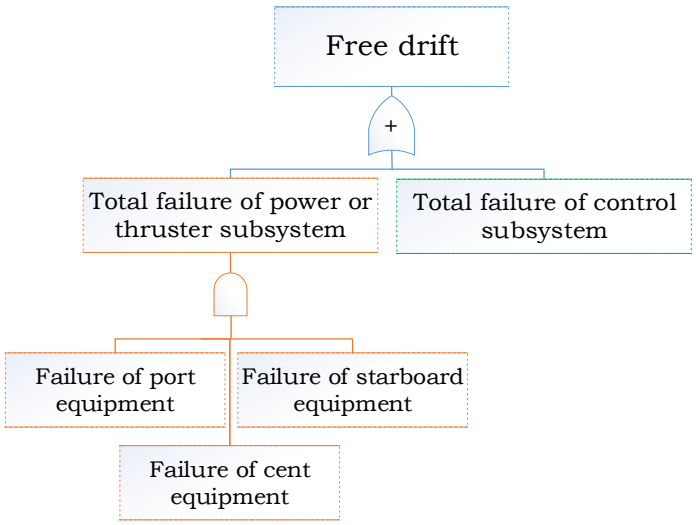


Figure 69 - Fault tree for free drift in case study #2

The total failure of the power or thruster subsystem occurs if all sections of the vessel fail (port, center and starboard) as shown previously in Figure 64, Figure 66 and Figure 67.

As for the control subsystem, the total failure will occur if all position control means are unavailable (control computers, backup control station and IJS), see Figure 70.

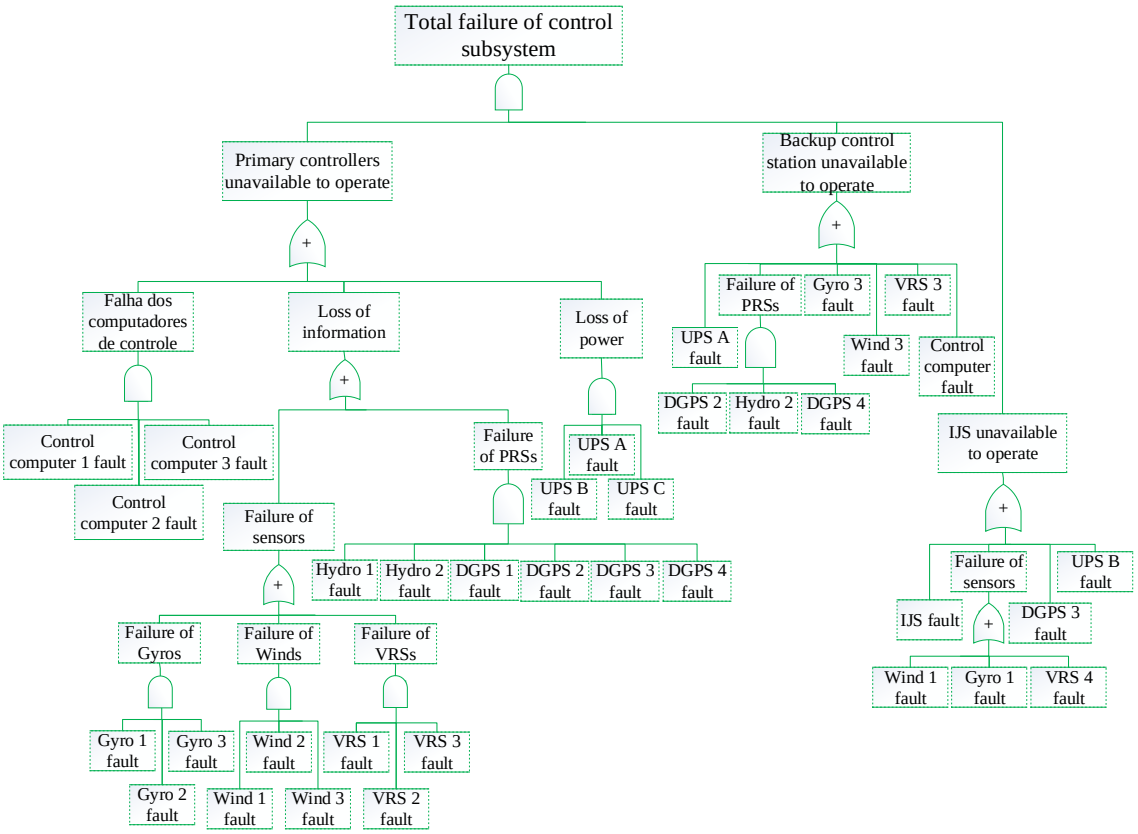


Figure 70 - Fault tree for control subsystem for case study #2 (free drift)

5.1.5 Fault Tree quantification

Once having designed the FTs, as the objective of continuing the reliability analysis, each tree was quantified based on the current technological maturity and the failure rates of components reported by the offshore industry. The methodology developed for calculating the probabilities of top events (free drift and controlled drift of vessels) is further discussed in the following sections.

5.1.5.1 Data collection for quantification of FTs

The failure rates in FTs are based on the failure rate of components published in OREDA - Offshore and Onshore Reliability Data (2015), IEEE 493-IEEE (2007), the handbook of reliability prediction procedures for mechanical equipment of NSWC - Naval Surface Warfare Center (2011), the Failure Report, Analysis and Corrective Actions of the National Institute of Oceanic Technology of India, NIOT-FRACAS (2015) and a review of the reliability of electric distribution system components of EPRI - Electric Power Research Institute (2001).

Table 11 shows the failure rate associated with each component and the source of information used to obtain this value.

Table 11 - Failure rate data used for the analysis

Component	Failure rate[failures/h]	Source
Engine (online)	1.13E-05	OREDA (2015)
Engine (standby)	5.49E-05	OREDA (2015)
Generator (online)	1.82E-05	OREDA (2015)
Generator (standby)	3.00E-05	OREDA (2015)
Circuit Breaker	2.29E-06	EPRI (2001)
AGP	2.85E-06	Martini (1993)
PMS	1.74E-05	OREDA (2009)
Switchboard 11kV	2.05E-06	IEEE STD 493 (2007)
Transformer (switchboards)	7.08E-07	EPRI (2001)
Switchboard 480V	1.08E-06	IEEE STD 493 (2007)
Switchboard 440V	9.16E-08	IEEE STD 493 (2007)
Emergency engine	5.46E-06	OREDA (2015)
Emergency generator	2.66E-05	OREDA (2015)
Emergency switchboard (480V)	1.08E-06	IEEE STD 493 (2007)
Emergency switchboard (440V)	9.16E-08	IEEE STD 493 (2007)
Bus-bare	1.71E-07	EPRI (2001)
HV cabo of power	2.11E-07	IEEE STD 493 (2007)
Panel of thruster	6.07E-07	IEEE STD 493 (2007)
Auxiliary panel of thruster	6.07E-07	IEEE STD 493 (2007)
Siplink	1.30E-10	Bala et al. (2012)
Auxiliary siplink	1.30E-10	Bala et al. (2012)
TMCC	1.14E-05	Bala et al. (2012)

Component (continuation)	Failure rate [failures/h] (continuation)	Source (Continuation)
Transformer (thruster)	1.71E-06	EPRI (2001)
RexCU	1.14E-05	Fankhauser (2001)
DCU	1.14E-05	Fankhauser (2001)
VFD	3.12E-06	TMEIC (2013)
UPS	8.95E-06	OREDA (2015)
ACU	1.14E-05	Fankhauser (2001)
FS	2.20E-06	Blischke and Murthy (2003)
Hydraulic mover	4.35E-09	Thies, Flinn and Smith (2009)
Hydraulic pump (online)	2.36E-05	OREDA (2015)
Hydraulic pump (standby)	3.57E-05	OREDA (2015)
Solenoid valve	2.32E-08	OREDA (2015)
Gear box	1.02E-05	NSWC (2011)
Mover of thruster	2.06E-05	OREDA (2015)
VRS	1.13E-05	NIOT (2015)
Wind	5.15E-05	NIOT (2015)
Gyro	3.33E-05	NIOT (2015)
Control computer	1.74E-05	OREDA (2015)
IJS	1.74E-05	OREDA (2015)
DGPS	1.02E-05	Vedachalam and Ramadass (2017)
Hydro	2.85E-05	NIOT (2015)
Pump SW (online)	5.69E-06	OREDA (2015)
Pump SW (standby)	6.15E-06	OREDA (2015)
Mover of Pump SW (online)	1.74E-05	OREDA (2015)
Mover of Pump SW (standby)	1.74E-05	OREDA (2015)
Pump FW (online)	5.69E-06	OREDA (2015)
Pump FW (standby)	6.15E-06	OREDA (2015)
Cooler	2.26E-05	OREDA (2015)
Transfer fuel oil pump (online)	6.22E-05	OREDA (2015)
Transfer fuel oil pump (standby)	7.20E-05	OREDA (2015)
Supply fuel oil pump (emergency)	3.57E-05	OREDA (2015)
Supply fuel oil pump (online)	6.22E-05	OREDA (2015)
Supply fuel oil pump (standby)	7.20E-05	OREDA (2015)
Supply lubrication pump (online)	2.36E-05	OREDA (2015)
Supply lubrication pump (standby)	3.57E-05	OREDA (2015)

(*) The failure rates collected in OREDA correspond to critical failures (failures that cause immediate and complete loss of an equipment unit capability of providing its outputs).

In cases where the data are composed of a single population; the failure rate corresponds to homogenous populations. Whereas in cases we do not have a homogeneous sample of data, i.e. the information comes from

various samples may have different failure rates and different amount of data; the so-called "OREDA estimator" of the "average" failure rate in a multi-sample is used.

Regarding standby components, the failure rate used is the rate reported in operational time; while for the online equipment, we considered the calendar time.

Calendar time is the interval of time between the start and end of data collection for a particular item. Operational time is the period of time during which a particular item performs its required function(s) between the start and end of data surveillance (OREDA, 2015).

For the information collected from the databases, it was assumed that the failure rate is in the second phase of bathtub curve, in other words, the failure rate is constant during the useful life phase provided it is properly maintained; this means that the item is not deteriorating during this phase (Portinale & Codetta, 2015).

Thus, it is possible to define the failure rate (λ) of the components/subsystems according to the following equation:

$$\lambda = \frac{number\ of\ failures}{Aggregated\ time\ in\ service} \tag{5.1}$$

Either as calendar time or operational time may measure the aggregated time in service, and the failure rate can be expressed in failure/hours.

So, the failure probability of a component/subsystem F(t) in a continuous period of operation t with a failure rate λ is calculated based on the following equation:

$$F(t) = 1 - e^{-\lambda t} \tag{5.2}$$

Consequently, the equation that stablishes reliability of a component/subsystem is:

$$R(t) = 1 - F(t) = e^{-\lambda t} \tag{5.3}$$

Considering that the instants of equipment failures can be represented by the exponential distribution, the FTs were quantified for a one-year operating period (8760 hours), nine, six and three months (6570, 4380 and 2190 hours respectively). There will be a further discussion of the result of this quantification in the following section.

5.1.5.2 Probability Calculation of top event

The top event probability is calculated from the fault tree using the probabilities that are input for the basic events.

There are several computational tools available for the quantification of FTs; commercial software commonly used to solve these analyses as SHAPIRE (Systems Analysis Programs for Hands-on Integrated Reliability Evaluations), developed by the U.S. Nuclear Regulatory Commission (U.S.NRC., 2011a).

However, for the analysis of DP systems, SAPHIRE is not helpful because the FTs of the DP systems in analysis have more than 300 Minimal Cut Sets and the method used to calculate the exact probability of top events in SAPHIRE is viable when the number of cut sets is small (generally less than 50). In addition, the proposed method by SAPHIRE for quantifying FTs with many Minimal Cut Set is the Upper Bound Method, yet this method can be considered questionable since the Minimal Cut Sets of FTs are not mutually exclusive (U.S.NRC., 2011b).

Therefore, the computation tool used in the quantification of FTs is the Engineering Reliability Analysis Software (ERAS), developed in the Analysis, Evaluation and Risk Management Laboratory - LabRisco at University of Sao Paulo (Taverna, 2017).

The software ERAS is able to calculate the exact probability of top event for the FTs with more than 400 Minimal Cut Sets (Taverna, 2017).

Table 12 presents the results obtained when quantifying the FTs of DP systems in study for mission periods of 12, 9, 6 and 3 months.

Table 12 - Probability of events of interest to each vessel in study

Subsystem	12 months		9 months		6 months		3 months	
	DP2	DP3	DP2	DP3	DP2	DP3	DP2	DP3
Partial failure of power or thruster subsystem	82,69%	15,23%	51,53%	6,94%	33,45%	2,00%	16,46%	0,18%
Partial failure of control subsystem	24,11%	18,95%	15,33%	11,87%	7,68%	5,87%	2,15%	1,33%
Controlled drift	***86,86%***	***31,29%***	***58,96%***	***17,99%***	***30,57%***	***7,75%***	***18,26%***	***1,52%***
Total failure of power or thruster subsystem	18,80%	1,49%	1,79%	0,41%	4,98%	0,06%	1,33%	0,00%
Total failure of control subsystem	7,13%	6,53%	3,53%	3,18%	1,25%	1,09%	0,20%	0,16%
Free drift	***24,58%***	***7,92%***	***13,94%***	***3,58%***	***6,16%***	***1,15%***	***1,52%***	***0,16%***

Table 12 shows the importance of evaluating the system for each mission time, i.e., the occurrence probability of top events is not linear, then, it is not advisable to evaluate the probability for 12 months and assume that the probability of this same event of interest for 3 months is a quarter of the probability obtained - it will be much smaller than that.

Another analysis that it is possible to develop from Table 12 is a comparison between the results obtained and the quantitative reliability analysis of DP systems published by other researchers.

Vedachalam and Ramadass (2017) present a quantitative evaluation of the reliability for three DP systems classes (DP1, DP2 and DP3) considering one year of mission time. The result is that the probability of failure of the DP system class 1 is 97%, while the classes 2 and 3 have 37.3% and 32.8% respectively.

Although this thesis and the research developed by Vedachalam and Ramadass (2017) have important differences, as this thesis does not evaluate DP systems class 1, the study of Vedachalam and Ramadass does not analyze mission times different from 12 months, nor the partial failure events of the main subsystems. It is possible to qualitatively evaluate the FTs

of the DP2 and DP3 systems for total faults (free drift) and to identify where possible differences in design that may result in the quantitative differences between the studies.

The FTs of DP2 system designed by Vedachalam and Ramadass (2017) showed that the vessel under study has only 3 units of PRSs and the same type (all PRSs in this study are DGPS), two control computers (the authors do not model the IJS as alternative control of the ship) and the vessel does not have the Siplink. These differences may lead Vedachalam and Ramadass (2017) getting 37.3% for the failure probability of DP2 system, while the semisubmersible platform under study in this thesis presents a failure probability of 24.6%.

Regarding the FTs of the DP3 system, Vedachalam and Ramadass (2017) argue that the DP system probability of failure is 32.8% while the drillship in study presents only 7.9% of probability of total failure. This may be explained by the fact that Vedachalam and Ramadass (2017) did not model the alternative control stations in a DP3 system (IJS and Backup Control Station), the vessel used by the authors has only one bus-bar and the PRSs modeled do not meet the diversity rule set out in international standards.

In short, although the values obtained by other authors when evaluating the DP systems are different from the values obtained in the thesis, it is possible to identify that the structures of the FTs are similar but the differences are due to the fact that each author draws the FTs for the vessel under study considering its particularities.

Once the reliability was estimated for the case studies, Monte Carlo Simulation evaluated the Minimal Cut Sets (see Appendix D), in order to compare the results obtained, and subsequently to use the technique in the maintainability and availability analysis. There is further exploration on the topic in the following sections.

5.2 Maintainability analysis

The aim of the analysis presented in this section is to evaluate the probability distribution function of the time to failure and the time to repair (duration times of a free

drift), for each DP configuration. For this analysis, all the minimal cut sets of the fault trees of free drift are identified in SAPHIRE (from a non-exact quantification method), and then the logic of minimal cut set selection presented in Appendix D is applied. The minimal cut sets identified were used to establish an equivalent system of the DP configurations under study and ERAS was used as a computational tool to apply the Monte Carlo Simulation.

Therefore, to fulfill this objective, a Monte Carlo Simulation (available in ERAS) was used, which uses the following assumptions:

i. The system can have a subdivision up to the level of its components, for which two states are possible: available or unavailable.
ii. The Fault Tree qualitative analysis provides all Minimal Cut Sets. As discussed earlier, in this context, a Minimal Cut Set indicates an irreducible combination of components that, when simultaneously unavailable, result in the system unavailability.
iii. Each component has two probability distributions as a function of time:

    a) A probability distribution of time to failure, which defines the transition from the available to the unavailable state. In these case studies, this distribution was considered exponential, as reported by the offshore industry (see Table 11).

    b) A probability distribution of time to repair, which defines the transition from unavailable to the available state. Given the characteristics of the collected data, for the case studies of this thesis a uniform distribution was considered with a domain between the minimum value and the maximum value of the active maintenance repair rates reported by the offshore industry or in some cases a triangular distribution (see section 5.2.1).

Thus, the maintenance study begins by determining the Minimal Cut Sets of FTs in which the top event is free drift, because in these cases the DP system became unavailable leading the vessel to a free drift. For each simulation of the system, the application of the

inverse transform sampling defines the transition instants of each component for the available or unavailable state.

The system, in turn, changes from available state to unavailable state when at least one of its Minimal Cut Sets has all its components unavailable; while the transition back to the available state occurs at the moment when all the Minimal Cut Sets have available at least one of their components.

Figure 71 illustrates the types of events that are simulated by the computational tool, as previously discussed.

$$t_1 - 0 = Time\ to\ failure_1$$
$$t_3 - t_2 = Time\ to\ failure_2$$

$$t_2 - t_1 = Time\ to\ repair_1$$
$$t_4 - t_3 = Time\ to\ repair_2$$

Figure 71 - Example of simulated fault and repair events in ERAS software

In Figure 71, a minimal cut set (C_j) occurs at t_1 leading to system downtime, so the time difference between t_1 and the beginning of the simulation where the system was available represents the time to failure. In addition, at time t_1 a repair begins that lasts until time t_2, at which point the system resumes operation until a new minimal cut set (C_k) occurs, which leads the system back to become unavailable.

These are randomly simulated events done in order to obtain a set of repair times and times to failure that can be studied as a good representation of reality. Given that in the previous section the probabilities of failure of the case studies have already been estimated

(see Table 12), the following sections detail the process of analysis of the repair times obtained in the simulation for each of the case studies.

5.2.1 Data collection to evaluate the duration of free drift events

As previously explained, before developing the Monte Carlo Simulation, it is necessary to define the probability distribution function of repair times of the components that make up the Minimal Cut Sets. That is, given its Minimal Cut Sets, an equivalent system can model the system being studied, drawing only the probability distributions of repair time of the basic events that constitute the Minimal Cut Sets allows to emulate the repair times of the system of interest.

OREDA - Offshore and Onshore Reliability Data Edition 6 (2015), IEEE 493-IEEE - Institute of Electrical and Electronics Engineers (2007), review of maintenance and repair times for components in technological facilities of INL - Idaho National Laboratory (2012) and the review of the reliability of electric distribution system components of EPRI - Electric Power Research Institute (2001) were some of the sources used for the maintainability and availability analysis.

Table 13 shows the active maintenance times associated with each component of Minimal Cut Sets and the source of information used to obtain this value.

Table 13 - Repair times used for the analysis

Component	Active repair time [h]		Source
	Mean	Max	
Engine	10.00	24.00	OREDA (2015)
Generator	13.92	27.00	Igba et al., (2015), OREDA (2015)
Circuit Breaker	1.00	4.00	INL (2012)
AGP	0.10	0.10	Garg and Shah (2011)
PMS	24.00	24.00	OREDA (2009)
Switchboard 11kV	2.30	4.60	IEEE STD 493 (2007)
Bus-bare	3.50	7.00	EPRI (2001)
RexCU	4.00	8.00	Garg and Shah (2011)
DCU	4.00	8.00	Garg and Shah (2011)
VFD	0.50	2.00	TMEIC (2013)
UPS	12.00	24.00	Karpati et al., (2012)
Gear box	12.73	19.60	Igba et al., (2015), Aksu and Turan (2006)
Mover of thruster	9.50	24.00	Chang et al., (2008), OREDA (2015)
VRS	10.00	20.00	Ebrahimi (2010)
Wind	0.20	3.00	VAISALA (2002), Ebrahimi (2010)
Gyro	0.50	1.00	RAYTHEON (2010), SAFRAN (2014)
Control computer	2.00	4.00	Marine Technology Society (1997)
IJS	2.00	4.00	Marine Technology Society (1997)
DGPS	0.05	1.00	Hartnett et al., (2003)
Hydro	2.00	4.00	Marine Technology Society (1997)
Cooler	1.03	8.00	Sikos (2010), Flamm and Luis (1992)
Transfer fuel oil pump	4.00	4.00	OREDA (2015)
Supply lubrication pump	4.00	4.00	OREDA (2015)

Two types of repair probability distributions were implement in the analysis. For the active maintenance times collected in OREDA (2015), the triangular distribution was used. Considering that OREDA (2015) does not present the minimum value of the active maintenance times, this value is assumed as

$$a = b - (c - b) \tag{5.4}$$

where a is the minimum value, b represent the mean value and c correspond to maximum value. The smallest value that a can take is zero.

In the case where the data source was different from OREDA (2015), two situations could occur:

i. There is only one data source that presents the average value of the active repair time only.
ii. There is more than one source of information for the average value of the active repair time.

Approaching the first situation was possible by assuming a triangular distribution where the minimum value is zero and the maximum is twice the presented average; in the second situation, a uniform distribution was assumed between the repairs times reported in the different source of information.

With these considerations and the identification of the Minimal Cut Sets the Monte Carlo Simulation was applied; the following sections discuss the outcome of this application for each of the case studies.

Note that the selection of these distributions (triangular and uniform) responds to type of data available for the study. That is, applying some distributions was not possible given the nature of the data collected, for example, with current data calculate the standard deviation of the data is not possible. However, in cases where the maintenance teams have databases of the repair times of the equipment, other distributions can be applied (as lognormal, gamma, normal).

5.2.2 Time duration of free drift events for case study #1: DP2 Semi-submersible platform

From the Monte Carlo Simulation, the repair times for the Semi-submersible platform (case study #1) were calculated through 1,000,000 simulations, considering operating times of 3, 6, 9 and 12 months. The choice of quantity of simulations respond to results obtained in Appendix D, where 1,000,000 simulations show be an adequate quantity for model the DP system operation.

It is worth mentioning that the term “repair times” refers to the time duration of free drift events, i.e. the time the maintenance team takes to recover the dynamic positioning system after a free drift (total failure of DP system).

For the operation time of one year, there were 1,974 identified faults, which required an average of 3.67 hours to be repaired. Figure 72 shows the histogram of the times obtained during the simulations.

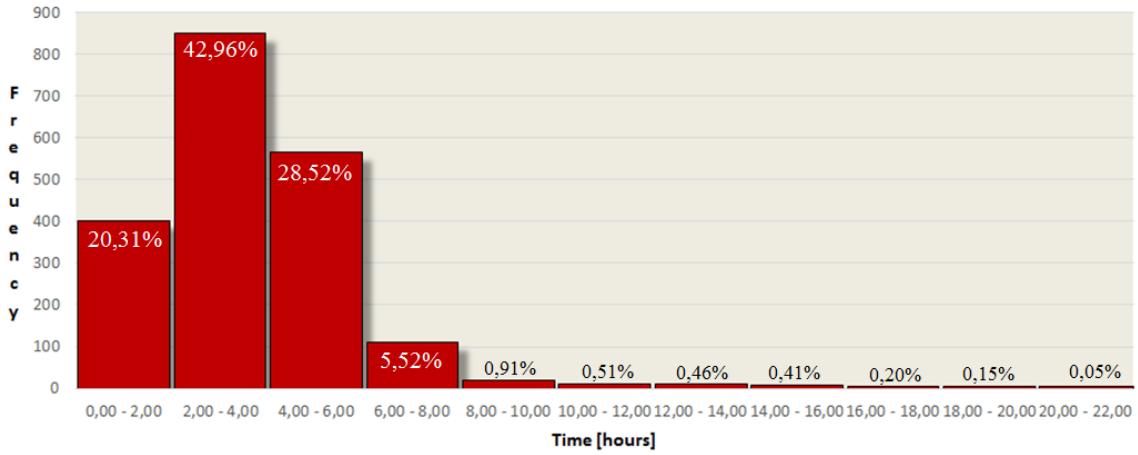


Figure 72 - Repair times for the semi-submersible platform obtained in the one-year operation simulations

The histogram of Figure 72 shows that the repair times of the case study #1 are mainly in the first 6 hours, that is, 91.79% of the repair times are between 0 and 6 hours, having a high concentration of times between 2 and 4 hours.

