University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization: Offshore Technology Marine and Subsea Technology	Spring semester, 2015 Open / ~~Restricted access~~
Writer: Vahid Rasoulzadeh Khorasani	V. Rasoulzadeh K. (Writer's signature)
Faculty Supervisor: Professor Ove Tobias Gudmestad	
Title of project: Risk Assessment of Diesel Engine Failure in a Dynamic Positioning System	
Credits (ECTS): 30	
Keywords: Risk Assessment, Diesel Engine, DP System, Fault Tree Analysis, Bow-Tie Analysis	Pages: 86 + enclosure: 23 + 1 CD Stavanger, June 29, 2015 Date/Year

ABSTRACT

The high demand for hydrocarbons as the major source of energy has forced humans to expand the oil and gas industry beyond the shore. Because of the challenges of oil and gas exploration and production in deep waters, the marine and offshore industry is becoming heavily reliant on Dynamic Positioning (DP) systems.

This study aims to demonstrate how a slight defect (that are often ignored in offshore DP operations) in ordinary and secondary components of a vessel's system can cause a significant failure in a Dynamic Positioning system and consequently lead to a catastrophe.

The DP system, including various sub-systems, DP classes and applications, are introduced and discussed. In addition, the concept and procedure of risk management and its major steps (risk analysis, risk evaluation and risk assessment) are explained. A method is specified for each of these risk management steps and the methods' pros and cons are mentioned.

In the DP system, the diesel engine is the most significant machinery and prime mover for generating electrical power. The risk analysis of diesel engine failure was carried out by Fault Tree Analysis to determine the possible scenarios of failure and their root causes. For doing the analysis, DP class 1, which has the least redundancy, was considered. Since there is no backup system in DP class 1, the failure of the diesel engine leads to the loss of positioning system. It should be noted that the emergency generator (the reserve engine) would not have sufficient power to manage the DP system on a normal vessel should the main generator stop.

Furthermore, with regard to people, environment, asset, and reputation, the risk of diesel engine failure was evaluated using the risk matrix method. The analysis concluded that the risk was categorized as a high level of risk, which is unacceptable before risk mitigation. The risk associated with the use of diesel engines is thereafter assessed by Bow-Tie Analysis to provide a visual understanding of risk and helpful foundation for decision-making. Subsequently, several primary and secondary preventative barriers are specified to mitigate the occurrence of initiating events which may lead to diesel engine failure and consequently, to DP system failure.

In conclusion, since there are many interactions between the diesel engine and other systems/machinery, every possibility and cause of diesel engine failure must be taken into account. One should not underestimate and ignore any simple fault that may seem irrelevant to the diesel engine failure. The engineers and crews must not only be familiar with their own job tasks, but should also be informed about others' duties. This allows engineers to realize the importance of their assigned machinery, and its influence on the other equipment and vice versa. Finally, the managers or high-ranked personnel who can see the big picture (from slight component failure to the catastrophe), should share their perceptions and educate the staff by conducting training courses and directorial meetings.

ACKNOWLEDGMENT

I would never have been able to finish my dissertation without the guidance of my noble supervisor, and support from my sympathetic wife and compassionate family.

I would like to express my heartfelt and deepest gratitude to my supervisor, Prof. Ove Tobias Gudmestad at the University of Stavanger, Norway, for his immense knowledge, excellent guidance, caring, patience and providing me with an excellent atmosphere for studying and doing research. I attribute the level of my Master's degree to his encouragement and effort and without him this thesis, too, would not have been completed or written. One simply could not wish for a better or friendlier supervisor.

I offer my wholehearted thankfulness to my adorable wife, Shiva Etehadieh. She was always there encouraging me and stood by me through the good times and tough. Her support, encouragement, and endless love made this thesis and Master's degree a success.

I am also grateful to the staff of the University of Stavanger, my colleagues and friends, and one and all, who directly or indirectly, have supported and encouraged me.

My gratitude also goes to the Norwegian government, for the opportunity of free education with higher quality.

Last but not the least, my sincerest appreciation also goes to my supportive family: my parents, Ahmad Rasoulzadeh Khorasani and Fatemeh Javanshiri, and my younger sister, Vida Rasoulzadeh Khorasani. They were always supporting me by their unsparing help and encouraging me unceasingly with their best wishes.

Vahid Rasoulzadeh Khorasani

Stavanger, Norway

June 2015

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ABS	American Bureau of Shipping
AC	Alternating Current
ALARP	As Low As Reasonably Practicable
ARPA	Automatic Radar Plotting Aid
BTA	Bow-Tie Analysis
BV	Bureau Veritas
CPP	Control Pitch Propeller
DARPS	Differential Absolute and Relative Positioning System
DC	Direct Current
DGPS	Differential Global Positioning System
DNV	Det Norske Veritas
DP	Dynamic Positioning
DR	Dead Rocking
EMF	Electro Magnetic Force
FPSO	Floating Production, Storage and Offloading
FSO	Floating, Storage and Offloading
FTA	Fault Tree Analysis
GL	Germanischer Lloyd
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning System
HAZID	Hazard Identification
HLV	Heavy Lift Vessel
HPR	Hydro-acoustics Positioning System
IMO	International Maritime Organization
INMARSAT	International Maritime Satellite Organization
IR	Insulation Resistance
LAN	Local Area Network
LR	Lloyd's Register
MODU	Mobile Offshore Drilling Unit
MRU	Motion Reference Unit
NAVTEX	Navigational Telex
NK	Nippon Kaiji Kyokai

OLT	Offshore Loading Terminal
OSV	Offshore Supply Vessel
PID	Proportional Integral Derivative
PSV	Platform Supply Vessel
RADAR	Radio Detection And Ranging
RPM	Revolutions per Minute
UHF	Ultra High Frequency
UPS	Uninterruptible Power Supply
VRS	Vertical Reference Sensors

CHAPTER 1 INTRODUCTION

1.1 Background

Due to 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. The challenging environment of the 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. 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.

Due to the critical nature of offshore oil and gas operations and potential for catastrophe, risk management activities have become important for operations. Thus, to ensure safe and secure operations, risk management principals and their methods of implementation are reviewed and reconsidered. The following issues have become the major industry concerns: identifying the hazards, determining the events that may cause the occurrence of hazards, distinguishing the consequences in the case of hazards occurrence, and assigning the risk reducing measures.

Considering the issues mentioned above, risk management of deep-water operations using the DP system technology have become essential in the offshore oil and gas industry.

On one hand, a DP system is comprised of several sub-systems and machinery that must work properly for the DP system to be operational and efficient. Thus, the reliability of the sub-systems and components have been taken into account. For this reason, the technical aspects of different machinery and components were considered when determining failure modes and effects.

On the other hand, a risk management procedure includes different stages that should be carried out to reduce the risk of operations and ensure safety. Therefore, various methods could be utilized to identify the hazards, determine initiating events and consequences, and lastly, to assign and propose the risk reducing measures.

1.2 Objective

The main goal of this thesis work is to demonstrate the significance of the slight faults in the ordinary components that are often ignored in the offshore DP operations and which may result in a disaster.

This thesis is intended to identify the most significant sub-system and machinery in a DP system. Thus, specifying the main components and their possibilities of failure is also a target of this thesis. This will be done by a Fault Tree Analysis. Accordingly, a DP system will be considered from a technical point of view to analyze the different sub-systems and components. This aims to determine the various failure modes and effects of those components, and analysis will reveal the root causes of the system failure. In addition, this study shall evaluate and assess the risk of diesel engine failure by aid of risk matrix and Bow-Tie analysis, respectively.

Finally, the study will identify several barriers for preventing initiating events to escalate. This provides a helpful foundation for decision-making.

1.3 Scope and Limitations of Work

1.3.1 Scope

The thesis will introduce the DP system with consideration to its history, different sub-systems, components, and their operational aspects. The varying DP classes, the corresponding requirements, and redundancy in different classification societies also will be covered. Additionally, the various applications of DP systems will be mentioned.

This study will also bring forward the concept and main steps of risk management. Risk analysis, risk evaluation, and risk assessment will be introduced as the main activities of risk management. A method will be specified for each of these risk management steps. The principals and methods' pros and cons will be discussed.

The thesis will cover risk analysis for failure of a diesel engine which is specified as the most significant machinery in a DP system. A Fault Tree Analysis will be the tool for performing the qualitative risk analysis of diesel engine failure. Different diesel engine-related equipment and components will be studied to determine their failure modes and effects. The interactions between the diesel engine and auxiliary systems also will be considered.

The risk of diesel engine failure will be evaluated by the aid of a risk matrix as the means of risk evaluation. Considering people, the environment, asset, and reputation, the level of the risk will be characterized and the risk level will be noted as high, medium or low. To eliminate or mitigate the risk, there are different requirements that shall be fulfilled based on the risk level.

Finally, risk assessment of the diesel engine failure will be carried out by Bow-Tie Analysis. This analysis will show the entire process of the risk assessment and provide a visual risk understanding by a single figure. Meanwhile, several risk reducing measures will be assigned as preventive barriers to reduce the probability that initiating events develop into a top event (diesel engine failure). The required barriers will be specified based on the level of the risk which is determined beforehand.

This thesis aims to contribute to the body of knowledge by demonstrating the applied assessment of the most significant machinery in a Dynamic Positioning System.

1.3.2 Limitations

The technical analysis (in the risk analysis section), the practical appraisal (in the risk evaluation chapter), and the technical barriers (in the risk assessment chapter), are subjective and arise from experience and mechanical comprehension of the writer. Therefore, one might consider the distinct analysis, evaluation, and assessment in accordance with his experience and insight.

The Fault Tree Analysis of the diesel engine will be done in-depth, and the majority of the components will be studied to determine the failure causes. Collecting reliable data about the failure rate of entire diesel engine’s components was not feasible, however. Thus, a qualitative risk analysis method was chosen rather than a quantitative to avoid misguided conclusions and unreliable results.

CHAPTER 2 OVERVIEW OF DYNAMIC POSITIONING

2.1 Introduction

Undoubtedly, the high demand for hydrocarbons has leaded the humankind to increase exploration and production of oil and gas. Consequently, they became interested in offshore locations and marine environment. Further, the people became more eager even to deeper waters and harsher environment that requires special facilities for exploration and production. This was the initial drivers for finding new solutions to maintain the position of offshore floating structures. The *Dynamic Positioning System* has been introduced as the new solution.

Dynamic positioning can be defined as "*Automatic control of vessel's position and heading by the use of thrusters with respect to one or more position references*" (IMCA, 2007).

It was in early 1960s that the idea for mounting thrusters to the vessel for position keeping proposed by "Willard Bascom". The vessel was called "CUSS 1" (shown in Figure 2.1), which was an exploration floating drill ship. They wanted to see if she could hold her position enough to do drilling without an anchor. In the meantime, the "Bill Bates" who was the marine division manager of Shell and had worked in the CUSS 1 project, convinced the Shell to build a small drilling ship with position maintaining the facility. The vessel named "Eureka" (shown in Figure 2.2).

The "CUSS 1" had modified with four direct engine steerable thrusters mounted at each her four corners. The direction and engine speed had controlled manually in addition to measuring the heading that had been controlled by compass. The test of CUSS 1 was done in Mach 1961 that 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 pre-assigned buoy ring (Dynamic Positioning Committee).

The "Eureka" constructing ended up with two steerable thrusters that had 200 horsepowers and was driven electrically. In this case, the speed and direction of thrusters had been adjusted manually. 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 operation (Dynamic Positioning Committee).

Figure 2.1: The “CUSS 1” Vessel (Dynamic Positioning Committee)

Figure 2.2: The “Eureka” Vessel (Dynamic Positioning Committee)

The popularity of DP system was dramatically increased after good establishment in 1970 as such the number of DP vessels reach 65 in 1980 and 150 in 1985. Nowadays, nobody knows the exact number of DP vessels in the world, however, the professionals guess over 2000 DP vessels worldwide are in operation (Dynamic Positioning Committee).

2.2 DP System Principals

Since a vessel in marine and the offshore environment is exposed to different external forces namely wave, current and the wind, she needs to have a system to keep her correct position for doing her operation properly. 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 such the surge and sway are related to the vessel position, and yaw is associated with the vessel heading.

For both position and heading, a set point is predetermined regarding the vessel operation. Also, 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 DP system. In Figure 2.3, the environmental forces and relevant vessel motions can be seen.

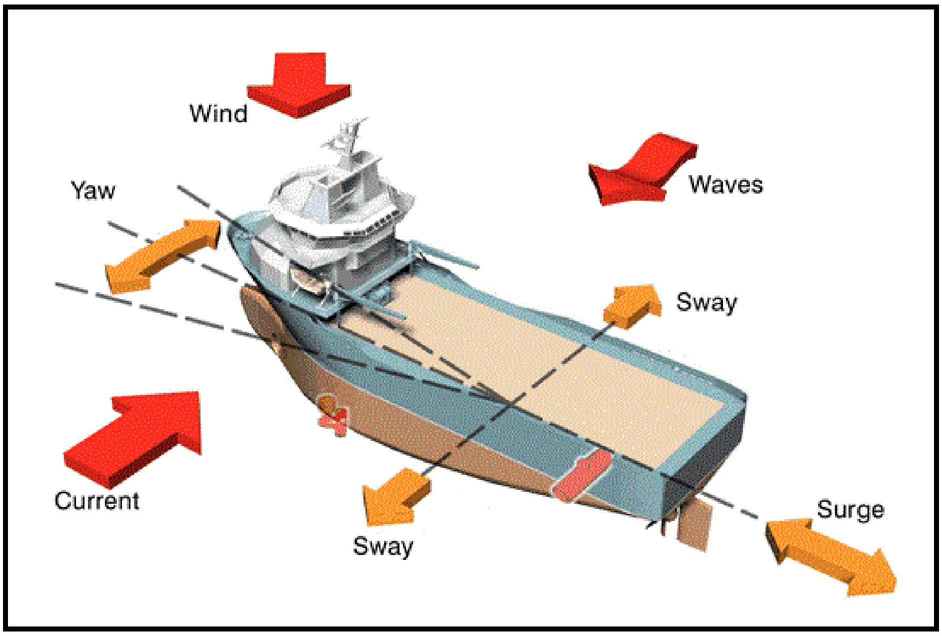


Figure 2.3: Basic external forces and relevant vessels motions ("Dynamic positioning-basic principles")

A dynamic positioning system includes all equipment and components that support the automatic maintaining and correcting vessel position. For position correction by DP system automatically, 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 to adjust the position and heading respect to the new data that are given by DP Operator (DPO). The DPO can also tune the speed of vessel during correction action.

Depending on the type of vessel and desired operation, adjustment and maintaining the vessel position and her heading can be different. For instance, some vessels like MODU or FPSO must be able to weathervane and be in a specified area. Others like pipe laying vessels and dredgers shall follow a path that is predetermined. Furthermore, there are some vessels such as ROV or diver support vessels should track a moving object. In this case, instead of pre-assigned or fixed location, the moving object is the reference for vessel positioning.

In terms of DP principals, there are two types of Dynamic Positioning systems in the market, *Proportional Integral Derivative (PID)* regulation based and *Model control* based.

2.2.1 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).

2.2.2 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's sensors continuously read and record the 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 deteriorated. It should be noted, the duration of position keeping in case of failure of the reference system is short (5-15 minutes) depending on environmental condition and external forces. However, the DR system helps DPO for taking the right action and for not being a rush to change the system from automatic to manual (IMCA, 2007).

2.3 DP System Components

As mentioned in the last part, a DP system shall automatically control the vessel position and heading by an active trust. This is not only about the maintaining the correct position, but also is a matter of precise maneuvering by checking and tracking the data to adjust the position and heading according to new inputs.

To get the proper insight into a DP system and its operational and failure modes, it is needed to know the main components and their interrelations. Basically, the best method is to visualize a DP system based on their main elements.

Principally, in addition to DP operator, a DP system encompasses of seven major parts. The DP operator is the responsible person for giving data, checking, tracking and monitoring of the DP operation. The following are the major sub-systems of a DP system which are also illustrated in Figure 2.4.

- Position reference system
- Environment reference system
- Heading reference system
- Power generation system
- Propulsion system
- Control system
- Computers

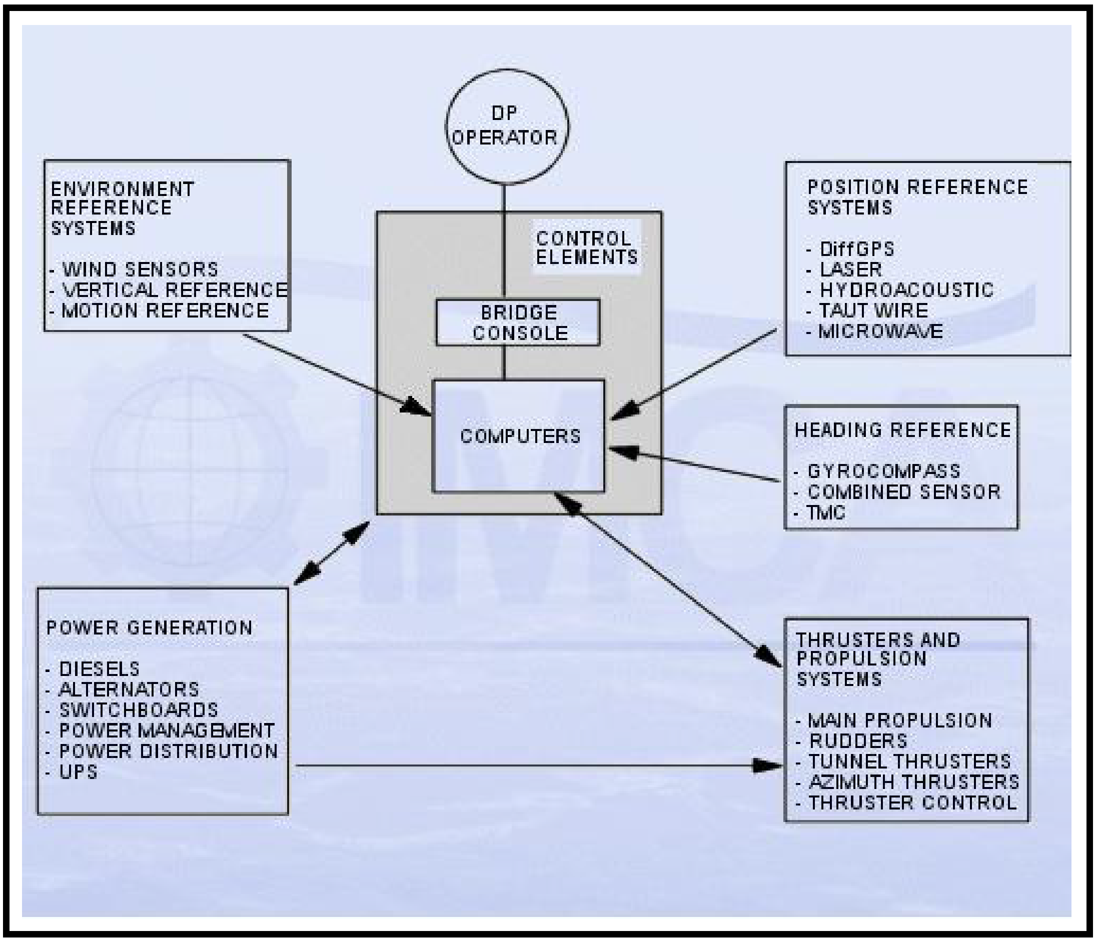


Figure 2.4: Schematic Diagram of a DP system Components (IMCA, 2007)

2.3.1 Position Reference Systems

This system acts as a reference for measuring the current position of vessel and amount of position deviation. There are different types of position reference system with different pros and cons. Types and number of position references which are used vessel onboard, very depend on risks and criticality of the vessel operation, the desired redundancy of operation, and availability and suitability of the position reference system. Some of the most common position reference systems are mentioned in following and can be seen in Figure 2.5.

- Differential Global Positioning System (DGPS)
- Hydro-acoustics Positioning System (HPR)
- Taut Wires
- Line-of-sight laser
- Microwave System

From one hand, the major concern of position reference systems is their reliability and, on the other hand, each type of system has varying capability and weakness. Therefore, a combination of different position reference systems are frequently employed in the marine and offshore industry to provide a more reliable system (DNV, 2012).

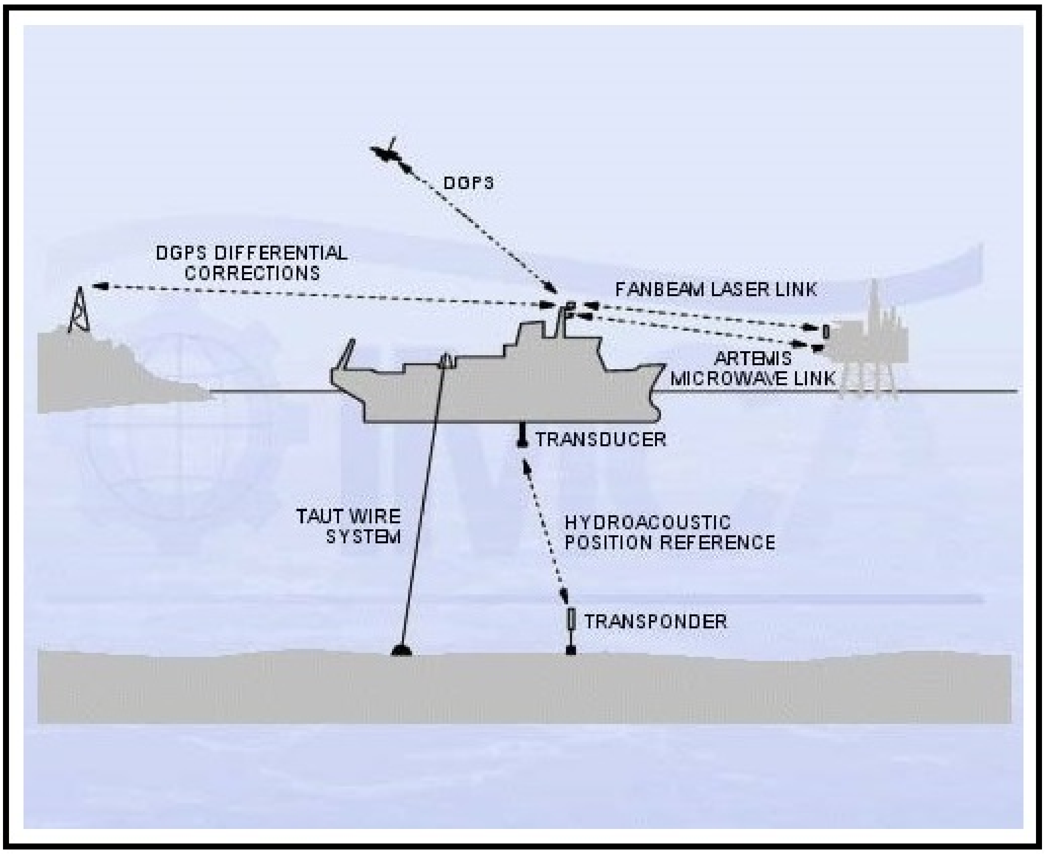


Figure 2.5: Position reference system (IMCA, 2007)

2.3.2 Environment Reference Systems

There are three main environmental forces which are applied to a vessel. They are the wind, wave and current that subject a vessel to change her position or/and heading.

The current measurements normally cannot be done by current meters because of high expenses, especially when the high reliability is needed. Fortunately, since the changing rate of the current force is slow the integral form of the meter is sufficient. Therefore, a facility which is called "*quick current update*" or "fast learn" is provided on the DP vessels. This equipment allows the DP system to react swiftly by reducing the time constant of an integral part in case of high change of position and heading (Bray, 2003; IMCA, 2007).

The waves are not measured purely. It is considered in the DP system as sea or current force. Of course, there is no any compensation by DP system for the applied waves, however, the amount of pitch and roll motions must be measured by the sensors called *vertical reference sensors (VRS)* or *motion reference unit (MRU)*. This is because of a modification that should be applied to the input of position reference sensors for determining the correct offset from the vessel center of gravity (Bray, 2003; IMCA, 2007).

Each wind sensor comprises of a simple transmitting anemometer that is usually in the rotating-cup type. All the DP systems have wind sensors. These are aimed for calculating the forces which are induced by subjected wind to the vessel's hull and structures. The speed of the wind can have the significant effect as well as its direction to change the position and/or heading of the vessel. Particularly, the wind direction is so important for some vessels like shuttle tankers and/or Floating, Storage and Offloading (FPSOs) that must have the best heading for maximizing the uptime. This is why the wind sensors are very considerable (Bray, 2003; IMCA, 2007).

2.3.3 Heading Reference Systems

Information about vessel heading is provided by gyrocompass that reads and transmits those data to the DP system. Depending on desired redundancy, numbers of gyros can be different from one to three.

2.3.4 Power Generation Systems

It is not weird if we say the power generation system of a DP vessel is the most vital onboard system. Generated power is supplied to the electrically driven thrusters, control system, and reference systems. Also, electrical power shall be supplied to all axillary machinery like pumps and monitoring system that are necessary for running the main propulsion system. Shipboard electrical power is produced in 3 phase AC. This is because of AC gives more power than DC in a same size. Furthermore, in the case of failure of one phase, the other 2 phase can still hold the circuit to produce power, this why, the 3 phase power is desirable because

Undoubtedly, the most power consumers on DP vessels are the propulsion components that are the front-line of a DP system. Propulsion means can be directly driven either by a diesel engine and normally act as vessel main propulsion system or they can be supplied by an electrical power that comes from diesel generators. In the latter case, they are generally bow or stern thrusters that are used for vessel maneuvering and positioning.

Since the environmental situation is prone to change rapidly, a DP system must capable to react accordingly. Therefore, the power system not only should be flexible and strength enough to provide the required electrical power for the DP system simultaneously but also, it should prevent the unnecessary power supply for minimizing the fuel consumption.

Figure 2.6 illustrates a typical offshore vessel power system. A power generation system includes *Diesel Engine, Alternator, Switchboard, Power Distribution, and UPS (emergency power supply).*

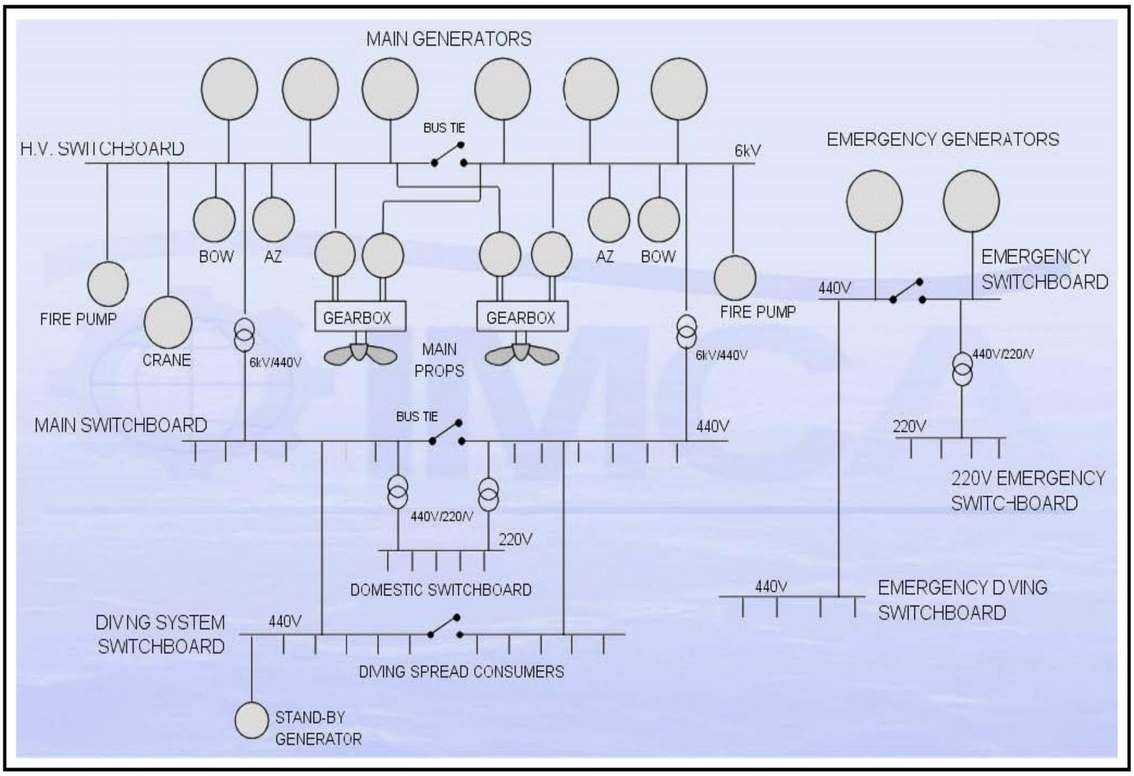


Figure 2.6: Power distribution system of a typical offshore vessel (IMCA, 2007)

2.3.4.1 Diesel Engine

A comprehensive study and FTA for a diesel engine will be carried out in the next chapter since the diesel engine failure in a DP system is the main focus of this thesis. Other main sub-systems of power generation are described briefly in this part as followings.

2.3.4.2 Alternator

The electrical power is generated by an alternator that is coupled to a diesel engine by a shaft. The combination of diesel engine and the alternator is called *Diesel-Generator* as can be seen in Figure 2.7. The alternators which are used in the majority of DP vessels are 3 phase and AC with the brushless self-exciting system. The alternators are designed based on standard voltage which is usually 440 V for most of the marine applications. According to the marine rules and regulations, voltages which are less than 1000 V are considered as low voltage (LV) while other voltages above that are considered as high voltage (HV).

An alternator is capable to generate AC electrical power at a specified frequency. This is also called synchronous generator because it produces electrical power at the same time and once it starts running. Electricity is generated in the alternator by electromagnetic induction. This works based on a principal that when a magnetic field around a conductor is interrupted or varying, an electrical current would be induced in the conductor. To generate electricity in the coil of the conductor, either the coil should rotate with respect to magnetic field or a magnetic field should rotate with respect to the coil. In the case of alternator, the latter approach is used.

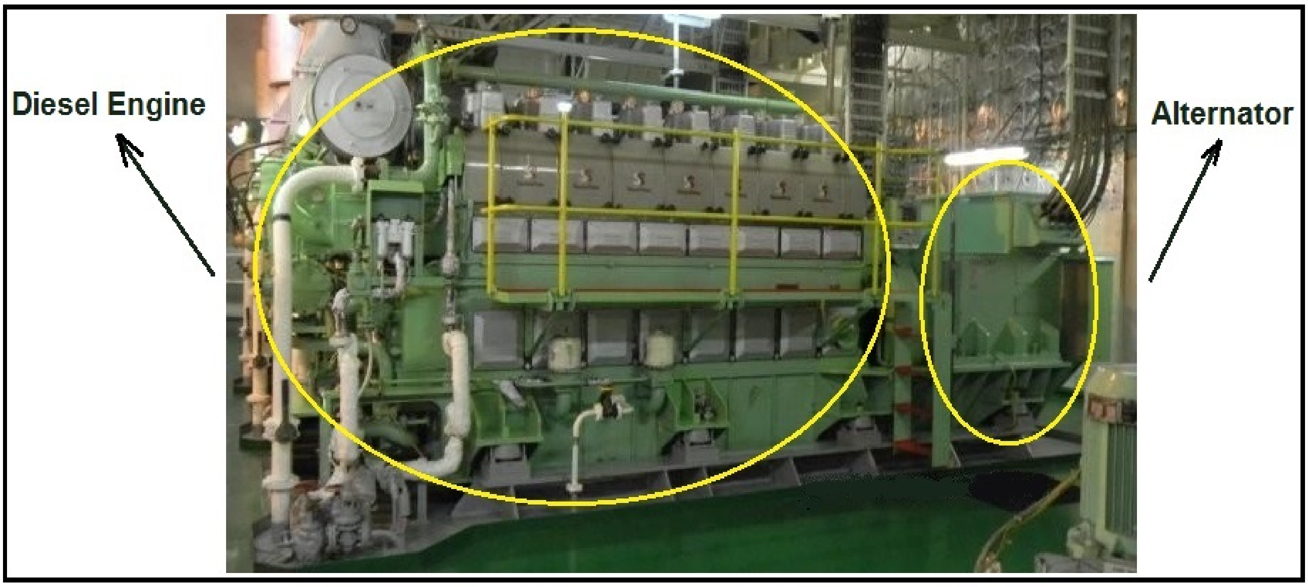


Figure 2.7: A typical Marine Diesel Generator (A Diesel Engine and an Alternator) (Anish, 2014)

An alternator comprises two main parts called *Stator* and *Rotor*. The stator is also called *Armature*, and it is a stationary part which is a collection of conductors in a coil with an iron core. A stator core is used to enhance the magnetic flux transfer. The rotor is a moving part which rotates by a diesel engine as the prime mover. The rotor produces rotating magnetic flux while rotating inside the stator. This rotating magnetic flux associated with the rotor, is cut across the stator, and induces electricity or EMF (Electro Magnetic Force) in the armature coils. A schematic of alternator components arrangement is shown in Figure 2.8. For producing 3-phase AC electricity, three coils that are in 120-degree phase difference with each other, are put in the stator winding. Generally, one end of these three coils are connected by *Star* configuration while 3-phase AC electricity is drawn from the other ends.

It should be noted, the magnetic field in a rotor is generated by an activity which is called *Excitation*. There are different ways of excitation however, the usual method is the use of electrical DC power source to energize the rotor and make it a magnet. Direct current is supplied to the rotor via a pair of *Slip Rings*. It can be supplied either from an external source or from a small DC generator that is fitted on the same alternator shaft (prime mover). An alternator with attached DC generator for excitation is called self-exciting alternator.

One should not that, the frequency of produced electricity has a direct relation to the engine speed. Thus, RPM of the diesel engine that is mentioned in former sections is really important to maintain the specified frequency of electricity.

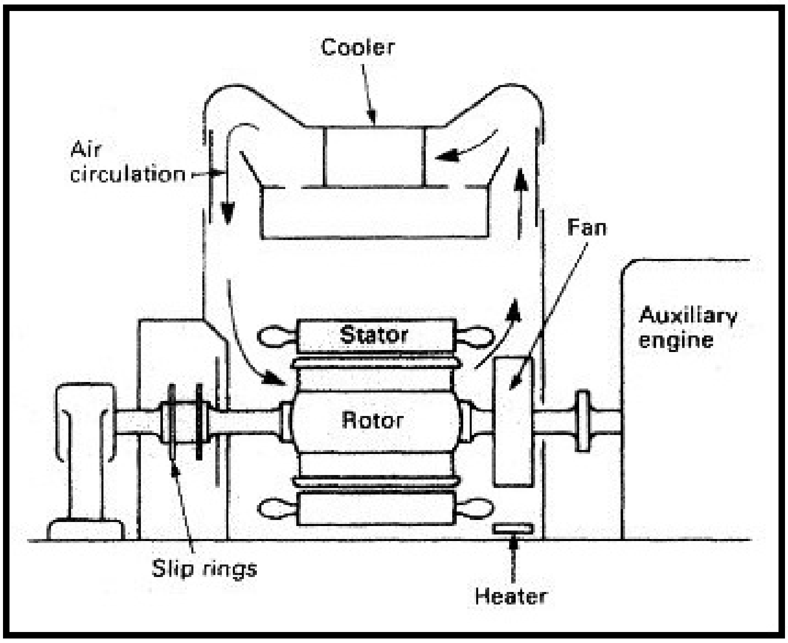


Figure 2.8: Schematic of an Alternator Construction with its Main Components ("Ships electrical plant and distribution system for the A.C. generators", 2010)

2.3.4.3 UPS (Uninterruptible Power Supply)

One of the significant issues related to the power system is capability to supply electrical power at all times even in the case of failure of the prime mover (diesel engine). In other words, a backup power supply system is required to be onboard.

The *Uninterruptible Power Supply (UPS)* is provided on all DP vessels for supplying the electrical power to the lighting, displays, computers, reference systems, control consul, and alarms. This electrical power can be provided by batteries which are not affected by vessel *Alternating Current (AC)* power fluctuations or other short-term interruptions. The power supplying by batteries must be minimum for 30 minutes (DNV, 2012).

Also, according to regulations and standard, an emergency diesel generator must be onboard. In the case of a blackout, the emergency diesel generator shall start and be loaded automatically.

Note: Neither the emergency generator nor batteries (UPS) can provide sufficient power for running the thrusters. This is due to the high power consumption of thrusters. Therefore, the number of main diesel generators as the principal means of power generation has to be increased. This is due to having some generator as standby (backup) to supply the power to the thrusters in the case of emergency.

2.3.5 Propulsion Systems

In the basis of definition of the propulsion system, there must be a means to create a force for an object movement. In marine subjects, the main propulsion facility is diesel engine(s) which drives propeller(s) to create thrust force and move a vessel. However, a main propulsion system can only enable a ship to move toward ahead or astern direction. This is a weakness of vessels especially to do critical maneuvering during offshore operations such as drilling, lifting, and offloading operation. This is why; vessels which are specified for those mentioned operations are required to have extra means of movement. These extra propulsion means are called thrusters that provide side thrust force. They give a high capacity of maneuvering to a vessel and make her able to steer and turn to maintain her heading at the same position.

A DP vessel gets her propulsion that is provided by thrusters. In general, thrusters are categorized into three types as *Main Propeller*, *Tunnel Thrusters*, and *Azimuth Thrusters*. The configuration of the propeller(s) and thrusters is conditional on the type of vessel. It means that the number of thrusters and their installation location depend on the vessel geometry and her applications. Hence, the general placing of thrusters in some offshore vessels are shown in Figure 2.9. For the shipshape vessels, the thruster's positions are at bow and stern while for the semi-submersible platforms the thrusters are usually positioned at each corner.

2.3.5.1 Main Propeller

Any conventional marine vessel is equipped with a main propeller(s) as the propulsion means, while this propeller(s) is a part of DP system in the DP vessels. The main propellers can be provided in a single or twin screw and are accompanied by a rudder and steering system as shown in Figure 2.10. Maine propellers can be designed as *Control Pitch Propeller (CPP)* or fixed propeller respect to the engine type and the vessel applications. A CPP allows the vessel to change the speed and direction in addition to optimizing the fuel consumption by changing the angle of the propeller. Furthermore, the propeller speed can vary either by changing RPM of reversible and variable diesel engine, or by utilizing a reduction gear which is coupled to a nonreversible engine with the constant speed.

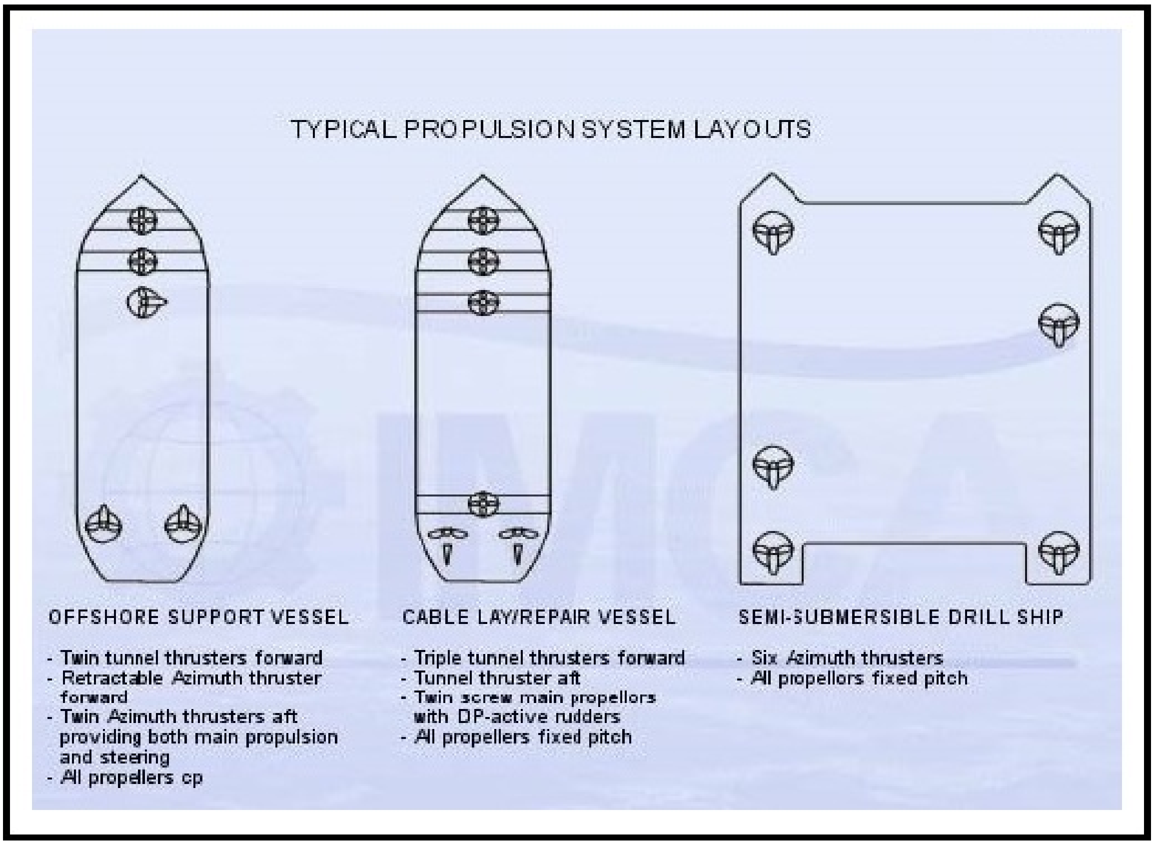


Figure 2.9: A typical thruster's arrangement layout for offshore vessels (IMCA, 2007)

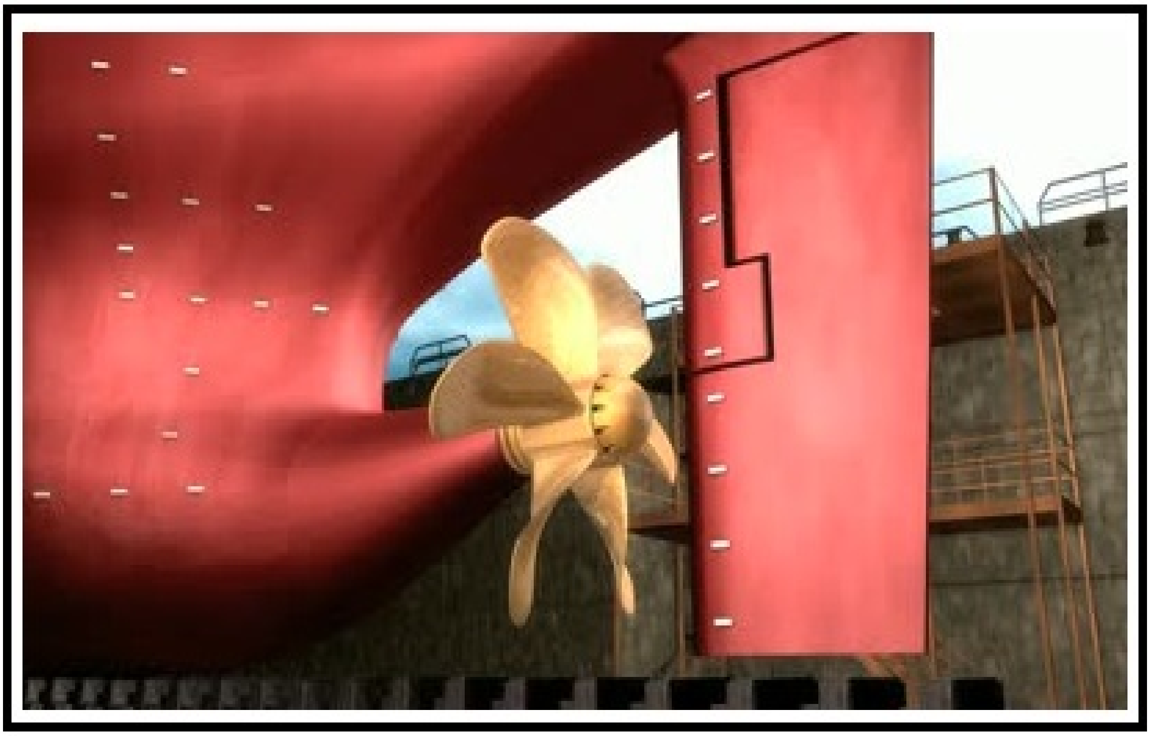


Figure 2.10: View of main propeller of a vessel accompanied with rudder ("Ship propeller")

2.3.5.2 Tunnel Thrusters

Normally, the tunnel thrusters are installed at the bow and stern (forward and aft position) of the vessels for slow speed maneuvering, docking, station keeping, and emergency steering. The thruster bounded in a tunnel as shown in Figure 2.11. This because the water flow in the tunnel has the higher velocity than the outside water thus this causes a pressure gradient that increases the thrust force. Furthermore, bounding the thruster in a tunnel helps to reduce the noise of propeller. Nevertheless, the overall effective thrust force in this type depends on vessel speed, length of the tunnel and the immersion depth of the propeller.

In tunnel type thrusters, the influencing factors should be in optimized condition to get the higher thrust force. For example, a short length of the tunnel cannot be efficient due to making turbulence while the long tunnel length increases the amountof friction loss. Position of the propeller should not be so near to the surface otherwise, due to air resistance and cavitation; the thruster efficiency will be dropped. The same rule is applied to vessel speed, meaning that if the vessel speed is high, the thruster efficiency will be declined due to higher friction (Deter, 1997).

2.3.5.3 Azimuth Thrusters

Since this type of thruster can provide thrust force in any direction-360 degree- it is called azimuth that can be seen in Figure 2.12. Usually, the azimuth thrusters are used for desired fine maneuvering and station keeping. However, depending on type of vessel also in some cases, it can be considered as a main propulsion system in lieu of conventional propellers.

They can be positioned in a different configuration, but some issues shall be considered such as space occupying, vulnerability for grounding, cost, and most importantly efficiency. For instance, the thruster can be installed underneath the vessel hull but this arrangement is risky for grounding, and the precaution considerations must be taken into account. Further, if the thruster is positioned near the surface, it could be safer but with lower efficiency. The solution could be using the retractable thruster. This thruster can be retracted in both vertical and horizontal direction in the hull. This allows installation in the best feasible position for best maximum efficiency plus minimizing the risk of grounding.

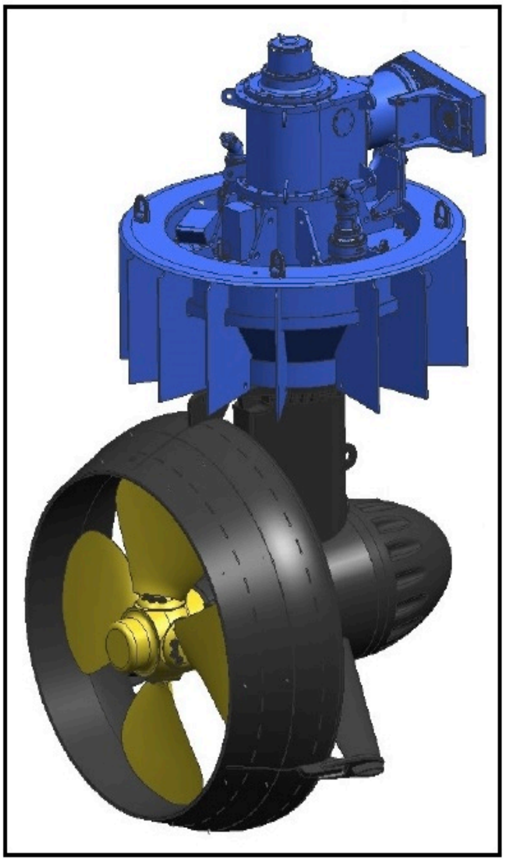


Figure 2.11: Tunnel Thruster ("Tunnel type thrusters for ships")

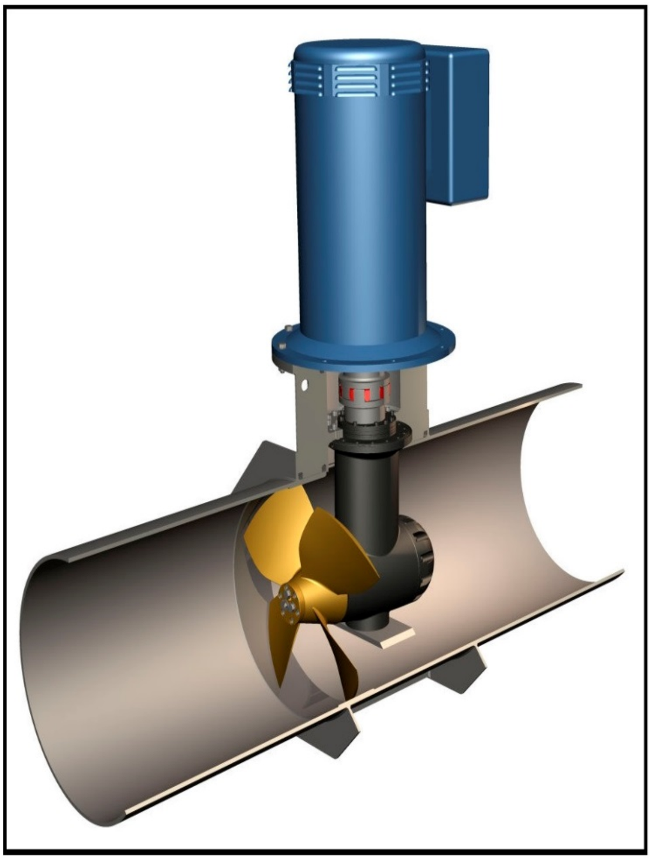


Figure 2.12: A view of Azimuth thruster ("Azimuth thrusters")

Some other azimuth thrusters are removable that can be valuable for the vessels which cannot use the retractable type either due to lack of enough space or in order to high cost. The vessels that are spending most of their time in deep waters preferred to use this thruster type. They can easily remove it once going to the shallow water. The azimuth thrusters can act at both ahead and astern direction and it is a remarkable advantage. Although, the reverse (astern) direction is not efficient more than 60 percent, however, for changing the heading by 180 degrees still the 60 percent astern efficiency is beneficial for precise maneuvering and station keeping. This is because the speed of backward sailing is higher than the rotation of vessel in the ahead direction (Bray, 2003; Deter, 1997).

It should be noted, in the case of tunnel and azimuth thruster, the main driver means is the electrical motor. For providing a variable speed, a fixed-pitch propeller needs a DC type of electrical motor.

A considerable concern related to a propulsion system is the thruster's effects on other thrusters, particularly when they are located close to each other. One must ensure about disturbance to a thruster. It may be caused by the stream of other thrusters or main propeller otherwise; the thrusters may get over-speed or low efficiency.

2.3.6 Control Consul

As it can be seen in Figure 2.13, the control consul is a collection of all facilities and instruments which enable a DPO for monitoring and controlling the DP system. A control unit includes screens, switches, bottoms, indicators, alarms, a panel of position and heading reference system, a panel of the communication system, and thruster control panel. Depending on the type of vessel, the position of the control consul may be varying. It can be at the forward bridge or the aft bridge or even at the bow control station like shuttle tankers. Basically, the control consul shall not be in a location where does not have an outside view.

Figure 2.13: A view of forward bridge DP control consul (Trewern, 2013)

2.3.7 Computers

The processing unit and software to do analysis and the calculation, is known as DP computer. Number of computers, strength of the software and operation manners directly depend on required redundancy level of DP system. For example, the computers can be installed in single, double or triple layout to make different redundancy. The computers are connected to each other and other instrument and facilities by either intranet or Local *Area Network (LAN)*. This provides the possibility of incorporation of the vessel control system with the DP system.

Figure 2.14 demonstrates the main components of a DP system and shows how they are interconnected and related to each other in a model based DP system. As mentioned earlier in the DP systems principals, the best and reliable method for control and processing is the model based DP system. This is done by the aid of *Kalman Filtering* and digital data transmission which are able to predict the proper required thrust force to prevent position/heading deviations. The following figure shows that where are the orders coming from and how the feedback is taken to ensure the order implemented.

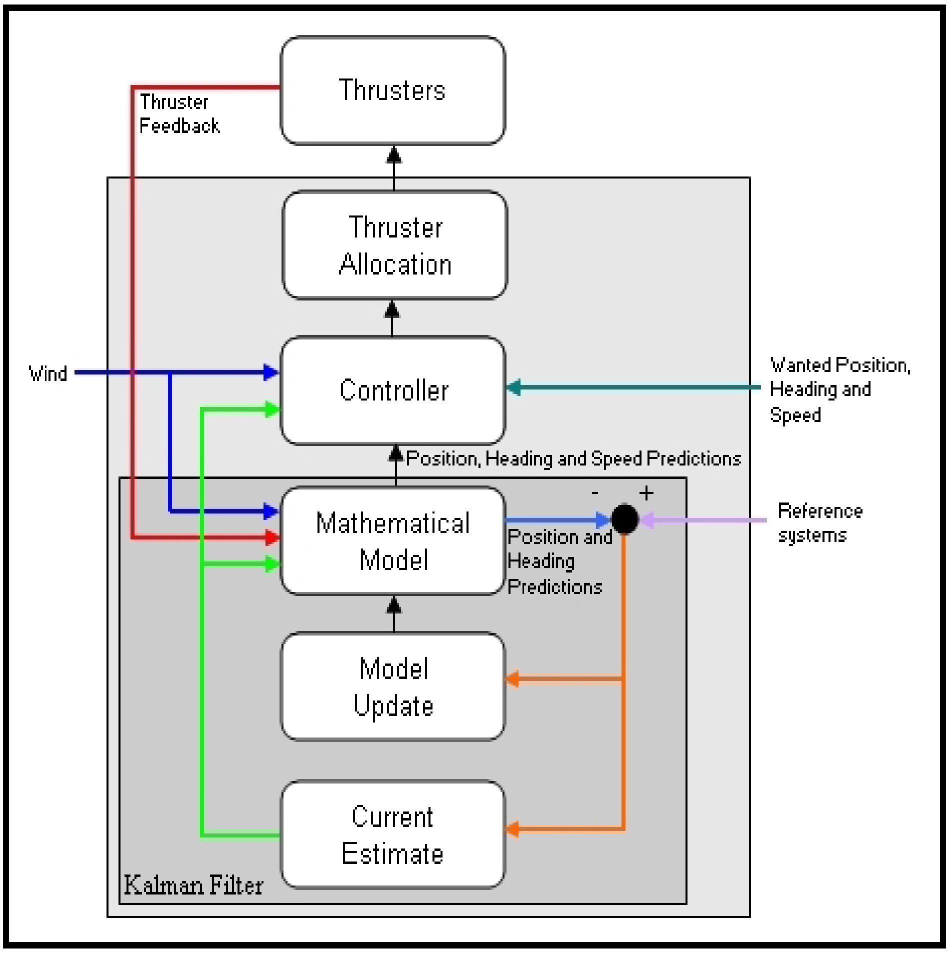


Figure 2.14: Schematic of DP system components and control ("Dynamic Positioning")

2.4 DP Classes and Redundancy

The *International Maritime Organization (IMO)* MSC/Circ.645 publication is the guideline for vessels with dynamic positioning system. According to the IMO regullations, all the classification societies have made some rules for the DP systems in terms of three main classes. The classifications of DP system is provided based on their risk resistance and redundancy of each class. Table 2.1 illustrates different DP classes notations in some well-known classification societies based on the IMO requirements.