In the case of nine months of operation time (6,570 hours), the semi-submersible platform presents 1,464 faults in 1,000,000 simulations. These faults required an average of 3.69 hours to be repaired. Figure 73 shows the histogram of the times obtained during the simulations.

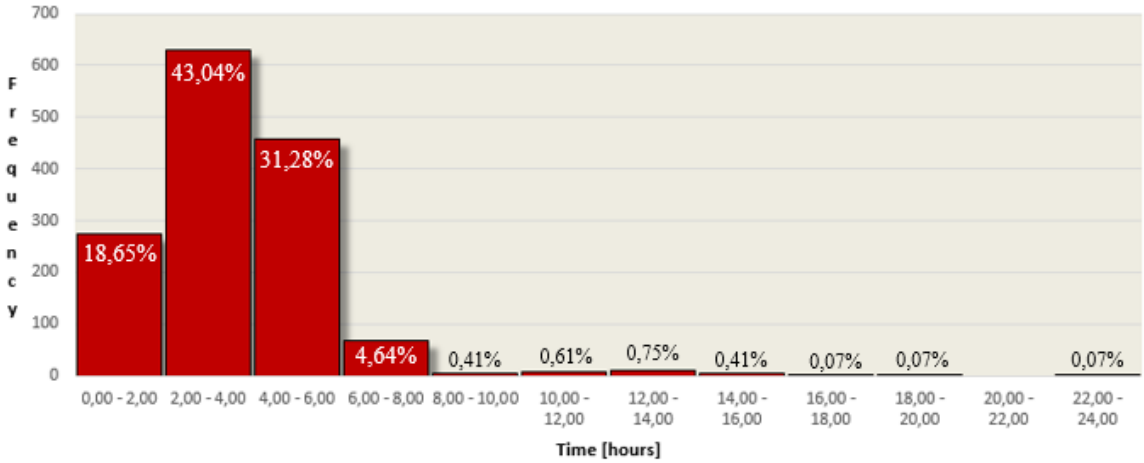


Figure 73 - Repair times for the semi-submersible platform obtained in the nine months operation simulations

Similar results appeared when considering an operating time equal to six months (see Figure 74). The histogram of repair times for six months' operation shows a higher concentration of repair times in the first six hours (92.67% of times). The analysis concluded that in 40.49% of free drifts simulated, the maintenance teams recover the vessel position in less than 3 hours.

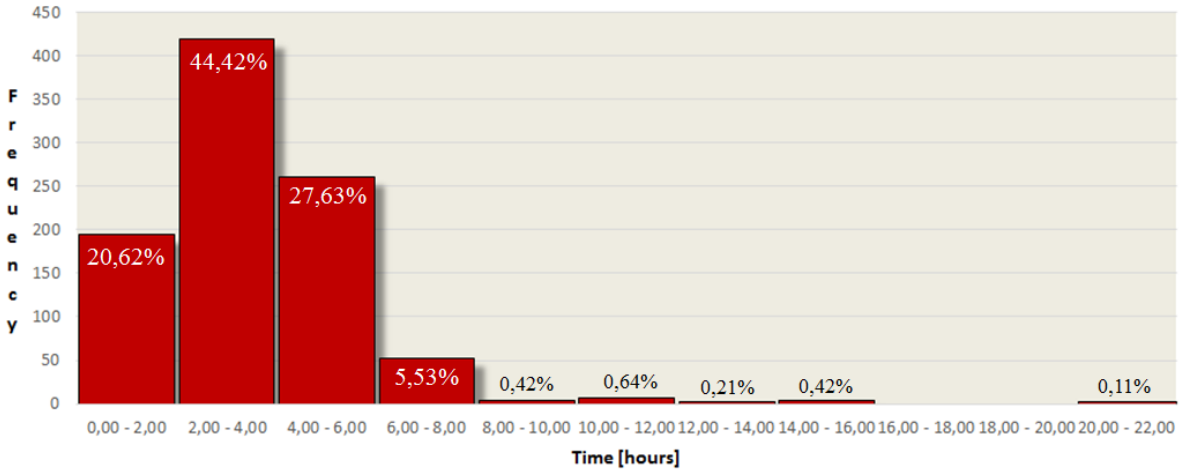


Figure 74 - Repair times for the semi-submersible platform obtained in the six months operation simulations

In general terms, the result obtained for three months operation is similar to the results obtained in simulations for six, nine and twelve months (see Figure 75). That is, considering that, the probability that a semi-submersible platform has a free drift in three months of operation is 1.52% (see Table 12); the simulations show that the recovery times are concentered in the first 6 hours (90.73% of the times are in the time interval from 0 to 6 hours).

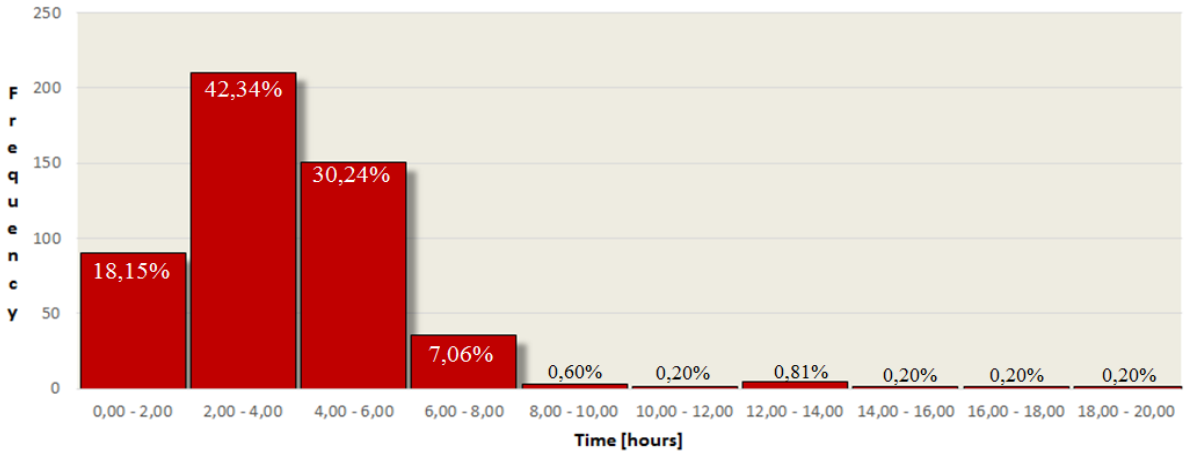


Figure 75 - Repair times for the semi-submersible platform obtained in the three months operation simulations

The simulations of three months of operation presented 496 failures that required repair between 0.01 and 18.59 hours.

An additionally analysis was developing, from repair times obtained in each operational time simulated (8760, 6570, 4380 and 2190), in order to obtain empirical pdf and theoretical pdf of data.

Using the KDE method, it is possible to estimate the empirical probability density functions of the repair times based on the Monte Carlo simulation of free drift event. Following the suggest proposed by Bhaveshkumar (2015) and Schindler (2011), the Kernel used in the design of the curves is Gaussian and the Rule-of-Thumb is used for selecting the Bandwidth (see Section 2.5.5).

Figure 76 presents the empirical pdf drawn from the repair times obtained from the simulations of DP2 semisubmersible platform.

It is worth noting that the software used to KDE implementation was the R studio; in this software the Rule-of-Thumb for choosing the bandwidth of a Gaussian kernel density estimator is already implemented and available. It defaults to 0.9 times the minimum of the standard deviation and the interquartile range divided by 1.34 times the sample size to the negative one-fifth *unless* the quartiles coincide when a positive result will be guarantee [according to Eq. (2.41)]. Thus, the bandwidth used for the pdf construction of one-year operation is 0.3397895; the pdf of nine months is drawn with a bandwidth of 0.3673646, whereas the bandwidths of six and three months are 0.4030248 and 0.4610043 respectively.

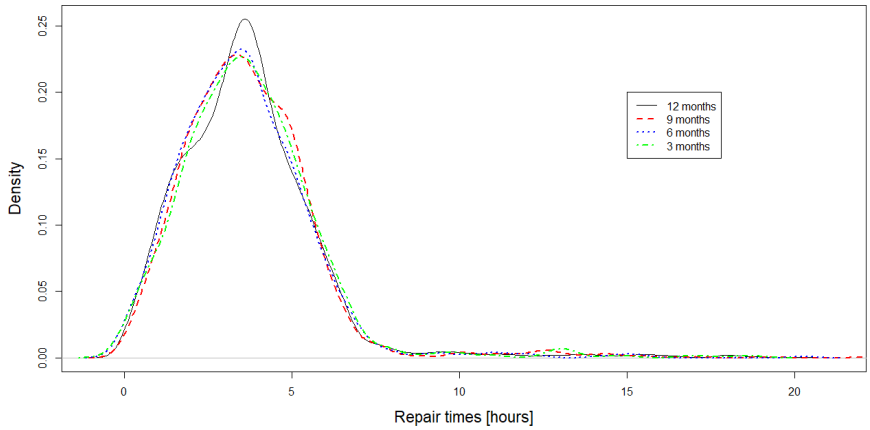


Figure 76 - Probability density functions of repair times of semisubmersible platform

Note that the curve of 12 months has a higher peak than the other three curves, however, in general all curves show similar behaviors. That is, all pdfs have a higher concentration of data at the beginning, representing that the probability of having repair times shorter than 5 hours is much greater than having repair times greater than this value.

It is important to mention that Figure 76 summarizes the results obtained, however, during the construction of pdf curves, the empirical cumulative distribution function is also studied. The empirical cumulative distribution function of repair times obtained during Monte Carlo Simulation for each different operational time of the semisubmersible platform (12, 9, 6 and 3 months) are presented. The histogram, the cumulative distribution function and the pdf for each operational time are displayed. Figure 77 presents the results obtained for 12 months of operation. Note that the empirical distribution function shows a rapid increase in the first few hours, and this responds to the fact that 91.79% of the repair times ranges from 0 to 6 hours.

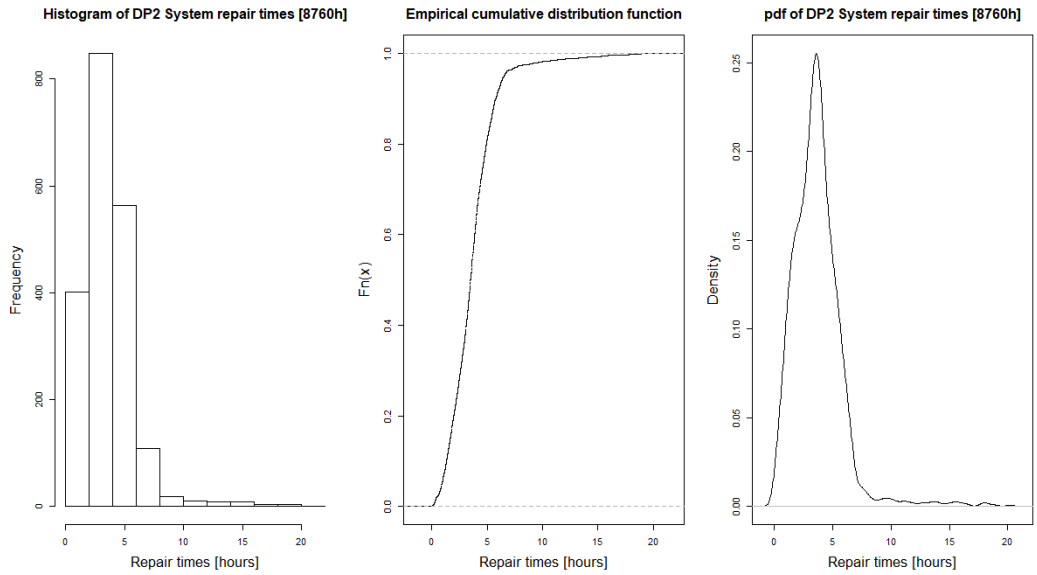


Figure 77 - Repair times obtained during simulation of 8760 hours of operation (DP2)

From Figure 78, it can be concluded that the behavior of empirical cumulative distribution functions for 9, 6 and 3 months of operation are similar with the curve for 12 months of operation. That is, assuming that the repairs are perfect, in 92% of the free drifts, the maintenance team recovers the dynamic positioning system in less than 6 hours (regardless of the time the platform has already been operating).

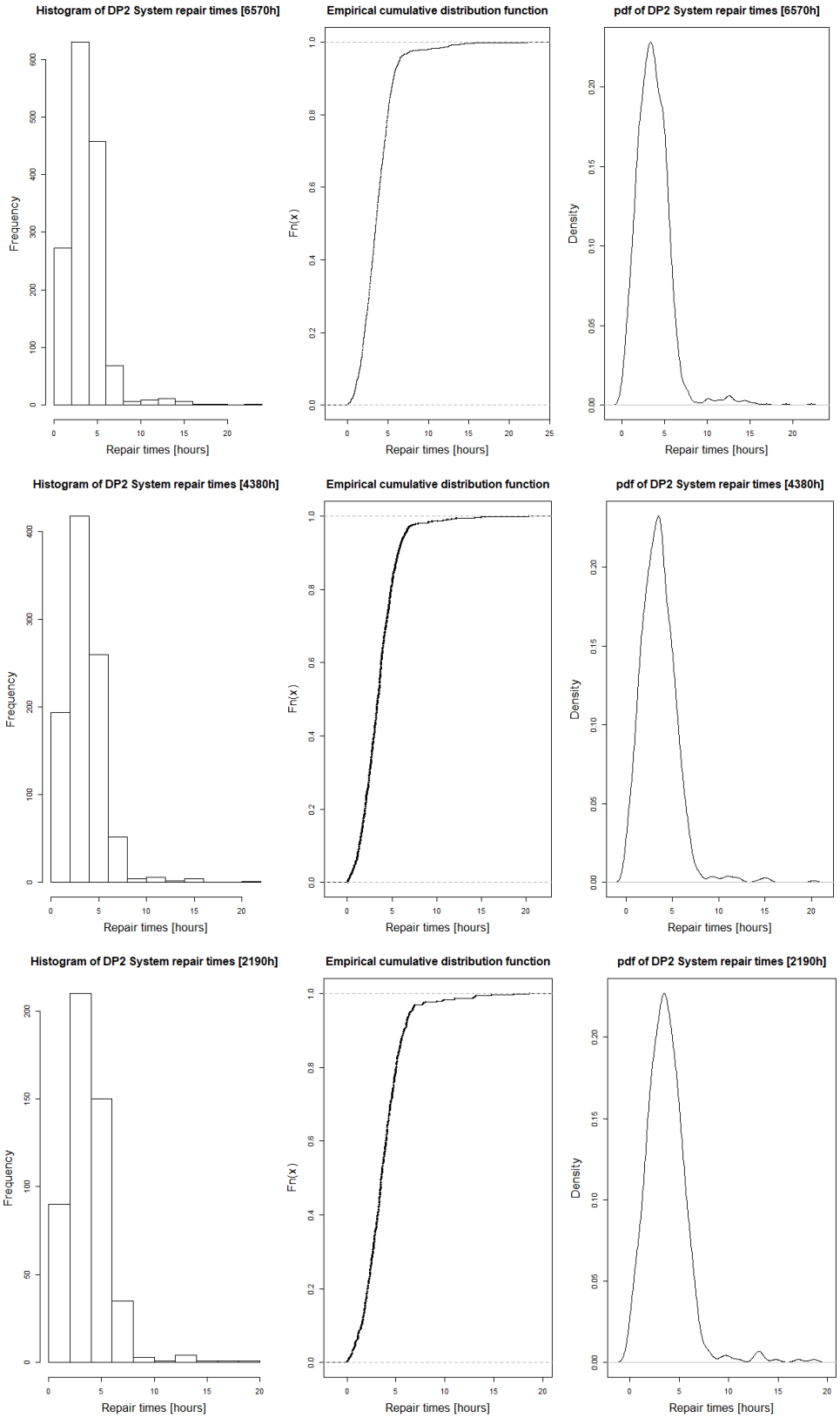


Figure 78 - Repair times obtained during simulation of 6570, 4380 and 2190 hours of operation (DP2)

In the software R studio, it is also possible to estimate the theoretical pdf of the repair times using the package GAMLSS – Generalized Additive Models for Location Scale.

GAMLSS are (semi) parametric regression type models. They are parametric, in that they require a parametric distribution assumption for the response variable, and "semi" in the sense that the modelling of the parameters of the distribution, as functions of explanatory variables, may involve using non-parametric smoothing functions. In the Appendix E the code used for estimate the parameters of the adequate distributions for the repair times simulated is exposed.

In general, Gamma is an adequate distribution for model the repair times of DP2 System (see Figure 79). However, the use of this distribution can be useful when there is no information on the repair times, for example, in this case study, the use of Gamma distribution would be interesting to estimate repair times at other operational times. In other words, when there are repair times data, it is better to consider the empirical distribution, because with parametric method some characteristics of the original pdf are lost.

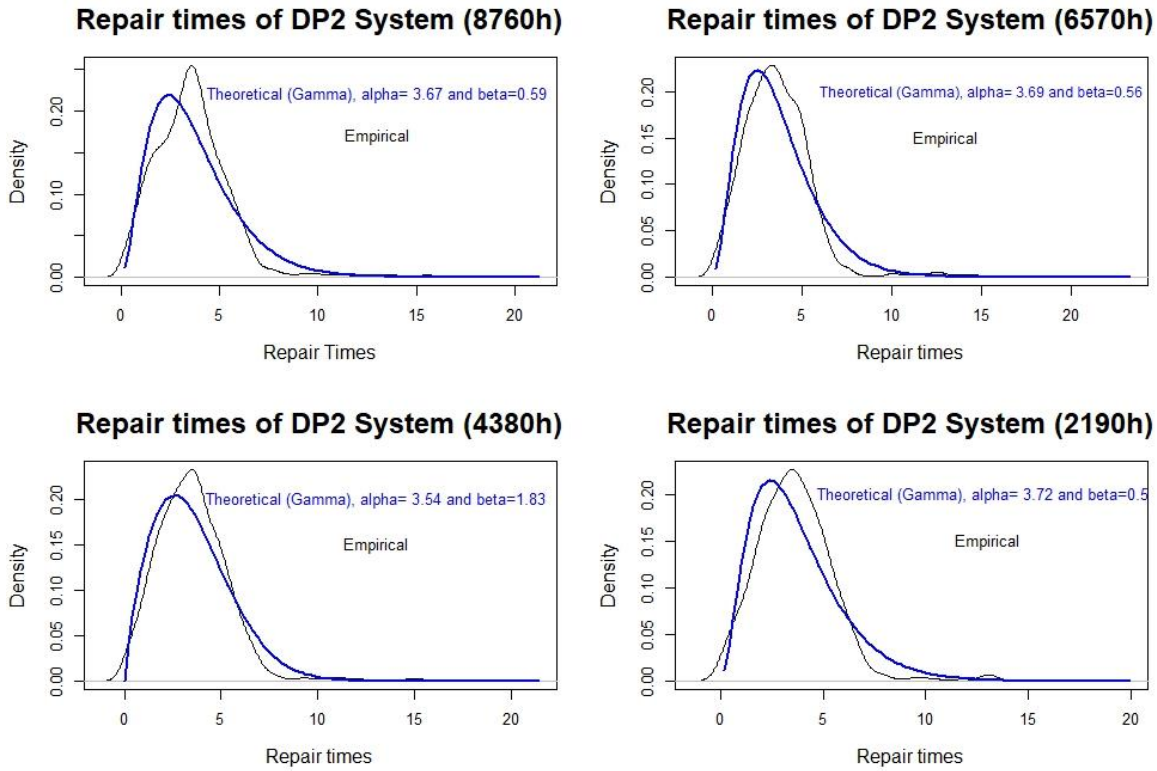


Figure 79 - Theoretical pdf of repair times simulated of DP2 system

If the reader urge explores the package GAMLSS (Stasinopoulos, Rigby & De Bastiani, 2018) and (CRANR-Project, 2019) are suggested references.

5.2.3 Time duration of free drift events for case study #2: DP3 Drillship

Regarding the DP system of drillship, there were 1,000,000 simulations of 1, 5, 10, 15, 20 and 30 years; but in none of the cases a significant amount of repair times (time duration of free drift) to construct the histograms was obtained. This is due to the fact that when the probability of system failure is very low, the computational cost to obtain downtimes from the Monte Carlo Simulation may be impracticable, a much large number of simulations will be required in order to obtain those events in which all components of a minimal cut set are unavailable.

It is worth noting that the reliability of the DP3 drillship for a year of operation is 92.08% (as presented in section 5.1.4). Additionally, by definition, the reliability is a probability that does not consider the possibility of having repair between failures of equipment during the mission time. That is, quantified FTs do not consider repairs, because after a component is unavailable, that will be its status until the end of quantification (the trees do not consider that the state of the components can present multiple transitions).

Knowing that repairs actually happen when a DP system component fails, the Monte Carlo Simulation models the transitions from unavailable to available of DP system from the repair probability distributions and shows that using the repair times presented in Table 13 and the Minimal Cut Sets obtained in the FT of the free drift event for drillship, the DP3 system unavailability times are practically null for the developed simulations.

However, there could be an additional analysis developed from the drift times modeled in the Monte Carlo Simulation is the calculation of the proportion of time in which the DP systems are available from the total simulated operating time. Next section presents the mentioned analysis.

5.3 Availability analysis

The availability analysis tries to study the probability that DP system of case studies (DP2 and DP3) will be found in the operating state at a random time in the future; and for this, it is proposed divide the analysis in two.

In the first part, the availability analysis considers prefect repairs, that is, the repair times obtained do not consider the possibility of the maintenance team making mistakes during repair. Whereas, in the second part, the availability analysis develops consider that maintenance errors can occur. Before discussing each analysis, it is worth noting that, the availability calculation in both analyses represent the asymptotic availability.

The asymptotic availability of a system refers to the steady state availability that is a stabilizing point where the system availability is roughly a constant value (Bahri, Ghribi, & Bacha, 2009); for the case studies, this probability was obtained from 100,000 simulations of 1, 5, 10, 15, 20 and 30 years to operation (see Table 14).

Table 14 - Availability of DP systems in study (consider perfect repairs)

Operational time [years]	Availability DP2	Availability DP3
1	99.9685%	100%
5	99.9831%	100%
10	99.9803%	100%
15	99.9816%	100%
20	99.9823%	99.9999%
30	99.9825%	99.9999%

As expected, the DP3 system presents a higher availability that the DP2 system for all mission times simulated.

Additionally, the result obtained in the availability analysis of the DP2 system shows a greater availability for the mission time of 5 years than for 1 year, but what it is really intended to show is the trend of the result to a constant value (the system reached its asymptotic availability value: 0.9998).

So far, the availability analysis has been developed considering perfect repairs, that is, until now the availability analysis has been developed considering that the maintenance action restores the DP system operating condition to as good as new and the probability of an error occurring during this maintenance action is zero. Knowing that, in reality, this probability of error is uncertain, therefore, impossible to guarantee it, an additional analysis using Monte Carlo Simulation was done.

The difference with the previously availability analysis is that in this Monte Carlo Simulation, when a Minimal Cut Set occurs and the system becomes unavailable, a random number is generated. If this generated number is less than or equal to the probability of an error maintenance occurrence, then the repair is considered as imperfect and the system continues in unavailable state. Afterwards, a new random number is regenerated to simulate the next round of maintenance. This cycle will occur until a perfect maintenance has happened, allowing the transition of the system to an available state (see Figure 80).

Note that the unavailability system time consider since the system fail until a perfect maintenance finish.

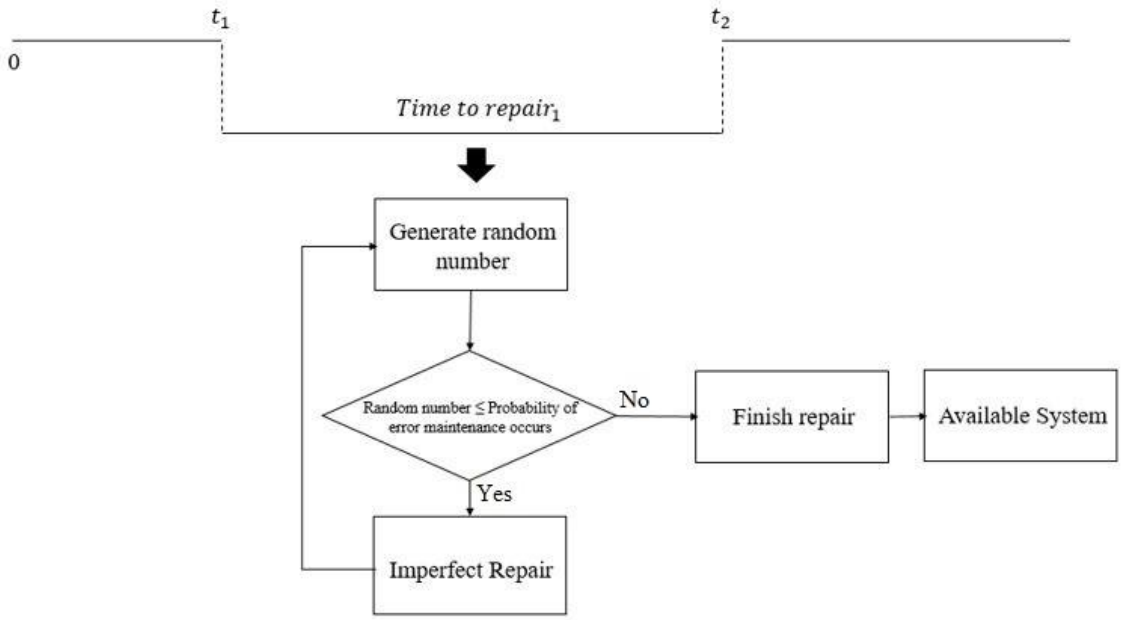


Figure 80 - Simulated repair events in ERAS software, considering probability of error maintenance occurs

Table 15 presents the availability value obtained when considering that the probability of occurrence of an error during a maintenance action is 30%, 60% or 90%.

Table 15 - Availability of DP systems in study considering errors in maintenance actions

Operational time [years]	DP2 System Probability of error maintenance occurs			DP3 System Probability of error maintenance occurs		
	0.3	0.6	0.9	0.3	0.6	0.9
1	99.9813%	99.9730%	99.2772%	100%	100%	100%
5	99.7435%	99.6114%	99.6618%	100%	100%	99.9999%
10	99.7541%	99.7830%	99.7249%	100%	99.9999%	99.9999%
15	99.7585%	99.7373%	99.7116%	99.9999%	99.9999%	99.9999%
20	99.7784%	99.8146%	99.7274%	99.9999%	99.9999%	99.9999%
30	99.8337%	99.8287%	99.7605%	99.9999%	99.9999%	99.9999%

In general, the data behavior is similar to the result obtained in the previous analysis (see Table 14). There is no fixed trend of decreasing data, since as previously commented the values presented refer to asymptotic availability. Note that DP3 system presents a higher asymptotic availability than the DP2 system for all the scenarios modeled (operational times of 1, 5, 10, 15, 20 and 30 years with any probability of occurrence of an error occur during a maintenance action).

Considering, that the evaluation of DP3 system does not present any important differences between the availabilities obtained, an analysis of an extreme scenario develops, in that the probability of a maintenance error occurs is 97%. Table 16 presents the results obtained.

Table 16 - Availability of DP systems in study considering an extreme case of error in maintenance

Operational time [years]	Probability of error maintenance occurs 0.97	
	DP2	DP3
1	99.9502%	99.9999%
5	99.9477%	99.9999%
10	99.9389%	99.9994%
15	99.9109%	99.9997%
20	99.9137%	99.9956%
30	99.8563%	99.9951%

Regarding the asymptotic availability analysis of the extreme case (probability of occurrence of an error in maintenance action = 0.97), it can be concluded that the DP3 system is more available than the DP2 system. As presented in Table 16, in general the availability of DP systems reduces as the operating times increases (this may be related to the fact that the greater the operational time, the greater the failure probability of components that will need repair and, therefore, will decrease the effective time of operation of the system).

The next section presents a proposal to evaluate the uncertainty on components failure rate in the reliability analysis. This proposal consists on the use of the Monte Carlo Simulation in order to evaluate the impact of the uncertainty about the occurrence of the basic events (equipment failure) on the top events of previously presented fault trees (free drift and controlled drift for each case study).

5.4 System reliability evaluation considering uncertainties in components failure rate

During a conventional analysis using fault trees in many engineering systems, the uncertainty of information about a given component is often ignored (A. Ferreira & Lapa, 2009).

In Section 5.1, there is a reliability analysis of the DP system developed for the typical configurations (semisubmersible platform with DP2 and drillship with DP3). In that analysis, equipment failure rates related to the basic events of fault trees are assumed to be exact; that is, FTs are quantified from the failure rates reported by the offshore industry, where the values correspond to constant failure rates and the time to failure following an exponential distribution.

Knowing that the failure rates present associated uncertainties due to the lack of knowledge about the exact value for each offshore installation under study (semisubmersible platform and drillship), an additional analysis developed considers uncertainties in the failure rate of the basic events in which the FTs are quantified through the method of Monte Carlo Simulation.

Thus, reliability modeling continues considering the exponential distribution as an adequate representation of the time to failure distribution, but having an uncertainty associated with the distribution parameter (λ). In other words, the times to failure of each component continues to be modeled by an exponential distribution, but their failure rates are also represented by a probability density function (uniform, gamma or triangular) due to the lack of certainty about their value.

In the following sections, the source of information used in the uncertainty analysis and the use of Monte Carlo Simulation as a method of quantification of the previously designed FTs (free drift and controlled drift for each DP system under study) will be present. In addition, the reader will find the 95% confidence interval for the probability of occurrence of the events of interest in each configuration under study.

Note that a 95% confidence interval is a range of values for which the analyst can be 95% certain it contains the true value.

5.4.1 Data collection for uncertainty analysis in the basic events

About 52% of the failure rates used to calculate the probability of the top events in previous section (see section 5.1) were obtained from OREDA (2015), while the remaining 48% were failure rates published in IEEE 493-IEEE (2007), the handbook of reliability prediction procedures for mechanical equipment of NSWC - Naval Surface Warfare Center (2011), the Failure Report, Analysis and Corrective Actions of the National Institute of Oceanic Technology of India, NIOT-FRACAS (2015) and a review of the reliability of electric distribution system components of EPRI - Electric Power Research Institute (2001).

For the analysis of uncertainty these sources of information together with research articles such as Omokhafe and Ambafi (2011), Martini (1993), Chavan (2016), Bala et al. (2012), Vedachalam and Ramadass (2017) and Carroll, McDonald and McMillan (2016) were used and it was necessary to take into account two different situations:

i. In the case where the initial failure rate is collected from OREDA (2015), the uncertainty over the exponential distribution parameter (λ) is obtained from the

implementation of the OREDA estimator, where a Gamma distribution is suggested and parameters α and β are established in the database OREDA - 2015;

ii. In the case where the initial failure rate is compiled from sources other than OREDA (2015), several values of the parameter λ are obtained and the uniform or triangular distribution is assumed for the uncertainty of the parameter. The uniform distribution is used in cases where the failure rates obtained from different sources present relatively similar values. The triangular distribution is used to represent the failure rates when three different sources recommend values with a difference greater than $1E-05\ \frac{failure}{hour}$, following the methodology presented by Ferrera and Lapa (2009), where the triangular distribution is used to represent the equipment failure rate.

Table 17 presents the uncertainty distribution for the parameter λ for each component, as well as the parameters of these distributions and the information source used.

Table 17 - Parameters of the distributions used to quantify the uncertainty of the parameter λ

Component	Uncertainty distribution	Parameter 1	Parameter 2	Source
Engine (online)	Gamma	7.72E-01	1.46E-05	OREDA (2015)
Engine (stand by)	Gamma	5.01E-01	1.10E-04	OREDA (2015)
Generator (online)	Gamma	1.32E+00	1.38E-05	OREDA (2015)
Generator (stand by)	Gamma	1.61E+01	1.86E-06	OREDA (2015)
Circuit Breaker	Triangular	2.29E-06	3.91E-05	EPRI (2001), Omokhafe and Ambafi (2011)
AGP	Triangular	9.36E-07	2.85E-06	EPRI (2001), Martini (1993)
PMS	Gamma	0.5318	3.27E-05	OREDA (2009)
Switchboard 11kV	Triangular	7.19E-08	4.57E-06	EPRI (2001), IEEE STD 493 (2007)
Transformer (switchboards)	Uniform	7.07E-07	7.09E-07	EPRI (2001)
Switchboard 480V	Uniform	9.16E-08	1.08E-06	IEEE STD 493 (2007)
Switchboard 440V	Uniform	9.16E-08	1.08E-06	IEEE STD 493 (2007)
Emergency engine	Gamma	2.93E-01	1.87E-05	OREDA (2015)
Emergency generator	Gamma	1.26E+00	2.12E-05	OREDA (2015)
Emergency switchboard (480V)	Uniform	9.16E-08	1.08E-06	IEEE STD 493 (2007)
Emergency switchboard (440V)	Uniform	9.16E-08	1.08E-06	IEEE STD 493 (2007)
Bus-bar	Uniform	1.71E-07	1.16E-06	EPRI (2001), IEEE STD 493 (2007)
HV cable of power	Uniform	6.16E-08	2.11E-07	IEEE STD 493 (2007)
Panel of thruster	Uniform	1.71E-08	1.27E-06	IEEE STD 493 (2007)

Component (continuation)	Uncertainty distribution	Parameter 1	Parameter 2	Source
Auxiliary panel of thruster	Uniform	1.71E-08	1.27E-06	IEEE STD 493 (2007)
Siplink	Uniform	1.04E-13	1.30E-10	Chavan (2016), Bala et al. (2012)
Auxiliary siplink	Uniform	1.04E-13	1.30E-10	Chavan (2016), Bala et al. (2012)
Transformer (thruster)	Uniform	2.28E-07	1.71E-06	EPRI (2001)
VFD	Uniform	3.12E-06	8.80E-06	TMEIC (2013), Vedachalam and Ramadass (2017)
UPS	Gamma	1.28E+00	6.99E-06	OREDA (2015)
Hydraulic mover	Uniform	4.35E-09	3.88E-07	Thies, Flinn and Smith (2009), Carroll, McDonald and McMillan (2016)
Hydraulic pump (online)	Gamma	1.00E+00	2.36E-05	OREDA (2015)
Hydraulic pump (stand by)	Gamma	1.00E+00	3.57E-05	OREDA (2015)
Solenoid valve	Gamma	1.00E+00	2.31E-08	OREDA (2015)
Gear box	Uniform	1.02E-05	1.76E-05	Vedachalam and Ramadass (2017), Carroll, McDonald and McMillan (2016)
Mover of thruster	Gamma	1.59E+00	1.30E-05	OREDA (2015)
VRS	Uniform	1.00E-05	1.13E-05	MTS (1997), Vedachalam and Ramadass (2017)
Wind	Uniform	5.15E-05	5.88E-05	Vedachalam and Ramadass (2017), MTS (1997)
Gyro	Uniform	3.33E-05	4.00E-05	Vedachalam and Ramadass (2017), MTS (1997)
Control computer	Triangular	1.74E-05	1.37E-04	Vedachalam and Ramadass (2017), MTS (1997)
IJS	Triangular	1.74E-05	1.37E-04	Vedachalam and Ramadass (2017), MTS (1997)
DGPS	Uniform	1.02E-05	5.41E-05	NOVATEL (2016), MTS (1997)
Hydro	Triangular	2.85E-05	2.50E-04	Vedachalam and Ramadass (2017), MTS (1997)
Pump SW (online)	Gamma	4.01E+00	1.42E-06	OREDA (2015)
Pump SW (stand by)	Gamma	4.01E+00	1.53E-06	OREDA (2015)
Mover of pump SW (online)	Gamma	4.00E+00	4.37E-06	OREDA (2015)
Mover of pump SW (stand by)	Gamma	4.00E+00	4.37E-06	OREDA (2015)
Pump FW (online)	Gamma	4.26E-01	1.34E-05	OREDA (2015)
Pump FW (stand by)	Gamma	4.97E-01	1.24E-05	OREDA (2015)
Cooler	Gamma	8.67E-01	2.60E-05	OREDA (2015)
Transfer fuel oil pump (online)	Gamma	1.50E+01	4.15E-06	OREDA (2015)
Transfer fuel oil pump (stand by)	Gamma	1.38E+01	5.21E-06	OREDA (2015)
Supply fuel oil pump (emergency)	Gamma	1.00E+00	3.57E-05	OREDA (2015)

Component (continuation)	Uncertainty distribution	Parameter 1	Parameter 2	Source
Supply fuel oil pump (online)	Gamma	1.50E+01	4.15E-06	OREDA (2015)
Supply fuel oil pump (stand by)	Gamma	1.38E+01	5.21E-06	OREDA (2015)
Supply lubrication pump (online)	Gamma	1.00E+00	2.36E-05	OREDA (2015)
Supply lubrication pump (stand by)	Gamma	1.00E+00	3.57E-05	OREDA (2015)

In the Gamma distribution parameter 1 corresponds to the shape parameter (α) and parameter 2 refers to the scale parameter (β). Parameter 1 in the uniform distribution corresponds to the minimum and parameter 2 to the maximum value of the domain. In the triangular distribution the minimum value is equal to difference between the maximum value and the mean, parameter 1 corresponds to the mean and parameter 2 provides the maximum value.

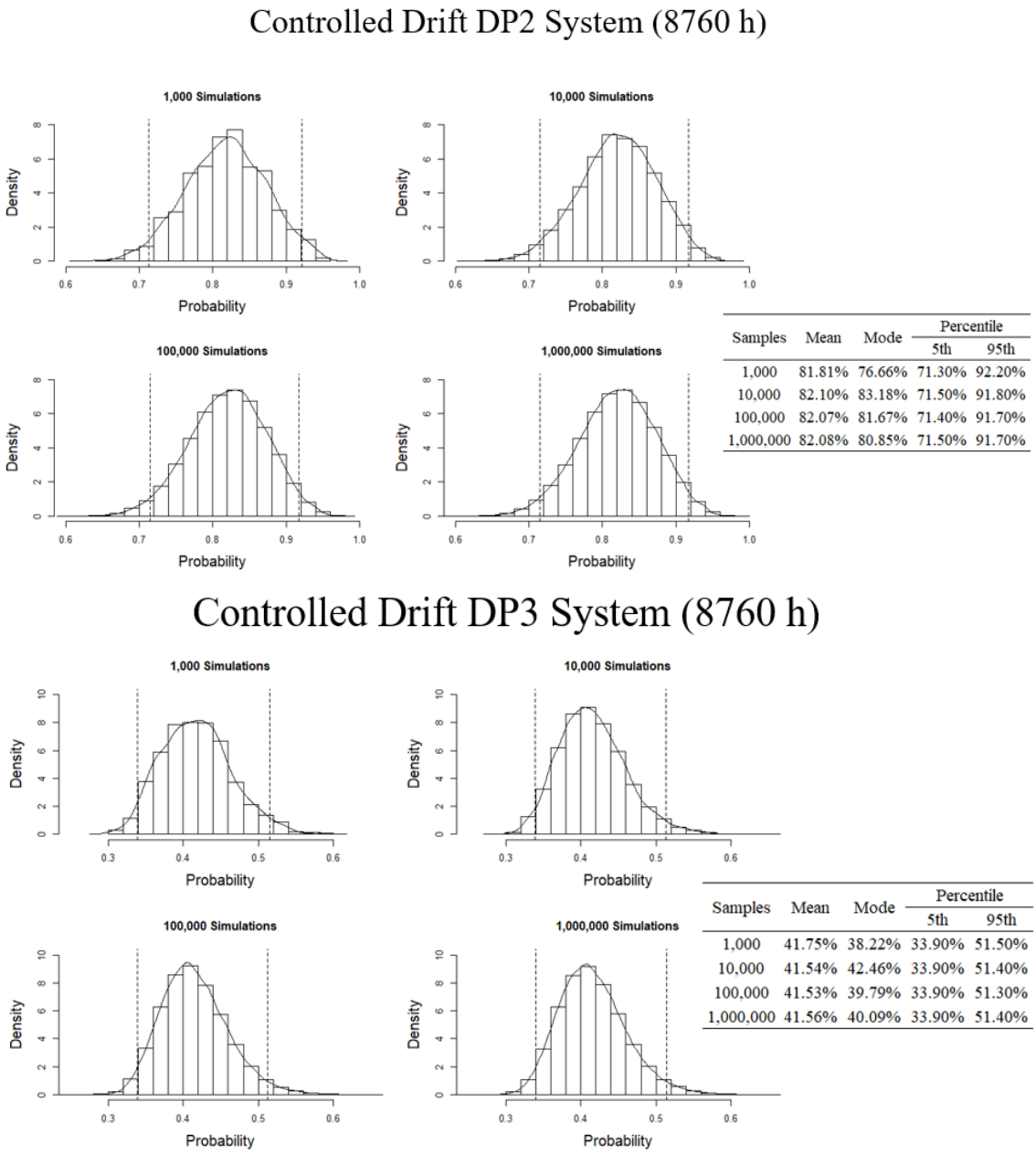
Finally, the application of Monte Carlo Simulation aims to quantify the FTs of the events of interest (free drift and controlled drift) for each case of study, considering now the uncertainty in the failure rate of the basic events, according to the information presented in Table 17.

The following sections discusses the results of this quantification for operating times of one year and three months.

5.4.2 Quantification of FTs considering uncertainty in the basic events for one year of operation

For each event of interest (controlled drift and free drift) there were 1,000; 10,000; 100,000; 1,000,000 simulations performed, supposing a period of operation of 8760 hours ~ 1 year.

Figure 81 presents the results of the uncertainty evaluation for the event of controlled drift, that is, probability of occurrence of a partial failure of the DP systems configurations under study.



Samples	Mean	Mode	Percentile	
			5th	95th
1,000	81.81%	76.66%	71.30%	92.20%
10,000	82.10%	83.18%	71.50%	91.80%
100,000	82.07%	81.67%	71.40%	91.70%
1,000,000	82.08%	80.85%	71.50%	91.70%

Samples	Mean	Mode	Percentile	
			5th	95th
1,000	41.75%	38.22%	33.90%	51.50%
10,000	41.54%	42.46%	33.90%	51.40%
100,000	41.53%	39.79%	33.90%	51.30%
1,000,000	41.56%	40.09%	33.90%	51.40%

Figure 81 - Results of quantification of uncertainty for the event: controlled drift (8760 h)

In Figure 81, the dotted lines correspond to the confidence interval of 95%. Note that this interval is narrower as the number of simulations increases; of course, this makes sense, because the Monte Carlo Simulation converges with increasing number of simulations.

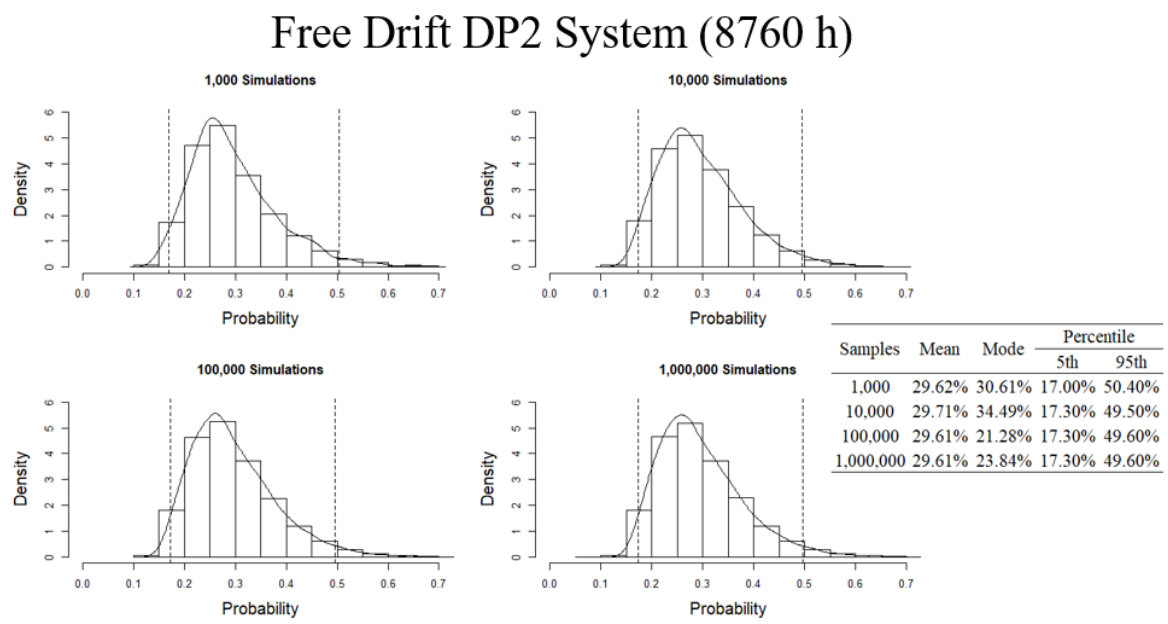
In order to compare the results, it is necessary to take into account the values obtained in the quantification of the FTs without uncertainty (analysis presented in the previous section – 5.1).

According to the previous analysis, the probability of occurrence of a controlled drift of a unit with a typical DP2 system configuration during a mission time of 8760 hours can be estimated as 86.86%, while for a unit with typical DP3 system configuration for the same mission time it is 31.29%. Note that the values of FTs without uncertainty are close to mean of the obtained confidence level with the simulations, considering the uncertainty presented in Figure 81.

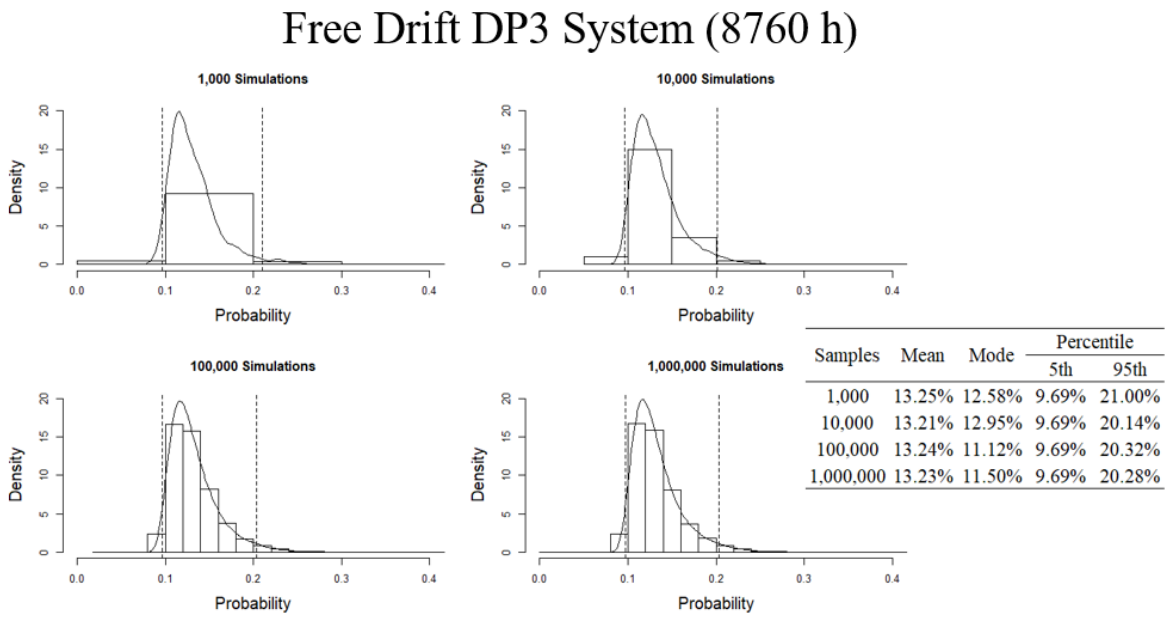
Additionally, observing Figure 81, the results obtained based on 100,000 simulations tend to be the same as the results obtained with 1,000,000 simulations, so that, running 1,000,000 simulations to analyze this system may not generate a relevant gain regarding computational cost.

The same analysis regarding the free drift event provides the results presented in Figure 82. The behavior of the data is similar to that seen in the controlled drift analysis, the higher the number of simulations, the more convergent there is in the simulation results will be.

Note that the probability presented in Figure 82 corresponding to the DP systems under study presents a total failure, resulting in a free drift to the unit.