Redundancy is defined as the ability to withstand. In a DP system, the redundancy means a single component failure or loss of equipment which is in operation, shall not cause total loss of the DP system that leads to losing position and/or heading. In a DP system, the single failure may happen for following components (IMO, 2013):

- Thruster
- Generator
- Position reference system
- Wind sensor
- Computer (Control system)
- Switchboards

As per the redundancy definition, the three worldwide DP classes can be described as followings (IMO, 2013):

DP Class 1: This class is not redundant, meaning that a single failure of any components can cause the total loss of DP system.

DP Class 2: The class 2 DP system is redundant against a single failure of any equipment which is active (in-line) like thrusters, diesel-generator, reference system and remote control components, etc. However, still the full failure of DP system may occur since this class is not redundant against malfunction of static parts such as pipes, cables, and manual control components.

DP Class 3: In this class, the DP system is redundant for single failure of in-line equipment. Also its redundancy incudes the fire burning and flooding of a compartment.

Note that, there is another DP class, which is not mentioned in some classification societies and even in the IMO guidelines, meaning that there is no consideration for this class in relevant DP standards. This class is pointed by * in the following table and can be named as the DP class 0. In fact, the DP class 0 does not have an automatic position control, only the heading control is done automatically.

Table 2.1: Different DP classes in different Classification Societies (DNV, 2014)

Classification Societies	**DP Class**			
IMO	*	**Class 1**	**Class 2**	**Class 3**
DNV-GL	DYNPOS-AUTS	DYNPOS-AUT & DPS1	DYNPOS-AUTR & DPS2	DYNPOS-AUTRO & DPS3
LR	DP(CM)	DP(AM)	DP(AA)	DP(AAA)
ABS	DPS-0	DPS-1	DPS-2	DPS-3
BV	*	DYNAPOS AM/AT	DYNAPOS AM/AT R	DYNAPOS AM/AT RS
NK	*	DPS A	DPS B	DPS C

Figure 2.15 illustrates the layout of DP system class 2 as an example for showing the redundancy. As it can be seen, two set of control consul, two gyrocompasses, two wind sensors, two computers, two vertical sensors and three position references are considered. In addition, two thrusters for bow and stern also two propellers for port and starboard sides are provided. The figure clearly illustrates that in the case of failure in any component, there will be a same component as a backup that is independent and can be substituted for the prevention of total DP failure.

The IMO did not mention that which kind of marine operation needs what class of DP systems to guide the DP ship owners and their clients. Therefore, the Norwegian Maritime Authority became the pioneer and released the guidelines to explain which DP class should be utilized for different operations. Various marine activities are categorized with regard to their criticality and risks. The followings are the four operation classes that were introduced by Norwegian Maritime Authority: ("Norwegian Maritime Authority")

- Class 0: The operation which loss of DP system does not lead to risks for the human lives or any human injuries.
- Class 1: The operation which the DP system failure may have small consequences for human injuries and environmental pollution.
- Class 2: The operation which loss of position keeping system may lead to human injuries, environmental pollution, and substantial economic damages.
- Class 3: The operation which failure of position keeping system may bring fatalities, severe pollution or major financial loss.

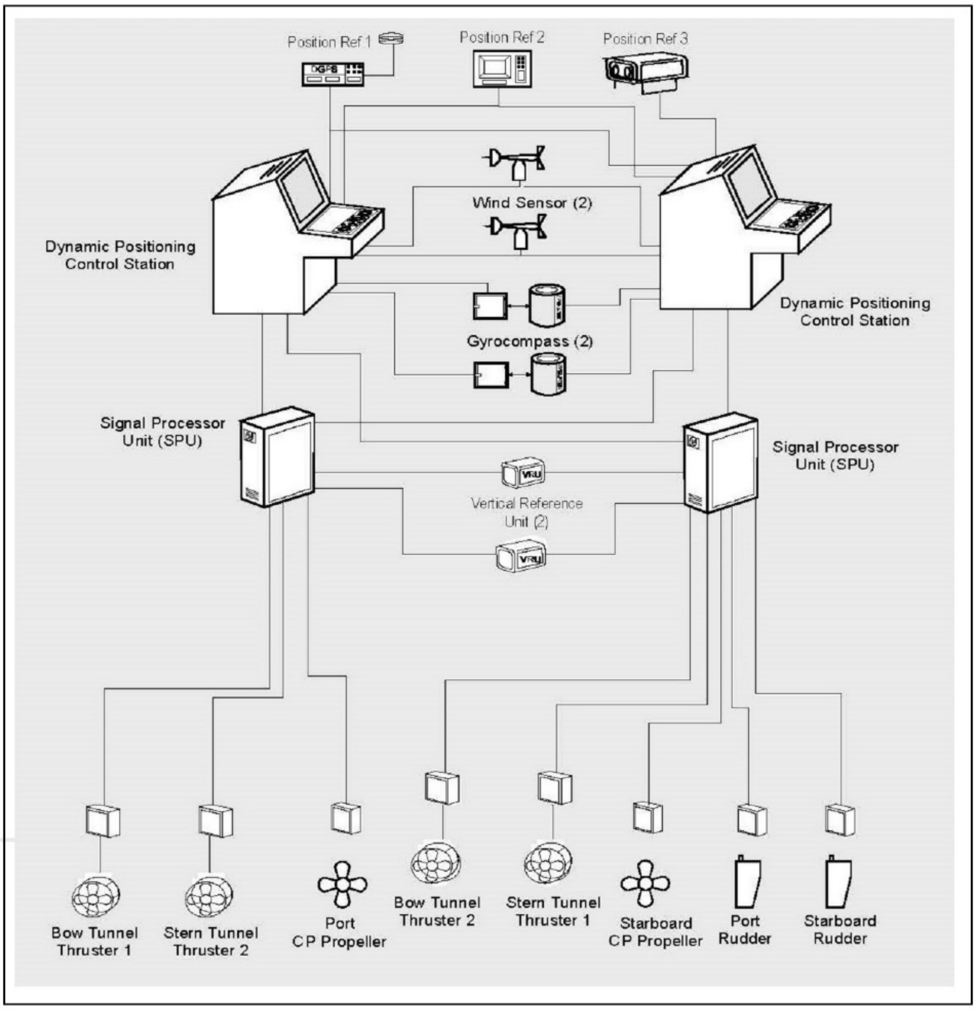


Figure 2.15: Schematic of Class 2 Dynamic Positioning System ("Dynamic Positioning")

According to criticality of mentioned operations, the DP vessels are specified as below:

- Class 1 DP unit that should use the DP system class 1.
- Class 2 DP unit that should use the DP system class 2.
- Class 3 DP unit that should use the DP system class 3.

2.5 DP Applications

Nowadays, usage of the DP system has many diversities from oil and gas related activities to shipping applications and even naval operations. Followings are some of the possible activities that are done by vessels facilitated with a DP system (Bray, 2003):

- Lifting (Top side or subsea)
- Well intervention and work-over

- Floating production (with/without storage)
- Shuttle tanker off-taking
- Heavy lift transportation
- Subsea structures installation
- Pipeline and risers laying
- Rock dumping for pipe protection
- Survey and repair
- Exploration drilling
- Firefighting operation
- Oceanography and seismic research
- Dredging
- Cargo ships maneuvering
- Passenger cruises maneuvering
- Accommodation in floating hotels
- Diving operation support
- Warship maneuvering
- Rocket launching

As far as those above operations shall be done by a specific vessel, many types of vessels currently need to be designed and built with DP system considerations. MODUs, FSOs, FPSOs, OSVs, HLVs, PSVs, Shuttle tankers, Drilling ships, Passenger ships and Warships are some examples of DP vessels.

CHAPTER 3 OVERVIEW OF RISK MANAGEMENT

3.1 Introduction

Despite different definitions of risk that is generated by varying conceptions and perceptions, commonly, risk can be defined as a negative consequence of an event. In term of description, a risk can be measured by the probability of an occurred event multiplied by the severity of its consequences while considering the uncertainties (Aven, 2008).

The diversity of risks can be vast and does directly depend on the type of operations. If the risks cannot be sufficiently managed, significant events and incidents may be accrued. Those incidents may cause catastrophes and disasters in the operation.

All the measures and activities carried out to manage the risk are defined as *Risk management*. "Risk management deals with balancing the conflicts inherent in exploring opportunities on the one hand and avoiding losses, accidents and disasters on the other" (Aven & Vinnem, 2007).

In other words, risk management usually, is considered as a continuous analysis process that exerted on project stages like the design, manufacture, commission, operation, maintenance. This continuous analysis represents a lifecycle for the risk management which is shown in Figure 3.1. By this definition, all actions and situations that may affect an organization to reach the goals, have relation to the risk management. However, identifying which condition, activity or occurrence are significant, will highly depend on the type of industry or enterprise.

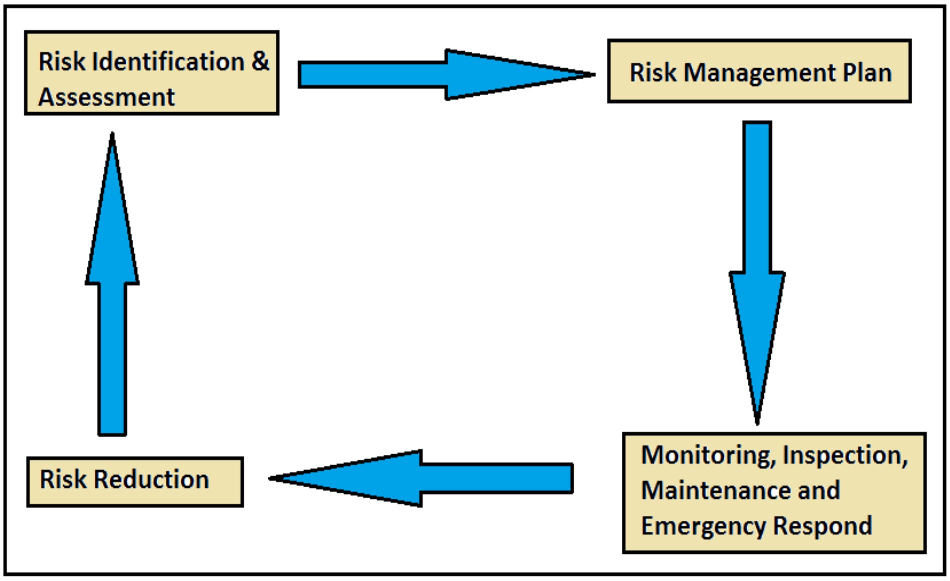


Figure 3.1: Risk Integrity Lifecycle

3.2 Risk Analysis

As mentioned, a continuous risk analysis is required as the major and central part of risk management. *Risk analysis* is defined as a systematic use of information to identify initiating events, causes and consequences of these events (Aven, 2013). The risk analysis usually has a basic structure, which is almost constant, regardless of the field of applications. There are various ways to represent the risk analysis process. Nevertheless, the following three key parameters are common. In addition, the main phases and steps of the risk analysis process are illustrated in Figure 3.2.

1. Planning
2. Risk assessment (execution)
3. Risk treatment (use)

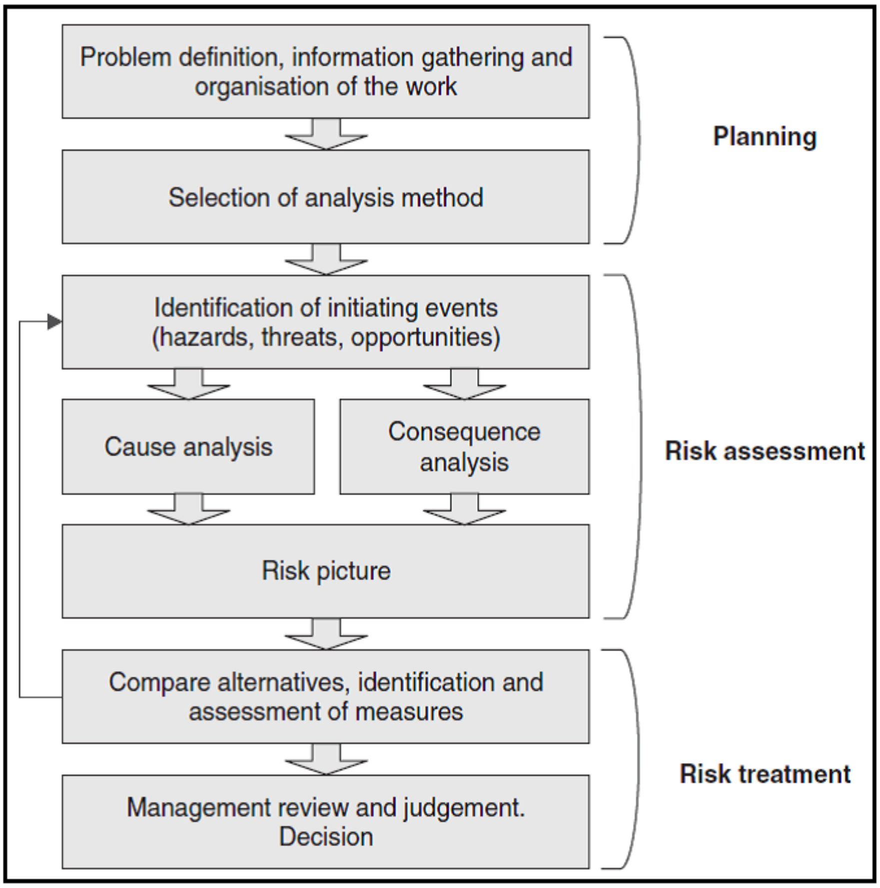


Figure 3.2: The main steps of the risk analysis process (Aven, 2008)

Before discussing the different methods of risk analysis, we need to know, why is the risk analysis necessary and what are the benefits? The simple answer to this question is: the objective of risk analysis is to describe risk, meaning that the risk analysis shall recognize the initial events and expand to determine the consequences.

As a detailed reply to the above question, the followings are the major outcomes of risk analysis:

- A risk picture will be established.
- The factors, conditions, systems which are critically related to the risk will be identified.
- The effect of those above essential elements with respect to the risk will be represented.
- The different solutions and other possibilities can be compared.

Once one follows the risk analysis procedures, a basis for further risk management steps will be provided. The outcomes of the risk analysis give the foundation to an organization, particularly to the managers or decision makers to:

- Placing some criteria for each solution and activity.
- Choosing the solutions among the diverse measures.
- Concluding on whether each solution or the measure can fulfill the requirements.
- The acceptable level of risk can be documented.

These days, risk analysis is mainly used to satisfy the requirements and regulations that are established by authorities. Although satisfying these rules is important, however, for utilizing the whole potential of risk analysis, one shall not only adhere to satisfying the regulations. This is because the risk analysis can be done in different phases in the life duration of a project or a system. The risk analysis is capable to be used from the early concept phase to the detailed engineering and up to construction, installation, operation, and abandonment. The overall benefit of the risk analysis goes to the decision makers that at the end of a process need to take a decision with a cost and safety balance.

3.2.1 Risk Analysis Methods

As discussed in previous section, the risk analysis is utilized for identifying the risk related initial events and developing the consequences. The way of doing risk analysis depends on the chosen method and how the results will be evaluated. However, the overall risk analysis intent that is describing the risk, is the same within any analyzing methods.

In the first step, the risk analysis methods may fall into three categories that are *Simplified*, *Standard,* and *Model-based risk analysis*. Table 3.1 describes these three risk analysis main categories in more details.

Table 3.1: Main categories of risk analysis methods (Aven, 2008)

Main category	Type of analysis	Description
Simplified risk analysis	Qualitative	Simplified risk analysis is an informal procedure that establishes the risk picture using brainstorming sessions and group discussions. The risk might be presented on a coarse scale, e.g. low, moderate or large, making no use of formalised risk analysis methods.
Standard risk analysis	Qualitative or quantitative	Standard risk analysis is a more formalised procedure in which recognised risk analysis methods are used, such as HAZOP and coarse risk analysis, to name a few. Risk matrices are often used to present the results.
Model-based risk analysis	Primarily quantitative	Model-based risk analysis makes use of techniques such as event tree analysis and fault tree analysis to calculate risk.

For risk analysis of a DP system due to the diesel engine failure, this thesis intends to utilize a tool which is named *Fault Three Analysis (FTA)* and is categorized into the model-based category. The following is the introduction to this risk analysis method that will be used in forthcoming chapters.

3.2.1.1 Fault Tree Analysis (FTA)

FTA is a top-down risk analysis that is done by the aid of a logical diagram. A fault tree diagram shows the potential failure of a system to identify the root causes of that failure. The failure of the specified system is the undesirable event which can also be called a *Top Event* while the causes of the top event can be named as *Basic Events.* Since each system includes some components and sub-components, these constitute the FTA basic events (Wang & Roush, 2000). As one can understand, the relation between failure of a system, components, and the barriers are shown by fault tree diagram. It should be noted that the basic event is not necessarily a system’s component failure; it could be a human error or another failure that has occurred.

The FTA was created for the nuclear and aviation industry in 1962 and then became more popular in other industries. Nowadays, the applications of FTA are found in many significant industries such as oil and gas, aerospace and nuclear. At present, the fault tree analysis is one the most used risk analysis methods. Accordingly, this thesis has chosen the FTA as a tool for risk analysis of a diesel engine in the DP system. In the upcoming chapters first, the reader will be introduced to a DP system by knowing the history, components and applications. Secondly, a detailed fault tree analysis will be prepared for a diesel engine, including all the subsystems and components.

A fault tree diagram consists of graphical symbols that are representing the top and basic events of the system in addition to their relations. These graphical symbols are called *logical gates*, and although they are varying in different standards, however, the most common, and significant ones are shown in Figure 3.3 along with their interpretation.

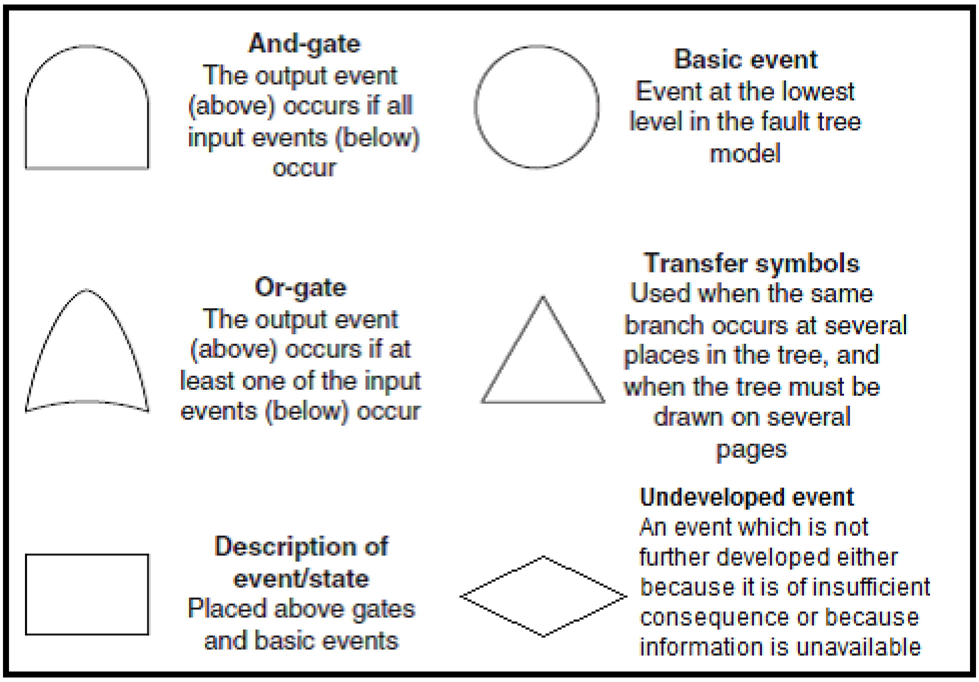


Figure 3.3: Fault Tree Analysis Symbols (Aven, 2008)

To construct a fault tree diagram, the start point is the top event and then the possible failures that can directly cause the top event shall be determined. These failures must be linked to the top event via logical gates. Further, the work will be continued respectively to reach the basic events. The ongoing process will be stopped once one reaches the appropriate stage of details. Meaning that depending on the severity of the analysis and organization policy, the basic events of fault tree analysis for a nominated system might be varying.

From one hand, the most important point in constructing the fault tree analysis is that the FTA is a deductive analysis. One shall repeatedly ask questions like “What are the direct causes of this failure?” or “How this event can happen?”

On the other hand, the most common mistake in FTA happens when one tends to do analysis and attain basic events too fast. It means that the development of fault tree branches must be done consistently by considering all the sub-events of each system's components. The fault tree analysis can be done in both *qualitative* and *quantitative* ways as described in the following, which is based on (Rausand & Høyland, 2004):

Qualitative FTA

For the qualitative fault tree analysis, there is a need firstly to identify the cut sets and secondly the minimal cut sets. In fault tree, a collection of basic events that their occurrence leads to the top event is called a *cut set*. If the cut set cannot be decreased and still the top event will happen, this is the *minimal cut set*. Once the minimal cut sets of the system are identified, one can determine which combination of basic events may lead to system failure for doing further risk treatment.

The criticality of minimal cut sets is specified based on the number of the events that they hold. This number of events is named the *order of the cut set*. In terms of ranking, a minimal cut set with one event is more serious than a cut set with two events since the system fails only by the occurrence of one single failure. The shorter minimal cut sets are riskier and more undesirable ones.

However, one should not just rely on the number of events in the cut set since the probability of the event's occurrence is not considered. For instance, the shorter minimal cut set might have a lower probability of happening, so there is a lower risk of system failure. Thus, a pure qualitative FTA can be misleading, and a quantitative FTA is needed to have a proper and reliable risk analysis.

Quantitative FTA

For a quantitative fault tree analysis, the probability of basic events occurrence shall be determined, which provides a basis for calculating:

1. The criticality of basic events in the tree;
2. The top event probability of occurrence.

For calculating the top event's probability of occurrence, there is a formula that will give a good approximation. After determining each basic event's probability of occurrence, the probability of each cut set shall be calculated by summing these probabilities and the top event occurrence probability will be gained.

3.3 Risk Evaluation

3.3.1 Introduction

To determine the risk is acceptable /tolerable or not, we need to evaluate the risk. The *Risk Evaluation* can reveal that whether the certain risk is acceptable, or it needs to be reduced as low as reasonably practicable (ALARP) by applying some risk-reducing activities. The risk evaluation is normally done by use of either the *Risk Accept Criteria* or the results that are gained from quantitative analysis. In this thesis, the first method is chosen meaning that, the risk of diesel engine failure in a DP system is evaluated by the aid of the risk accept criteria.

3.3.2 Principals

Before performing the risk evaluation, one should be introduced to the principals of risk accept criteria. In this method, the evaluation of risk is done by considering the probability of event occurrence and severity of consequences. An appropriate and very often practical tool for finding the risk accept criteria is the *Risk Matrix*. A risk matrix includes three categories related to the main aspects of risk assessment (personnel, the environment, assets, and reputation) which are mentioned previously. The risk matrix categories are:

1. Consequence Category

According to the safety policies of a company and critically of the marine operation, consequences are divided into different levels based on their severity. For instance, the followings are the most used terms for severity ranking of the consequences respect to the people:

- Many fatalities (5 or more)
- Single or few fatalities
- Single or few serious injuries
- Minor injury
- No injury

2. Probability Category

This category is also divided into some levels of the likelihood that are qualitative based on some quantitative values. They are determined according to previous and similar experiences. For example, the followings are usual levels of likelihood:

- Frequent (10)
- Probable (1.0E -1)
- Unlikely (1.0E -3)
- Very unlikely (1.0E -5)
- Extremely unlikely (1.0E -7)

3. Risk Result Category

Previously, the risk was defined as a product of consequence and probability. Accordingly, the last two above categories (consequence and probability) are used to evaluate the risk and for finding the risk accept criteria. The evaluated risk category also is divided into varying levels that have been recommended at the DNV-RP-H101 for marine operations as:

- Low or Acceptable (Green area)
- Medium or Tolerable or ALARP zone (Yellow area)
- High or Unacceptable (Red area)

The reader is kindly referred to Chapter 5 in which the risk evaluation for the diesel engine failure in a DP system is done.

3.4 Risk Assessment

The reader should make the clear differences between risk analysis, risk evaluation, and risk assessment. The overall process of the risk analysis and risk evaluation is called *Risk Assessment* (DNV, 2003). In other words, risk assessment is the whole procedure of evaluation of risks and elements that can influence the safety of a project. The risk assessment involves investigation to find out the dangerous events and their correlation to possible causes. Accordingly, risk assessment should be done in different levels respect to different steps of the project (API, 2009). The results that are gained from risk analysis methods must be evaluated to find whether the level of the risk is high or low, whether it is necessary to implement the risk reducing measures and whether the measures are compared with each other (Aven, 2008).

Based on the DNV Recommended Practice, the best way to do a preliminary risk assessment in marine operations is the simplified method which is called *Qualitative Risk Assessment (QRA)*. During execution of qualitative risk assessment, the parameters that are listed in Table 3.2 should be evaluated (DNV, 2003).

In this thesis, a model-based method is chosen for performing the risk assessment of diesel engine failure in a DP system. That is called *Bow-tie Analysis* and will be described in following section.

Table 3.2: Risk Assessment Parameters (DNV, 2003)

Assessment Parameter	**Keywords for Assessment**
Personnel exposure	• Qualification and experience of personnel • Organization • Required presence • Shift arrangements • Deputy and backup arrangements
Overall project particulars	• Delay • Replacement time/cost • Repair possibilities • No. of interfaces and contractors or subcontractors • Project development period
Existing field infrastructure	• Infrastructure – surface • Infrastructure – subsea
Handled object	• Value • Structural Strength/Robustness
Marine operation method	• Novelty and feasibility • Robustness • Type of operations • Previous experience • Instability
Equipment used	• Margins/robustness • Condition/Maintenance • Previous experience • Suitability • Experience with operators or contractors (track record)
Operational aspects	• Cost of mobilized equipment and spread • Language barriers/hindrance • Season/Environmental conditions • Local marine traffic • Proximity to shore

3.4.1 Bow-Tie Analysis

3.4.1.1 Introduction

The *Bow-Tie* analysis is a method of doing a risk assessment in risky scenarios by demonstrating a causal relationship. In this method, the risk assessment is done by the aid of a bow-tie diagram which is shaped like men's bow tie. A bow-tie diagram provides a simple, visual and understandable explanation of the risk, in only one single picture. It also gives an overview of multi-possible scenarios that may happen in a specific operation. ("Bowtie Method", 2015)

The two main purposes of a bow-tie diagram are:

1. Providing a visual summary for all the possible accidents, and

2. Identifying some measures to control and prevent those accidents.

After establishing these two goals, the bow-tie diagram should go further to identify the situation in which the prevention measures fail. Also, some other measures must be introduced to control failure of the primary control measures. The second type of measures has indirect but serious effects on the main scenario. By this way, the overall weakness and control measures of a system in addition to their relation can be seen. (Vinnem, 2013)

The management system of a company can consider the bow-tie analysis for its safety issues. It shall be integrated into the bow-tie diagram for having control on activities which prevent the occurrence of risky conditions, in addition to nominating and monitoring the personnel who perform the preventive measures. By this procedure, it could be beneficial for managing the risks to an acceptable level based on ALARP (As Low As Reasonably Practicable) principals.

It is not entirely clear that when and how the bow-tie method gets its origin. However, the first bow-tie diagram with today shape is utilized in 1979 at the University of Queensland Australia in the course of "Hazard Analysis" related to the chemical industry.

The disastrous incident of *Piper Alpha* in 1988 was an alert, especially to oil and gas industry. The incident report concluded that there was too little understanding of hazards and their associated risks. The report showed that there is a high need for developing a systematic method for evaluating the possible risk with along with associated events for ensuring the control of the different situation. ("History of Bowtie", 2015)

The first company that is utilized the bow-tie analysis in its standards for managing the risk was *Royal Dutch Shell* in the early nineties. They did a lot of researches and development besides making strict rules for using the bow-tie diagram. At the beginning, it was just for ensuring the improving risk control ability on their operations.

After the *Shell* project, other companies in the industry start the using and supporting bow-tie method rather than substituting any other risk analysis tools. This happened since the bow-tie diagram became popular as the simple and visual risk evaluation tool. Nowadays, the bow-tie analysis is fully developed in oil and gas industry in addition to spreading in other industries like aerospace, maritime, mining, etc.

3.4.1.2 Principals

To start for the bow-tie analysis and drawing the diagrams, one shall be familiar with some important terms that are introduced as following. Figure 3.4 shows the schematic of bow-tie diagram and its symbols. ("Risk Support", 2014)

Hazard

In general, the things which have the potential to cause organization's damages, are *Hazards.* These things are the normal aspects of the organization or operation. However, loss of control on these aspects will have the negative impact on the company. For instance, the position keeping in offshore operations is a normal issue. Nevertheless, the loss of control on position keeping may be ended up with the catastrophes in different ways like collision or pollution.

Finding the hazards is the first step of the bow-tie analysis. The rest of analysis shall be developed to specify the ways for keeping the normal operation without turning to the undesired event. Basically, there is a good way which is called HAZID (Hazard Identification) to determine different hazards. Then, the most critical identified hazards are chosen for analysis by the bow-tie method.

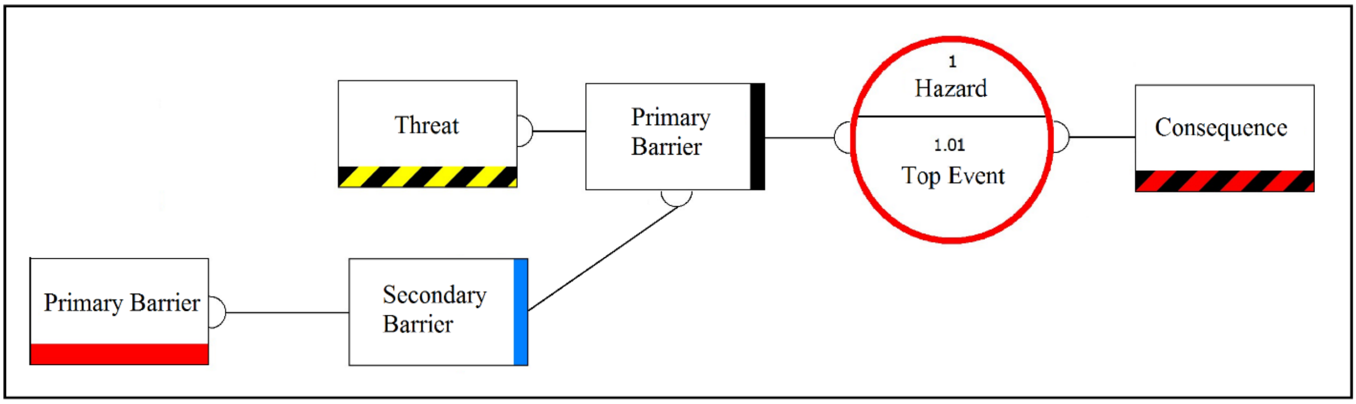


Figure 3.4: Schematic and symbols of bow-tie diagram ("Active Bow Tie", 2014)

Top Event

The next step after choosing the hazard is defining the *Top Event*. Top event is the time when the control of normal activity is lost. Although at this moment still there is no damage or disaster, however, it is close to happening. In other words, the top event is the thing or the time exactly before the main damage occurs. For example, in the case of position keeping which is mentioned in last part, the failure of the DP system can be a top event. To a large extent, choosing the top event is practical and subjective this is why it may be redefined several times during the development of bow-tie diagram.

Threats

The *Threats* can be any activities which cause the top event. These are also known as *Initiating Events*. For our considered example, failure in any sub-systems of the DP system can be position reference system failure, thruster's failure and power generation failure to name a few.

Consequences

The outcomes of the top event are consequences which can be more than one for a single top event. For example, in the case of position keeping, the consequences of loss of DP system can be an oil spill, collision and operation stoppage.

Primary Barriers

The measures which help to prevent the occurrence of a top event and happening of consequences are called *Barriers*. The barriers exist on both sides of bow-tie diagram and once they are identified, the underlying understanding of how the risk can be managed, will be achieved. Also, the barriers are helpful for realizing the system's weaknesses.

Referring to mentioned position keeping example, the barrier for the top event (DP system failure) prevention can be increasing the redundancy by using backup systems. While the barrier for mitigating of consequences can be using a standby tugboat to control the collision scenario.

Barrier Decay Modes

Usually, each primary barrier has one or some failure mode(s) that is called *Decay Mode.* The barrier decay modes are utilized to illustrate the weaknesses, failures, or ineffectiveness of the primary barrier. Simply, these are the things which lead a barrier to fail. As an example, failure of the backup system due to a common fault can be a decay mode for a redundant DP system.

Secondary Barriers

Once we identify the decay modes of primary barriers, they can be controlled by some other barriers called *Secondary Barriers*. The secondary barriers are just the preventive measures which prevent the happening of barriers decay mode and consequently top event. To follow our example, a proper planned maintenance for the standby machinery, can be a secondary barrier for failure of the DP system as a top event.

A detailed bow-tie analysis for the diesel engine failure will be done in Chapter 6.

CHAPTER 4 RISK ANALYSIS OF DIESEL ENGINE FAILURE BY FAULT TREE ANALYSIS

As discussed in Chapter 2.3, a DP system consists of seven main sub-systems. Each one is divided into other systems. These are the most critical ones, since their failure leads the whole DP system to fail. The upcoming analysis reveals the chain relations between the systems and components and helps the reader to understand the basic events that may lead to loss of DP system.

Based on importance, complexity and criticality, the *Diesel Engine* in *Power Generation System* is chosen for the technical analysis and the cause of failure of its main sub-systems and components are identified. This analysis will be performed based on the FTA principals introduced in section 3.2.1.1. This will be carried out in addidtion to DP technical understanding introduced in section 2.3. All technical assessment particularly, the relations between the components and sub-components for reaching the failure, has been done according to the writer's job experiences. These experiences are based on several years working as a marine maintenance engineer on board of different vessels while dealing with several types of machinery and systems, especially DP and propulsion systems.

As was mentioned in previous chapters, power generation systems are the most important and critical systems on the shipboard. This is because of the DP system and other vessel machinery that require electrical power as a source of energy for operation. Among power generation systems, a diesel engine is the most significant one since it acts the prime mover role for generating electricity. The readers are encouraged to refer to FTA Diagrams in the *Appendices* while reading the following sections. A comprehensive studying and fault tree analysis of a diesel engine is provided as following.

4.1 Diesel Engine Failure (Fault Tree Diagram A.1)

Diesel engine is prominent machinery that provides the initial driving force for generating electrical power. It was previously mentioned that the size and numbers of the diesel engine which are utilized for producing electrical power, depend on the amount of electrical power that is consumed by vessel onboard. Further, the electrical power consumption depends on the size and diversity of onboard equipment. It means that specific offshore vessels have specific equipment for doing specific marine operations. Since different equipment have varying power consumption, each offshore vessel may have different numbers of diesel engines with different sizes for electrical power production. Also, the capacity of the electrical production of a vessel is normally more than it is required for operation. In other words, some diesel engines and generators that are aboard of vessel are just on a standby and will be utilized as backup.

Note: In a DP vessel, number of diesel engines depends on DP class. In DP class 1 which has the least redundancy, there is no more diesel engine that can be utilized as backup in the case of other engines' failure. Meaning that, if one of the diesel engines fails, the DP operation will be stopped due to shortage of the electrical power. Accordingly, the failure of diesel engine in DP class 1 is chosen to be analyzed.

The failure of one or more diesel engines causes the shortage of electrical power or even a total blackout. In the first case, some critical equipment cannot be operated when needed while in the case of blackout, the vessel and all the operations will be dead due to no electrical power to run the machinery. The shortage or lack of electrical power can affect several parts of a DP system such as auxiliary machinery for main propulsion, computers, referencing systems, electromotor for driving thrusters etc. The writer, therefore, has decided to focus on the diesel engine as it is the most critical machinery for providing the electrical power in a DP system.

A diesel engine which drives an alternator for producing electrical power is basically a 4-strock cycle type and doesn't have a direct role for vessel propulsion. As can be seen in Diagram A.1, there are eight individual systems that are contributing in running a diesel engine. A single failure of each of these systems can cause the diesel engine failure. Followings are detailed explanation of the diesel engine sub-systems and their failures analysis.

4.1.1 Mechanical Components Failure (Fault Tree Diagram A.1.1)

The components of this category are the main and largest parts of a diesel engine as illustrated in Diagram A.1.1. Many of them have rotatinal or reciprocating movements such as *piston, connecting rod* and *crankshaft* while some others are stationary like *cylinder head* and *liner*. The components which have movements are more vulnerable to fail because of wear and tear. The major cause of moving parts wear in a diesel engine is overheating and high rate of friction. Since for the moving parts both cooling and minimizing the frictions are done by the aid of lubrication oil, the shortage or lack of the lubrication causes failure of engine moving parts. For instance, the movement of piston inside the liner or turning the crankshaft through the bearings require proper amount of oil for cooling and reducing friction. Otherwise, the rate of wear and tear will increase and cause seizing or failure of the system.

The story is a bit different for the stationary parts. For the cooling purpose on the fixed components a fresh water cooling system is established. For example, a liner with the cylinder head above where provide the combustion chamber space, are cooled by fresh water that circulate in a closed system outside area of their bodies. This cooling is essential to reduce the high temperature associated with combustion. The lubrication goal is established by lubricating oil, for example, the inner area of the liner where has high contact with piston surface, is lubricated by oil to decrease friction.

If the parts fail whether due to fatigue or because of wear and tear, the overheating due to lack of cooling water also being wearied because of low lubrication respectively, will be the main reasons for failure.

4.1.2 Fuel System Failure (Fault Tree Diagram A.1.2)

An engine needs fuel for starting and running, therefore, without fuel either an engine cannot be start or run. The system that provides fuel to an engine via storage, transfer, purification and supplying, will be considered later in the *Auxiliary System* of a diesel engine. In this part only the components and sub-components of the diesel engine fuel system are taken into account. In other words, the writer just looks into the fuel related sub-systems that are attached to a diesel engine and provide the fuel for combustion into the engine.

A diesel engine fuel system consists of four sub-systems as shown in Diagram A.1.2. Each has duty to prepare the fuel for burning in the engine combustion chamber.

4.1.2.1 Attached Fuel Pump

This is a small centrifugal pump that provides the fuel flow and send it to the next stage. The suction side of the pump is the beginning point of the engine fuel system meaning that, the fuel which comes from auxiliary fuel system through the pipeline, first reach the attached pump. The attached pump is driven by aid of gears that are attached to the rotational parts of the engine, particularly crankshaft.

As can be seen in FTA Diagram A.1.2, since attached pump cannot supply the proper fuel flow to the next stage (cylinder fuel pumps), the whole fuel system will be affected and diesel engine will be shut down. The improper fuel flow can be either less flow or even no fuel flow which is caused by significant leakage and stopped pump respectively. The leakage may occur due to either the seal failure or the breakage of pump casing while the pump stoppage could be due to the failure of driver or pump's internal components.

It is weird that the pump stops due to loss of driving force since the engine itself gives the driving force. The only reason for stopped pump due to loss of driving force is a failure of transmitting gears due to fatigue, wear or stoppage of the rotational engine's parts. Usually, the attached pump is stopped because of internal components failure like impeller and shaft that are basically failed with the same cause such as fatigue or wear.

In the case of leakage, it must be really large to affect the fuel flow and cause the engine to shut down because of lack of fuel. However, it may also happen if a seal is totally failed, or the pump casing is broken. Apart from fatigue and wear and tear, the seal can fail due to overheating that its root cause normally is the lack of fuel. It means that if the fuel (that acts as a lubricator and cooling medium as well) doesn't reach the fuel pump, the pump is continuously working dry and causes the seal to overheat and fail. The casing crack is usually caused by external damages like dropped object. In addition, the fatigue or corrosion of the casing may cause the breakage and crack.

4.1.2.2 Cylinder Fuel Pumps

This is a kind of reciprocating pumping system that is installed on each cylinder (unit) of the diesel engine. The purpose of this boosting system is to provide the proper pressure for the fuel that must be atomized into the combustion chamber of each cylinder by the fuel injector. The pressure that is needed for opening the fuel injectors and spraying the fuel varys among the types of engines, however, the pressure range normally is between 280 and 340 bar that is provided by cylinder fuel pump.

The cylinder fuel pump consists of two main parts called *Barrel* and *Plunger*. They act as a cylinder and as a piston respectively. The fuel from attached fuel pump enters the barrel through the suction port when the plunger inside the barrel has downward motion. During the upward stroke of the plunger, the suction port will be closed, and the discharge port will be opened by the aid of helix pathway that is designed on the plunger. Thus, the fuel obtains required pressure by plunger reciprocating motion in the barrel.

Furthermore, the plunger in the barrel rotates (up to some limited degrees) to maintain the proper position of the helix for opening and closing the suction and discharge ports. The plunger rotation is achieved by a linkage named *Fuel Rack,* which receives the order from the engine governor to regulate the engine speed. The fuel rack regulates the engine speed by increasing or decreasing the amount of fuel to the cylinder fuel pump. This is performed by the aid of turning the plunger in the barrel as described.

The things that can affect the cylinder fuel pump efficiency are either significant leakage or stopping of the pumping action. The causes of the leakage is either seal failure or breakage of the pump casing as shown in Diagram A.1.2 and described in previous section. The failure of barrel or plunger also may lead the pump to stop boosting. Since these are mechanical components with motions, wear and fatigue can be the causes of pump failure by seizing of the plunger in the barrel.

4.1.2.3 Fuel Injectors

This is also named *fuel valve* and equips each engine cylinder to spray and atomizing the fuel for making it ready for mixing with air and burning in each cylinder combustion chamber. A fuel injector comprises of the main components including *body, nozzle, spring and seal* that any defects on each of these parts may cause the failure of the fuel valve. Once one or more engine's fuel injectors do not work properly, the engine combustion will be interrupted and may lead to engine shutdown or bad combustion which causes engine damages in long-term operation.

A fuel injector has an opening and atomizing pressure (between 280 and 340 bar depends on the type of engine) that shall be provided for the fuel by each cylinder fuel pump, as described in previous part. At the tip of a fuel injector, there is a nozzle with tiny holes where the fuel leaves the injector in the shape of vapor cloud by the presence of sufficient pressure. The opening and atomizing pressure can be adjusted by a spring and numbers of different adjustment discs. If the fuel valve pressure setting is not adjusted correctly or the cylinder fuel pump doesn't supply the fuel with proper pressure, fuel cannot enter the combustion chamber or it enters in a liquid phase. These can be the causes of no or bad combustion respectively.

There are other problems like leakages and getting stuck that cause the fuel injector to fail. The leakages may occur due to the defective nozzle, body or the seal while the clogged nozzle and spring malfunction can be the causes of getting stuck. The basic causes of injector failure are demonstrated in Diagram A.1.2, and some of them are common causes like fatigue and wear and tear. However, it should be mentioned that the overheating of the nozzle is because of the excessive heat from the combustion chamber. In addition, the clogging reason of nozzle is remarkable and happen due to the accumulation of carbon deposits that are residuals of combustion action.

4.1.2.4 Fuel pipes and joints

In the fuel system of a diesel engine, many pipes and joints are utilized. From attached fuel pump to each cylinder pump, and from the cylinder pumps to each fuel injectors, the fuel is transferred by those pipes. Consequently, for attaching and fixing the pipes to the components, several different joints including bolts, nuts, washers and gaskets are used. As mentioned in Diagram A.1.2, the main causes of pipes and joints failure are fatigue, corrosion and external damage that their resistance, to some extends depends on the type of material. The material of pipes and joints are varying based on engine type and application location, however, the usual materials are steel and copper that has different strength against corrosion, fatigue, and external damage.

4.1.3 Lubricating System Failure (Fault Tree Diagram A.1.3)

As it was briefly touched, the main purpose of lubrication is to reduce friction, particularly in parts and areas which movement exist. The minor reason for lubrication could be cooling as well for some components. Apart from these goals, there is another critical issue which shall be done by the aid of lubricating oil. This is cleaning of cylinder liner's surface in the combustion chamber by the detergency specifications of lubricating oil.

The reason for cleaning of inner liner surface is because of the sulfur content of the fuel. The fuel sulfur causes the combustion to create acid that is corrosive and is harmful to the shiny liner inner surface. This also increases the amount of wear and tear. Thus, along with lubricating features, the oil must have some detergency specifications to decrease the rate of failure in the long term.

As illustrated in the diagram A.1.3, the main parts of a diesel engine lubricating system are *Attached Oil Pump*, and *Pipes and Joints.* Their failure will cause the lubricating system failure and consequently the diesel engine failure. In a 4-strock diesel engine, lubricating oil system has a closed circulation from/to the engine sump. The attached oil pump sucks the oil from sump and also does oil pressurizing and distribution to the some components. The used oil will go back to the sump by splashing and leaking between parts.

The operational aspects and defects of attached oil pump and pipes are very similar to the same parts in *Fuel System*. Therefore, to reduce repetition, the reader is kindly referred to the previous section (Fuel System Failure) to see the failure reasons of attached pump, and pipes in the lubricating system. Note that, in this system the fluid is lubricating oil while fuel is the fluid in the previous system.

4.1.4 Water Cooling System (Fault Tree Diagram A.1.4)

There is a need for a cooling system in an engine due to the high temperature of combustion. The cooling system maintains the temperature of components which deal with combustion by being in the adjacent area. The most important parts are Cylinder Liner and Cylinder Head that create the combustion chamber. The engine manufacturer assigns a space called *Jacket* in the *Engine Body* where exactly covers the outer area of the cylinder liner also allows the fresh water to flow and cool down the cylinder liner. There are also, some passages in the cylinder head in which the cooling water circulates to maintain the cylinder head temperature.

In the engine cooling system, the cooling medium is fresh water that flows in a closed cycle. The purpose of using fresh water instead of seawater is the prevention from scaling and corrosion that are harmful to the engine components.

The facilities which provide the fresh water with the proper temperature for an engine will be discussed in *Auxiliary System* in the forthcoming section. However, an engine cooling system consists of an *Attached pump*, and *Pipes and Joints* as shown in Diagram A.1.4. Once more, to prevent repetition, the writer recommends to see the Fuel System Attached Pump and Pipes & Joints to get familiar with the Cooling Water System components. Note that, in this case, the medium fluid is fresh water instead of fuel.

In comparison with Fuel and Lubricating System, the only difference and important issue in the case of failure of Water Cooling System is corrosion which is not a concern for the inner components of Fuel or Lubricating System. This is due to the existence of water. This is why the engine cooling water needs to have some treatment by the aid of special chemicals like Inhibitors and rectifiers to prevent corrosion and scaling.

4.1.5 Scavenge and Exhaust System Failure (Fault Tree Diagram A.1.5)

The combustion process in a diesel engine requires air for fulfilling the fire triangle (burning material, air, and heat). Now to make a right combustion, fuel-air mixing ratio shall be optimized which demands an excessive amount of air. For providing this volume of air, the engines are equipped with *Turbocharger* and its function is called *Supercharging*.

A turbocharger from turbine side, takes the combustion exhaust gas as a driving force and, from the other compressor side, it sucks huge volume of air and force it into the engine. After the air passed through a manifold, it is distributed to each engine cylinder and will be entered to each combustion chamber by opening the cylinder intake valves (depending on the engine fire order). After completion of unit combustion, the exhaust valves become open to let the produced exhaust goes out. All the coming exhausts from the engine cylinders pass through a manifold and reach the turbocharger turbine blades. Once the turbine blades are driven by exhaust gas, this motion will be transferred to the compressor blades by a shaft. Once again, the compressor blades will collect and send the air into the engine. This process continus as long as the engine is running. It should be noted that opening and closing of intake and exhaust valves are based on the engine fire order that is controlled directly by engine’s *Camshaft*.

As mentioned and also can be seen in Diagram A.1.5 a turbocharger has three main parts: turbine, compressor, and shaft. The cause of turbocharger failure is usually due to one of these three main parts. The turbine and compressor sides have almost the same operational configuration so; their failure causes are similar which is fatigue or wear and tear on the blades or bearings. A shaft that connects two sides of the turbocharger may fail due to the same reasons meaning fatigue and wear and tear. The failure causes of turbocharger components are mostly due to high rotational speed rather than other factors.

Although, the turbocharger is the main sub-system of scavenge and exhaust system, the air and exhaust manifold in addition to intake and exhaust valves may cause the system failure. Accordingly, the common reasons for their defects are fatigue and wear. Nevertheless, the exhaust valves may fail due to high combustion temperature. This could also be because of non-efficient combustion due to wrong fuel-air ratio.

4.1.6 Starting System Failure (Fault Tree Diagram A.1.6)

Before generating the electrical power and as an initial action, the diesel engine must provide the mechanical power for the alternator to produce electrical power. As a rule of thumb, all the diesel engines in marine and offshore environment particularly, onboard the vessels and platforms start by the aid of pressurized air. The systems that are designed and installed for supplying the air with the proper pressure for engine starting and other usage will be discussed in the Auxiliary System. In this part, the focus will be on the starting system of a diesel engine as an attached system.

A typical diesel engine starting system and its associated components are shown in Diagram A.1.6. This system includes *Starting Air Lines, Distributor,* and *Valves*. Once after supplying the pressurized air by auxiliary equipment, the starting air enters the engine air distributor. Depending on the distributor adjustment, which depends on engine fire order, the starting air is pushed to the nominated cylinders by passing through air lines. This is done once the starting handle is activated (manually starting) or the solenoid valve is actuated (automatic starting). Now, the starting air reaches the determined units and lifts the unit’s starting valve to open the path into the cylinder. The air is applied on top of the pistons and forces them to move downward and cause the engine turning. Once the engine starts turning, all the attached systems including fuel pump will be turned. By fuel injection, the combustion will be started, and engine can continue running in the normal condition. In this stage, the starting air flow is blocked by returning the starting handle to the initial position. It should be noted that, the position of air distributor to choose the cylinder for sending air, is controlled by the camshaft and based on the engine fire order.

Failure of the starting system also can be the relevant causes as is shown in Diagram A.1.6. In general, blocking the air way or preventing air to reach to the top of the piston, is the main reasons for starting system failure. This may occur in any of three main system’s component (starting air pipes, air distributor, and valves).

In addition to fatigue and wear, the components that start the air also can fail due to being stuck or become corroded. Since the distributor and starting air valve are the moving parts, they may be seized because of impurities in the air flow or lack of lubrication. Further, the humidity and moisture in the airflow can be the cause of corrosion in the inner spaces of distributor and pipes. Moreover, the abrasive particles that are carried over by airflow are reasons for erosion that leads to the high amount of wear. Note that, the external damage also can be a source of failure as it can break the air pipelines.

4.1.7 Auxiliary Systems Failure (Fault Tree Diagram A.1.7)

Auxiliary systems are the collection of several systems for providing fuel, lubricating oil, cooling water and pressurized air. These goals are the essential principals that must be established when working with machinery for power generation and propulsion. Any component failure causes an interruption in providing the main supply of fuel, oil, water or air to the engine. As described earlier, an engine cannot either be started or continue running without these four main supplements.

4.1.7.1 Fuel System

During the vessel fuel bunkering operation, the required fuel oil for the vessel can be taken from the shore or at anchorage by the aid of tanker truck and bunker barge respectively. The fuel is stored in different ship's tanks then it is transferred to the machinery room *Settling Tank* as needed by the fuel transferring pumps that are gear-type positive displacement pumps. The fuel shall be settled for water separation that is frequently done by settling tank draining. Also, some fuel oil treatments are done in the settling tank by special chemicals. The next stage is fuel purification using fuel purifiers. A purifier attached pump sucks the fuel from settling tank and pushes it to the purifier bowl that separates water and heavy particles from the fuel based on centrifugal force. The purifier outlet also is pure and ready for burning in the engine combustion chamber. However, this fuel is stored in another tank called *Service Tank*. For all those transferring and purification, several pipelines, pumps, and purifiers are utilized besides some filters. The engine attached fuel pump (described in section 4.1.2.1) gets its suction from service tank to bring the fuel to the engine.

As shown in Diagram A.1.7, breakage in pipelines, pumps, and purifiers and also filter clogging can cause the fuel system to fail. One should note that the failure of purifier mechanical components are not discussed since this is not a critical issue for a diesel engine failure. However, other reasons either mentioned in A.1.7 diagram like pipeline breakage or are illustrated in other diagrams for convenience.

Furthermore, it is recommended to pay some attention to an auxiliary fuel system like chemical treatment and frequent draining of Setting and Service tanks. These are necessary to ensure proper fuel condition for burning. Otherwise, a fuel with the high amount of water or insoluble particles may disturb an engine running condition and cause engine stoppage.