Samples	Mean	Mode	Percentile	
			5th	95th
1,000	29.62%	30.61%	17.00%	50.40%
10,000	29.71%	34.49%	17.30%	49.50%
100,000	29.61%	21.28%	17.30%	49.60%
1,000,000	29.61%	23.84%	17.30%	49.60%



Samples	Mean	Mode	Percentile	
			5th	95th
1,000	13.25%	12.58%	9.69%	21.00%
10,000	13.21%	12.95%	9.69%	20.14%
100,000	13.24%	11.12%	9.69%	20.32%
1,000,000	13.23%	11.50%	9.69%	20.28%

Figure 82 - Results of quantification of uncertainty for the event: free drift (8760 h)

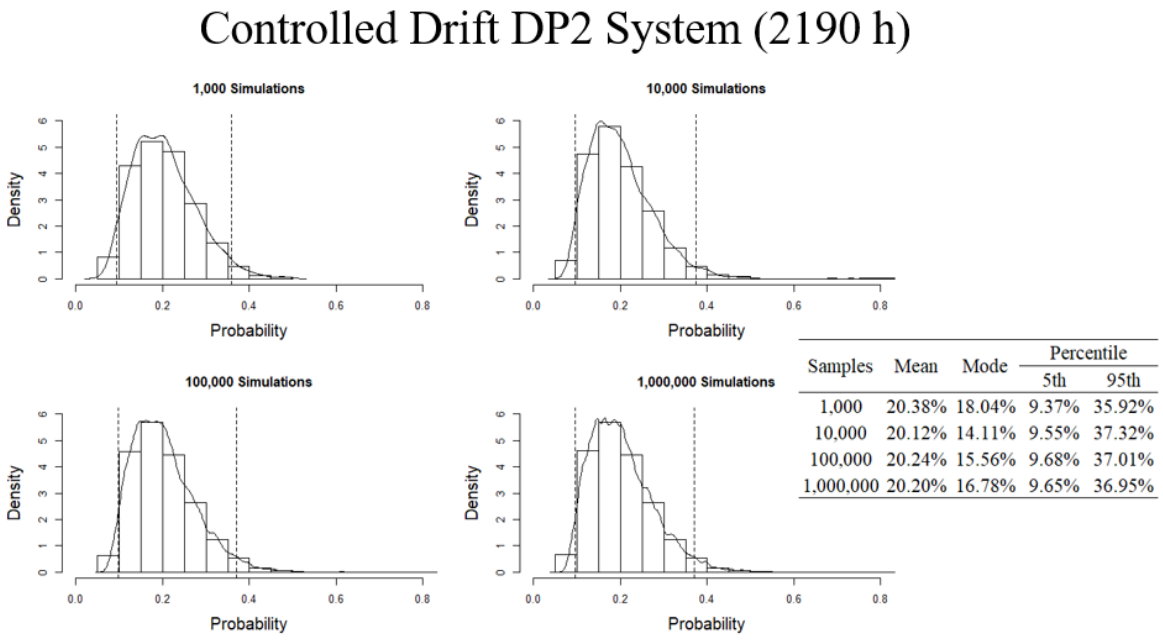
The previous analysis of the FTs (analysis without uncertainty) concludes that the probability of a free drift occurrence by total failure of DP2 system is 24.58% (considering one year of operation), and the probability of this event for drillship with DP3 system is 7.29% (for same operational time).

Considering the values obtained in the quantification without uncertainty, a conclusion reached from research and observation is that the mean obtained from simulations of the FTs with uncertainty in their basic events is greater than the probability obtained during the FT quantification without uncertainty; in general, this difference is less than 6%.

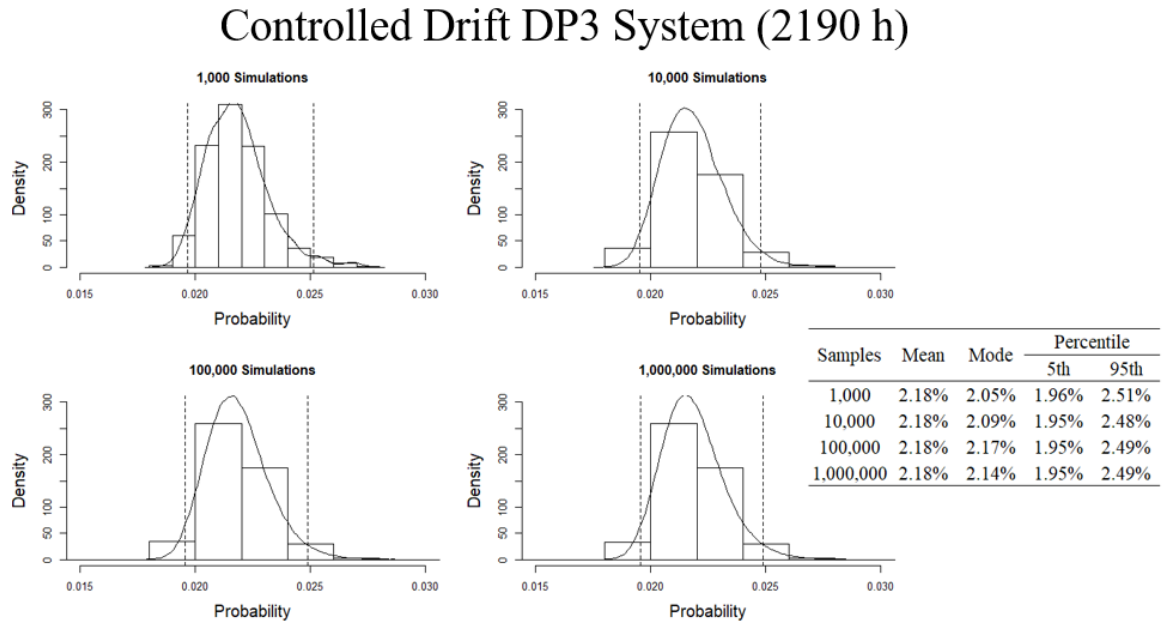
5.4.3 Quantification of FTs considering uncertainty in the basic events for three months of operation

According to the quantification of FTs without uncertainty (see section 5.1), the estimated probability for 3 months of operation of the semisubmersible platform with DP2 system presenting a controlled drift is 18.26%, while the estimated probability that the drillship with DP3 system presents a partial failure for the same operational time is 1.52%.

Figure 83 presents the results obtained in each group of simulations (1,000; 10,000; 100,000 and 1,000,000) of FTs that study the controlled drift event considering uncertainty in the basic events.



Samples	Mean	Mode	Percentile	
			5th	95th
1,000	20.38%	18.04%	9.37%	35.92%
10,000	20.12%	14.11%	9.55%	37.32%
100,000	20.24%	15.56%	9.68%	37.01%
1,000,000	20.20%	16.78%	9.65%	36.95%



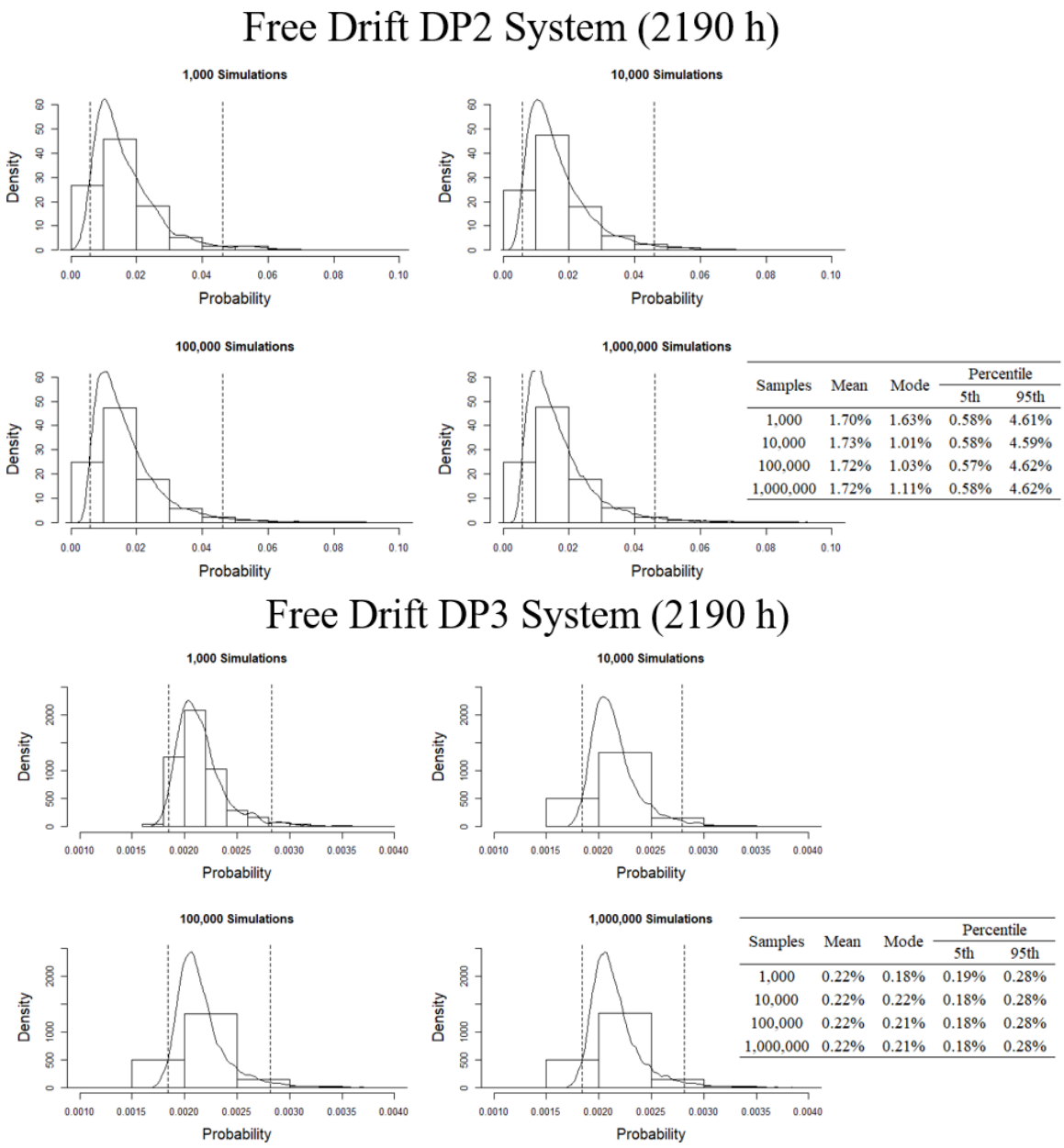
Samples	Mean	Mode	Percentile	
			5th	95th
1,000	2.18%	2.05%	1.96%	2.51%
10,000	2.18%	2.09%	1.95%	2.48%
100,000	2.18%	2.17%	1.95%	2.49%
1,000,000	2.18%	2.14%	1.95%	2.49%

Figure 83 - Results of quantification of uncertainty for the event: controlled drift (2190 h)

The results presented in Figure 83 allow concluding that, in general, the mean value of the occurrence probability of a controlled drift is similar between the groups of simulations, and the larger the number of simulations, the smaller the confidence interval of results.

Regarding the free drift event, the same group of simulations (1,000; 10,000; 100,000 and 1,000,000) is executed for an operational time of 3 months. Figure 84 summarizes the results obtained.

The values shown in Figure 84 corresponds to the probability that the vessels under study present a free drift due to a total failure of DP system.



Samples	Mean	Mode	Percentile	
			5th	95th
1,000	1.70%	1.63%	0.58%	4.61%
10,000	1.73%	1.01%	0.58%	4.59%
100,000	1.72%	1.03%	0.57%	4.62%
1,000,000	1.72%	1.11%	0.58%	4.62%

Samples	Mean	Mode	Percentile	
			5th	95th
1,000	0.22%	0.18%	0.19%	0.28%
10,000	0.22%	0.22%	0.18%	0.28%
100,000	0.22%	0.21%	0.18%	0.28%
1,000,000	0.22%	0.21%	0.18%	0.28%

Figure 84 - Results of quantification of uncertainty for the event: free drift (2190 h)

In order to analyze the values in Figure 84, it is necessary to consider that the quantification of free drift trees without uncertainty for a 3 months operational time resulted in an occurrence probability of 1.52% for the semisubmersible platform and 0.16% for the drillship.

Note that in Figure 84, the mean occurrence probability of a free drift in the DP2 system is 1.72% and the mean for the drillship is 0.22% (values relatively close to the results of quantification of FTs without uncertainty).

In summary, the Monte Carlo Simulation showed to be a useful method to evaluate the effect of the uncertainty on the failure rates of the system components in the top events of the previously quantified FTs; however, the analysis requires a minimum number of 100,000 simulations to guarantee the convergence.

In general, the mean values of the occurrence probability of top events obtained in the simulation groups for three months of operation showed values 2% higher than the mean value obtained in the quantification of the FTs without uncertainty in the same scenario (operating time of 2190 hours). The mean values obtained in the simulations groups that considered a mission time of 8760 hours resulted in two behaviors. i.e. for controlled drift the uncertainty obtained values up to 10% higher than the values obtained in the quantification of the FTs without uncertainty and for the event of free drift the uncertainty analysis showed a mean 5% higher than the values obtained in FTs without uncertainty.

In Appendix F, the pdfs of the results obtained in FTs quantification considering uncertainty are available; this analysis is developed for two different operational times (8760 hours and 2190 hours).

6. CONCLUSIONS

DP failures may lead to accidents involving potential environmental impacts and economic losses. Therefore, reliability is the key requirement for DP systems configurations used in vessels and platforms engaged in complex offshore operations. The main aim of this thesis was to propose a methodology for a RAM analysis of DP system of two different DP generations (DP class 2 and DP class 3) to define their restriction diagrams. Literature survey and RAM analysis techniques have been the two fundamental cornerstones of the work at hand, which have allowed addressing the particular goals defined in the introduction.

The conclusions of the study can be classified into methodological conclusions and practical conclusions. That is, methodological conclusions refer to the knowledge acquired in the application of techniques and methods for RAM analysis; whereas practical conclusions are closely related to the operation and structure of the DP system.

The main methodological conclusions to be drawn from the framework of this thesis are the following:

- Qualitative and quantitative evaluations can be performed based on a FT. Whereas a qualitative evaluation supplies information about Minimal Cut Sets, the quantitative evaluation supplies information about the probability of top event occurrence. For example, in the case studies considered, the qualitative evaluation showed that the bus bar in the power subsystem, the motor thrusters in the thruster subsystem and UPS in the control subsystem are the most critical components; while the quantitative evaluation allowed to calculate the probability that a unit with DP system class 2 or class 3 present a free drift or controlled drift; that is, the probability that the DP system fails.

- To quantify the FTs, the exact probability method should be used. However, given the high computational cost for complex FTs, some approximations can be used (rare events or Minimal Cut Sets upper bound). It is enough to remember that the method of rare event approximation is useful if the probability of occurrence of each Minimal

Cut Sets is small, while the Minimal Cut Sets upper bound will only provide the exact probability of top event occurrence, in cases where the Minimal Cut Sets are mutually exclusive.

- RBD are advantageous when the system under analysis can be decomposed into parallel-series configurations, that is, when the system is simple because it is easy to obtain an analytical expression. However, in this study, the fault tree tends to be more advantageous because it allows the systematic modeling of complex systems. Whether they are larger or with configurations beyond the simplest (parallel-series).

- A FT can always be turned into an equivalent set of Boolean equations. These Boolean equations can be obtained from the Minimal Cut Sets of the system, that is, consider a FT that consisting of three levels: the top event composes the first level, the minimal cut sets composes the second level and the elements of each minimal cut set composes the third level; an OR gate connect the first and second levels whereas AND gates connect each minimal cut set with its set of basic inputs necessary and sufficient to cause the top event, so there is a new fault tree, equivalent to the FT original (Ahmad, 2016). In other words, a RBD with all Minimal Cut Sets in series is an equivalent system of the original system.

- The application of the Monte Carlo Simulation shows that in cases where the probability of occurrence of the events of interest is small, a large number of simulations are needed, which may generate a high computational cost.

- During the applications of KDE (to evaluate the repair times of semisubmersible platform and uncertainty analysis – see Appendix F), the bandwidths always tends to decrease when the simulated operational time increases. In other words, the *Rule-of-Thumb* implies that the larger the amount of data, the smaller the bandwidth [see Eq. (2.41)]. Clearly, the longer the simulated operation time, the more information about the DP system is collected.

- The parametric methods can be useful for obtain the theoretical pdf of repair times when the aim is forecast the repair times of DP Systems without information about the maintenance, or even for develop other analysis with DP Systems related to those studied in this thesis. However, when the objective is to guarantee the real curve adjustment, the use of parametric method may omit some information.

- The uncertainty analysis is important because it allows taking into account the lack of information about the real value of failure rates of equipment for each configuration. Also, the uncertainty analysis allows knowing the pdf of the probability values of the drift events for each configuration under study, curves that cannot be drawn from the quantification of FTs without uncertainty (Section 5.1.5) and of course, know the confidence intervals of the variables in study.

- The study of Reliability, Availability and Maintainability allows identifying the behavior of the system considering different operational characteristics. That is, there can be highly reliable systems with low availability or highly available systems with low reliability. The first case can occur in those systems that almost never fail but when the system fails it takes a long time to restore its operation. The second case occurs when the repairs of the system are very fast (the inoperable time of system is close to zero), but it constantly fails.

Regarding practical conclusions, the analysis of DPS class 2 and DPS class 3 shows that:

- The International Organizations and Classification Societies as ABS, DNV and ISO specify redundancy levels of equipment for each DP class, but the vessel owner, client and coastal authorities are which to assess the level of equipment redundancy (DP class) best achieves the desired reliability requirements for any given operations. Therefore, in this context the RAM analysis of DP system is useful for making decisions in order to reduce the risk of offshore operations.

- Even when the DPS class 2 has the Siplink (component that increases the reliability of the DP system, see Section 4.1), the probability of failure of power subsystem in this class has always been greater than the probability of failure to power subsystem in DP3. This difference between the probability of failure can be attributed to the operational differences between the bus bar in the configurations in study; i.e., with the open buses (DPS3) even severe failures in the power subsystem do not cause a total blackout of the unit as can occur with the buses closed (DPS2). However, note that in operations with open buses, the advantage of running with a higher average load on the motor-generators is lost, making it possible to save fuel and attenuate the effects of carbonization on the motor.

- The quantification of FTs (without considering uncertainty in the parameters of basic events) for one year of operational time showed that the power and thruster subsystem contributes 18.80% to the total DP2 system failures, whereas the control subsystem contributes 7.13% (see Table 12).

- From the analysis of the DP3 system results for an operational time of one year, it can be seen that incorporating additional redundancies the probability of total failure of DP system reduces until 16.66%, i.e., note that the total failure probability of the DP system reduces from 24.58% (DP2 system) to 7.92% (DP3 system), see Table 12.

- Reliability analysis showed to be aligned with the study presented by EBrahimi (2010), while EBrahimi obtains a reliability of 75.46% for one year of operation considering a DP system class 2 (total failure), this study shows in Table 12 that the reliability for the case study with DP2 system is 75.42% for one year of operation. However, in the study of EBrahimi, the reliability calculation is performed considering some elements that make up the DP system, that is, the author does not detail the DP2 system configuration and only presents the failure rate of some group of equipment.

- Power and thruster subsystems are more critical in DP class 2, while the control subsystem is the critical subsystem in DP class 3. Nevertheless, it is worth noting that

this conclusion is not general for DP systems. To conclude whether these subsystems are the most critical on all semisubmersibles platforms with DP2 and all drillship with DP3 would be necessary to evaluate other configurations of DP systems and consequently other vessels.

- Although most of the measures of importance evaluated the bus-bar as the equipment with the greatest need for prioritization in DP2 system, it is worth noting that when evaluating the inspection importance measure, the coolers, PMS, lubrication pumps, transfer oil pumps, wind sensors and UPS are more critical equipment than the bus-bar.

- In the case of the DP3 system, all the measures of importance evaluated indicate that the wind sensors are the most critical components followed by the gyros in the prioritization order; and in general, the DGPS and the VRS are indicated as the least critical components of the system.

- FTs are designed considering usual operating and maintenance procedures. In other words, if the fault trees do not model the human factor, they consider that in the case of control computer loss, the operator will use the alternative control station (backup station or IJS).

- The Monte Carlo Simulation allows concluding that more than 90% of the repair times (duration times of free drift events) in the two case studies will be concluded in the first 6 hours. That is, in more than 90% of the cases, the maintenance teams of the DP systems under study are able to recover the system failure in the first 6 hours; and in 43% of simulated free drifts, the maintenance teams are able to recover the system failure in an interval lower than 3 hours.

- Definitely, the asymptotic availability analysis of DP3 system is consistent with the conclusions presented in Zio (2018), which analyzes highly reliable systems, i.e., systems characterized by very small probabilities of failures, result in high computational cost for the simulation. Zio (2018) proposes two main strategies that

can improve the simulations. The first strategy consists in simulate a large sets of system life histories and the second suggests programming simulation by adaptive sampling. It is worth mentioning that the first strategy was raised, but when trying to implement this strategy, the result shows that the current configuration of the DP3 system would require a simulation of 4,380,000 hours ~ 500 years to obtain enough data to build a histogram (considering perfect repairs), note that the quantity of hours required in the simulation responds to the fact that in 30 years simulated only 6 failures were obtained. Regarding the second strategy, its implementation is not possible because at present the ERAS software is not designed for this type of programming.

- The confidence interval allows showing with 95% certainty the possible values that the probabilities of the analyzed FTs top event will take. It is also noticed that the mean obtained in the uncertainty analysis is relatively close to the probability values obtained in the analysis without uncertainty (Section 5.1.5).

- If the probabilities obtained in the analysis without considering uncertainty in the basic events of the fault trees are assumed as reference values of the events of interest, it is possible to conclude that the longer the operational time, the more uncertainty about the probability of interest drifts (controlled and free). i.e. the analysis of FTs considering uncertainty concludes that for 3 months operating time the mean value of the failure probability obtained in the simulation is 2% higher than the value obtained in the analysis without uncertainty (comparison between Table 12 and means exposed in Figure 81 and Figure 82), but this difference is up to 10% when the operating time increases to 12 months (comparison between Table 12 and means shown in Figure 83 and Figure 84).

Knowing that at present, the DP system requires an operator for its operation, future research should consider the human factor during the development of the RAM analysis, and for this, the human reliability could use for future studies. Another future study can be the uncertainty analysis in the parameters of repair times, in order to complement the maintainability and availability presented in this thesis.

REFERENCES

ABS. (2013). "Guide for Dynamic Positioning Systems." *American Bureau of Shipping*.

Aderibigbe, A. (2014). *Monte Carlo simulation*. (University of Ibadan, Ed.), *Department of Electrical and Electronic Engineering*. Ibadan. https://doi.org/10.1201/9781315163666-3

Ahmad, Arshad. (2016). *Fault Tree Analysis (Minimal Cutset)*. edited by University of Technology Malaysia. Kuala Lumpur.

Aksu, S., & Turan, O. (2006). Reliability and availability of Pod propulsion systems. Quality and Reliability Engineering International, 22(1), 41–58. https://doi.org/10.1002/qre.747

Amari, S. V. (2007). Steady-state availability and MTBF of systems subjected to suspended animation. *International Journal of Performability Engineering*, *3*(2), 282–284.

ARR. (2015). Our beloved bathtub curve might not commonly occur. Retrieved from https://apexridge.com/blog-14/

Bahri, S., Ghribi, F., & Bacha, H. Ben. (2009). A study of asymptotic availability modeling for a failure and a repair rates following a Weibull distribution. Reliability & Risk Analysis: Theory & Applications, 2, 30–42.

Bala, S., Pan, J., Das, D., Apeldoorn, O., & Ebner, S. (2012). Lowering failure rates and improving serviceability in offshore wind conversion-collection systems. PEMWA - Power Electronics and Machines in Wind Applications. https://doi.org/10.1109/PEMWA.2012.6316362

Balchen, J., N. Jenssen, E. Mathisen, and S. Saelid. (1980). "A Dynamic Positioning System Based on Kalman Filtering and Optimal Control." Modeling, Identification and Control 1(3):135–63.

Barlow, R., & Proschan, F. (1981). Statistical Theory of Reliability and Life Testing. (Silver Springs, Ed.). California.

Bazovsky, I. (1999). Reliability Theory and Practice. edited by Springer. New York.

Bhaveshkumar, D. (2015). The Gram-Charlier A Series based Extended Rule-of-Thumb for Bandwidth Selection in Univariate and Multivariate Kernel Density Estimations. *Dhirubhai Ambani Institute of Technology - DAIICT*. Retrieved from http://arxiv.org/abs/1504.00781papers3://publication/uuid/D291DA98-5818-4B78-B026-65D1BB806A63

Birnbaum, Z. (1969). *On th importance of different components in a multicomponent system*. (A. Press, Ed.), *Contract*. New York.