4.1.7.2 Lubricating System

There are several types of lubricating oil that are used for different types of engine. In this thesis, the writer focuses on a 4-strock diesel engine which is often used in most electrical power generation. In this section, the associated auxiliary lubricating system is going to be described. There is only one type of lubricating oil that is used in 4-strock diesel engines. During the bunkering, the oil is stored in nominated storage tanks and whenever is needed it is transferred directly to a diesel engine oil sump by the transferring pump. The closed circulation from/to the sump by engine attached oil pump was covered in 4.1.3.

From one hand, some of the 4-strock engine lubricating oil is burnt in the combustion chamber and, on the other hand, the oil becomes dirty also it loses the proper viscosity and detergency. Accordingly, it is a normal activity to refill an engine sump frequently. The time interval for an engine sump refilling is based on oil level of the sump and lubricating oil condition that shall be examined by a responsible engineer in routine everyday check.

Apart from a purifier, a transferring pump, pipelines and filters are the main parts that their failure are similar to the fuel system (4.1.7.1) as shown in Diagram A.1.7.

4.1.7.3 Water Cooling System

Depending on the machinery room arrangement, there are two types of water cooling configurations. The first one is an individual cooling system that is the old version. In this method each machinery has its own cooler which is usually *Shell and Tube* type heat exchanger, and also these coolers are independent of each other. The newest method is a central cooling system that is used a *Plate Type* heat exchanger as the cooler. The outlet fresh water flow in the cooling system of all machinery reach to a common pipe and it will be sent to the cooler to cools down by the aid of seawater. Then, freshwater will be distributed to different machinery by several pipelines.

In this study, the central cooling system is chosen which is popular and more reliable in marine and offshore industry. Due to value and shortage of freshwater vessel onboard, a freshwater cooling system shall be a closed system. It means that the freshwater should not be sent overboard, and it must circulate through a closed system that consists of the cooler, circulating pump and pipelines plus *expansion tank*. In addition to making head pressure for a freshwater cooling system, an expansion tank is used as a replenishing tank for refilling and maintaining the amount of freshwater. Further, an expansion tank has a duty for de-aeration of the freshwater system to prime it and release the air bubbles.

In addition to freshwater that is circulating and passing through the cooler, the sweater also passes through this cooler as a cooling medium to reduce the freshwater temperature. Thus, any faults in a cooler can happen in both freshwater and seawater sides. Since freshwater does not have any problem associated with blocking cooler's pathways by scaling, the only reason of cooler freshwater side failure is a lack of water. This can happen due to leakage from pipelines or expansion tank in addition to circulating pump failure as shown in Diagram A.1.7.

However, in the cooler seawater side, a fault may happen due to pathway blockage because of scaling. Here, lack of seawater can also cause a cooler failure that occurs due to faulty seawater pump, pipeline breakage or *sea chest* clogging. Main seawater pumps are the centrifugal type, and their reasons for failure are mentioned in the separate diagram. Pipelines, joints, and valves can become leaky and lead the cooling system to fail.

Sea chest is a vessel's seawater suction port where is positioned under the vessel waterline. Seawater comes to a vessel seawater lines through the sea chest by head pressure, and it is sent to the cooler by main seawater pumps. After the seawater cools the freshwater, it will be sent to overboard, meaning that a vessel's seawater system is not a closed system. A sea chest is normally clogged by the accumulation of marine growth, however, during vessel operation in a cold climate area, the icing also can block the sea chest. Once the sea chest becomes blocked, the amount of seawater input is decreased. It affects the cooling system as such all the machinery temperature increases and most probably they have to be stopped.

4.1.7.4 Air System

Usage of pressured air onboard a vessel is varying from starting diesel engines to pneumatic control systems. Also, it is used for service air for daily workshop tasks and also operating ship's horn. Thus, a separate air system must be established aboard vessel to supply needed air for those purposes. An air system as an auxiliary system includes *Air Compressor, Air Reservoir* (air bottle), *Air dryer*, and pipelines.

An air compressor sucks air from the ambient area after passing through a filter then compresses and prepares the air for storing. There are different types of compressor like a screw and reciprocating type that normally compress the air in at least two stages. The air is compressed up to a predetermined pressure at the first stage (usually 10 bar) and will be pressurized up to 32 bar in the final stage. Afterward, the air is sent to air bottles for storing. Different lines and pipes are branched from air bottles to varying places and machinery for different applications.

Leakages of pipes, joints and valves can cause air system faults, especially since the system is under high pressure. The air compressor also can fail due to mechanical components failure or driving motor failure that leads an air system to fail. Note that the compressor's mechanical components failure is not a critical issue in our study, this is why it is not developed in Diagram

A.1.7. The main source of air system failure associated with air reservoir is leakage. This is mostly occurring in the inlet, outlet and relief valves that lose pressured air due to fatigue, corrosion, and bad adjustment. The last part of an air system is air dryer that has responsibility for taking air moisture and humidity. This is because of the sensitivity of pneumatic control systems in addition to prevention of corrosion in pipes and machinery. Failure of air dryer does not have significant effects which lead an air system to fail so; it is not developed in Diagram A.1.7.

In an air system and regarding the diesel engines starting procedures, there is a remarkable matter which must be taken into account. During air compression, air contains some moisture and oil that can be carried over by air from the compressor to the air bottles. The moisture will become water by condensation and settle down at the bottom of air reservoirs as well as carried over oil. The water in starting air lines cause corrosion while the oil content is more dangerous since it can be the cause of *Air Starting Explosion*. By the occurrence of air starting an explosion, the starting lines of an engine will be damaged which can cause inability of engine starting. Note that, draining of water and oil in air bottles is very important and shall be done in regular basis (usually two times per day and especially before starting a diesel engine).

4.1.8 Control and Safety System Failure (Fault Tree Diagram A.1.8)

To control a diesel engine and to have a safe operation, several devices and equipment are utilized and attached to the engine. The control device is the engine *Governor* while the safety measures are different types of *Sensors* which prevent the engine from damages in emergency cases.

A governor handles adjusting the engine RPM by increasing or decreasing the rate of fuel pumping. This adjustment is done through a linkage called fuel rack that connects the governor to each cylinder fuel pump. By this system, an engine becomes self-controlled meaning that, the engine's governor receives the inputs from fuel rack and give the respond to fuel rack as well to tune the RPM.

As shown in Diagram A.1.8, a governor can fail either because of its rotational part's failure or due to faulty fuel rack that leads the governor to the improper response. In both scenarios, the governor cannot give an accurate respond to the fuel rack so the engine may get either over speed or slowdown due to high and low amount of fuel respectively. These cause the diesel engine to shut down in both cases and losing electrical power consequently. Failure of governor's rotational parts is not among this study focuses so; it is not developed in FTA. To prevent failure of fuel rack, one must consider lubricating the rack since this is a moving part that is prone to fatigue and wear. The in charge engineer of a watch shall check visually and lubricate all diesel engine's fuel rack to ensure their free movements.

Engine's safety devices are categorized to tow category. The first ones just raise an alarm for notifying the engineers. They include alarms of *High Cooling Water Temperature*, *High Exhaust Temperature,* and *Low Lubricating Oil Pressure*. The second group takes action automatically by itself to prevent engine damages. This group consists of *Over-Speed Trip*, of *Very High Cooling Water Temperature* and *Very Low Lubricating Oil Pressure* which lead the engine slow down/shut down.

An engine over-speed trip works independently and takes the input data from *Tachometer*. A tachometer can be mechanical or electrical which determines the engine RPM. Specifying an engine RPM in the electrical type of tachometer is done by sensing and counting the nominated points on the engine flywheel by an electronic eye. In a mechanical type of tachometer, a linkage connects a rotational part like crankshaft or flywheel to a meter which shows the engine RPM on a gauge. Once the tachometer senses an RPM, which is more than a pre-assigned number, a signal will be sent to the fuel rack to be pulled and shut the fuel pumping to stop the engine. Therefore, any faults in sensing of the engine RPM or the fuel rack responding, may be a cause of over-speed trip failure that may lead the engine to heavy breakdown. As the preventive action for over-speed trip failure, one should consider visual checking and lubricating the fuel rack in addition to examining the sensor or linkage of the tachometer.

Other safety devices either for raising alarms or doing engine slowdown/shutdown have a common operational procedure. They all consist of pressure or temperature transmitters that sense the engine exhaust temperature, cooling water temperature and lubrication oil pressure. These transmitters continuously read the data and send some electrical signals. The signals are received by automation and processing unit, and they will be compared to predetermined settings. Depending on deviation range of readings from settings, firstly, an alarm will be raised to make the engineers aware of some faults which happened in the engine. Secondly, if the engineers do not take a proper action to solve the problem, the reading deviation range will be increased which activate the engine's fuel rack by sending signals to slow down the engine automatically. If the problem still presents, the engine will shut down further.

As drawn in Diagram A.1.8, the problems which occur in alarm raising systems can be due to transmitter faults or processing unit. A transmitter may fail because of loss of electrical insulation or wires disconnection while a processing unit can face many different faults due to electrical or programming issues that are not the focuses of this thesis.

Nevertheless, safety reactions which are related to engine slowdown/shutdown can also fail due to improper or no respond of fuel rack. In the case of stuck or broken fuel rack, it cannot respond accurately to slow down or shut down the engine. This is why, lubricating the fuel rack plus frequent visual checking is important for ensuring the correct fuel rack response in the emergency cases.

In summary of this chapter, the diesel engine failure was analyzed through fault three analysis. The basic events which may cause the diesel engine failure were determined by considering varying relevant sub-systems and machinery. Now, one understands the different ways and possibilities which lead to the diesel engine failure.

CHAPTER 5 RISK EVALUATION OF DIESEL ENGINE FAILURE BY RISK MATRIX

The risk analysis of a diesel engine failure in a DP system was done in the previous chapter by the aid of the fault tree analysis. Once, one understands how a diesel engine fails and what are the failure root causes, he/she should proceed further to specify the risk value.

Now and in this chapter, the writer is going to evaluate the risk of diesel engine failure in a DP system class 1 to find out how critical that situation can be. The purpose of this chapter (risk evaluation) is determining the criticality of diesel engine failure based on its occurrence likelihood and severity of consequences.

Note: All the upcoming risk evaluations are subjective and are based on the writer's background knowledge and his risk perception.

As it is mentioned beforehand, in this thesis, the risk evaluation tool is the risk matrix that was introduced in Chapter 3.3. The main four aspects of the risk evaluation also were touched previously. They are people, the environment, asset and reputation and any risk shall be evaluated in accordance with them.

One part of a risk matrix is the likelihood of diesel engine failure which is constant. According to the writer's experience and available data, the probability of diesel engine failure is considered as *Probable,* which means 1.0E -1or 0.1 % probability of occurrence per year. Pursuant to the specified likelihood of occurrence, the risk now can be evaluated based on the severity of consequences and effects on different groups.

5.1 Risk Evaluation with Consideration of People

Once the diesel engines fail onboard a vessel, in addition to the loss of positioning and propulsion system, the vessel may go into blackout that affects all the onboard facilities. So, to determine the consequences of diesel engine failure with consideration of people, one shall think about all the possibilities and different scenarios in which the people can be influenced. For instance, some varying situations that can affect the people are mentioned as following:

- Loss of propulsion system causes the drifting of the vessel, especially, in a rough sea state. This is the reason of large vessel rolling/pitching which make the people seasick and hurt them.

- Loss of lightning can cause people hurting themselves. People injuries happen due to falling or clashing with objects since they do not have the proper vision.
- Ship collision may lead to some injuries depending on the intensity of the accident.
- In the worst-case scenario, if the vessel sinks or catch fire (which could normally happen after a collision), the consequences may be major injuries or even fatalities.

As can be seen in Table 5.1, the overall severity of consequences for the people in the case of diesel engine failure is determined as level 3 which is a major injury. As a result and by considering the probability and consequences, the value of risk appears in the cell D3 that shows major injury to the people. The D3 cell is in the red area and has the meaning of intolerable risk.

Table 5.1: Risk Evaluation of Diesel Engine Failure with Consideration of People

Likelihood / **Consequences**	Extremely unlikely (A)	Very unlikely (B)	Unlikely (C)	Probable (D)	Frequent (E)
No injury (1)	A1	B1	C1	D1	E1
Minor injury (2)	A2	B2	C2	D2	E2
Major injury (3)	A3	B3	C3	**Diesel Engine Failure** D3	E3
Single fatality (4)	A4	B4	C4	D4	E4
Multiple fatalities (5)	A5	B5	C5	D5	E5

5.2 Risk Evaluation with Consideration of Environment

For evaluating the risk of diesel engine failure that can affect the environment, the same procedure as above is followed. Some of the different situations which may cause environmental damages are listed as following:

- Fuel, oil or any other cargo pollution because of the rupture of vessel's tanks which happens due to collision in the loss of positioning situation.
- Spill of drilling mud, contaminated water or drilling cutting caused by drilling riser failure that takes place due to loss of positioning in the drilling operation.
- Hydrocarbon pollution because of production riser failure that occurs due to loss of positioning in the production operation.
- Hydrocarbon pollution because of hawser failure which happens because of loss of positioning in the FPSO-Shuttle tanker offloading operation.

Table 5.2 shows the evaluated risk of diesel engine failure that can affect the environment. The overall value of this risk falls into cell D5 that represents the catastrophic damage, and this is the highest level of environmental damage. In terms of severity, diesel engine failure can cause significant harms and negative global and national effects to the environment. This is intolerable risk since it appears in the red area.

Table 5.2: Risk Evaluation with Consideration of Environment

Likelihood / **Consequences**	Extremely unlikely (A)	Very unlikely (B)	Unlikely (C)	Probable (D)	Frequent (E)
No damage (1)	A1	B1	C1	D1	E1
Minor damage (2)	A2	B2	C2	D2	E2
Significant damage (3)	A3	B3	C3	D3	E3
Major damage (4)	A4	B4	C4	D4	E4
Catastrophe damage (5)	A5	B5	C5	**Diesel Engine Failure** D5	E5

5.3 Risk Evaluation with Consideration of Asset

Risk evaluation of diesel engine failure with consideration of asset, also follows the principals similar to the last two ones. To have a broad understanding, some cases in which the asset can be affected are mentioned:

- Ship collision is one of the major asset loss which may happen due to positioning system failure. This is because of the high cost of vessels from both CAPEX and OPEX points of view.
- Delay to start a planned operation due to lack of electrical power or positioning system can be costly for a company.
- Stopping an ongoing operation especially hydrocarbon production can be a heavy loss for an organization.

The finalized risk value for the case of diesel engine failure that may affect a company's asset is illustrated in Table 4.3. The evaluated risk is located to cell D4, which demonstrate the major damage that may cost the company over 1 million NOK. This is also in the red zone that shows an unacceptable risk.

5.4 Risk Evaluation with Consideration of Reputation

There is a discussion in the industry that says the company's asset includes the reputation as well. However, still many risk professionals separate those two aspects and evaluate the risk in both cases individually. By pursuing this method, some of the situations in which a company's reputation can be affected due to diesel engine failure are mentioned as following:

- Major injuries or fatalities can hurt the reputation of a company and cause negative effects on the personnel who are working and the one who wants to join the company. In this case, the company may face human resources and recruiting problems.
- Pollution occurrence has national or international influences depending on size and intensity of pollution. Challenging the governmental authorities and voluntary organizations are the issues which happen in the case of pollution.
- Too many emergencies and delays on a scheduled operations cause the company to lose the market.

- Large losses of personnel, damage to the environment and/or loss of asset will reduce the company's share value and cause higher interest rates for loans etc.

Table 5.4 illustrates the evaluated risk of diesel engine failure for an organization's reputation. It is not surprising anymore if we say the risk value for this case is placed in cell D5 that represents an international effect. This is the highest and most severe level of consequences, and clearly, it is not tolerable.

Table 5.3: Risk Evaluation with Consideration of Asset

Likelihood / **Consequences**	Extremely unlikely (A)	Very unlikely (B)	Unlikely (C)	Probable (D)	Frequent (E)
No damage (No cost) (1)	A1	B1	C1	D1	E1
Minor damage (Cost >100 k NOK) (2)	A2	B2	C2	D2	E2
Significant damage (Cost >500 k NOK) (3)	A3	B3	C3	D3	E3
Major damage (Cost >1 mill NOK) (4)	A4	B4	C4	**Diesel Engine Failure** D4	E4
Catastrophe damage (Cost >10 mill NOK) (5)	A5	B5	C5	D5	E5

Table 5.4: Risk Evaluation with Consideration of Reputation

Likelihood / **Consequences**	Extremely unlikely (A)	Very unlikely (B)	Unlikely (C)	Probable (D)	Frequent (E)
No effect (1)	A1	B1	C1	D1	E1
Minor effect (2)	A2	B2	C2	D2	E2
Major effect (3)	A3	B3	C3	D3	E3
National effect (4)	A4	B4	C4	D4	E4
International effect (5)	A5	B5	C5	**Diesel Engine Failure** D5	E5

The acquired results from the risk evaluation process could be shocking if they are directly mentioned at the beginning. However, since we started to do risk analysis by the aid of FTA, those results are now understandable and make sense. The FTA helped us to figure out the process of failure. It revealed all the actions and interactions of the systems and sub-systems which may lead to a failure. This is why; it is not weird when we say the failure of diesel engine can cause a catastrophe to the personnel, the environment and to the company.

Once the risk evaluation is done, the next and final stage will be the risk assessment. Until now, we have understood how a diesel engine can fail, what the consequences of its failure are, and how critical these consequences will be. In the next step, we need to determine and implement several preventive and risk reducing measures as barriers. This is necessary to prevent/mitigate the threats or/and consequence.

Depending on the risk value and its severity gained from the risk evaluation, the DNV recommends some criteria for applying barriers. Table 5.5 shows the requirements for exerting barriers in three different risk areas.

So far, we saw that the risk evaluations for the diesel engine failure resulted in intolerable risk in all four risk areas. Accordingly, in the next chapter, the appropriate barriers will be introduced, and the risk assessment procedure will be done by the aid of bow-tie analysis.

Table 5.5: Barriers criteria for the evaluated risk (DNV, 2003)

Evaluated Risk	**Barriers criteria**
Acceptable	Requires a minimum of one effective barrier in place for all threats
	Requires a minimum of one effective barrier (recovery measure) in place for each identified consequence
Tolerable (ALARP)	Requires a minimum of two effective barriers in place for all threats
	Requires a minimum of one effective barrier (recovery measure) in place for each identified consequence
	Requires a minimum of one effective control in place for each barrier failure/decay mode
Unacceptable	Requires a minimum of three effective barriers in place for all threats
	Requires a minimum of two effective barriers (recovery measures) in place for each identified consequence
	Requires a minimum of one effective control in place for each barrier failure/decay mode

CHAPTER 6 RISK ASSESSMENT OF DIESEL ENGINE FAILURE BY BOW-TIE ANALYSIS

In the previous chapter, the risk evaluation for a diesel engine failure was done. It aided to understand the criticality and severity of occurrence of a diesel engine failure. The completion of risk management process depends on the execution of final step (risk assessment) which is a combination of risk analysis and risk evaluation (as described in former chapters). In other words, to complete a risk management process, one need to determine several risk reducing measures to either prevent the happening of initial events (threats) or decreasing the negative effects of consequences.

Since the focus of this thesis is diesel engine failure which is a threat to loss of DP system class 1, only the barriers for the left side of bow-tie diagram will be determined and proposed. In other words, no barriers or preventive measures will be introduced on the right side of the bow-tie diagram (consequences side). The thesis will just name some possible consequences which may happen due to loss of positioning originated from diesel engine failure.

For doing the risk assessment, the bow-tie analysis method is chosen that was introduced in advance in Chapter 3.4.1. Also, to draw the bow-tie diagrams and to connect the different parts to show a visual risk picture, a free version of the software called ABT (Active Bow Tie) is used. The ABT is “a tool for displaying and improving hazard analysis and energizing safety management” ("Risk Support", 2014). The ABT software was programmed, developed and published by the *Risk Support*, which is a risk management consultancy company located in London, United Kingdom.

6.1 Bow-Tie Analysis of DP system Failure (Bow-tie Diagram B)

In this case, the loss of positioning was determined as the hazard while the failure of DP system is the top event. In Bow-tie Diagram B, the different threats which can be causes of DP system failure are shown. As it is shown in the FTA as well, the threats for the DP system failure are the failure of its varying sub-systems. In the right side of Bow-Tie Diagram B, the possible consequences of DP system failure are mentioned. For example, delay to start an operation, stopping an ongoing operation, vessel to vessel or vessel to platform collision and consequently, pollution can be the severe outcomes of the DP system failure.

As we discussed earlier, the power generation system is the most important system onboard a vessel and accordingly, this is the vital sub-system of a DP facility. Further, the diesel engine is the heart of power generation system since it works as a prime mover. Thus, in order to importance and interlock between the diesel engine and DP system and other shipboard machinery, the bow-tie analysis of diesel engine is going to be done.

6.2 Bow-Tie Analysis of Diesel Engine Failure (Bow-tie Diagram B.1)

In the Bow-Tie Diagram B.1, failure of a diesel engine is shown as the top event while the loss of electrical power (blackout) is the hazard. As discussed in Chapter 4, a diesel engine consists of eight individual systems that their proper working condition keeps a diesel engine operational. Therefore, each and every of these systems failure can lead the diesel engine to fail. The sub-systems of diesel engine are *Mechanical Components, Fuel System, Lubricating System, Cooling System, Scavenge and Exhaust System, Starting System, Auxiliary System and Control and Safety System* that will be analyzed by aid of bow-tie method in the forthcoming sections.

Moreover, on the right side of Bow-Tie Diagram B.1, some consequences which are probable to happen in the case of diesel engine failure, are illustrated and described as following.

DP System Failure: As one can see, loss of the DP system is one of those consequences. As introduced, different parts and sub-systems of a DP system works by the electrical power like position and heading reference systems, computers, and even thrusters. Therefore, without the electrical power that is the driver of DP system's devices, the DP system cannot be operational.

Loss of maneuvering ability: This is another consequence of diesel engine failure. This is because of propulsion system failure that fails in the absence of electrical power. Many of the axillary machinery like different pumps that are used in the main propulsion system are driven by an electrical motor. Therefore, without electrical power neither those pumps nor the main propulsion can work.

Failure of Navigational Aids: Some systems like GPS, NAVTEX, RADAR, ARPA, GMDSS are installed onboard a vessel and are used for the navigational purposes. These systems do work directly by electrical power and will shut down immediately in the case of a blackout.

Operation Stoppage: Due to lack of electrical power, all the machinery which are driven electrically and used in particular vessel operation will be stopped. For example, cranes, derricks, winches, ballast pumps, and hatch covers can be some of them.

Loss of Living Quarter Facilities: There are many appliances and devices which work directly by electricity in a vessel's living quarter. The domestic water system for drinking and washing, electrical stoves (hot plates) for the cooking purpose in the galley, and entertainment facilities like TV and players, are some the accommodation facilities that fails in the case of blackout.

Communication Devices Failure: The devices which are utilized onboard a vessel for global communications, can only be operational in the presence of electricity. The Telephones, The Internet, and VHF are some examples that some of them need to get a connection with International Maritime Satellite Organization (INMARSAT).

Loss of Lighting: This is the first sensible effect of diesel engine failure. Loss of lighting can be very dangerous in terms of the vessel and her operation. Also, the personnel can be very affected since they do not have the proper view, and they make wrong decisions.

6.2.1 Mechanical Components Failure (Bow-tie Diagram B.1.1)

6.2.1.1 Primary Barriers

Survey in Proper Intervals: All the mechanical components especially the rotational ones including main bearings, journal bearings, connecting rod, camshaft, and crankshaft, shall be surveyed. The representative of classification society normally does the survey. The survey should be done in the appropriate time interval to ensure the good condition of components at all the time.

Running the Engine at Allowed Temperature: The engine operator (engineers) shall not run the engine at higher allowed temperature. The high temperature of the engine is shown by the cooling water or exhaust temperature that in both cases, either the problem must be rectified or the engine will shut down.

Running the Engine with Minimum Wear: Since, these are rotational components with high-speed operation, one shall reduce the rate of wear. This can be done by ensuring a good lubricating system. The engine lubricating oil pressure is important to be monitored.

Running the Engine at the Allowed Speed: Once the engine is driven over the speed limit, the risk of fatigue and breakage will increase. So, one shall make sure about the proper speed of the engine.

Reducing fatigue rate: Failure due to fatigue is a common fault for all the systems and components of a diesel engine. The fatigue itself is caused mostly due to vibration. Thus, reducing the fatigue rate and its decay modes which is excessive vibration, in addition to secondary barriers, are just mentioned once to prevent from repetition.

The components are prone to fail due to fatigue especially once they have to move. Therefore, the main reason of fatigue which is vibration should be minimized.

6.2.1.2 Barrier Decay Modes

Inappropriate Planning: To survey the mechanical components of an engine, the engine must be dismantled and will become out of operation. Thus, the right time shall be predetermined for doing a survey. For example, the time when the vessel is not in operation or another engine is available as a backup.

Irresponsible Surveyor: Occasionally, the official who is responsible for surveying is not professional. So, the approval certificate may be issued even the condition of engine components are not satisfactory.

Unprofessional Vessel's Engineer: In some cases, in order to reduce the working load or laziness, the vessel engineers insist to get the approval certificate from the surveyor by cheating or bribing without dismantling the engine and checking the components.

Water Cooling System Failure: This causes the engine to be run at higher than allowable temperature. It will be discussed in detail in upcoming sections.

Engine Overloading: This is another cause of high engine temperature. Overloading can happen due to different problems that force the engine to works at higher speed and consequently higher temperature.

Lubricating System Failure: This can results in higher rate of wear in the engine which may end up with stuck or broken components. It will be discussed in detail in upcoming sections.

Excessive Vibration: In general, a moving system especially an engine has some amount of vibration which is normal and is considered by the manufacturer in the design and installation phase. However, the excessive vibration is the thing that definitely increases the fatigue rate of components and was not taken into account beforehand.

6.2.1.3 Secondary Barriers

Vessel Schedule Consideration: To ensure proper timing for the engine survey, one should consider the vessel schedule. The vessel schedule shows the future operations, durations, and locations of the vessel. Therefore, engineers can plan for the engine survey in the free time or less critical time of the vessel.

Contacting the Classification Society: For engine surveying, the classification society also must be informed. This is because of booking the time and request for sending surveyor. So, a proper planning shall be done in cooperation with classification society.

Contacting the Port Authority: In the case of engine surveying, the local port authority must be also informed. The vessel must be given a mobilization letter before preparing the engine for the survey. This is because of safety issues that may affect the vessel during the surveying. When the engine is dismantled and is out of operation, the capability and redundancy of vessel are low. Thus, the ports authority has to be informed to prepare the facilities which may be needed in the case of emergency.

Professional Personnel: Hiring the professional and experienced personnel has a positive effect on the proper timing of engine survey.

Hiring reputable Classification Society: Once a company deal with a globally famous and reputed classification society, it can be sure about the quality of services that are offered by that society, especially for surveying operations.

Surveying at the reliable port: Having a good plan to do the surveying in reliable port (country), can prevent some problems like bribing or negligence.

Contribution of Vessel's Engineers in Survey: In the case of irresponsible or negligent surveyor, the vessel's engineers shall contribute to the survey and make sure about the good condition of engine components.

Personnel Training: Training the responsible engineers can affect the survey positively. Having some fresh and inexperienced engineers onboard cannot bring the high quality of the vessel and company, since the survey operation needs some former experience or at least special training.

Hiring Qualified Personnel: This also can be another solution to prevent mistakes and negligence during the survey. As mentioned, the survey activity demands the experiences and trained engineers.

Proper Electrical Load Sharing System: It can be a barrier for preventing from engine overloading. The load sharing system is the electrical mechanism that always balances the amount load between diesel generators. In the case of starting and stopping of machinery which consume electrical power, this system distributes the load to all the diesel engines equally. Otherwise, one diesel engine gets less amount of load while the other becomes overloaded.

Good Condition of Governor: For prevention from overloading, also the engine governor must work properly to adjust the RPM in accordance with taken load. By starting and stopping the electrical consumers, the engine RPM is changed. This is the duty of the governor to maintain the engine speed within the allowable limit.

Good Condition of Fuel Rack: As described in Chapter 3, the governor has a transmission to/from fuel rack. Thus, if the fuel rack does not work appropriately, the engine can become overloaded due to the wrong amount of supplied fuel.

Good Condition of Over Speed Trip: As a safety device, the over speed trip can handle the emergencies by shutting down the engine. When the engine gets over speed, it will be overloaded. So, the over speed trip can be one of the barriers for prevention from engine overloading.

Professional Engineers: The experienced or well-trained engineers know how to operate and run an engine to prevent the engine overloading. Also, in the emergency cases, they can swiftly distinguish the signs of overloading and take the right reaction.

Tightening Engine Bolts: The loose engine's bolts especially for the moving parts make excessive vibration. Thus, the engineers should check the tightness of bolts based on predetermined torque. Among these bolts, some like cylinder head bolts, main and journal bearings bolts are really important.

Using the Resilience Mountings for Engine Foundation: Normally, the engines have some vibration dampers called resilience mountings on their foundation. They are assembled during engine installation, however, depending on engine's running hours and external conditions, these dampers need to be renewed or replaced.

Using Dampers: In some situations when the engine must be operated even with excessive vibration, the engineers can use the temporary dampers for minimizing the vibration. These dampers can be just ordinary support bars that are welded or attached to the engine from one side, and to the walls or fixed structure on the other side. The temporary dampers can hold the engine in position and prevention from vibrating.

6.2.2 Fuel System Failure (Bow-tie Diagram B.1.2)

6.2.2.1 Primary Barriers

Proper Performance of Attached Pump: The fuel pump which is attached to a diesel engine is a go-between to link the auxiliary fuel system to the engine fuel system.

Proper Performance of Unit Pump (Cylinder Pump): The fuel that is going to burn in the engine shall be pressurized beforehand by cylinder fuel pumps.

Proper Performance of Fuel Injectors: for having a good burning into the combustion chamber, the fuel must be atomized which is done by injectors.

6.2.2.2 Barrier Decay Modes

Failure of Attached Pump's Components: The attached pump must be in a magnificent condition. Accordingly, all the components like impeller and shaft shall be in sound condition to make the fuel flows . Otherwise, the engine will be stopped.

Failure of Unit Pump's Components: If the cylinder's pump does not work properly, the fuel cannot enter the combustion chamber due to lack of pressure for triggering the injectors. Thus, the cylinder pump's components such as barrel and plunger must be healthy.

Failure of Injector's Components: In the case of the bad condition of injector's components, either the fuel does not enter the chamber or enters in the liquid phase that both are undesired.

6.2.2.3 Secondary Barriers

Ensuring the Fuel Flow from the Fuel Axillary System: The fuel shall be supplied from the axillary system for prevention from of attached pump dry working, which leads to sealing failure.

External Damages Prevention: The attached pump should be preserved from external damages like dropped objects. Otherwise, the casing and joints can be harmed.

Corrosion Prevention Methods: The outer area (casing) of attached pump is vulnerable to corrosion. So, some methods like painting can be helpful as a preventive action.

Ensuring the Fuel Flow from Attached Pump: To prevent from seal damage in the unit pump, the fuel must be supplied from attached pump to prevention from working dry.

Prevention from External Damages: The cylinder pumps also can be damaged by external impacts so, they need to be protected by some covers for example.

Corrosion Prevention Methods: Since the cylinder pump's outer surface has contact with ambient, the casing can be corroded. Thus, painting can be a good means for protection.

Injectors Pressure Testing: This is a way for ensuring the good condition of fuel injectors. The fuel injectors shall be pressure tested frequently to check whether the opening pressure is in the limit or needs adjustment.

Injectors Leakage Testing: The injectors also must be checked by leakage test to confirm the fuel atomization. This is to prevent from entering the fuel into the combustion chamber in the liquid phase that leads to the bad combustion.

Testing Injectors Angle of Spray: To have a proper combustion, the injector shall spray fuel into the chamber in an accurate and predestined angle. This test shows whether the angle of spraying is correct to send the fuel to the right location for burning.

6.2.3 Lubricating System Failure (Bow-tie Diagram B.1.3)

6.2.3.1 Primary Barriers

Proper Performance of Attached Pump: The lubricating attached pump is an inductor between the auxiliary lubricating system and engine components which need lubrication.

6.2.3.2 Barriers Decay Modes

Failure of Attached Pump's Components: If the components of attached pump fail, the oil does not flow, and the engine will face serious problems due to friction.

6.2.3.3 Secondary Barriers

Ensuring the Oil Flow from Lubricating Axillary System: We need to make sure the proper oil flow from the axillary system. Otherwise, the attached pump operates in a dry condition, and its seal will be damaged.

Prevention from External damages: The attached pump especially its casing must be protected from external impacts like dropped object.

Corrosion Prevention Methods: The attached pump is in the ambient condition so it may be corroded. Thus, it shall be protected for example by painting the casing.

6.2.4 Water Cooling System Failure (Bow-tie Diagram B.1.4)

6.2.4.1 Primary Barriers

Proper Performance of Attached Pump: The attached pump acts as an inductor between the cooling auxiliary system and the engine's parts which requires to be cooled.

6.2.4.2 Barriers Decay Modes

Failure of Attached Pump's Components: The components of attached pump like impeller and shaft shall be in a good condition to allow the pump to make the water flow.

6.2.4.3 Secondary Barriers

Ensuring the Water Flow from Cooling Auxiliary System: The fresh water must be supplied from the auxiliary system to the attached pump. Otherwise, the pump works dryly and it seal will be damaged.

Prevention from External Damages: The attached pump shall be protected from external impacts to prevent from casing damages. It can be done by placing a cover.

Corrosion Prevention Methods: The attached pump is in the ambient condition so it may be corroded. The painting can be a real remedy for the pump casing corrosion prevention.

6.2.5 Scavenge and Exhaust System Failure (Bow-Tie Diagram B.1.5)

6.2.5.1 Primary Barriers

Proper Performance of Turbocharger: The turbocharger shall work properly by absorbing the energy of exhaust gas to do the supercharging for providing the adequate amount of air for combustion.

Proper Performance of Intake and Exhaust valves: The opening and closing orders of these valves in addition to their physical condition are important. This is to allow the air to come into the combustion chamber plus to send the exhaust gas out of the chamber.

6.2.5.2 Barriers Decay Modes

Failure of Turbocharger's Components: Any faults in the turbocharger components like blades, bearings or shaft, leads to failure and malfunction of the turbocharger.

Overheating: Lack of cooling water, improper cooling water temperature, and bad combustion can be causes of intake or exhaust valves overheating. Consequently, the valves overheating is a cause of fatigue and valves failure.

6.2.5.3 Secondary Barriers

Maintaining the Turbocharger Cooling Water: Overheating can cause damages to the blades of turbine side of the turbocharger.

Maintaining Turbocharger Lubricating Oil: Lack or shortage of lubrication damage the bearings of the turbocharger in both turbine and compressor side.

Maintaining the Engine Cooling Water: A sufficient amount of fresh water with proper temperature can prevent the intake and exhaust valves from overheating.

Maintaining the Engine Lubrication: The proper flow of lubricating oil is essential for intake and exhaust valves failure prevention due to friction.

6.2.6 Starting System Failure (Bow-Tie Diagram B.1.6)

6.2.6.1 Primary Barriers

Proper Performance of Air Distributor: The airflow which comes from the air auxiliary system is distributed to different engine cylinder by the aid of air distributor for the purpose of starting.

Proper Performance of Air-Starting Valves: The air-starting valve at each cylinder shall open the way to allow the air reach the top of the piston to push it down and turn the engine.

6.2.6.2 Barriers Decay Modes

Getting Stuck: The air distributor and starting valves may get stuck and fail during the operation. This can happen due to lack of lubrication and presence of rough particles that come by air.

6.2.6.3 Secondary Barriers

Maintaining Engine Lubrication: Having a good lubrication for both air distributor and air starting valves prevents from getting stuck.

Corrosion Pretension Methods: Air distributor has an outer surface that is in ambient. It is corrosion prone and shall be protected by painting. Further, its inner area is also vulnerable against corroding due to moisture in the coming air. Thus, in addition to the dried air, the presence of lubricating oil can mitigate corrosion.

6.2.7 Auxiliary Systems Failure (Bow-Tie Diagram B.1.7)

6.2.7.1 Primary Barriers

Proper performance of Fuel System: The fuel auxiliary system must work in a good way to purify and transfer the sufficient amount of fuel from different ship's tanks to the diesel engine.

Proper Performance of Lubricating System: The lubricating auxiliary system handles purification and transferring the proper amount of oil from the storage tank to the diesel engine.

Proper Performance of Water Cooling System: For maintaining the diesel engine working temperature within the allowed limit, the water cooling auxiliary system shall provide the right amount of freshwater with the right temperature to the diesel engine.

Proper Performance of Air System: The diesel engine cannot be started without the correct volume of air that is supplied by the air auxiliary system.

6.2.7.2 Barriers Decay Modes

Fuel Transferring Pump Failure: By failure of transferring pump, the fuel cannot be transferred from bunkering tanks to the engine room thanks (settling or service tanks). Consequently, there will be no fuel for purification and supply to the diesel engine.

Fuel Filters Clogging: Because of impurities and solid particles in the fuel, there is a high possibility of filter clogging before purification. It can be a cause of reduction or stoppage of the fuel flow.

Fuel Purifier Failure: Failure of fuel purifier does not affect the operation of diesel engine immediately. The fuel can be supplied directly from the settling tank to the engine in the case of purifier failure. However, this should be done only in the critical situation when the engine must be operated by any chance. Otherwise, due to impurities and harmful content of the fuel, the engine will be highly damaged in short-term.

Oil Transferring Pump Failure: In the case of failure of oil transferring pump, the right volume of lubricating oil cannot be transferred to the engine’s sump and consequently the engine will shut down due to low oil pressure.

Oil Filters Clogging: During the lubrication of different parts of a diesel engine, the oil is contaminated by the fine metallic particles of the engine. This is why the oil has to be purified otherwise particles in the oil can be the cause of filter clogging.

Oil purifier Failure: The Oil purifier failure does not have a sudden effect on the operation of a diesel engine. However, it will damage the engine after some while if the lubricating oil is supplied without purification.

Freshwater Circulating Pump Failure: This failure is a cause of freshwater circulation cease which leads to the lack of cooling in the engine and high temperature and shut down consequently.

Cooler Malfunction: Any fault in the cooler can result in a failure of the freshwater circulation. This can happen either by affecting the freshwater side directly or by influencing the seawater which is medium for cooling the freshwater.

Air Compressor Failure: Once the air compressor fails, the sufficient volume of air cannot be pressurized and stored in the air reservoir. Therefore, there will be no enough air for starting the diesel engine.

Air Reservoir Failure: Any faults that lead to the air leakage in the air bottle, reduces the volume and pressure of air which is needed for engine starting.

6.2.7.3 Secondary Barriers

Electrical Motor Insulation Resistance (IR) Test (Megger Test): To prevent from short circuit and failure, all the electrical devices especially motors must be checked by insulation resistance (IR) test which is generally called megger test. The IR test shows the condition of insulation between two conductive components as such the higher resistant indicates the better insulation. To avoid repetition, the IR test will not be covered for other electrical sub-systems. However, it is one of the main secondary barriers for electrical motors failure.

Ensuring Fuel Feeds from Tanks: Checking the lines and valves to be in the correct condition to allow the fuel reaches the transferring pump from the tanks is essential. Otherwise, the pump works dry and will become faulty.

Good Quality of Received Fuel: If the vessel engineers or the company consider the quality of fuel which is going to be ordered, the risk of filter clogging will be decreased in addition to less consideration for purification and treatment. Usually, the fuel quality check is done by sampling during the bunkering. The samples will be sent to the lab for testing.

Cleaning the Filters Frequently: Cleaning the fuel filters at the proper intervals can be very effective in preventing clog.

Ensuring Feeding of Sealing and Operating Water: To have a good purification, the sealing, and operating water are must. The purifier is sealed by water which prevents fuel leakage. Also, the operating water is needed for washing the fuel and separating unwanted content.

Proper Number of Separation Disks: The number of separation disks is vital to have a real purification. Otherwise, either the resulted fuel is not clean enough or the outlet fuel rate is reduced.

Ensuring the Flow of Oil from Tanks: It prevents the pump from operating dry.

Good Quality of Received Lubricating Oil: It follows the mentioned procedure for prevention from filter clogging.

Ensuring Flow of Freshwater from Expansion Tank: It follows the mentioned principal to prevent the pump from working dryly. Also, the freshwater must be supplied to the cooler as well for being cooled by the aid of seawater. This can be done by prevention from leakages and filling up the expansion tank to maintain the volume of freshwater all the time.

Frequent Cleaning the Cooler Pathways: The pathways of the cooler, especially in the seawater side become clogged due to scaling. Thus, by dismantling the cooler and cleaning those pathways, one can be sure about sufficient flow of sea/fresh water and good heat transferring which leads to the high cooler efficiency.

Maintenance of Seawater Pump: The seawater pumps have the critical role in the water cooling system. As mentioned in the FTA section, the seawater is circulated by the aid of seawater pumps to cool the freshwater. Therefore, the proper condition of seawater pumps is important, and their monitoring and maintenance shall be taken into account.

Frequent Cleaning of Sea Chest: The vessel's sea chest is the main port for providing seawater. It is usual that the sea chest becomes clogged by marine growth or the ice. In the case of clogging, the flow of seawater dramatically decreases, and cooling system will be affected. Thus, cleaning the sea chest on a regular basis also, applying the steam for prevention from icing, are the barriers for sea chest clogging.

Maintenance of Compressor's Mechanical Components: To avoid sudden failure of the air system by air compressor failure, all the compressor's components including moving parts must be properly maintained. This shall be done by vessel engineers and according to the manufacturer instruction manual.

Frequent Draining the Oil and Water: The moisture in the air and the oil which is carried over by air from compressor settle at the bottom of air reservoir. The oil and water shall regularly be drained to avoid damages to the starting system.

Maintenance of Inlet, Outlet, and Relief Valves: All the valves which are placed on the air reservoir must be maintained for prevention from any leakage.

Prevention from External Damage: One should consider the protection of air reservoir and its mountings from dropped objects and other external impacts. This shall be done for prevention from rupture and leakage.

6.2.8 Control and Safety System Failure (Bow-Tie Diagram B.1.8)

6.2.8.1 Primary Barriers

Proper Performance of Temperature and Pressure Reading Devices: To have a good control and engine monitoring, the first step is collecting the real engine data like pressure and temperature. Therefore, the reading devices that are transmitters must be in a proper condition.

Proper Performance of Processing Software: The collected data was sent to a computer with the especial software for processing. The processing software shall works properly to analyze the gathered data.

Proper Performance of Engine's Governor: Since the governor is the device to control the engine speed in different loads, it must be in perfect condition.

Proper Performance of Over Speed Reading Device: In the case of governor failure, the over speed trip device must be activated to prevent the engine from major damages.

Proper Performance of Fuel Rack: This is the final and direct mechanical element for doing any speed control on the engine such as decreasing or increasing the RPM in addition to the engine shutting down.

6.2.8.2 Barriers Decay Modes

Transmitter Failure: If the transmitters fail, the engine data cannot be collected for processing or they will be unreliable.

Computer Failure: Due to the software or hardware faults, the processing computers may fail.

Governor's Components Failure: The governor comprises several small components with fine clearances. So, it is possible that those components fail due to high running hours and poor maintenance.

Tachometer Failure: If the tachometer fails, the right reading for the engine RPM cannot be collected. So, there is a possibility to over speed trip device is not activated due to wrong RPM reading.

Fuel Rack Getting Stuck: The fuel rack may get stuck or totally break, so the fuel controlling orders cannot be applied to the engine.

6.2.8.3 Secondary Barriers

Transmitter Insulation: Transmitter should have a high insulation to prevent from failure or to read wrongly. This can be checked by IR test frequently.

Transmitter Calibration: To decrease the tolerances and possibility of error, the transmitters must be checked and calibrated on a regular basis.

Prevention from External Damages: The transmitters, as well as fuel rack, are damage prone due to external impacts like dropped object. Thus, they shall be protected by some cover, or one should consider his/her surrounding while handling the objects.

Computer's Software Updating: The computer's software shall be updated or upgraded time to time for increasing the speed of processing or refreshing the computer's memory.

Proper Default Setting of Computer: The people who work with the computer (vessel's engineers) should define an appropriate setting for the default adjustment. This adjustment can be changed base on engine condition or the vessel operation.

Governor's Components Lubrication: The governor lubrication is critical to prevent from its components failure. The oil level of governor must be in a limit all the time and shall be checked by responsible engineer in daily routine.

Governor Adjustment: As it is mentioned about the fine clearances of governor's components, some critical adjustment shall be done to ensure the proper working of the governor. Normally, these adjustments are done by the manufacturer specialist.

Lubrication for Mechanical Tachometer: If the tachometer is the mechanical type which is a linkage, its lubrication must be considered to avoid the failure.

Proper Insulation for Electrical Tachometer: If there is an electrical type of tachometer, its insulation is really important to prevent the failure. Its insulation should be checked by IR test.

Fuel Rack Lubrication: The lubrication of fuel rack is one of the significant duties that a responsible engineer must do every day. This is essential for prevention from getting stuck or a breakage.

6.3 Bow-Tie Analysis of Power Generation System (Bow-Tie Diagram B.2)

As it was mentioned previously in different sections of this thesis, the diesel engine is the heart of a vessel. It works as a prime mover for generating electrical power that is essential for keeping a vessel alive for doing her operations. However, the diesel engine is one part (sub-system) of power generation systems. There are also other sub-systems and parameters which must work properly to generate, distribute and manage the electrical power. The combination of those parameters and diesel engine provides the sufficient and reliable electrical power which is consumed by the entire vessel's machinery, especially the DP system as the major electrical consumer.

As the last risk assessment case in this thesis, the writer would like to focus on the power generation system as a single system. The writer intends to consider other important factors (except the diesel engine and the parameters which are mentioned previously) to have a safe, reliable and redundant power generation system.

6.3.1 Primary Barriers

Planned Maintenance: Stablishing a scheduled maintenance system called planned maintenance can be very helpful for maintaining the different sub-systems and components of the power generation system in the operational condition. By using a planned maintenance system, the machinery is checked and examined in a predetermined time before they fail. The planned maintenance is usually done by dismantling the machinery, inspecting and then repairing if it is necessary.

Condition Monitoring: This is another type of maintenance that has some advantages in comparison with the planned maintenance. By applying the condition monitoring, the operational condition of the machinery is monitored continuously. In this method, the machinery is going to be dismantled and inspected if some signs which may cause the future failure are indicated. Otherwise, the machinery is allowed to continue its function with the current condition. By condition monitoring, the unnecessary dismantling and repair that is costly for the company is avoided.

Design Improvement: The betterment in the design of machinery and systems is beneficial for having a more efficient and reliable system. The design improvement can bring many benefits to the power generation system such as diesel generators with higher capacity of producing electrical power, reduction in the size and dimensions of diesel generator with the same capacity, the smarter control and automation system and etc.

Increasing the Redundancy: The power generation system can be more redundant when there is a backup system. For example, the numbers of diesel generators can be added to the system, or capacity of the UPS and emergency generator can be increased.

6.3.2 Barriers Decay Modes

Wrong Time Planning: The planned maintenance can be affected by the wrong timing for dismantling and repairing the machinery. Unnecessary maintenance is costly in terms of spare parts and manpower. Also, during the unnecessary maintenance the healthy parts of the machinery may be damaged.

Wrong Technical Procedure: The planned maintenance also can be affected by following the wrong repairing procedure.

Wrong Tools: Using the wrong or unsuitable tools affects the repairing of machinery by damaging the components.

Lack/Shortage of Spare Parts: The maintenance and repairing process of machinery cannot be done if the right and sufficient numbers of required spare parts are not available onboard a vessel.

Fault in Processing System: To do the condition monitoring, a processing system is required to show and process the condition of machinery. Once the processing system becomes faulty, the condition monitoring is affected and fails.

Fault in Data-Logging Instruments: The devices which collect the machinery data and sent them to the processing system may become faulty and result in the improper condition monitoring.

Wrong Interpretation of Data: The data which is gained from machinery and is shown by processing system, shall be interpreted properly by the professional engineer to decide whether the machinery should be dismantled for repairing or not.

Human Errors: This is a factor that may affect any systems during different operations. Despite having professional and trained personnel, in some specific situations, the personnel take the wrong actions that can be causes of the system failure or accident.

Inexperienced Client Company: If the company as a client does not have the sufficient experience and knowledge about the specific system like power generation, it cannot order and ask for the best design for that system. Thus, easily the company and consequently the operation suffer from poor design of the system.

Unprofessional Contractor Company: The contractor company, who becomes responsible for doing the design phase or design improvement, shall be professional in that particular task. Otherwise, the outcome will not be as efficient and suitable as the client wants.

Cost Deduction: In several cases, too much emphasis on the cost deduction by the company can lead to lowering the quality and efficiency of the system in the design phase.

Choosing an Improper DP class: As introduced previously, each DP class has its own requirements that shall be satisfied. If the company chooses the lower DP class for the vessels, the redundancy of the system will be affected. Further, the systems on the vessel will not be safe and reliable in accordance with her operation.

Weak Safety and Risk Management System: For analyzing and assessing different risky scenarios and for implementing the measures to prevent the incidents/accidents, the system of risk and safety management in a company must be strong and dependable.

6.3.3 Secondary Barriers

Coordination between Office Personnel and Vessel Crews: This can avoid many problems that may happen for the time planning of maintenance.

Considering the Running Hours of Machinery: Normally, in a planned maintenance, the machinery is dismantled for examining and repairing based on their running hours which are proposed by manufacturers.

Trained Personnel: The availability of trained personnel is an important barrier for different job tasks failure. For the right time planning, following the correct technical procedure, using the proper tools and spare parts, the trained people are highly required.

Reading the Machinery's Instruction Manual: For the machinery maintenance,

Consulting with Manufacturers: In the case of lack of information for repairing and overhauling, the manufacturer manuals need to be carefully studied or they need to be contacted for consultation.

Proper Supply Management: By establishing a good supplying system possibility of lack/shortage of spares parts will be reduced.

Using the Reliable Products: By purchasing and using the well-known products, the failure rate will be reduced. It can be done by referring to the previous similar experience in addition to dealing with trustworthy brokers.

Proper Installation: Many of the failures in a system are caused by improper installation. The excessive vibration that leads to the fatigue is the main consequence of inappropriate installation.

Professional Personnel: Hiring the professional personnel who have had the similar expertise in their former carriers has a significant positive effect on different tasks and phases of operation.

Training the Personnel: In the case of hiring the fresh graduates or doing some tasks which are not practiced before, the company shall provide the training facilities to give the depth practical knowledge to the personnel. Furthermore, the training should offer to the crews if the new version of the machinery is brought to the operation.

Preparing the Checklist and Standing Orders: This can prevent human error in critical situation. This allows personnel to follow the prepend orders in the case of emergency and make the right decision under pressure.

Consulting with Partners and Consultant Companies: If the client company does not have the sufficient experience to order the right and required design specifications, it needs to consult with its partners or consultant companies to get the right choice.

Carry out a Tender: To find out the valid company as the contractor, the design project can be announced through a tender. This may help to find the right candidate in accordance with cost and time.

Investigation and Company Background Check: Another way to choose the right company to depute the tasks is to perform an inquiry and check the company background, particularly with the similar issues.

Detailed Cost Effective Analysis: It can be a barrier for the occurrence of unnecessary cost deductions that harm the efficiency and quality of the system in the design phase.

Proper Budget Management: Following a systematic and efficient program for managing the company budget gives the possibility of tracking the capital which shall be invested in the necessary aspects. Therefore, this is helpful for preventing the dispensable cost deductions.

Consulting with Classification Societies: This helps the companies to choose the right DP class for their vessels. Consequently, the specifications of sub-systems like power generation will be determined to fulfill the DP class requirements.

Following the IMO Rules and Regulations for DP Vessels: This is another way to assure the appropriate DP class for a vessel. Nevertheless, the classification societies themselves develop their rules base on the IMO regulations.

Coordination between Management and Personnel: This is very useful to have a sound system for safety management. Asking for other's ideas, meeting the people in different departments, sharing knowledge, and accepting contribution of the low-ranking staff, lead to the coordination between management and personnel.

CHAPTER 7 CONCLUSION AND RECOMMENDATIONS

7.1 Conclusion

The main objective of this study was to demonstrate how a slight problem in an ordinary component of a vessel's system can be the cause of a major failure in a Dynamic Positioning (DP) system and consequently lead to a catastrophe. This thesis shows the importance of the slight faults in the secondary components that are mostly ignored in the real situation in the offshore oil and gas industry and that could lead to the catastrophes.

The methods implemented to reach the goal mentioned above have originated from the risk management concept. The methods were then applied to the writer's subjective technical knowledge of the specific systems.

For that purpose, in the first step, the DP system with its different sub-systems and their operational aspects was introduced. In accordance with the criticality of various sub-systems, which compose a DP system, the power generation was chosen as the most vital system onboard a vessel. The diesel engine was selected to be studied due to its role as the utmost significant element and heart of the power generation system.

In the second step, an overview of risk management principals was mentioned. Accordingly, the risk management concept was divided into three sections: risk analysis, risk evaluation, and risk assessment. The basics of these three parts were described and a method was chosen for performing each of them.

Thereafter, the risk analysis of diesel engine failure was done. The chosen technique was Fault Three Analysis (FTA) with the aim of identifying the basic events and root causes of diesel engine failure. However, since a diesel engine works in conjunction with some auxiliary systems, the root causes of failure can vary depending on the type and role of those auxiliary systems.

Subsequently, the risk of diesel engine failure has been evaluated by use of risk matrix. The risk evaluation was implemented with consideration to four major areas: people, environment, asset, and reputation. On the basis of the probability of occurrence and severity of the consequences, the results have shown that failure of diesel engine possesses a high risk in the four areas mentioned above. The risk level of diesel engine failure was characterized as unacceptable and intolerable risk. Therefore, risk-reducing measures must be applied.