Birolini, A. (2007). Reliability Engineering: Theory and Practice. edited by Springer. New York.

Blischke, W., & Murthy, D. (2003). *Case Studies in Reliability and Maintenance*. (Wiley, Ed.). New Jersey.

Brownlee, J. (2016). Introduction to Time Series Forecasting with Python. Retrieved from https://machinelearningmastery.com/time-series-forecasting-supervised-learning/

Cao, R., Cuevas, A., & González, W. (1994). A comparative study of several smoothing methods in density estimation. *Computational Statistics and Data Analysis*, *17*(2), 153–176. https://doi.org/10.1016/0167-

9473(92)00066-Z

Cargill, S. (2007). DP Innovation: A Novel Solution to Common Mode Failures in DP Class 2 Power Plant. Dynamic Positioning Conference.

Carroll, J., McDonald, A., & McMillan, D. (2016). Failure rate, repair time and unscheduled O&M cost analysis of offshore wind turbines. *Wind Energy*, *19*(6), 1107–1119. https://doi.org/10.1002/we.1887

Chang, D., Rhee, T., Nam, K., Chang, K., Lee, D., & Jeong, S. (2008). A study on availability and safety of new propulsion systems for LNG carriers. Reliability Engineering and System Safety, 93(12), 1877–1885. https://doi.org/10.1016/j.ress.2008.03.013

Chavan, S. (2016). Reliability Analysis of Transformer less DC/DC Converter in a Photovoltaic System. *Mediamira Science Publisher*, 579–582.

Chouaib, A. (2015). Kernel Estimator and Bandwidth Selection for Density and its Derivatives, 1–22.

Coast, E. (2012). "The Role of an Electric Switchboard in Power Flow." Retrieved (http://www.ecpowersystems.com/resources/switchboards/the-role-of-an-electric-switchboard-in-power-flow/).

Conlen, M. (2014). Kernel Density Estimation. Retrieved from https://mathisonian.github.io/kde/

CRAN-R Project. (2019). Package GAMLSS. https://doi.org/10.1111/j.1467-9876.2005.00510.x

DNV. (2013). "Dynamic Positioning Systems." *Det Norske Veritas*.

Doung, T. (2001). An Introduction to Kernel Density Estimation. *Weatherburn Lecture Series for the Department of Mathematics and Statistics, at the University of Western Australia*.

Dynamic Positioning Committee. (2012). "History of DP." Retrieved (http://www.dynamicpositioning.com/history-of-dp/).

Ebeling, C. (1997). *An Introduction to Reliability and Maintainability Engineering*. edited by MacGraw-Hill. Massachusetts.

Eberly College of Science. (2014). Probability Density Functions. Retrieved from https://newonlinecourses.science.psu.edu/stat414/node/97/?fbclid=IwAR2fraH5uYWwR_iWYn4zaciVnBQEthDmCssUYglM8zmv1w7uMRP56ycUqJk

EBrahimi, A. (2010). Effect analysis of RAMS parameter in design & operation of DP system in floating offshroe structure. Royal Institute of Technology, (October).

EPRI. (2001). A Review of the Reliability of Electric Distribution System Components. Electric Power Research Institute.

Fankhauser, H. (2001). Safety Functions versus Control Functions. In Springer (Ed.), *SAFECOMP - International Conference on Computer Safety, Reliability and Security* (pp. 66–74). Stockholm.

Ferreira, A., & Lapa, C. (2009). Análise de confiabilidade do sistema de refrigeração de componentes de ANGRA I considerando as incertezas na avaliação das árvores de falhas por um modelo Fuzzy. *Institute of Nuclear Engineering - Rio de Janeiro*.

Ferreira, D. (2016). "Confiabilidade de Sistemas de Geração de Energia Em Sondas de Posicionamento Dinâmico Por Simulação Monte Carlo." *UFRJ*.

Flamm, J., & Luisi, T. (1992). Reliability Data Collection and Analysis. (Springer, Ed.). Ispra.

Fussell, J. (1975). How to Hand-Calculate System Reliability and Safety Characteristics. *IEEE Transactions on Reliability*, (3), 169–174.

Garg, K. and S. Shah. (2011). "Dynamic Positioning Power Plant System Reliability and Design." PCIC Europe Conference.

Hartnett, R., Gross, K., Bovee, B., Nassar, S., Academy, U. S. C. G., Johnson, G., … Associates, J. J. M. (2003). DGPS Accuracy Observations and Potential Data Channel Improvements. 59th Annual Meeting, Institute of Navigation, 55–78.

Hauff, K. S. (2014). Analysis of Loss of Position Incidents for Dynamically Operated Vessels. NTNU - Department of Marine Technology, (June). Retrieved from https://brage.bibsys.no/xmlui/handle/11250/239192?locale-attribute=no

Holvik, Jon. (1998). "Basics of Dynamic Positioning." Dynamic Positioning Conference.

Hoyland, A., & Rausand, M. (1994). *System Reliability Theory: Models and Statistical Methods*. (Wiley, Ed.). New York.

Hwang, J., Lay, S., & Lippman, A. (1994). Nonparametric multivariate density estimation: a comparative study. *IEEE Transactions on Signal Processing*, *42*(10), 2795–2810. https://doi.org/10.1109/78.324744

IADC. (2014). "Class A-60 Division." Retrieved (http://www.iadclexicon.org/class-a-60-division/).

IEM. (2017). "Low Voltage Switchgear." Retrieved (http://www.iemfg.com/products/power-distribution/low-voltage-switchgear).

IEEE. (2007). Design of Reliable Industrial and Commercial Power Systems. IEEE Std 493-2007. Institute of Electrical and Electronics Engineers.

Igba, J., Alemzadeh, K., Henningsen, K., & Durugbo, C. (2015). Performance assessment of wind turbine gearboxes using in-service data: Current approaches and future trends. Renewable & Sustainable Energy Reviews, 50, 144–159.

IMCA. (2007). "Guidelines for the Design and Operation of Dynamically Positioned Vessels." International Marine Contractors Association.

IMO. (1994). "International Maritime Organization." The International Journal of Marine and Coastal Law 3(3):235–45.

INL. (2012). Review of Maintenance and Repair Times for Components in Technological Facilities. Idaho National Laboratory. Retrieved from https://inldigitallibrary.inl.gov/sites/sti/sti/5554588.pdf

Janssen, P., Marron, J., Veraverbeke, N., & Sarle, W. (1995). *Scale measures for bandwidth selection*. (Taylor & Francis Group, Ed.). London.

Jones, M., Marron, J., & Sheather, J. (1996). A Brief Survey of Bandwidth Selection for Density Estimation. *Journal of the American Statistical Association*, *91*(433), 401–407.

Kang, Young-ju. (2010). "THE FUNCTION TREE ANALYSIS & ITS APPLICATIONS." Altshuller Institute (82):1–37.

Kapur, C., & Lamberson, L. (2009). Reliability in Engineering Design. (W. I. P. Limited, Ed.). Mumbai.

Karan, C. (2017). "What Are Offshore Vessels?" Retrieved (https://www.marineinsight.com/types-of-ships/what-are-offshore-vessels/).

Karpati, A., Zsigmond, G., Voros, M., & Lendvay, M. (2012). Uninterruptible Power Supplies (UPS) for Data Center. In 10th Jubilee International Symposium on Intelligent Systems and Informatics (pp. 351–355).

Komal, S. P. Sharma, and Dinesh Kumar. (2010). "RAM Analysis of Repairable Industrial Systems Utilizing Uncertain Data." *Applied Soft Computing Journal* 10(4):1208–21.

Kongsberg. (2014). "Dynamic Positioning System, Triple Modular Redundant." Retrieved (https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/F85938EB2AE9BD86C1256A48004161A8?OpenDocument).

Lehmköster, J. (2014). "Oil and Gas from the Sea." *World Ocean Review* 47.

Leitch, R. (1995). *Reliability Analysis for Engineers: An Introduction*. edited by Oxford University Press. Oxford.

Lerche, I. and B. Mudford. (2005). "How Many Monte Carlo Simulations Does One Need to Do?" *Energy* Exploration & Exploitation 6:429–61.

Lewis, E. (1996). Introduction to Reliability Engineering. edited by I. John Wiley & Sons. New York.

LLC, Global Industries Offshore. (2009). "DP System Introduction." CONVERTEAM.

Martini, H. (1993). Failure rates for programmable logic controllers. Reliability Engineering and System Safety, 39(3), 325–328. https://doi.org/10.1016/0951-8320(93)90007-L

Martins, M. (2013). Considerações sobre análise de confiabilidade e risco. (University of São Paulo, Ed.). São Paulo.

Matsuoka Takeshi. (2013). "A Monte Carlo Simulation Method for System Reliability Analysis." Nuclear Safety and Simulation 1(4):44–52.

Metropolis, N. (1987). "The Beginning of the Monte Carlo Method." Nuclear Safety and Simulation 44–*52.*

MIL-HDBK-217F. (1991). MIL-HDBK-217E, MILITARY HANDBOOK RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT. Retrieved from https://snebulos.mit.edu/projects/reference/MIL-STD/MIL-HDBK-217F-Notice2.pdf

Modarres, M. (2006). *Risk Analysis in Engineering: Probabilistic Techniques, Tools and Trends. Edited by CRC Press. New York. ISBN: 978-1574447941, 424 pages.*

Modarres, M., M. Kaminskiy, and V. Krivtsov. (2009). *"Basic Reliability Mathematics: Review of Probability and Statistics." Pp. 15–70 in Reliability engineering and risk analysis, edited by CRC Press. New York.*

Mooney, C. (1997). *Monte Carlo Simulation. (S. Publications, Ed.). California.*

MTS. (1997). Reliability and Risk Analysis. Marine Technology Society.

*MTS. (2007). "Power Management Control of Electrical Propulsio*n Systems." *Marine Technology Society*.

MTS. (2012). "Description of the DP System: DP Vessel Design Philosophy Guidelines Part 2." *Marine Technology Society*.

Nakano, E. (2013). Possible values of P.D.F. (Probability density function). Retrieved from

https://www.researchgate.net/post/Can_the_value_of_PDF_Probability_density_function_greater_than_1?fbclid=IwAR0vkvm5q4m26qELlWvjE6HF1cQu0MPCzFFuM8BBfOl6oqPiSXm3dlqqUXM

NASA. (2002). "Fault Tree Handbook with Aerospace Applications." *NASA Handbook* XXXIII(8):218.

Natacci, F., Martins, M., & Souza, G. (2009). *Proposta de método de análise de confiabilidade de navios*. (U. of S. Paulo, Ed.). São Paulo.

NIOT. (2015). Assessment of the reliability of the Indian tsunami buoy system. *National Institute of Ocean Technology*, *32*(4), 255–270. https://doi.org/10.3723/ut.32.255

NOVATEL. (2016). MTBF specifications of GPS receivers. Retrieved from https://www.novatel.com/support/known-solutions/mtbf-specifications-for-gps-700-series/

NSWC. (2011). *Handbook of Reliability Prediction Procedures for Mechanical Equipment*.

O'Connor, P. (1981). *Practical Reliability Engineering*. edited by Wiley. New Jersey.

Oliveira, Carlos Alberto F. De, Eduardo Vardaro, Afonso A. Pallaoro, Breno P. Jacob, and Luciano T. Vieira. (2004). "Polar Restriction Diagrams for Dynamically Positioned Units." *Time* 1:367–72.

Omokhafe, T., & Ambafi, J. (2011). Reliability Study of Electric Circuit Breakers (a case study). *Innovations in Science and Engineering*, 104–114.

OREDA. (2009). *Offshore Reliability Data Handbook, 5th edition*. (SINTEF, Ed.). Oslo.

OREDA. (2015). *Offshore Reliability Data Handbook, 6th Edition*. edited by SINTEF. Oslo.

PANDUIT. (2014). "Routing/Pathways." Retrieved (https://www.panduit.com/en/products-and-services/products/cable-routing-and-pathways).

Park, B., & Marron, J. (1990). Comparison of Data-Driven Bandwidth Selectors. *Journal of the American Statistical Association*, *85*(409), 66–72.

Park, B., & Turlach, B. (1992). *Practical performance of several data driven bandwidth selectors*. (University Catholique of Louvain, Ed.), *Computational Statistics*. Louvain.

Patil, Virendra, Abhishek Ayare, Bhushan Mahajan, and Sushmita Bade. (2015). "A Review of Azimuth Thruster." *SSRG International Journal of Mechanical Engineering* 2(10):38–41.

Pérez, J. (2014). Estimación no paramétrica de funciones de densidad (Método Kernel). Retrieved from https://estadisticaorquestainstrumento.wordpress.com/2012/12/13/estimacion-no-parametrica-de-funciones-de-densidad-metodo-kernel/?fbclid=IwAR0P5KVQt3xqJLjStfL8-9DfXxFULDbh3SwpA3gnBio7kycuTDUzJO1BIaM

Petrobras. (2018). Pre-Salt. Retrieved from http://www.petrobras.com.br/en/our-activities/performance-areas/oil-and-gas-exploration-and-production/pre-salt/?fbclid=IwAR0fziTIOKdkLWl7hPqa2Bbq-_eC7K6J97VJtkeoPAsfI3FfFoL4VkoWAJQ

Pham, H. (2006). *System Software Reliability*. edited by Springer. New Jersey.

Portinale, L., & Codetta, D. (2015). *Modeling and Analysis of Dependable Systems: A Probabilistic Graphical Model Perspective* (W. Scientific, Ed.). London.

Puttlitz, K., & Stalter, K. (2004). *Reliability Aspects of Lead-Free Solders in Electronic Assemblies*. (C. Press, Ed.). Florida.

Rappini, S., Pallaoro, A., & Heringer, M. (2003). "Fundamentos de Posicionamento Dinâmico."

Rasoulzadeh, V. (2015). "Risk Assessment of Diesel Engine Failure in a Dynamic Positioning System." *University of Stavanger*.

RAYTHEON. (2010). Standard 22 M Gyro Compass System.

Rodriguez, C. E. P. (2012). "Redes Bayesianas No Gerenciamento E Mensuração De Riscos Operacionais." 270.

RStudio Team (2015). RStudio: Integrated Development for R. RStudio, Inc., Boston, MA URL http://www.rstudio.com/.

SAFRAN. (2014). Attitude & Heading Reference System.

Samsung Heavy Industries. (2012). *PRELIMINARY FMEA REPORT OF THE DP SYSTEM for QGOG DRILLSHIP*. edited by L. Samsung Heavy Industries Co. Panama.

Schenkelberg, F. (2014). "Fault Tree Analysis (FTA)." Retrieved (https://accendoreliability.com/intro-to-fault-tree-analysis/).

Schindler, A. (2011). *Bandwidth Selection in Nonparametric Kernel Estimation*. (Faculty of Economic Sciences of the Georg-August-Universität Göttingen, Ed.). Göttingen.

Schleder, A. (2015). Quantitative dispersion analysis of leakages of flammable and/or toxic substances on environments with barriers or semi-confined substances on environments with barriers or semi-confined. *University of São Paulo*.

Schonek, J. (2017). "Switchboard and Switchgear: Functions & Differences." Retrieved (http://engineering.electrical-equipment.org/panel-building/switchboard-switchgear-functions-differences.html).

Sharirli, M. (1985). *Methodology for system analysis using fault trees, success trees and importance evaluations*. (Department of Chemical and Nuclear Engineering, Ed.). Maryland.

Sheather, J. (1986). The performance of six popular bandwidth selection methods as same real data sets (with discussion). *Computational Statistics*, *7*, 225–250.

Shooman, M. (1990). *Probabilistic Reliability: An engineering approach, second edition*. (R. F. Krieger, Ed.). Melbourne.

Siddall, J. (1983). *Probabilistic Engineering Design: Principles and Applications*. edited by O. S. University. Ohio.

Siemens. (2010). "SIPLINK – Reliable and Economical." *Siemens*.

Sikos, L., & Klemeš, J. (2010). Reliability, availability and maintenance optimisation of heat exchanger networks. *Applied Thermal Engineering*, *30*(1), 63–69. https://doi.org/10.1016/j.applthermaleng.2009.02.013

Silverman, B. (1986). Density Estimation for Statistics and Data Analysis. *Monographs on Statistics and Applied Probability*, *33*(1), 43–54. https://doi.org/10.1177/030098589603300105

Stasinopoulos, M. D., Rigby, R. A., & De Bastiani, F. (2018). GAMLSS: A distributional regression approach. *Statistical Modelling*, *18*(3–4), 248–273. https://doi.org/10.1177/1471082X18759144

Taverna, D. (2017). “Desenvolvimento de Ferramenta Computacional Para Avaliação Da Disponibilidade de Sistemas de Engenharia.” *University of São Paulo* 21–34.

Thies, P., Flinn, J., & Smith, G. (2009). Is it a showstopper ? Reliability assessment and criticality analysis for Wave Energy Converters. *European Wave and Tidal Energy Conference*, (October), 21–30.

TMEIC. (2013). Variable Frequency Drives - a Comparison of VSI versus LCI Systems Introduction. *Toshiba Mitsubishi-Electric Industrial Systems Corporation*.

TRANSOCEAN. (2009). “SEDCO 706 FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS OF THE DP SYSTEM.”

U.S.NRC. (2011). *System Analysis Programs for Hands-on Integrated Reliability Evaluations*. Vol. 1.

VAISALA. (2002). USER ’ S GUIDE Combined Wind Sensor WMS301 and WMS302.

Vedachalam, N., & Ramadass, G. A. (2017). Reliability assessment of multi-megawatt capacity offshore dynamic positioning systems. *Applied Ocean Research*, *63*, 251–261. https://doi.org/10.1016/j.apor.2017.02.001

Wand, M., & Jones, M. (1995). *Kernel Smoothing*. (Taylor & Francis, Ed.). Boston.

Xu, X., Yan, Z., & Xu, S. (2015). Estimating wind speed probability distribution by diffusion-based kernel density method. *Electric Power Systems Research*, *121*, 28–37. https://doi.org/10.1016/j.epsr.2014.11.029

Zio, E. (2013). *The Monte Carlo Simulation Method for System Reliability and Risk Analysis*. (Springer, Ed.). London.

Zio, E. (2018). The future of risk assessment. *Reliability Engineering and System Safety*, *177*, 176–190. https://doi.org/10.1016/j.ress.2018.04.020

APPENDIX A - RULES OF BOOLEAN ALGEBRA

Table 18 - Rules of Boolean algebra

	Mathematical symbolism	Engineering symbolism	Designation
(1a)	X∩Y=Y∩X	X·Y=Y·X	Commutative Law
(1b)	X∪Y=Y∪X	X+Y=Y+X	
(2a)	X∩(Y∩Z)=(X∩Y)∩Z	X·(Y·Z)=(X·Y)·Z	Associative Law
(2b)	X∪ (Y∪Z)=(X∪Y) ∪Z	X+(Y+Z)=(X+Y)+Z	
(3a)	X∩(Y∪Z)=(X∩Y) ∪ (X∩Z)	X·(Y+Z)=X·Y+X·Z	Distributive Law
(3b)	X∪ (Y∩Z)=(X∪Y)∩(X∪Z)	X+Y·Z=(X+Y)·(X+Z)	
(4a)	X∩X=X	X·X=X	Idempotent Law
(4b)	X∪X=X	X+X=X	
(5a)	X∩(X∪Y)=X	X·(X+Y)=X	Law of Absorption
(5b)	X∪ (X∩Y)=X	X+X·Y=X	
(6a)	X∩X’=Φ	X·X’=Φ	
(6b)	X∪X’=Ω=1	X+X’=Ω=1	Complementation
(6c)	(X’)’=X	(X’)’=X	
(7a)	(X∩Y)’=X’∪Y’	(X·Y)’=X’+Y’	de Morgan’s Theorem
(7b)	(X∪Y)’=X’∩Y’	(X+Y)’=X’·Y’	
(8a)	Φ∩X=Φ	Φ·X=Φ	
(8b)	Φ∪X=X	Φ+X=X	
(8c)	Ω∩X=X	Ω·X=X	Operations with Φ and Ω
(8d)	Ω∪X=Ω	Ω+X=Ω	
(8e)	Φ’=Ω	Φ’=Ω	
(8f)	Ω’=Φ	Ω’=Φ	
(9a)	X∪ (X’∩Y)=X∪Y	X+(X’·Y)=X+Y	These relationships are unnamed but are frequently useful in the reduction process
(9b)	X’∩(X∪Y’)=X’∩Y’=(X∪Y)’	X’·(X+Y’)=X’·Y’=(X+Y)’	

(*) The symbol 1 is often use instead of Ω to designate the Universal set. In engineering notation Ω is often replaced by 1 and Φ by 0.

According to relations (1a) and (1b), the union and intersection operations are commutative. In other words, the commutative laws permit interchange of the events X, Y with regard to an "AND" or "OR" operation. It is important to remember that there are mathematical entities that do not commute; e.g. the vector cross product and matrices, in general.

Relations (2a) and (2b) are similar to the associative laws of ordinary algebra: A(BC)=(AB)C and A+(B+C)=(A+B)+C. If a series of "OR" operations or a series of "AND" operations are under consideration, the associative laws permit grouping the events any way desired.

The distributive laws, relations (3a) and (3b) provide the valid manipulatory procedure whenever a combination of an "AND" operation with an "OR" operation is under consideration. By proceeding from left to right in the equations, the left-hand expression is reduce to an unfactored form. In relation (3a), for example, operating with X on Y and on Z results in the right-hand expression. Operating form right to left in the equations simply factors the expression. For instance, in relation (3b) X is factor out to obtain the left-hand side. Although relation (3a) is analogous to the distributive law in ordinary algebra, relation (3b) has no such analog.

The idempotent laws, relations (4a) and (4b), "cancel out" any redundancies of the same event.

The laws of absorption, relations (5a) and (5b), can easily be validate by reference to an appropriate Venn diagram. Relation (5a) can also be argue in the following way. Whenever the occurrence of X automatically implies the occurrence of Y, then X is said to be a subset of Y. This situation can be represent in symbolic form as $X \subset Y$ or $X \rightarrow Y$. In this case X+Y=X and X·Y=X. In relation (5a), if X occurs then (X+Y) has also occurred and $X \subset (X+Y)$; therefore X·(X+Y)=X. A similar argument can be develop in the case of relation (5b).

De Morgan's theorems, relations (7a) and (7b), provide the general rule for removing primes on brackets. Suppose that X represents the failure of some component. Then X' represents the non-failure or successful operation of that component. In this light, relation (7a) simply states that for the double failure of X and Y not to occur, either X must not fail or Y must not fail.

As an application of the use of these rules, consider the simplification of the expression

$$(A + B) \cdot (A + C) \cdot (D + B) \cdot (D + C)$$

Applying relation (3b) to (A+B)·(A+C) results in

$$(A + B) \cdot (A + C) = A + (B \cdot C)$$

Likewise,

$$(D + B) \cdot (D + C) = D(B \cdot C)$$

An intermediate result produced is

$$(A + B) \cdot (A + C) \cdot (D + B) \cdot (D + C) = (A + B \cdot C) \cdot (D + B \cdot C)$$

Letting E represent the event B·C results in

$$(A + B \cdot C) \cdot (D + B \cdot C) = (A + E) \cdot (D + E) = (E + A) \cdot (E + D)$$

Another application of relation (3b) yields

$$(E + A) \cdot (E + D) = E + A \cdot D = B \cdot C + A \cdot D$$

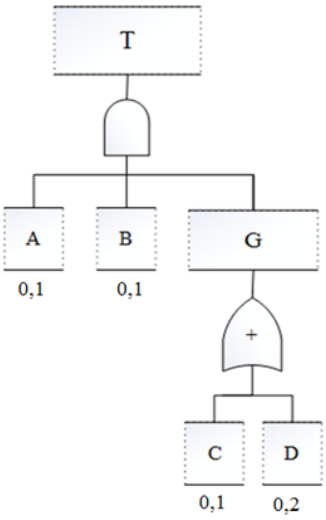
Therefore, the result is

$$(A + B) \cdot (A + C) \cdot (D + B) \cdot (D + C) = B \cdot C + A \cdot D$$

The original expression has been substantially simplified for purposes of evaluation (NASA, 2002).