Therefore, the risk of diesel engine failure was finally assessed by the bow-tie method to provide a visual risk understanding. The bow-tie technique allows the visualization of the whole procedure of risk management in one picture and provides a helpful basis for decision-making. The bow-tie diagram consists of diesel engine failure as the top event in addition to different consequences and threats. The bow-tie analysis allows insertion of different barriers as risk reducing measures. Several primary and secondary barriers were suggested to avoid the occurrence of various threats, which could be the causes of diesel engine failure.

In conjunction with diesel engine failure possibilities, numerous cases were studied in the discussion section. In this section, the seawater cooling auxiliary system is selected (as a sample of different cases that were analyzed) to provide an understanding of a complete process of diesel engine failure and consequently, DP system failure and occurrence of a catastrophe.

The FTA has shown that the accumulation of marine growth and icing are examples of root causes of diesel engine failure through the failure of the seawater cooling system. Icing and accumulation of marine growth can make the vessel’s sea chest clogged and prevent the entering of seawater flow to the vessel. Due to lack of seawater, the freshwater that is responsible for cooling the diesel engine cannot be cooled by the seawater in the heat exchanger. Thus, the freshwater temperature increases and consequently, the temperature of the diesel engine increases which leads to engine failure by high temperature shutdown safety action. The blackout occurs by diesel engine shutdown, and the DP system fails due to no electrical power. Due to loss of the positioning system, a catastrophe such as collision or oil pollution may eventually occur.

In the bow-tie analysis section, some barriers were suggested by the writer for the case mentioned above to prevent the occurrence of the threats and their decay modes. The following are some of the proposed barriers: cleaning the sea chest on a regular basis, availability of second sea chest, preparation for redirecting the seawater flow from the clogged sea chest to the standby one, applying steam (through steam pipes) to the sea chest to prevent icing in the cold area.

In the conclusion we shall emphasis that every possibility and cause of diesel engine failure must be taken into account, particularly since there are many interactions between the diesel engine and other systems/machinery. One should not underestimate and ignore any simple fault that may seem irrelevant to the diesel engine failure. Furthermore, different machinery onboard a vessel has different engineers in charge; all the engineers and crews must not only be familiar with their own job tasks, but should also be informed about others' duties. This allows engineers to realize the importance of their assigned machinery, and its influence on the other equipment and vice versa. Finally, the managers or high-ranked personnel who can see the overall picture (from the slight component failure to the catastrophe), should share their perceptions and educate the staff by conducting training courses and directorial meetings.

7.2 Recommendations for Further Work

This thesis work has provided applied risk management knowledge of a DP system with emphasis on the diesel engine as the most significant machinery on a vessel/platform. The study was quite extensive with various sensitive analyses to see how changes in the different components of different machinery will affect the operation of a diesel engine and subsequently, the DP system. In accordance with the power generation system of a DP system, all identified slight and miniscule faults in different sub-systems, which have relevance to a diesel engine operation have been considered.

However, it can be said that further work still needs to be carried out; there are other constitutive sub-systems of the DP system that are also significant for its proper and safe operation.

In light of the above, the following are recommendations for further work that needs to be considered for deployment of risk analysis and risk assessment of a DP system failure:

- In the case of availability of reliable data for the failure rate of different components, one can consider the quantitative risk analysis for the various sub-systems and machinery in a DP system. By this method, real numbers can be inserted in risk analysis techniques such as Fault Tree Analysis and Event Tree Analysis. Then, drawing the reliability block diagram of the system becomes feasible. Afterwards, the overall reliability of the system can be calculated which is beneficial for specifying the vulnerable components and sub-systems. The barriers, risk-reducing measures, and the maintenance policy can then be defined in accordance with the specified vulnerable sub-systems.
- Other sub-systems of the power generation system including alternator, switchboard and power distribution system should be considered. Types of excitation in the alternator, methods of load sharing and electrical power distribution are the issues that should be discussed for determination of their failure causes, in addition to defining barriers for the prevention of failures.

- Different types of thrusters like azimuth and tunnel thrusters should be considered in combination with the main propeller. Their pros and cons, efficiency and interaction analysis should be carried out in addition to a detailed Fault Tree Analysis to specify the safest and the best way for DP operations.
- Operational aspects, fault finding and risk mitigation procedures for different DP reference systems should be carried out. In the DP system, position, heading and environmental reference systems have important roles to maintain a vessel or floating platform’s position.
- A similar analysis could be carried out for DP class 2 that is more redundant due to more machinery and equipment as backup. The study should be continued to consider the backup systems and to analyze how the tasks are delivered to the backup system after the failures to let the DP operation to be continued.
- In the case of the failure of the seawater cooling system, which can affect the standby diesel engines as well as the main one, using DP class 2 will not make the DP system more redundant, unless there are two independent seawater intakes. The only means of electrical power supply independent of seawater cooling will be either the emergency generator or the UPS (Uninterruptible Power Supply). The emergency generator is cooled by freshwater in an air-cooled radiator and the UPS provides the electrical power by batteries. Thus, the capacity and reliability of the emergency power supply (UPS and emergency generator) should be taken into account to determine the redundancy of the system in a specific case. Some solutions like increasing the number of battery sets or the capacity of the emergency generator can be implemented for improvement.

REFERENCES

Anish. (2014). *10 Situations When Ship's Generator Must be Stopped Immediately*. Retrieved 10.05.2105, from http://www.marineinsight.com/marine/marine-news/headline/10-situations-generator-must-stopped-immediately/

API (2009). *API RP 17N Recommended Practice subsea production system reliability & technical risk management*. Dallas, Texas.

Aven, T. (2008). *Risk analysis: assessing uncertainties beyond expected values and probabilities*: John Wiley & Sons.

Aven, T. (2013). Practical implications of the new risk perspectives. *Reliability Engineering & System Safety, 115*, 136-145.

Aven, T. & Vinnem, J. E. (2007). *Risk management, with applications from the offshore oil and gas industry.* NY: Springer Verlag.

Azimuth thrusters. Retrieved 09.03.2015, from http://www.rolls-royce.com/customers/marine/about-marine/products.aspx

Bowtie Method. (2015). Retrieved 25.05.2015, from http://www.cgerisk.com/knowledge-base/risk-assessment/thebowtiemethod

Bray, D. (2003). *Dynamic Positioning. Oilfield Seamanship Series, Vol. 9*: Oilfield Publications, Incorporated.

Chen, H., & Moan, T. (2002). *Collision risk analysis of FPSO-tanker offloading operation.* Paper presented at the ASME 2002 21st International Conference on Offshore Mechanics and Arctic Engineering.

Deter, D. (1997). *Principal aspects of thruster selection.* Paper presented at the Marine Technology Society, Dynamics Positioning Conference.

DNV (2003). *Risk management in marine-and subsea operations*, (Vol. DNV- RP-H101,, pp. 54,). Høvik: DNV.

DNV (2012). *Dynamic Positioning Vessel Design Philosophy Guidelines*, (Vol. DNV-RP-E306, pp. 117). Høvik: DNV.

DNV (2014). *Dynamic Positioning Systems*, (Vol. Rules for classification of ships, Part 6 Chapter 7, pp. 53). Høvik: DNV.

Dynamic Positioning. Retrieved 10.03.2015, from Wikipedia, http://en.wikipedia.org/wiki/Dynamic_positioning

Dynamic Positioning. Retrieved 07.03.2015, from http://hornbeckoffshore.com/fleet/vessel-attributes

Dynamic positioning-basic principles. Retrieved 07.03.2015, from http://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/BD306BBB3E7DA73FC1256DAB00353083?OpenDocument

Dynamic Positioning Committee. History of DP. Retrieved 07.03.2015, from http://dynamic-positioning.com/history-of-dp/

Floating production storage and offloading. Retrieved 30.03.2015, from Wikipedia, http://en.wikipedia.org/wiki/Floating_production_storage_and_offloading

History of Bowtie. (2015). Retrieved 25.05.2015, from http://www.cgerisk.com/knowledge-base/risk-assessment/the-bowtie-methodology

Holvik, J. (1998). *Basics of Dynamic Positioning*. Paper presented at the Dynamic Positioning Conference, Houston, Texas.

Hughes, J. M. (1997). *Close Proximity Study, Shuttle Tanker Operations*. Paper presented at the Dynamic Positioning Conference, Houston, Texas.

IMCA (2007). *Guidelines for the Design and Operation of Dynamically Positioned Vessels* (pp. 76). London.

IMCA (2009). *International guidelines for the Safe Operation of Dynamically Positioned Offshore Supply Vessels* (pp. 45). London.

IMO (2013). *Guidelines for vessels with dynamic positioning systems* (Vol. MSC Circular 645).

Norwegian Maritime Authority Retrieved 11.03.2015, from http://www.sjofartsdir.no/en/

Rausand, M. & Høyland, A. (2004). *System reliability theory: models, statistical methods, and applications* (Vol. 396): John Wiley & Sons.

Risk Support (2014). Active Bow Tie (Version 1.7c). London, United Kingdom

Ship propeller Retrieved 09.03.2015, from http://www.shutterstock.com/video/clip-4149724-stock-footage-ship-propeller.html

Ships electrical plant and distribution system for the A.C. generators (2010). Retrieved 10.02.2015, from http://www.machineryspaces.com/alternating-current-generators.html

Trewern, S. (2013). Kongsberg Maritime. Retrieved 12.03.2015, from http://www.saltwaterpr.com/story/Story.aspx?story=6008

Tunnel type thrusters for ships. Retrieved 09.03.2015, from http://www.nauticexpo.com/prod/global-marine-engineering-bv/tunnel-type-thrusters-bow-ships-28950-193604.html

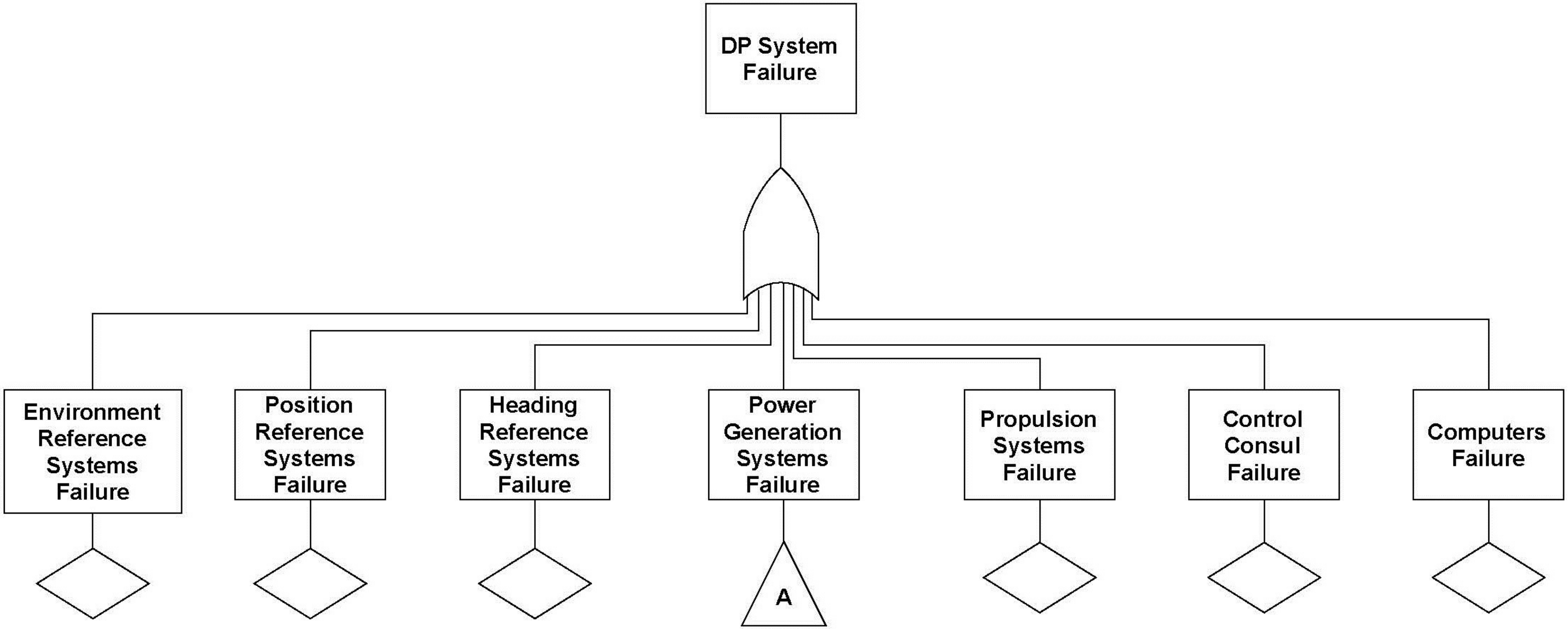
Vinnem, J. E. (2013). *Offshore risk assessment: principles, modelling and applications of QRA studies*: Springer Science & Business Media.

Wang, J. X. & Roush, M. L. (2000). *What every engineer should know about risk engineering and management*: CRC Press.

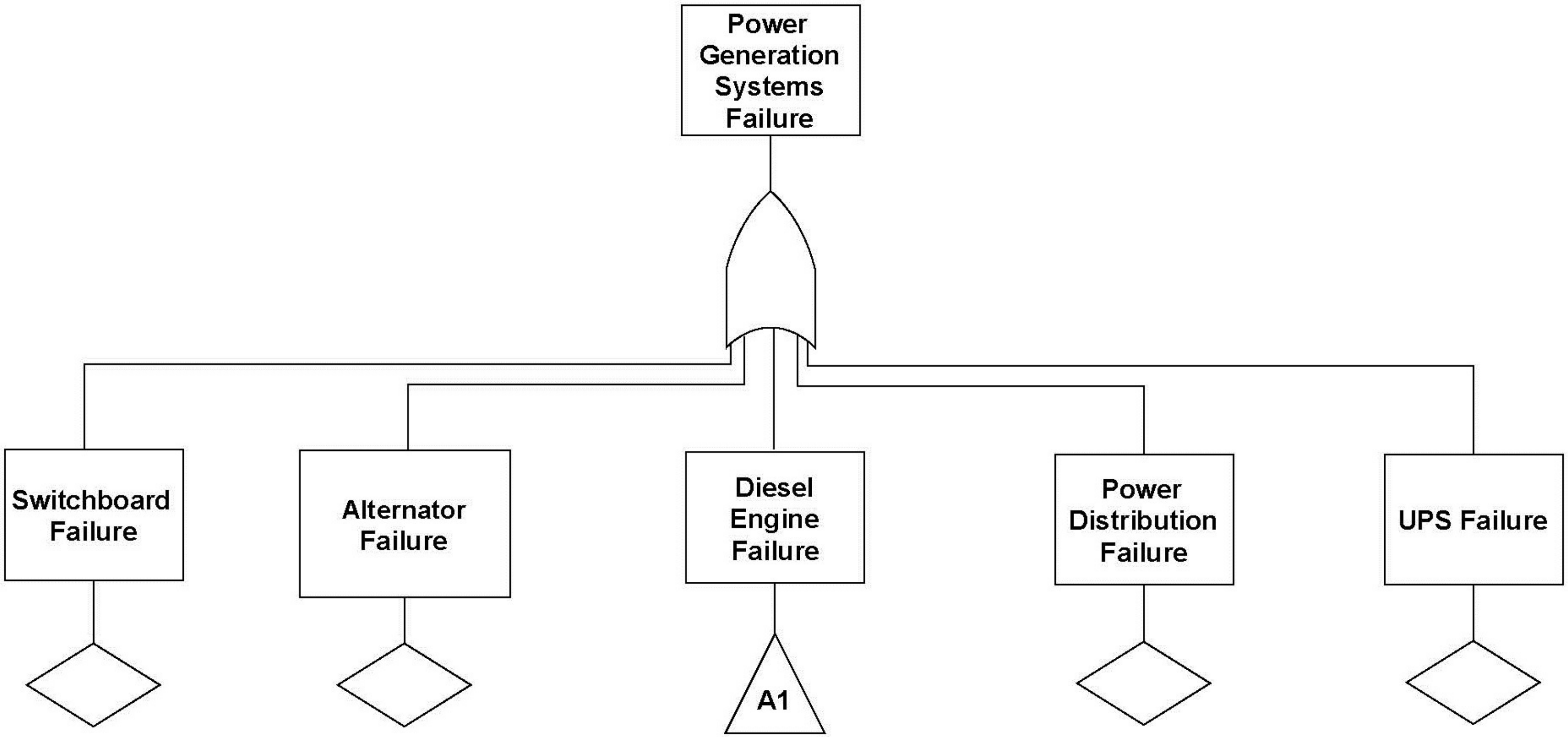
APPENDICES

Appendix A: Fault Three Diagrams

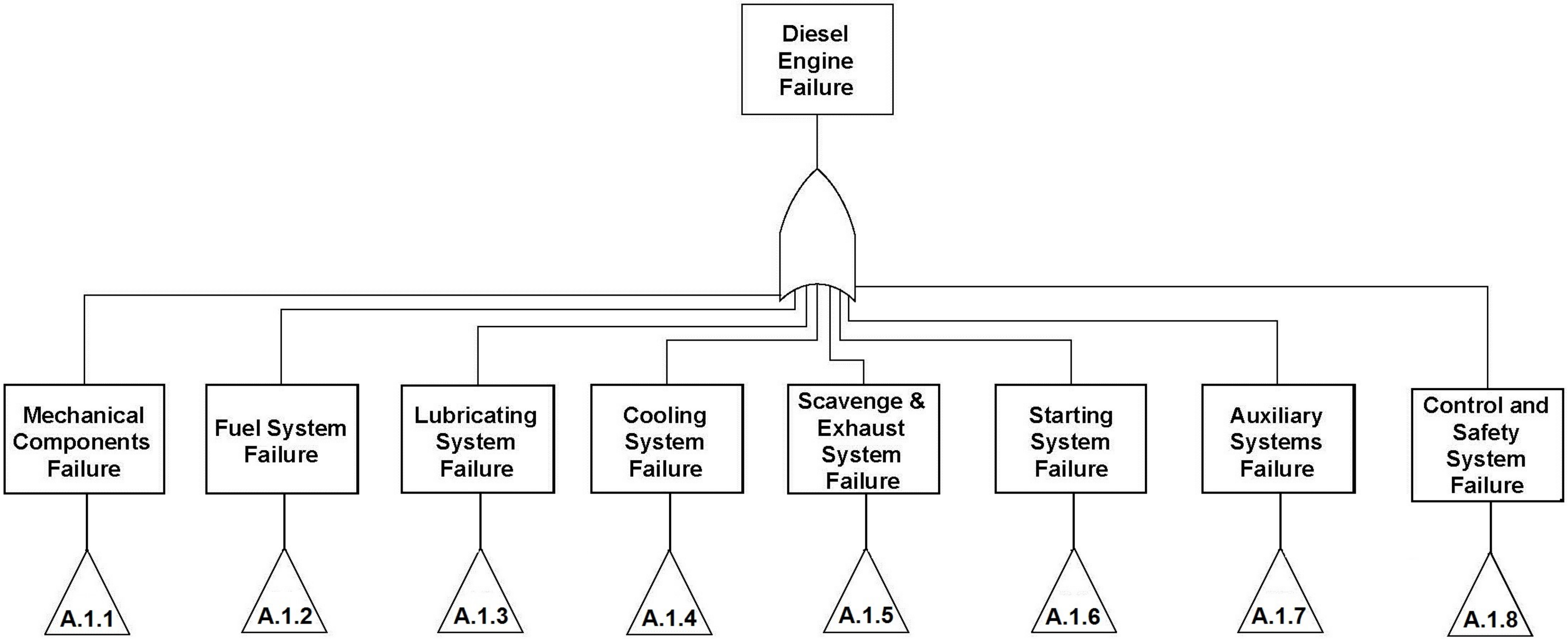
FTA Diagram 1: DP System Failure



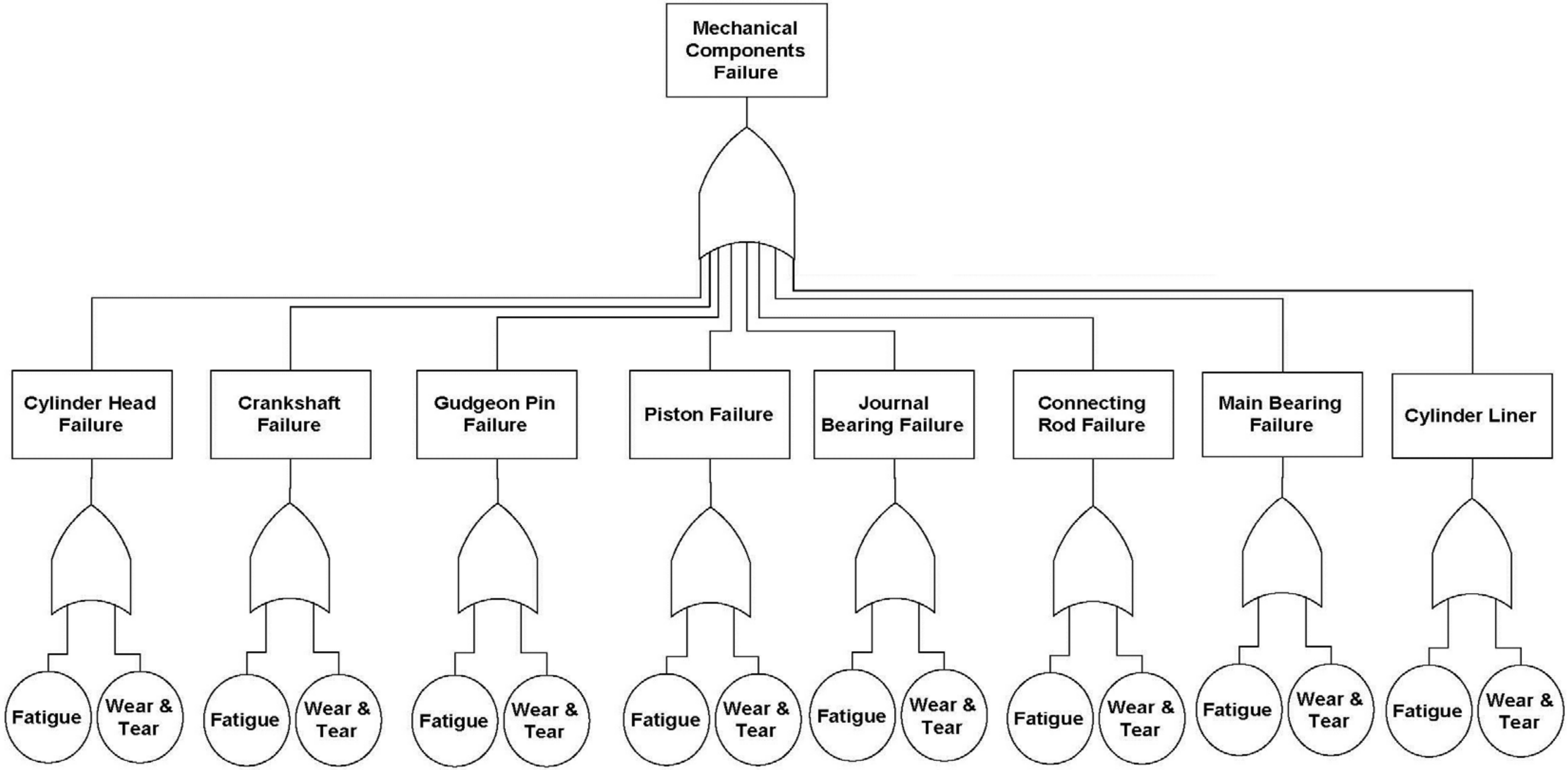
FTA Diagram A: Power Generation Systems Failure