APPENDIX B – MINIMAL CUT SETS UPPER BOUND VS EXACT PROBABILITY

Figure 85 presents a simple example where the Minimal Cut Sets have basic replicated events (Event A and Event B). In this case, the Minimal Cut Sets Upper Bound Method provides the upper limit of the probability of the top event and not the exact probability; that is, when the Minimal Cut Sets have basic replicate events, the Minimal Cut Sets Upper Bound Method is only an approximation of the real probability of top event.



Minimal Cut Sets Upper Bound

$$S = 1 - \prod_{i=1}^{m}(1 - C_i)$$

$$S = 1 - [(1 - 0{,}001) * (1 - 0{,}002)]$$

$$S = T = 0{,}002998$$

Minimal Cut Sets

$$C_1 = ABC$$

$$C_2 = ABD$$

Exact Probability

$$T = ABC + ABD$$

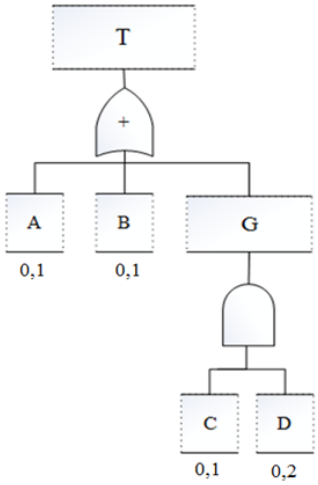
$$T = [P_r(A) * P_r(B) * P_r(C)] + [P_r(A) * P_r(B) * P_r(D)] - [P_r(A) * P_r(B) * P_r(C) * P_r(D)]$$

$$T = 0{,}001 + 0{,}002 - 0{,}0002$$

$$T = 0{,}002800$$

Figure 85 - Example of Minimal Cut Sets with common basic events

However, in the case that the Minimal Cut Sets do not have basic replicated events (see Figure 86), the Minimal Cut Sets Upper Bound Method results in the exact probability of the top event. This situation happens because when the Minimal Cut Sets of FT have replicated events, the Minimal Cut Sets Upper Bound expression will consider these events each time the term $(1 - C_i)$ is computed, and this leads to an over consideration of probabilities by developing an upper limit of the real value.



Minimal Cut Sets Upper Bound

$$S = 1 - \prod_{i=1}^{m}(1 - C_i)$$

$$S = 1 - [(1 - 0{,}01) * (1 - 0{,}01) * (1 - 0{,}02)]$$

$$S = T = 0{,}2062$$

Minimal Cut Sets

$C_1 = A$

$C_2 = B$

$C_3 = \mathrm{CD}$

Exact Probability

$$T = A + B + CD$$

$$T = [P_r(C_1)] + [P_r(C_2)] + [P_r(C_3)] - [P_r(C_1) * P_r(C_2)] - [P_r(C_1) * P_r(C_3)] - [P_r(C_2) * P_r(C_3)] + [P_r(C_1) * P_r(C_2) * P_r(C_3)]$$

$$T = 0{,}1 + 0{,}1 + 0{,}02 - 0{,}01 - 0{,}002 - 0{,}002 + 0{,}0002$$

$$T = 0{,}2062$$

Figure 86 - Example of Minimal Cut Sets mutually exclusive

APPENDIX C – IMPORTANCE RANKING IN PROBABILISTIC RELIABILITY ASSESSMENT

Knowing that during the design reliability analysis, some components and their arrangement may be more critical than others in terms of system reliability (Modarres et al., 2009), it is proposed to develop an analysis of measures of importance for the main components of the DP system.

To define which are the main components of the DP system are taken into account the Minimal Cut Sets selected during the application of Monte Carlo Simulation (see Appendix D), and for each component that composes this minimal cut sets, the measures of importance as Birnbaum, Criticality Importance, Fussell-Vesely, Risk-Reduction Worth (RRW) and Risk-Achievement Worth (RAW) are applied.

In the next section, the measures of importance applied and the result obtained for each DP system will be presented.

- **Birnbaum Measure of Importance**

The Birnbaum importance I_B, is defined as the rate of change in reliability of system with respect to change in a reliability element (Birnbaum, 1969), for success space [as described by Sharirli (1985)] is defined as

$$I_i^B(t) = \frac{\partial R_s[R(t)]}{\partial R_i(t)}$$

Where $R_s[R(t)]$ is reliability of the system as a function of the reliability of its individual components, $R_i(t)$.

If, for a given component i, $I_i^B(t)$ is large, it means that a small change in the reliability of component i, $R_i(t)$, will result in a large change in the system reliability $R_s(t)$.

According to Hoyland and Rausand (1994), if system components are assumed independent, the Birnbaum measure of importance can be represented by

$$I_i^B(t) = R_s[R(t)|R_i(t) = 1] - R_s[R(t)|R_i(t) = 0]$$

Where $R_s[R(t)|R_i(t) = 1]$ and $R_s[R(t)|R_i(t) = 0]$ are the values of reliability function of the system with the reliability of component i set to 1 and 0, respectively.

Figure 87 presents the Birnbaum importance for main components of DP systems in study (semisubmersible platform DP2 and drillship DP3). Regarding DP2 system, the figure shows that the bus bar is the most important component, that is, improve the reliability of bus-bar can result in a large change in the system reliability.

Other components that could generate great change in the reliability of the DP2 system are the coolers, PMS, HV switchboards, lubrication pumps and oil transfer pumps. Note that all the equipment mentioned so far are part of the power subsystem.

In the DP3 system, the priority levels are lower that the DP2 system, because no equipment has a I_B greater than 0.02.

It is worth noting that in both cases of studies, the control subsystem equipment that has the highest priority is the wind sensor.

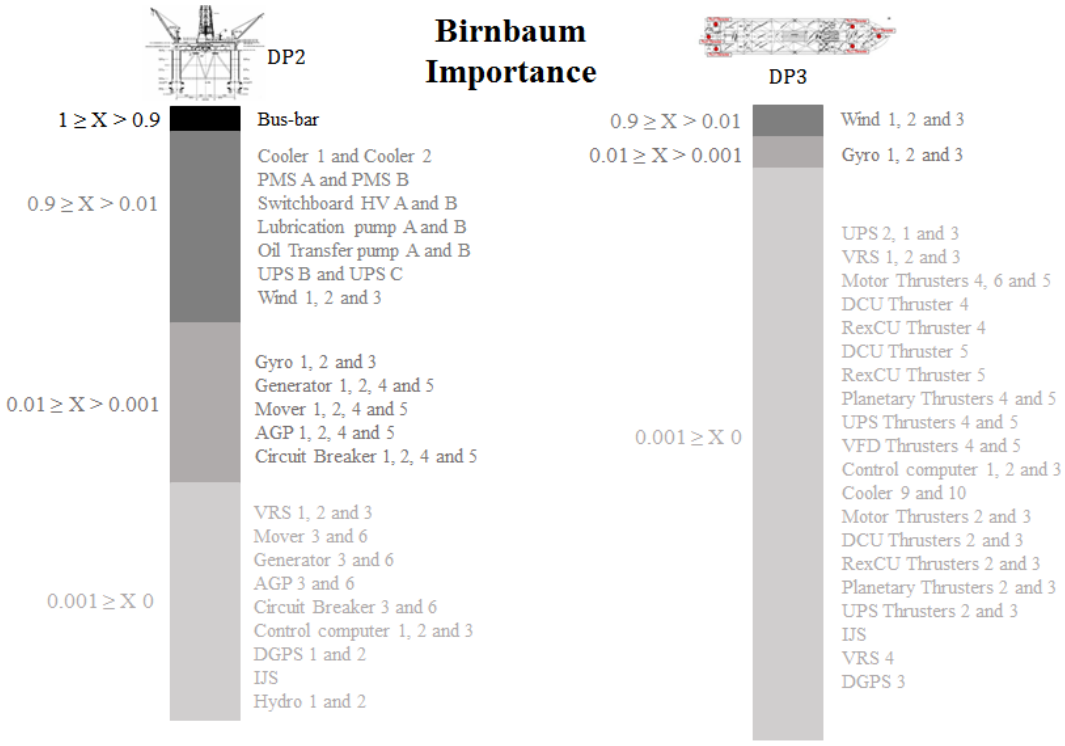


Figure 87 - Birnbaum Importance

Note that the Birnbaum measure does not consider the present or baseline performance (probability of success or failure of an element) so, it would be hard to use it for reliability-informed decision making, since low-failure probability items are not necessarily the prime candidates for any change (Modarres, 2006). To remedy this shortcoming, an extended version of this measure called criticality importance may be used.

- **Criticality Importance**

The Criticality importance I_{CR}, of component i is defined as

$$I_i^{CR}(t) = \frac{\partial R_s[R(t)]}{\partial R_i(t)} \times \frac{R_i(t)}{R_s[R(t)]}$$

or

$$I_i^{CR}(t) = I_i^B(t) \times \frac{R_i(t)}{R_s[R(t)]}$$

It is worth noting that the Birnbaum importance is correct for reliability of the individual components relative to the reliability of the whole system. Therefore, if the Birnbaum importance of a component is high, but the reliability of the components is low with respect to the reliability of the system, then criticality importance assigns a low importance to this component.

For the DP systems in study, I_{CR} is calculated (see Figure 88). Although the bus bar (in the case of the DP2 system) and the wind sensors (in the DP3 case) continue to be the highest priorities, it is worth mentioning some substantial differences between the results of I_B (see Figure 87) and I_{CR} (see Figure 88).

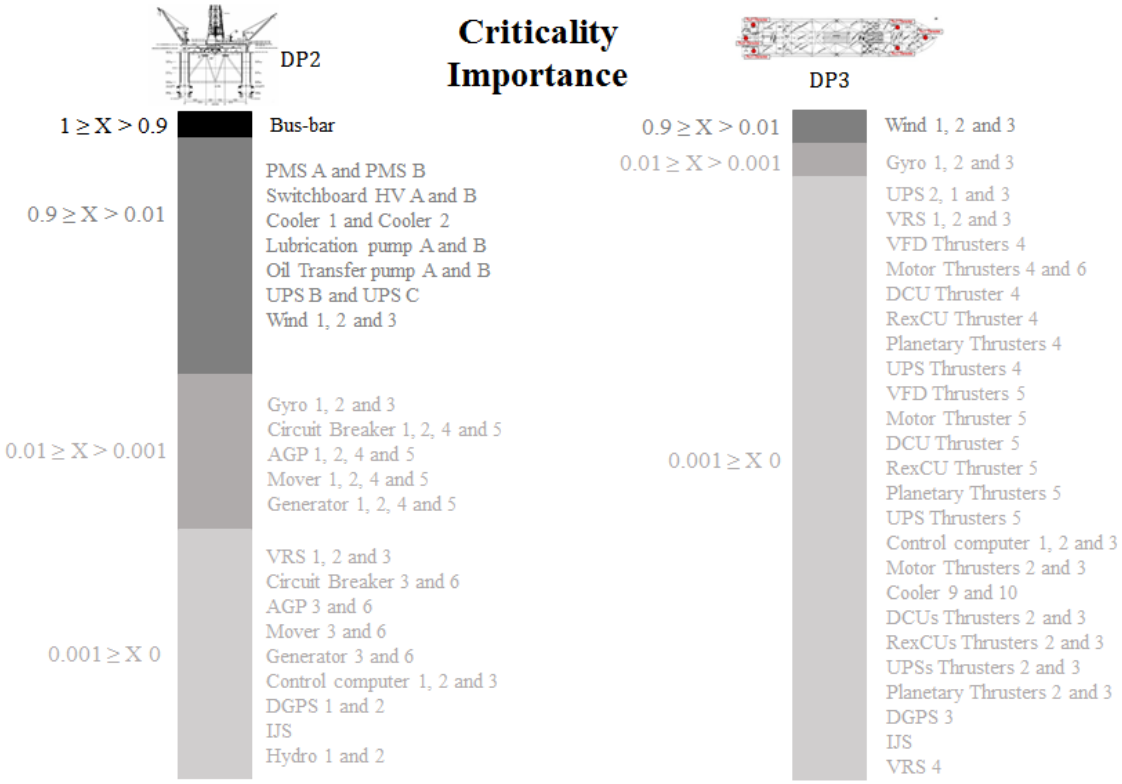


Figure 88 - Criticality Importance

From the point of view of criticality, the PMS and the HV switchboards are most critical than the refrigerators, while in the Birnbaum vision, the coolers are the most critical. Other difference is that in the DP3 system, the Birnbaum vision pointed to DGPS as the least priority component, but the criticality indicator shows that really the least priority in the DP3 system is the VRS4.

An interesting difference is that the result of the Birnbaum indicator showed that between mover-generators equipment (mover, generator, AGP and Circuit Breaker) of DP2 system, the movers and the generators are most important, however, the criticality importance suggests prioritizing the efforts in improve the circuit breakers and the AGP and later evaluate the operating conditions of movers and generators.

A subset of the criticality importance measure is the inspection importance measure.

- **Inspection Importance**

The inspection importance measure (I_i^W) is defined as the product of the Brinbaum importance times the failure probability (unreliability or unavailability) of the component. Accordingly,

$$I_i^W(t) = I^B(t) \times Q_i(t)$$

This measure is use to prioritize operability test activities to ensure high component readiness and performance.

When answering the question which equipment to inspect first? It can be expected in response that the bus-bar (in the case of the DP2 system) and the wind sensors (in the DP3 case) must first be inspected. However, the inspection importance shows that the response is not so intuitive for the semisubmersible platform, since the coolers, PMS, lubrication pumps, transfer oil pumps, wind sensors and UPS status should be checked first before checking the bus-bar (see Figure 89).

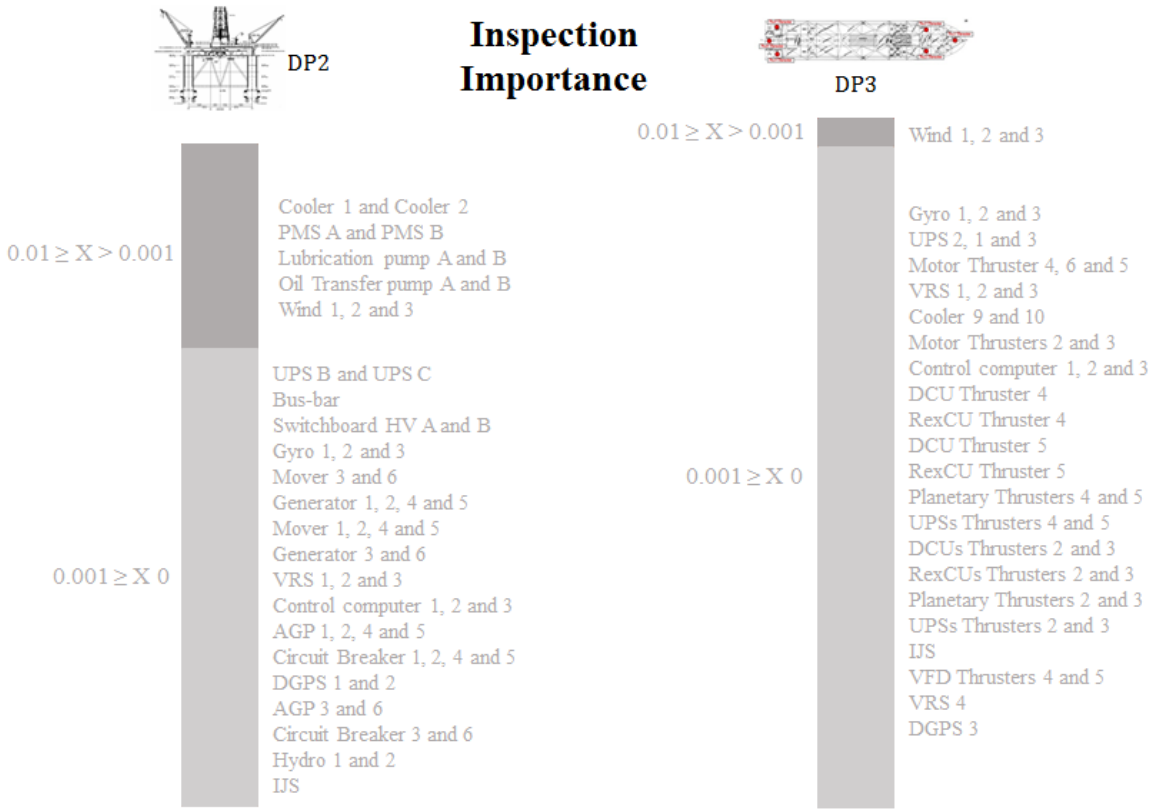


Figure 89 - Inspection Importance

- **Fussell-Vesely Importance**

In the cases where component i contributes to system reliability, but is not necessarily critical, the Fussell-Vesely importance measure can be used. This measure, introduced by W.E. Vesely and latter applied by Fussell (1975), is in the form of

$$I_i^{FV}(t) = \frac{R_i[R(t)]}{R_s[R(t)]}$$

where $R_i[R(t)]$ is the contribution of component i to the reliability of the system. Similarly, using unreliability or unavailability functions,

$$I_i^{FV}(t) = \frac{F_i[Q(t)]}{F_s[Q(t)]}$$

where $F_i[Q(t)]$ denotes the probability that component i is contributing to system failure.

According to Modarres (2006), $I_i^{FV}(t)$ can be rewritten as

$$I_i^{FV}(t) = \frac{F_s[Q(t)] - F_s[Q(t)|Q_i(t) = 0]}{F_s[Q(t)]}$$

where $F_s[Q(t)|Q_i(t) = 0]$ is the system unreliability (unavailability or risk) when unreliability (or unavailability) of component i is set to zero.

In reliability elements with large Fussell-Vessely importance measure, it is imperative not to allow their long-term average probabilities to further increase. Accordingly, in an aging regime, I_{FV} can be interpreted as the amount of allowed degradation of performance as a function of failure probability increase (Modarres, 2006). This measure also shows the importance relative to the long-term averaged performance of a component (so, it is not appropriate for measuring importance of a set of similar components instantaneously taken out of service).

The Fussell-Vesely importance suggests that in the case of the DP2 system, the operating and maintenance team should be interested mainly in the power subsystem components that have a single redundancy, i.e. the PMS, fuel transfer pumps, lubrication pumps and coolers. While operating and maintenance team of DP3 system should treat with priority the wind sensors and gyrocompasses, on all other components (see Figure 90).

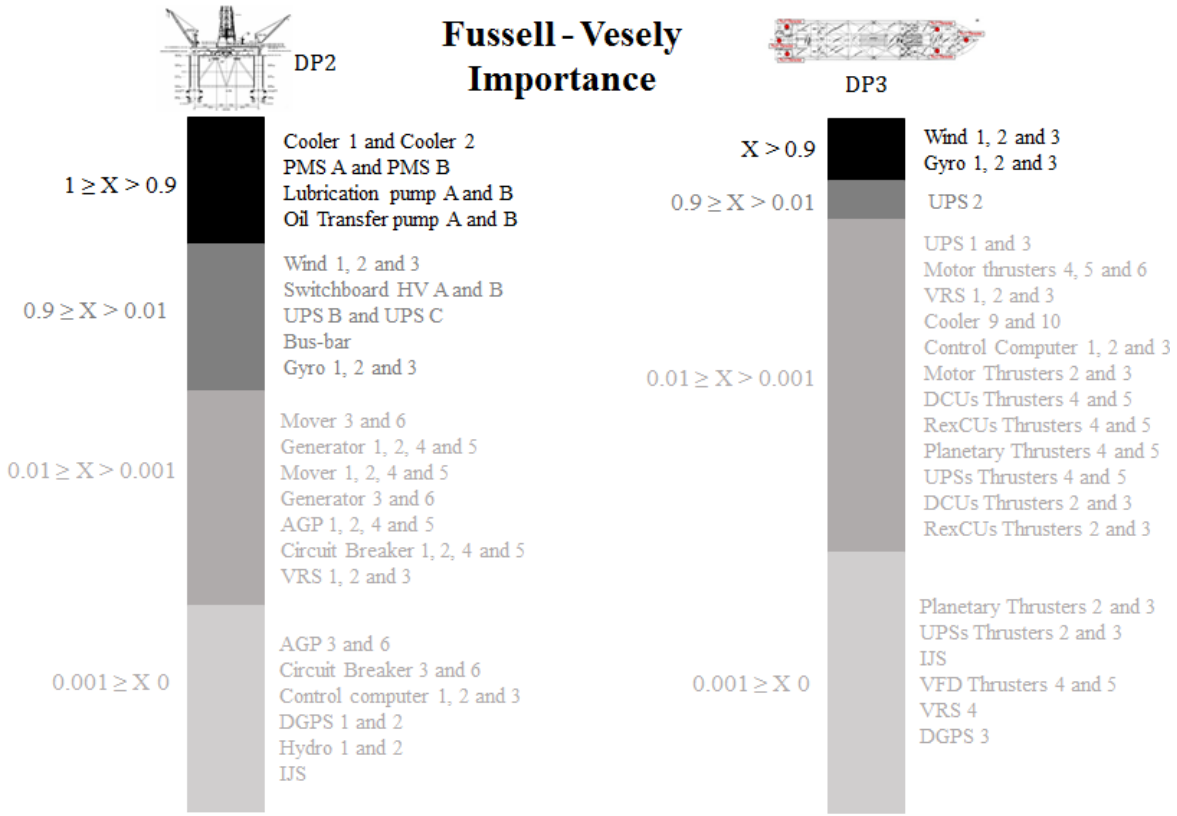


Figure 90 - Fussell-Vesely Importance

Note that the most redundant DP system (that is the DP3 system), presents less equipment at the most critical levels than the DP2 system. In other words, while the DP2 system has 9 components in the first two levels of Fussell-Vesely Importance, the DP3 system only has 3.

- **Risk-Reduction Worth Importance**

The Risk Reduction Worth (RRW) importance is a measure of the change in unreliability (unavailability or risk) when an input variable, such as the unavailability of component, is set to zero-that is, by assuming that a component is “perfect” (or its failure probability is zero) and thus eliminating any postulated failure. This importance measure shows how much better the system can become as its components are improved.

This importance measure is used in failure domains, although it can also be used in the success domain. The calculation may be done either as a ratio or as a difference. Accordingly, as a ratio,

$$I_i^{RRW} = \frac{F_s[Q(t)]}{F_s[Q(t)|Q_i(t) = 0]}$$

and as a difference,

$$I_i^{RRW} = F_s[Q(t)] - F_s[Q(t)|Q_i(t) = 0]$$

where $F_s[Q(t)|Q_i(t) = 0]$ is the system unreliability (unavailability or risk) when unreliability (or unavailability) of component i is set to zero.

In practice, this measure is used to identify elements of the system (such as components) that are the best candidates for improving system reliability (risk or unavailability).

Figure 91 shows the results of RRW importance for the DP systems in study. The result of RRW importance is similar with the criticality importance (see Figure 88); however, for the DP2 system, RRW importance suggests prioritizes the HV switchboards, while the criticality importance prioritizes the UPSs and the bus-bar; and the RRW differs with

criticality importance when prioritizing the AGP of the mover-generators 1, 2, 4 and 5; on the control computers and the VRSs.

Regarding the DP3 system, the order in which the components should be prioritized is the same according to the criticality importance and the RRW.

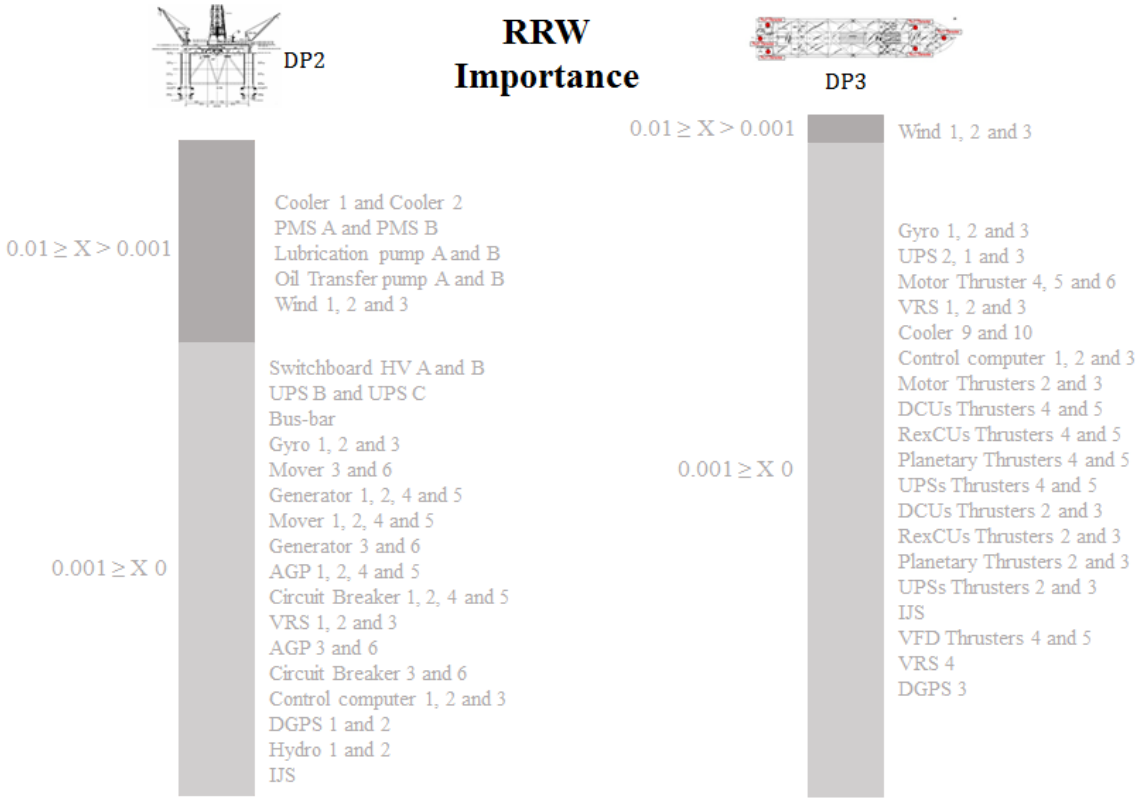


Figure 91 - RRW Importance

- **Risk-Achievement Worth Importance**

The Risk- Achievement Worth (RAW) importance is the inverse of the RRW measure. In this case, the input variable (e.g., component unavailability) is set to one, and the effect of this change on system unreliability (unavailability or risk) is measured. Similar to RRW, the calculation may be done as a ratio or a difference. By setting component failure probability to one, RAW measures the increase in system failure probability assuming the worst case of failing the component. As a ratio, RAW measure is

$$I_i^{RAW} = \frac{F_s[Q(t)|Q_i(t) = 1]}{F_s[Q(t)]}$$

and as difference,

$$I_i^{RAW} = F_s[Q(t)|Q_i(t) = 1] - F_s[Q(t)]$$

where $F_s[Q(t)|Q_i(t) = 1]$ is the system unreliability (unavailability or risk) when unreliability (or unavailability) of component i is set to one.

The risk increase measure is useful for identifying elements of the system that are the most crucial for making the system unreliable (unavailable or increasing the risk). Therefore, components with high I^{RAW} are the ones that will have the most impact, should their failure probability unexpectedly rise.

The result of RAW importance, suggests again the bus bar as a critical component for the DP2 system, as well as the components of the power subsystem that present a single redundancy (coolers, PMS, HV switchboard, lubrication pumps and transfer pumps). While in the case of the DP3 system, the wind sensors and the gyrocompass are still the most impact components for the system (see Figure 92).

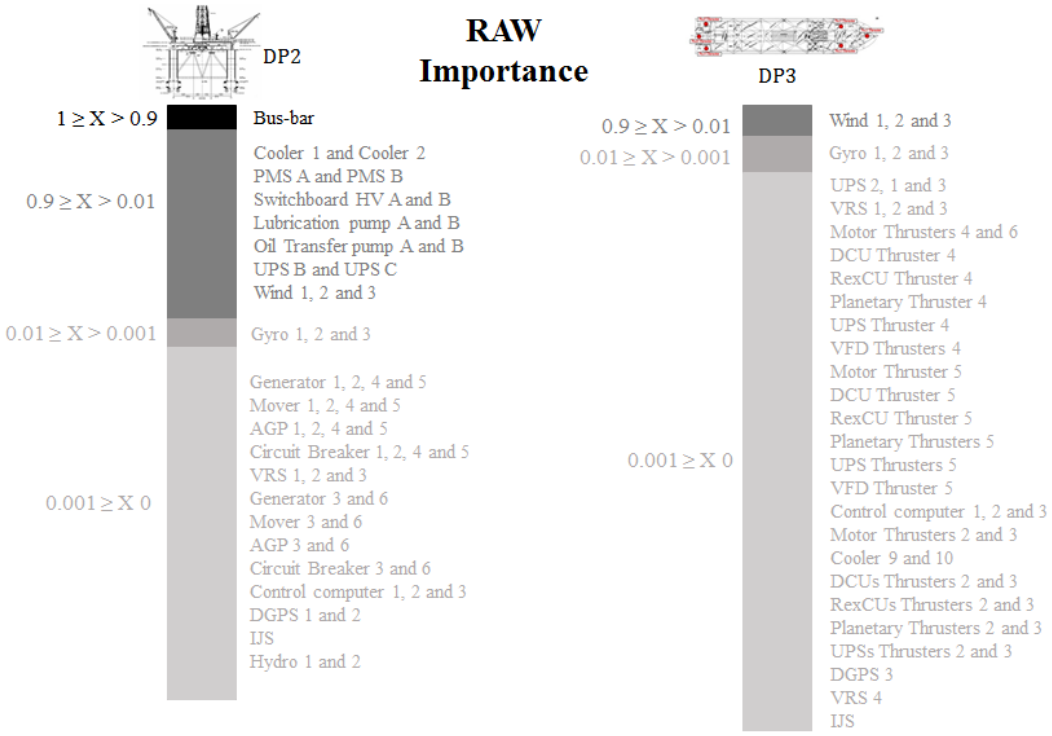


Figure 92 - RAW Importance

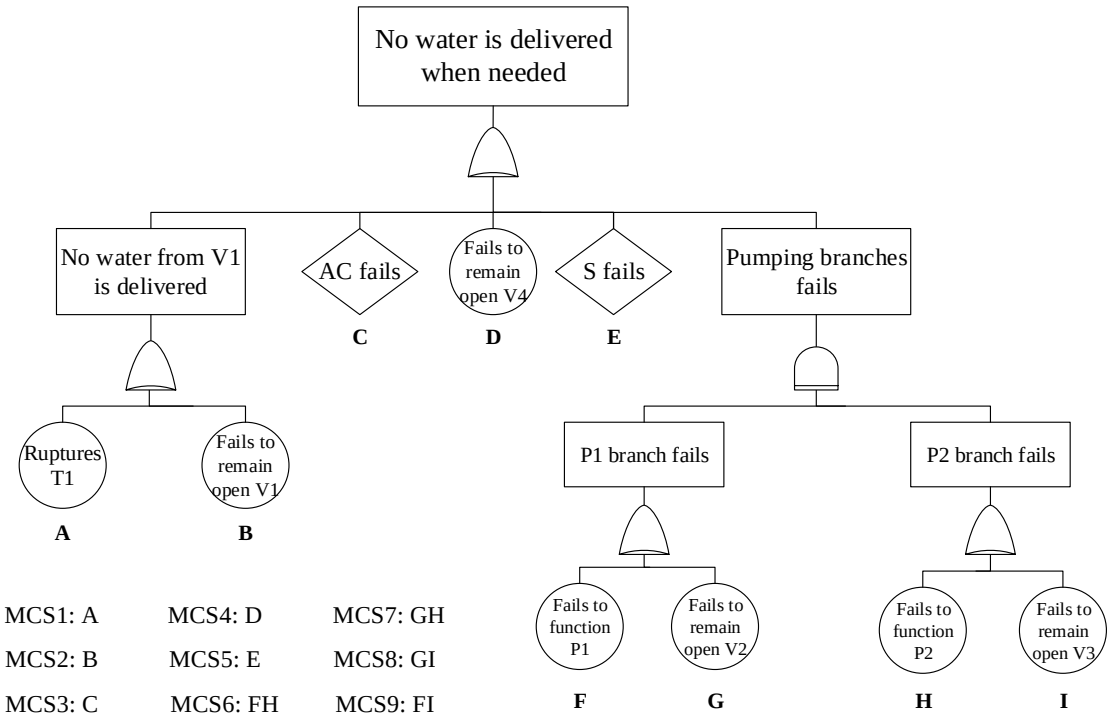
In short, all the measures of importance tend to suggest that the components of the power subsystem of the DP2 system should be prioritized over the components of the other subsystems, while in the case of the DP3 system, the results tend to point to the wind sensors and the gyrocompasses as the most critical components of the system, in general. Although all the components are relevant in the operation, the analysis of measure of importance is interesting because in the operation, the resources are limited and the prioritization actions must be assertive to achieve an efficient operation.

APPENDIX D – MONTE CARLO SIMULATION VS FAULT TREES

The Minimal Cut Sets may be used to represent an equivalent system of the system being analyzed in the FT, that is, addition to representing the minimum set of basic events, whose occurrence will cause the top event; Minimal Cut Sets also represent a series RBD of the system under analysis, where each block represents a minimal cut set.

For the example of the pumping system (see Figure 16) presented in section 2.5.3, an equivalent system would be the series RBD presented in Figure 93.

Fault Tree



Equivalent system

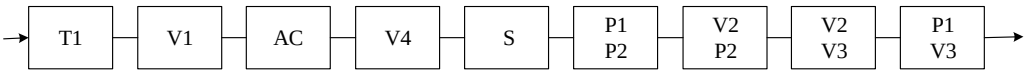


Figure 93 - RBD equivalent to FT

That is, when at least one of its Minimal Cut Sets (a block of series diagram) has all its components unavailable, the system will fail.

This logic was implemented in the FTs of free drift of the DP system, in order to test whether from the equivalent system (series block diagram drawn from the Minimal Cut Sets) one could obtain the probability of total failure of the DP system using Monte Carlo Simulation.

However, to use the Monte Carlo Simulation, it is necessary to select minimal cut sets that assure to represent probabilistically the DP system but that represent an amount that can be simulated, because the computational cost of evaluating all minimal cut sets of FTs could make the application of Monte Carlo Simulation impracticable, so it is proposed to select the minimal cut sets that have a probability of occurrence equal to or greater than 2.2831E-05 (1 failure in 5 years).

It is worth noting that the high computational cost respond to that each FT has a larger number of minimal cut sets (see Table 19), and that the Monte Carlo Simulation is a method that requires a great number of samples to reach the desired results (Aderibigbe, 2014).

Table 19 - Total number of minimal cut sets and number of minimal cut sets proposed for the event: free drift

Minimal Cut Sets		
DP system	All	Probability ≥ 2.2831E-05
DP2	110,453	209
DP3	130,528	362

The minimal cut sets selected ensure that the probability of occurrence to top events do not suffer a significant difference. Figure 94 presents the probability of occurrence of each top event when the exact method is applied and the result of the quantification of FTs from the selected minimal cut sets (using the method of Monte Carlo Simulation, modeling 10.000, 100.000 and 1.000.000 times a mission period of three months).

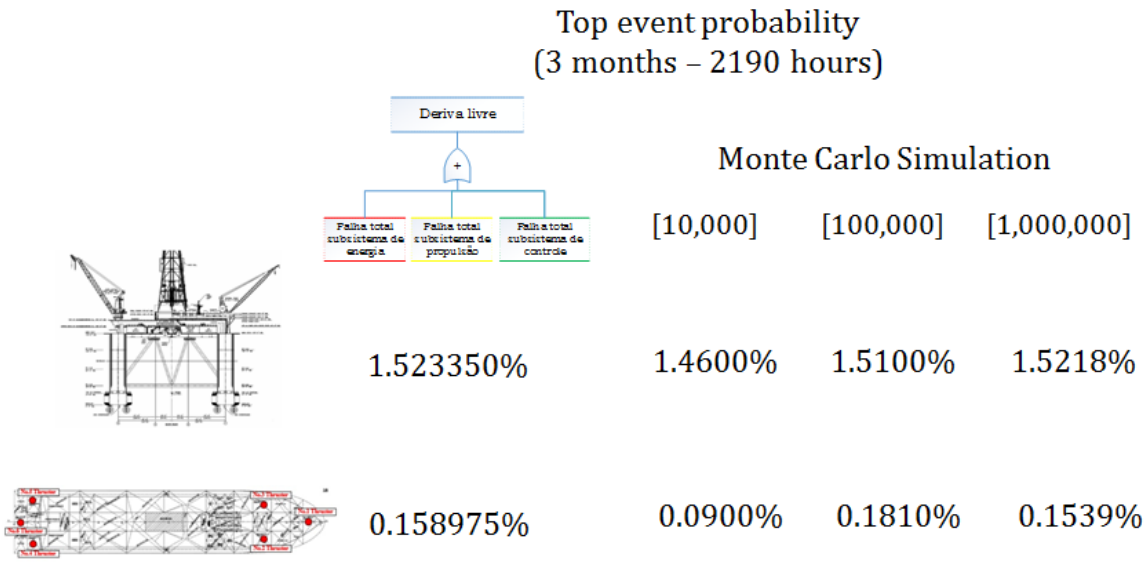
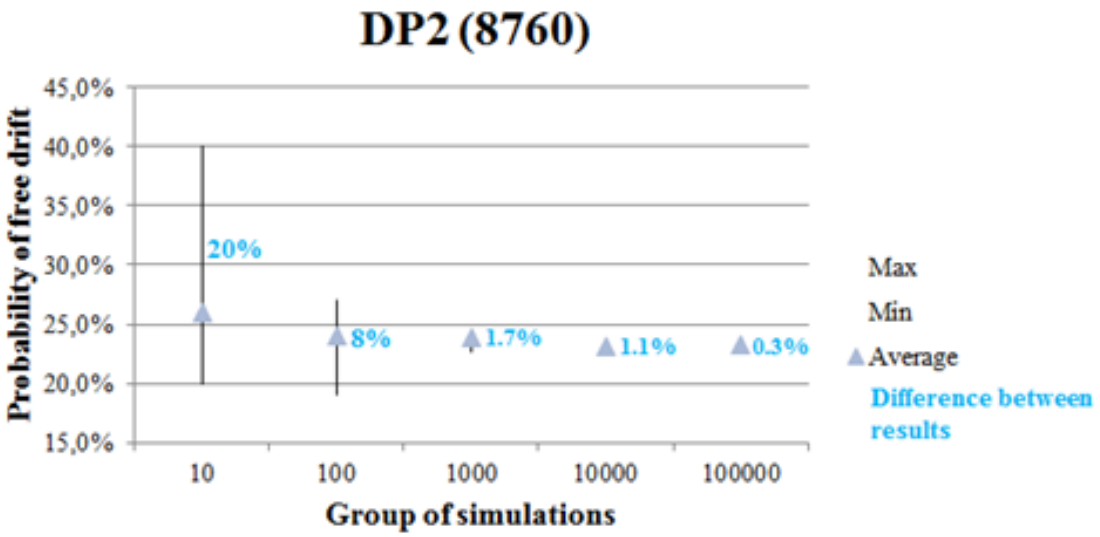


Figure 94 - Comparison between the results obtained from free drift probability from the FTs and Monte Carlo Simulation

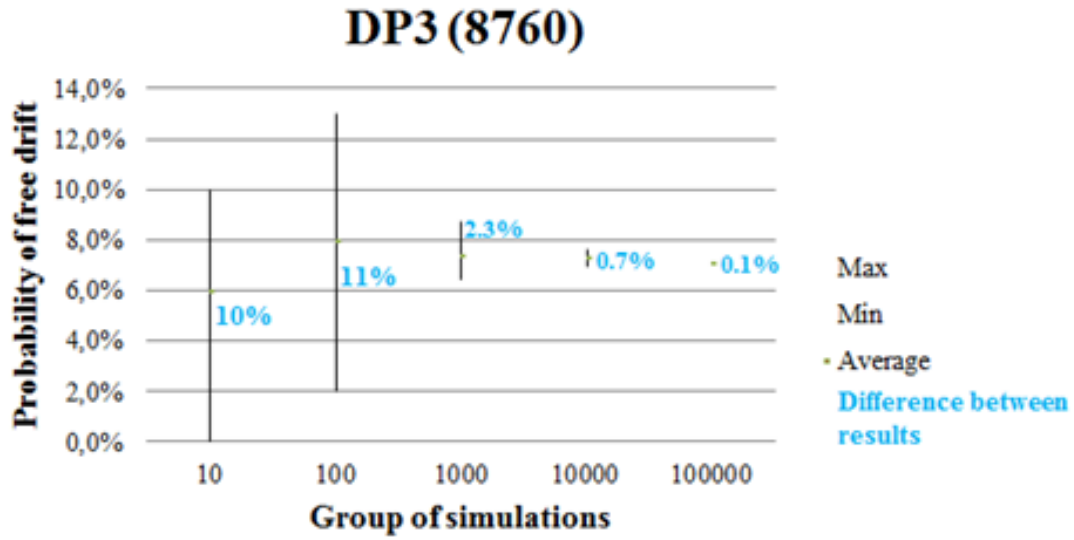
As expected, the number of simulations is proportional to the accuracy of the result. Therefore, the result obtained with 1,000,000 simulations is similar to the result of exact probability than the result obtained with 10,000 simulations. This responds to the Central Limit Theorem, which guarantees that, as the number of trials increases, the standard error around the mean heads towards a constant value and the standard error in the mean is progressively proportional to $n^{1/2}$ (Lerche & Mudford, 2005).

An additional analysis developed during the review of the Monte Carlo Simulation and Fault Trees was the study of the number of simulations necessary to evaluate the DP system; i.e., if it was intend to solve the question of how many Monte Carlo Simulations have to be made to ensure the DP system modeling.

Figure 95 presents the difference of results (probability of free drift for one-year operation) for each group of simulations, i.e., with 100 simulations of DP2 system, the difference between the results for one year of operation (maximum probability obtained – minimum probability obtained) is 8% whereas 100,000 simulations, the difference between the probability obtained for DP2 system only is 0.3%. Thus, it is possible to conclude that from 100,000 simulations the obtained values begin to converge to the value of the exact probability.



	10	100	1000	10000	100000
Max	40,0%	27,0%	24,4%	23,7%	23,5%
Min	20,0%	19,0%	22,7%	22,6%	23,2%
Average	26,0%	24,0%	23,8%	23,1%	23,3%



	10	100	1000	10000	100000
Max	10,0%	13,0%	8,7%	7,6%	7,1%
Min	0,0%	2,0%	6,4%	7,0%	7,0%
Average	6,0%	8,0%	7,4%	7,3%	7,1%

Figure 95 - Difference between the results obtained in the Monte Carlo Simulations (free drift for operational time of one-year)

APPENDIX E – CODE FOR ESTIMATE THEORETICAL PDF PARAMETERS

```
# Data
require(Rcmdr)

# First MASS library is called with the package GAMLSS
require(MASS)
library(gamlss)

################## DP2 ##################
################## 12 MONTHS ###########

# Visualization the histogram and empirical pdf of simulated data
par(mfrow=c(1, 2))
hist(TR_DP2$RTIME.8760, freq = FALSE, main ="Repair times of DP2 System
(8760h)",xlab="Repair Times",ylab="Density", cex.main=1)

# Empirical solution
plot(density(TR_DP2$RTIME.8760),main ="Repair times of DP2 System
(8760h)",xlab="Repair Times",ylab="Density", cex.main=1)

# Parametrical solution
x1 <- TR_DP2$`RTIME.8760`
prueba1 <- fitDist(y=x1, type="realplus", k=2)
## Type represent the type of distribution to be tried that for this case the distribution must
represent plus value
## k represent the penalty for the GAIC - Generalised Akaike Information Criterion, that is,
for distributions with more than 2 parameters the code applied a penalty. Default value of k
is 2
prueba1$fits
opc1 <- gamlss(x1~1, family=GA)
summary(opc1)

#### Parameters estimation
mu_est <- exp(coef(opc1, what="mu"))
sigma_est <- exp(coef(opc1, what="sigma"))

#Plot of both solutions
density <- function(x) dGA(x, mu=mu_est, sigma=sigma_est)
curve(density, from = 0, col='blue', lwd=2, add=TRUE)
text(x=13, y=0.15, "Theoretical (Gamma)", col='blue')
text(x=13, y=0.10, "Empirical", col='black')
```

```
################## 09 MONTHS ############
# Visualization the histogram and empirical pdf of simulated data
par(mfrow=c(1, 2))
hist(DLDP29MONTHS$RTIME.6570, freq = FALSE, main ="Repair times of DP2 System
(6570h)",xlab="Repair times",ylab="Density", cex.main=1)

# Empirical solution
plot(density(DLDP29MONTHS$RTIME.6570),main ="Repair times of DP2 System
(6570h)", xlab="Repair times", cex.main=1)

# Parametrical solution
x2 <- DLDP29MONTHS$RTIME.6570
prueba2 <- fitDist(y=x2, type="realplus", k=2)
prueba2$fits
opc2 <- gamlss(x2~1, family=GA)
summary(opc2)

#### Parameters estimation
mu_est <- exp(coef(opc2, what="mu"))
sigma_est <- exp(coef(opc2, what="sigma"))

#Plot of both solutions
density <- function(x) dGA(x, mu=mu_est, sigma=sigma_est)
curve(density, from = 0, col='blue', lwd=2, add=TRUE)
text(x=13, y=0.15, "Theoretical (Gamma)", col='blue')
text(x=13, y=0.10, "Empirical", col='black')



################## 06 MONTHS ############
# Visualization the histogram and empirical pdf of simulated data
par(mfrow=c(1, 2))
hist(DLDP26MONTHS$RTIME.4380, freq = FALSE, main ="Repair times of DP2 System
(4380h)",xlab="Repair times",ylab="Density")

# Empirical solution
plot(density(DLDP26MONTHS$RTIME.4380),main ="Repair times of DP2 System
(4380h)")

# Parametrical solution
x3 <- DLDP26MONTHS$RTIME.4380
prueba3 <- fitDist(y=x3, type="realplus", k=2)
prueba3$fits
opc3 <- gamlss(x3~1, family=WEI3)
summary(opc3)
```

```
#### Parameters estimation
mu_est <- exp(coef(opc3, what="mu"))
sigma_est <- exp(coef(opc3, what="sigma"))

#Plot of both solutions
density <- function(x) dWEI3(x, mu=mu_est, sigma=sigma_est)
curve(density, from = 0, col='blue', lwd=2, add=TRUE)
text(x=13, y=0.15, "Theoretical (Gamma)", col='blue')
text(x=13, y=0.10, "Empirical", col='black')


################### 03 MONTHS ############
# Visualization the histogram and empirical pdf of simulated data
par(mfrow=c(1, 2))
hist(DLDP23MONTHS$RTIME.2190, freq = FALSE, main ="Repair times of DP2 System
(2190h)",xlab="Repair times",ylab="Density")

# Empirical solution
plot(density(DLDP23MONTHS$RTIME.2190),main ="Repair times of DP2 System
(2190h)")

# Parametrical solution
x4 <- DLDP23MONTHS$RTIME.2190
prueba4 <- fitDist(y=x4, type="realplus", k=2)
prueba4$fits
opc4 <- gamlss(x4~1, family=GA)
summary(opc4)

#### Parameters estimation
mu_est <- exp(coef(opc4, what="mu"))
sigma_est <- exp(coef(opc4, what="sigma"))

#Plot of both solutions
density <- function(x) dGA(x, mu=mu_est, sigma=sigma_est)
curve(density, from = 0, col='blue', lwd=2, add=TRUE)
text(x=13, y=0.15, "Theoretical (Gamma)", col='blue')
text(x=13, y=0.10, "Empirical", col='black')
```

APPENDIX F – PDF OF THE RESULTS OBTAINED IN FTs QUANTIFICATION (CONSIDERING UNCERTAINTY)

The KDE is used to construct the probability density function of the results obtained in the uncertainty analysis previously presented in Section 5.4. For design, a Kernel Gaussian is assumed and the Rule-of-Thumb is used as the bandwidth selector method.

Figure 96 shows the logic used during the programming of KDE method in the statistical software R.

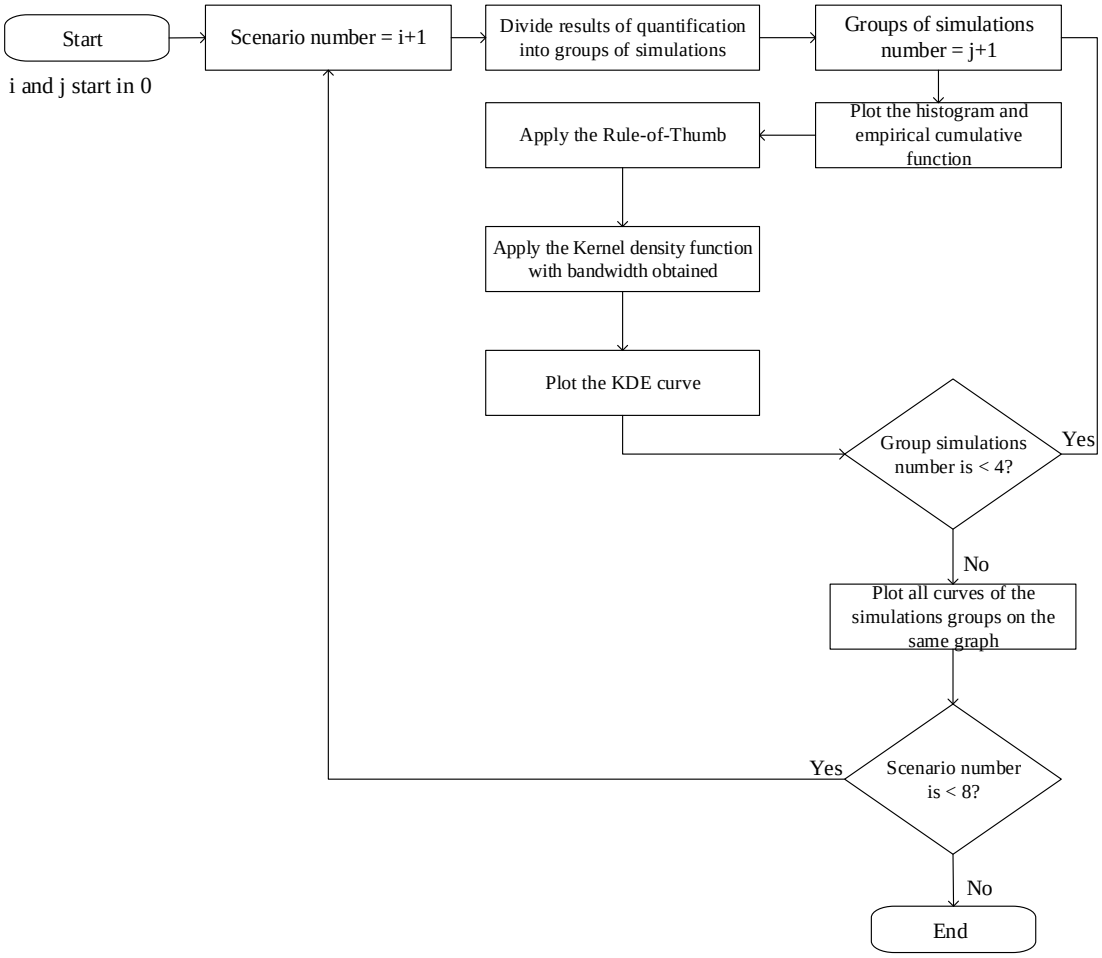


Figure 96 - logic used for obtain the pdf of the results of analysis with uncertainty

The inputs are the results obtained in Monte Carlo Simulation application for FTs quantification. It is worth noting that during the application of Monte Carlo method, each drift event (controlled drift and free drift) of each typical configuration (semisubmersible platform and drillship) is simulated for two operational times (8760 and 2190 hours), for this

reason, there exists eight scenarios and each scenario is simulated four times generating groups of simulations (1,000; 10,000; 100,000 and 1,000,000 simulations). Thus, the KDE implementation is divided in groups of simulations and in scenarios, in order to obtain four pdfs for each scenario; in Figure 97 the scenarios are specified.

For known the data behavior, the histogram and empirical cumulative distribution function are plotted. Then, the Rule-of-Thumb is applied and the bandwidth is obtained (see Table 20), with this information, the density function available in R is applied and then the curve is plotted.

When the four pdfs that correspond to each group of simulations are obtained for the same scenario, all curves are plotted in the same graph, in order to analyze possible differences between the results.

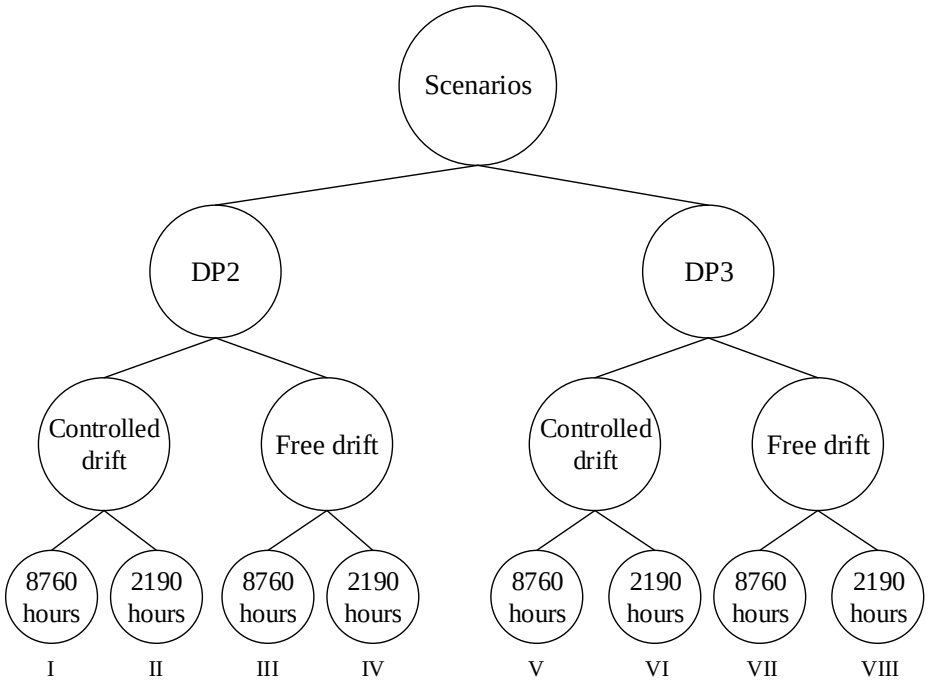


Figure 97 - Scenarios used for develop the analysis with uncertainty

In the next sections, the curves obtained in KDE implementation are presented, as well as the inferences obtained during the analysis.

Table 20 presents the bandwidths used during this implementation.

Table 20 - Bandwidth selected from Rule-of-Thumb

		8760 Hours		2190 Hours	
		DP2	**DP3**	**DP2**	**DP3**
Controled drift	1,000	1.2194	1.0341	1.6139	0.0285
	10,000	0.7434	0.6312	1.0208	0.0187
	100,000	0.4696	0.3927	0.6479	0.0117
	1,000,000	0.2964	0.2494	0.4083	0.0074
Free drift	1,000	1.7352	0.5208	0.1901	0.0042
	10,000	1.1557	0.3343	0.1180	0.0026
	100,000	0.7192	0.2131	0.0740	0.0017
	1,000,000	0.4544	0.1331	0.0466	0.0010

- **Controlled drift**

In the quantification of FTs without considering uncertainty in the failure rate of basic events, it is concluded that the probability of occurring a controlled drift due to partial failure of the DP2 system for operational times of 8760 hours and 2190 hours are 86.86% and 18.26% respectively; whereas in the case of drillship, these probabilities are 31.29% and 1.52%.

Figure 98 shows the pdf of controlled drift event for operational time of 2190 hours. Note that, in general, the curves present a high data concentration in probabilities higher than those obtained in analyzes without uncertainty. That is, the curves show that most of the data is between 15-30% in the case of the semisubmersible platform and 2-2.8% in the case of the drillship.

This possible overestimation of the top event probability during the uncertainty analysis is also reflected in the curves obtained in the implementation of one-year operation (see Figure 99).

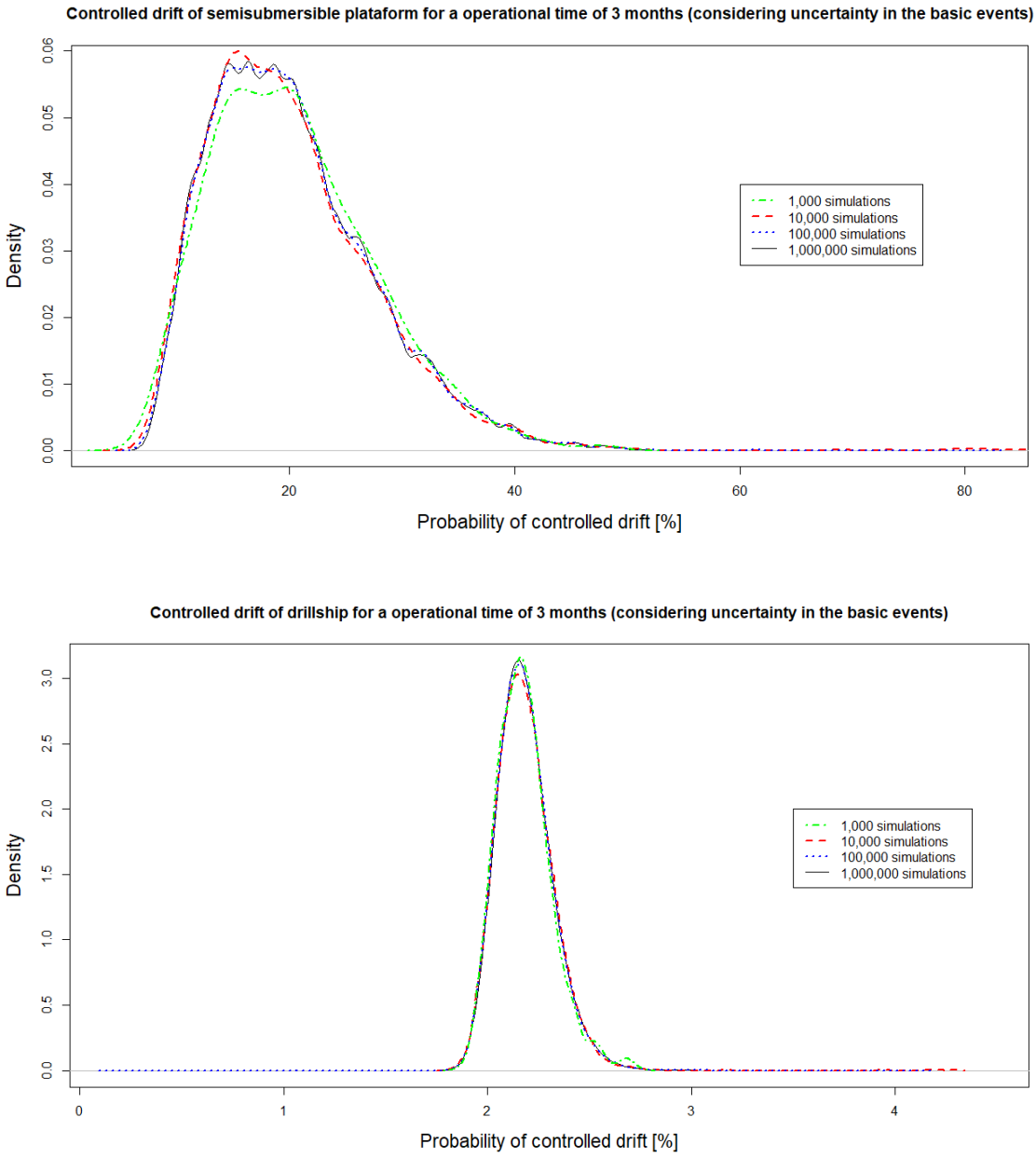


Figure 98 - pdf of controlled drift event (2190 hours)

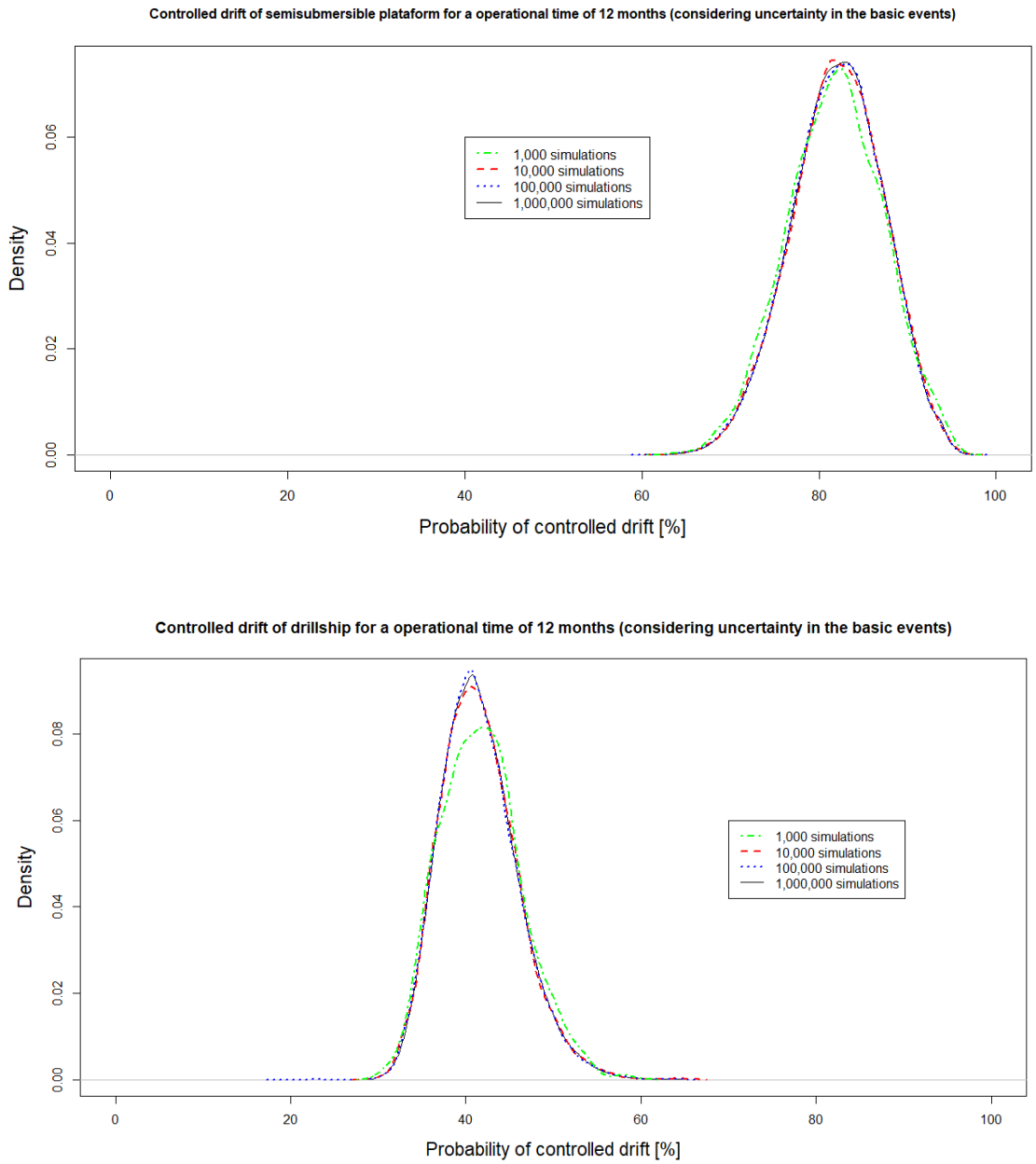


Figure 99 - pdf of controlled drift event (8760 hours)

The qualitative analysis of the curves allows concluding that, in general, the curves of the drillship are narrower than the curves obtained in the simulation of the operation of the platform.

- **Free drift**

Figure 100 presents the pdfs of each group of simulations for the free drift event when the operational time is 2190 hours. Note that, in general, the curves do not present important

differences between them. However, the qualitative analysis allows to conclude that as in the case of controlled drift, the curves obtained in free drift event of the drillship are narrower than the curves obtained in the simulation of the operation of the platform; and this responds to the fact that for all scenarios (controlled drift and free drift) the data obtained in the platform simulation groups have a standard deviation greater than the drillship data (see Figure 81, Figure 82, Figure 83 and Figure 84).

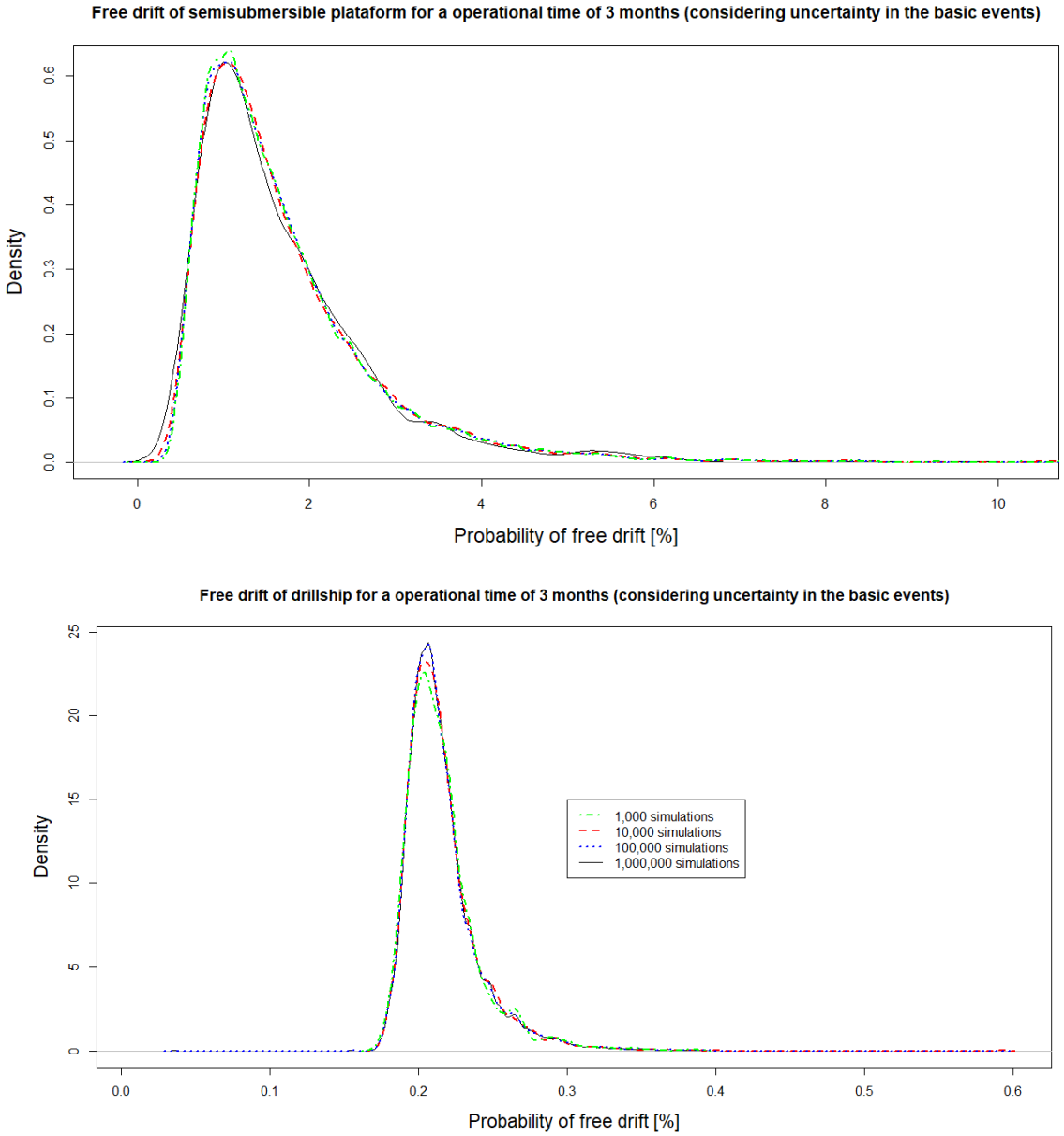


Figure 100 - pdf of free drift event (2190 hours)

Note that, in general, the curves designed for longer operational times (8760 hours) are broader than the curves designed for small operational times (2190 hours). For example, Figure 100 presents the results of case studies when the free drift event is analyzed for 2190 hours of operation, in this figure the curves of the semisubmersible platform present high data concentration between 0.5% and 4%; however, the curves of this same case study (DP2) for the same drift event (free drift) considering a longer operational time (8760 hours) show high concentration in a greater range of data (18% - 60%), see Figure 101. This result is consistent with Brownlee (2016), who argues that it is more difficult to predict behavior when the system tends to be studied for longer period of times, that is, shorter time horizons are often easier to predict with higher confidence, because for longer times of operational the uncertainty of failure rates increase.

Finally, to analyze the curves that represent the results of the free drift event when the operational time is one year, the results obtained in the analysis without uncertainty must be considered. According to Table 12, for an operational time of 8760 hours, the probability of the semisubmersible platform present a free drift is 24.58% while this probability for drillship is 7.92%.

When the curves of Figure 101 are analyzed, it is possible to conclude that considering uncertainty in the basic events of FTs, the probability of the free drift event is in greater proportion between 20% - 40% in the case of the semisubmersible platform and 10%-18% for the DP3 system. That is, when the results of Figure 101 are compared with the previous analysis (analysis without uncertainty) it is concluded that, in general, the curves present higher probabilities than those obtained (there is an overestimation of the probability presented by the curves).

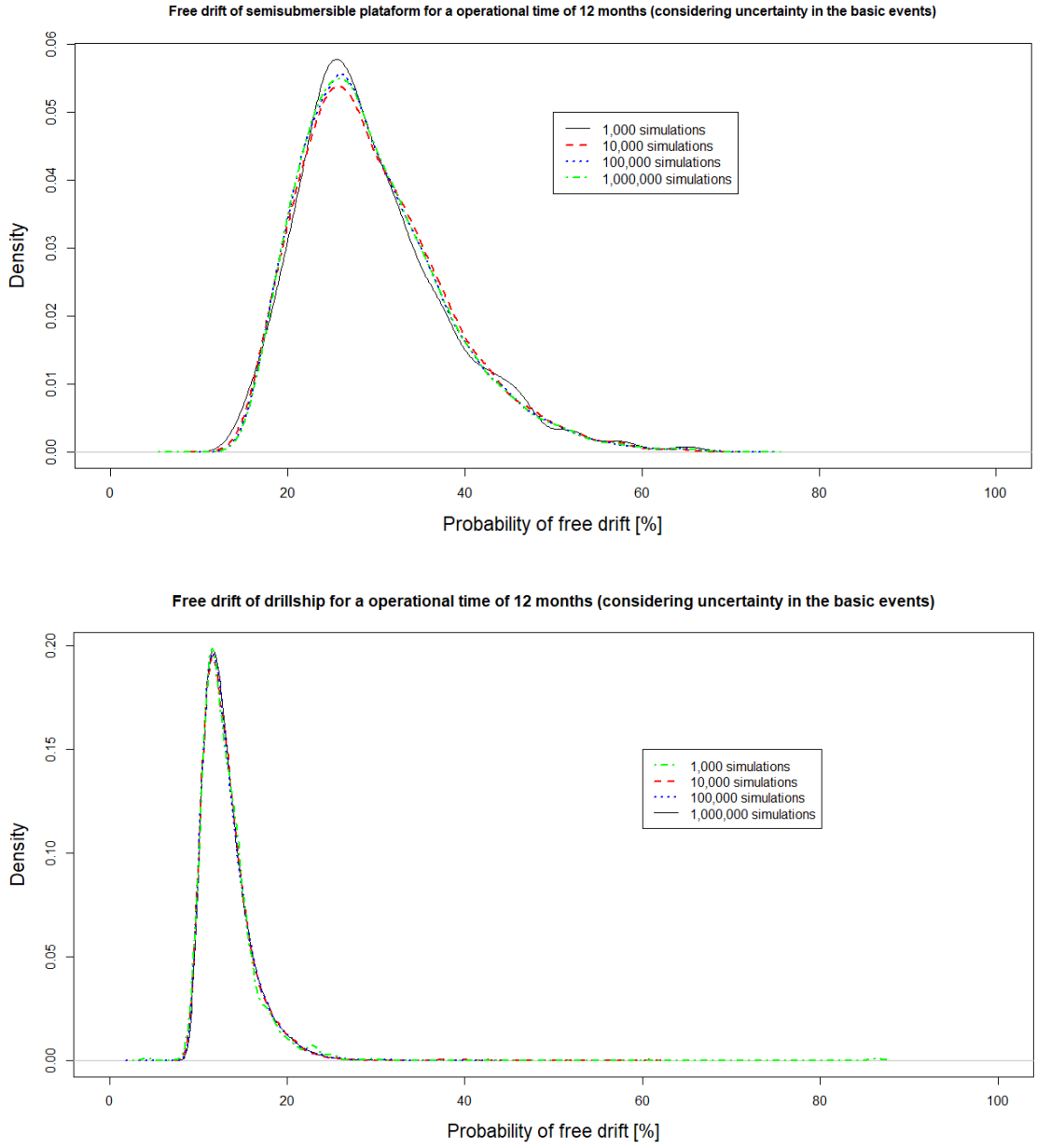


Figure 101 - pdf of free drift event (8760 hours)