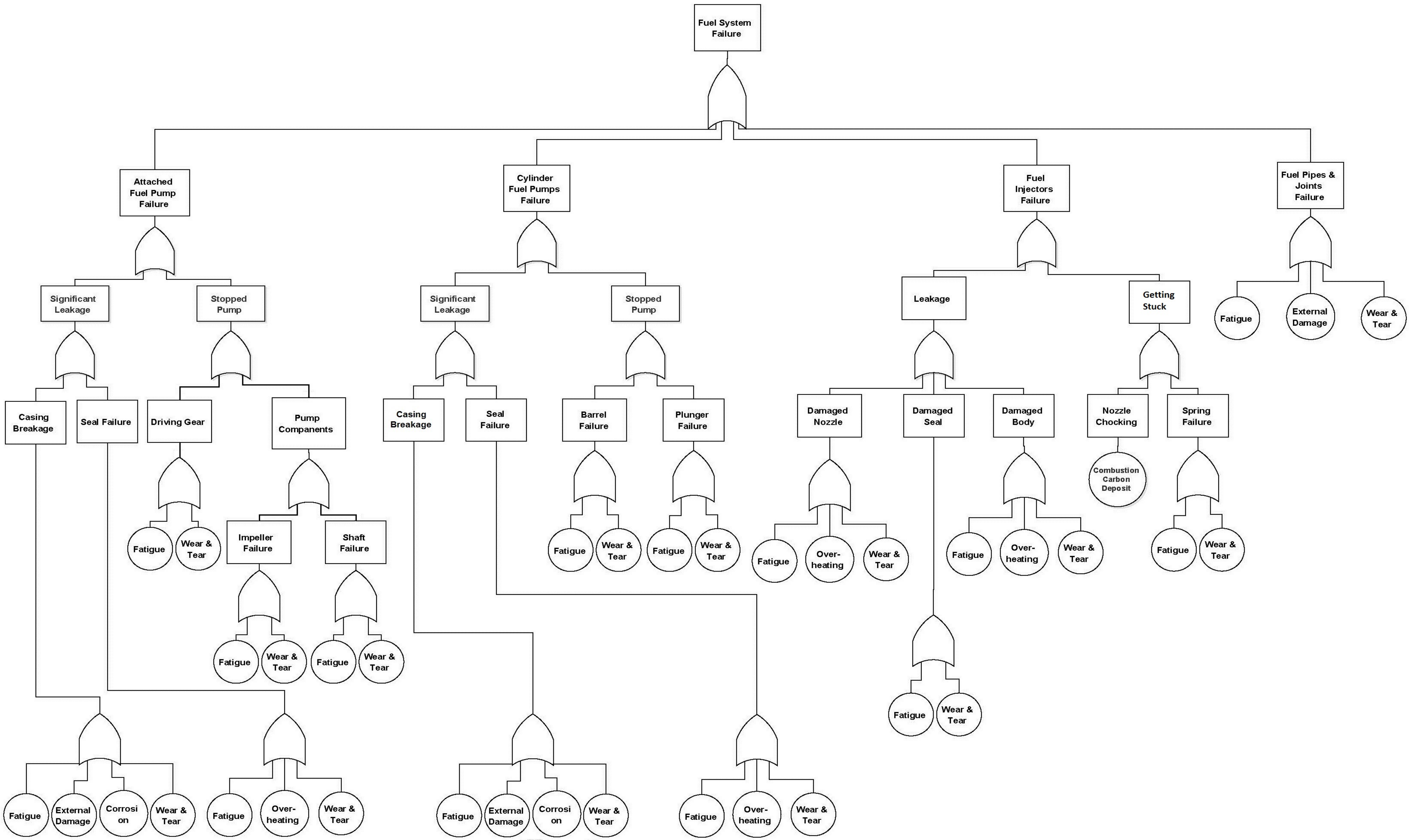
FTA Diagram A.1: Diesel Engine Failure



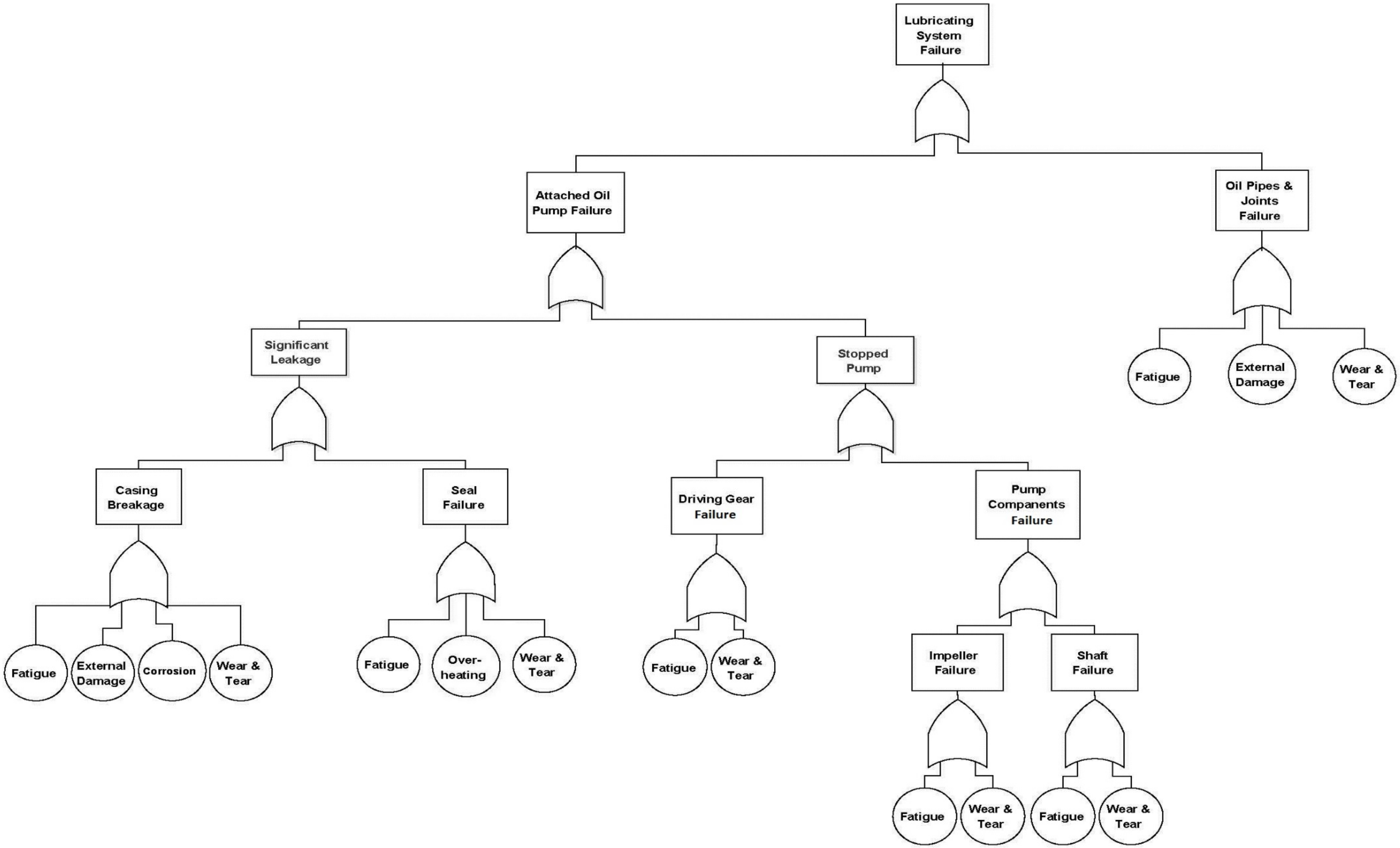
FTA Diagram A.1.1: Mechanical Components Failure



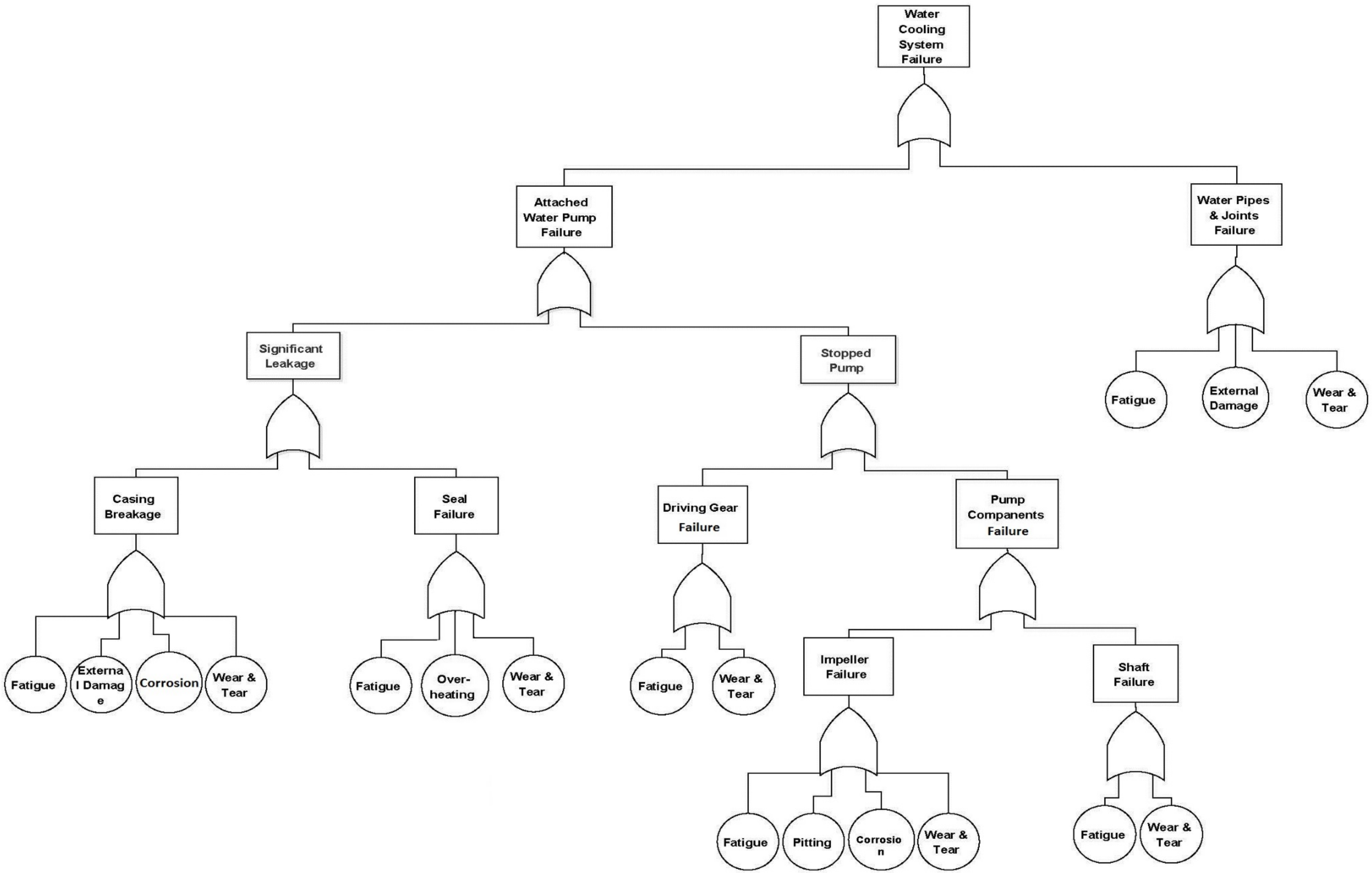
FTA Diagram A.1.2: Fuel System Failure



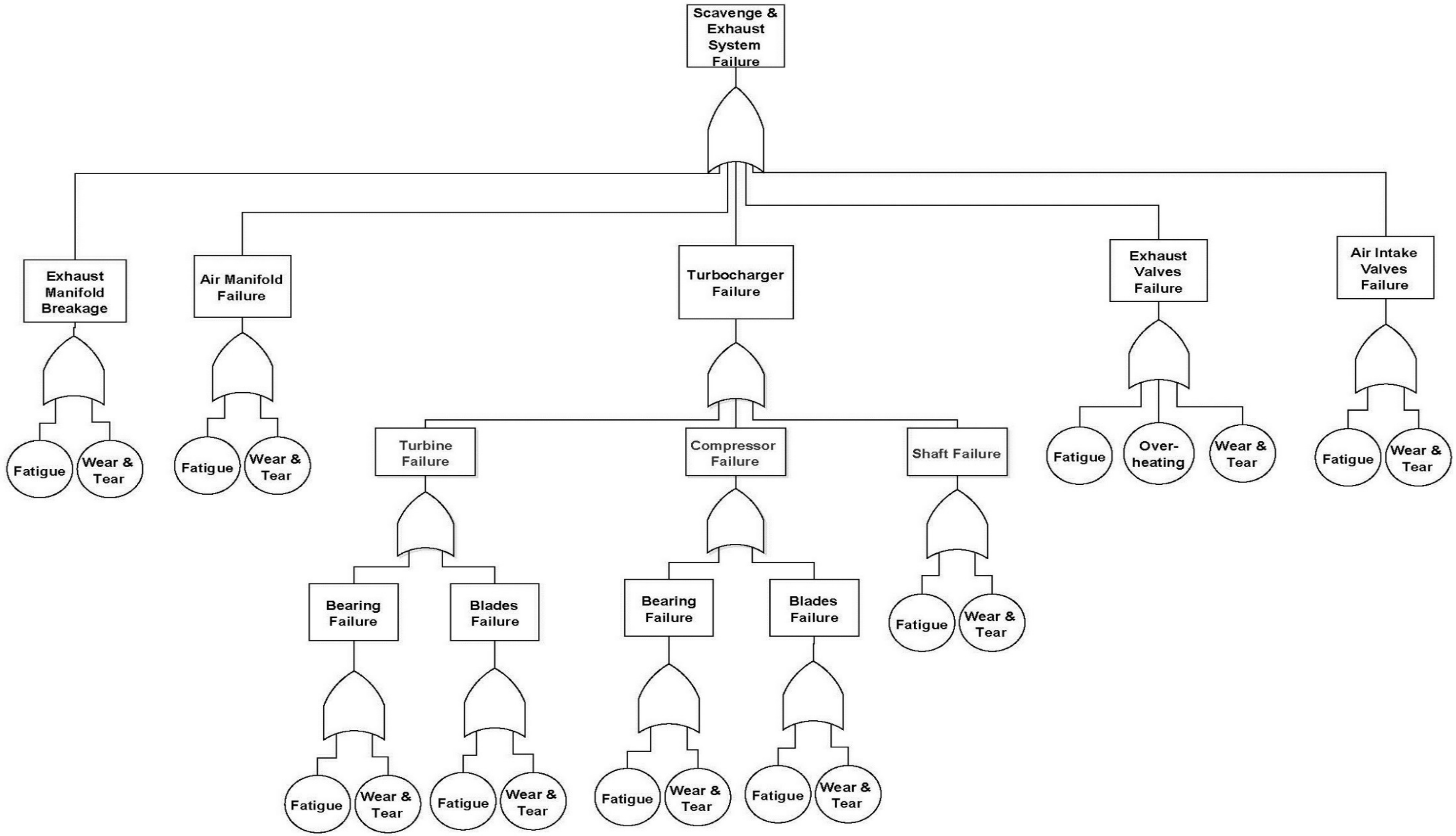
FTA Diagram A.1.3: Lubricating System Failure



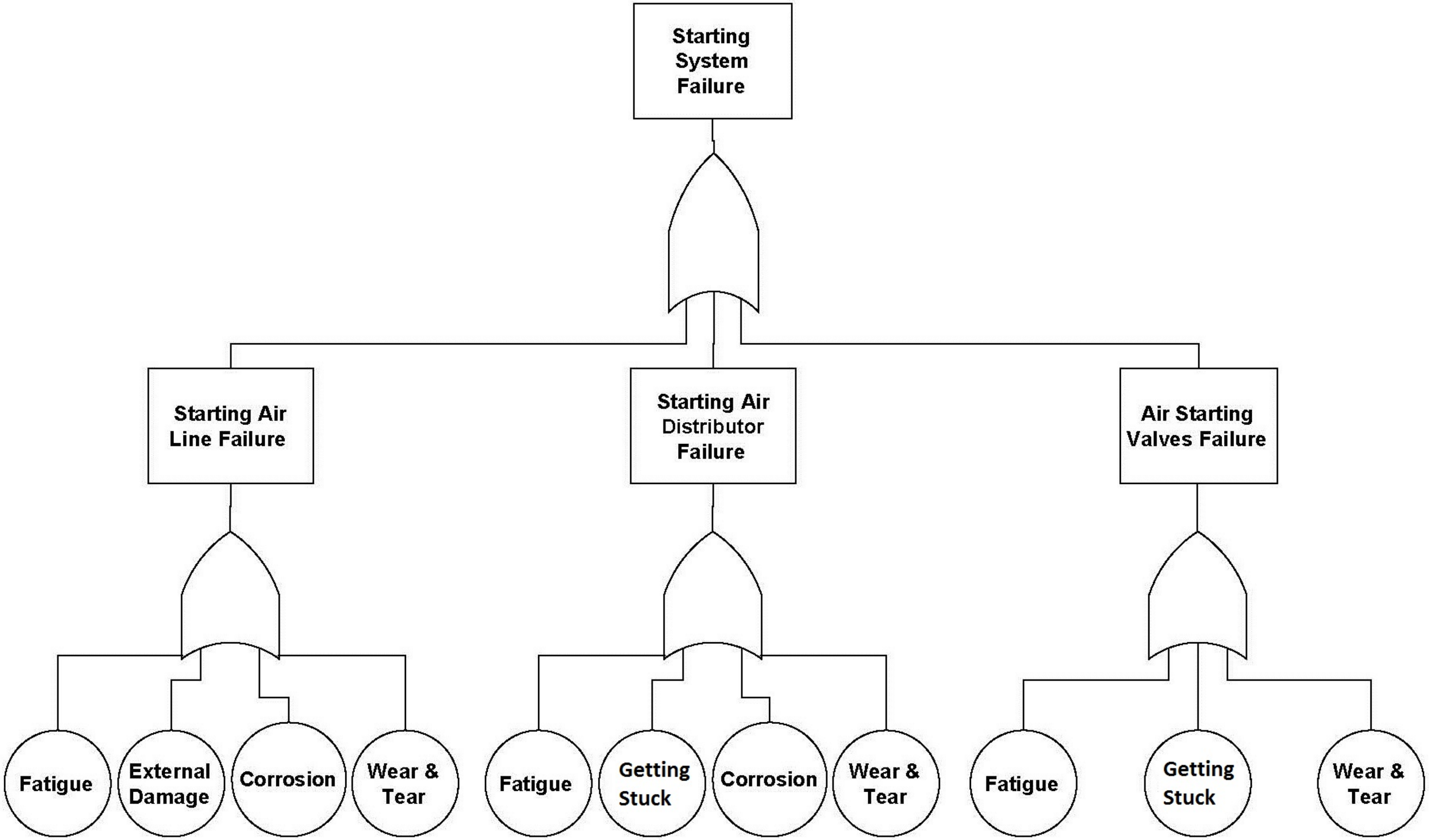
FTA Diagram A.1.4: Water Cooling System Failure



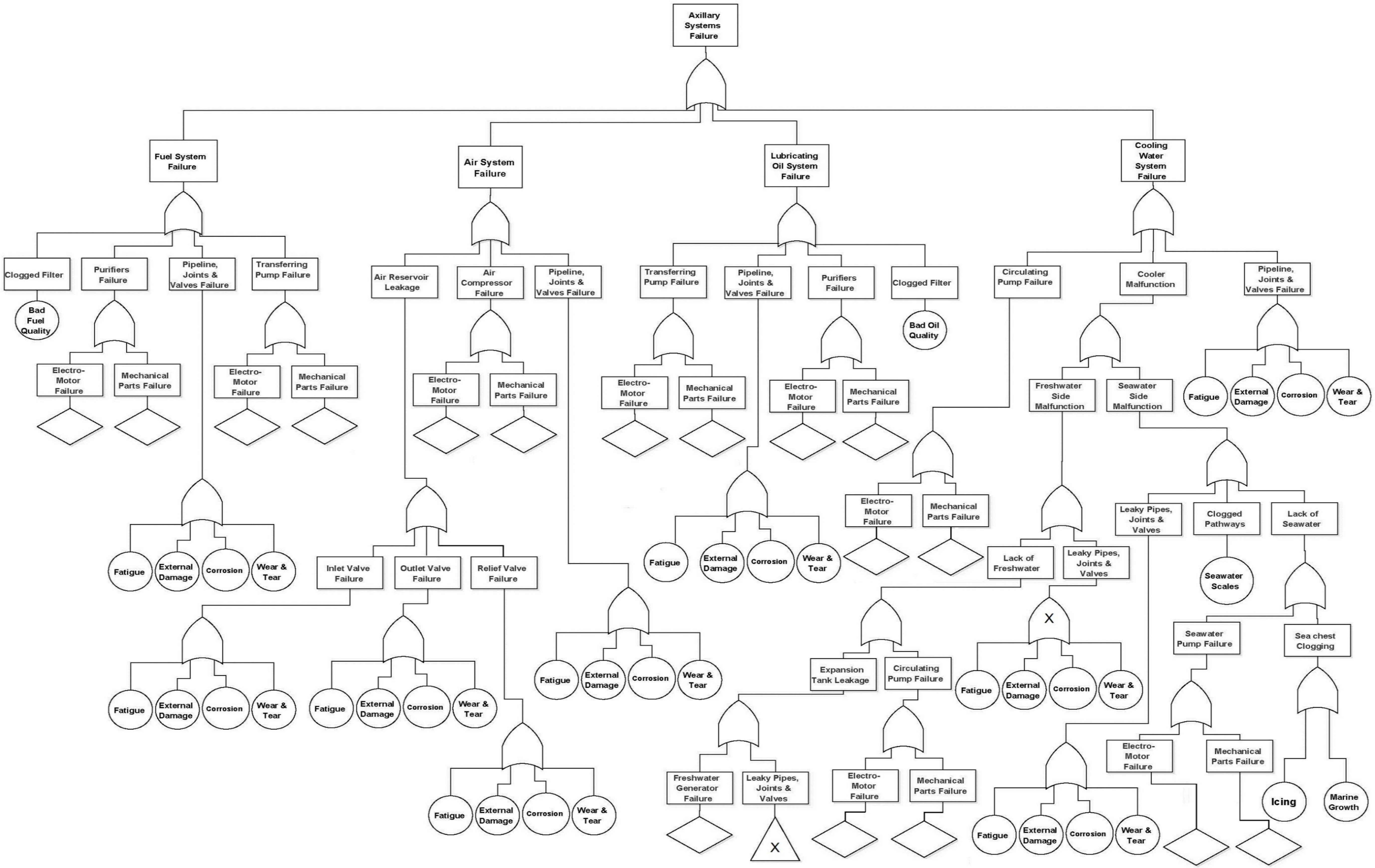
FTA Diagram A.1.5: Scavenge and Exhaust System Failure



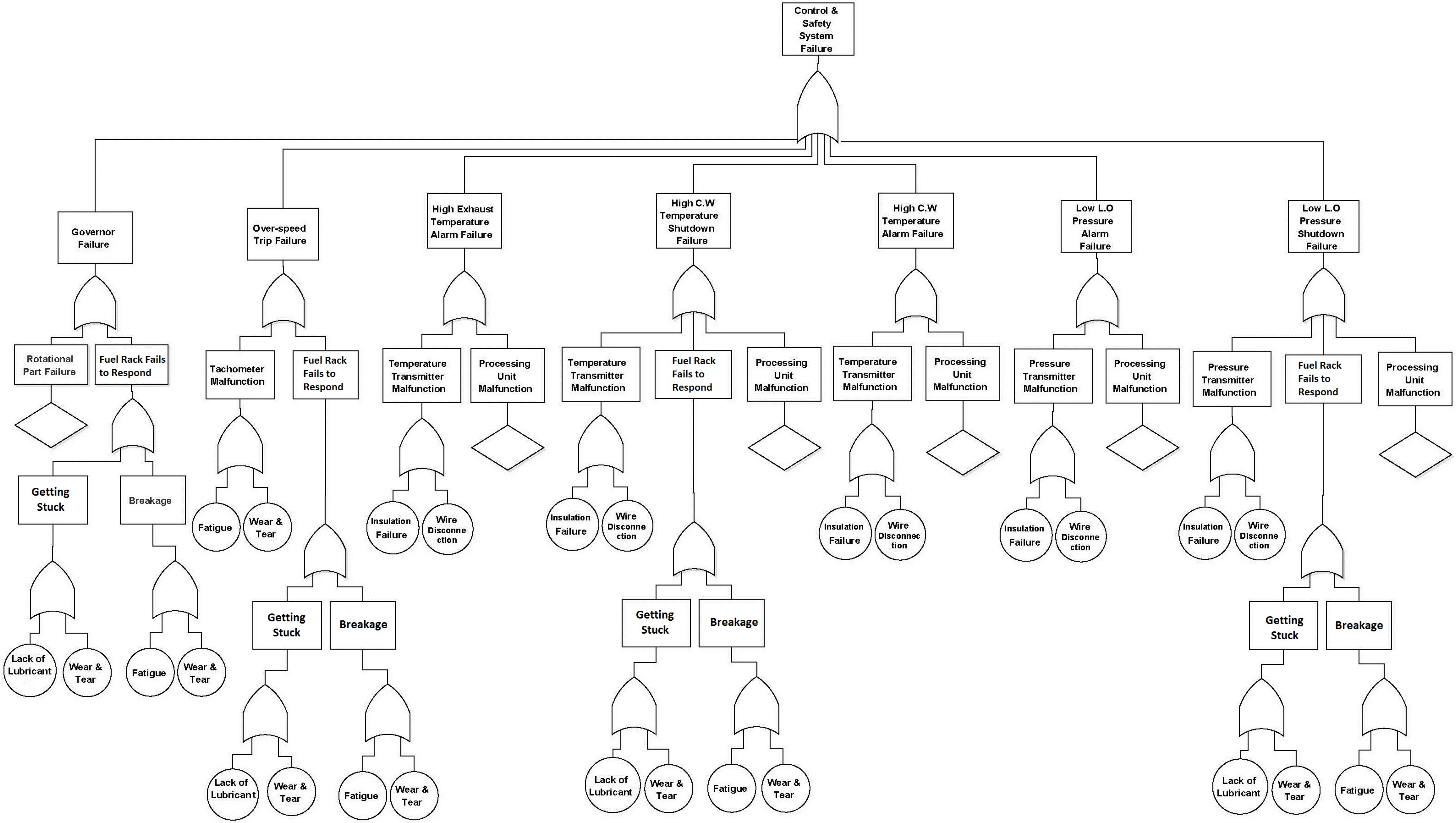
FTA Diagram A.1.6: Starting System Failure



FTA Diagram A.1.7: Auxiliary System Failure

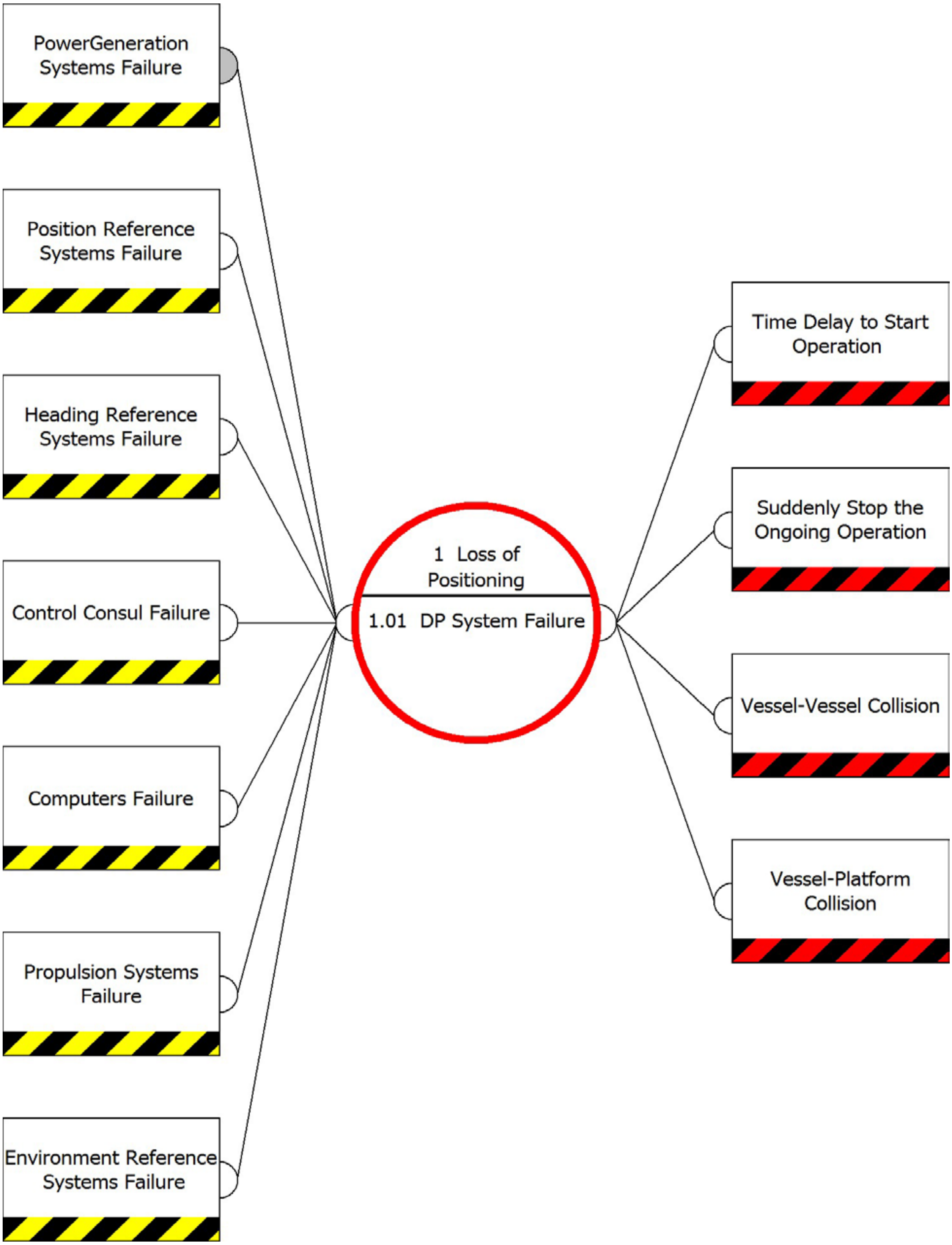


FTA Diagram A.1.8: Control and Safety System Failure

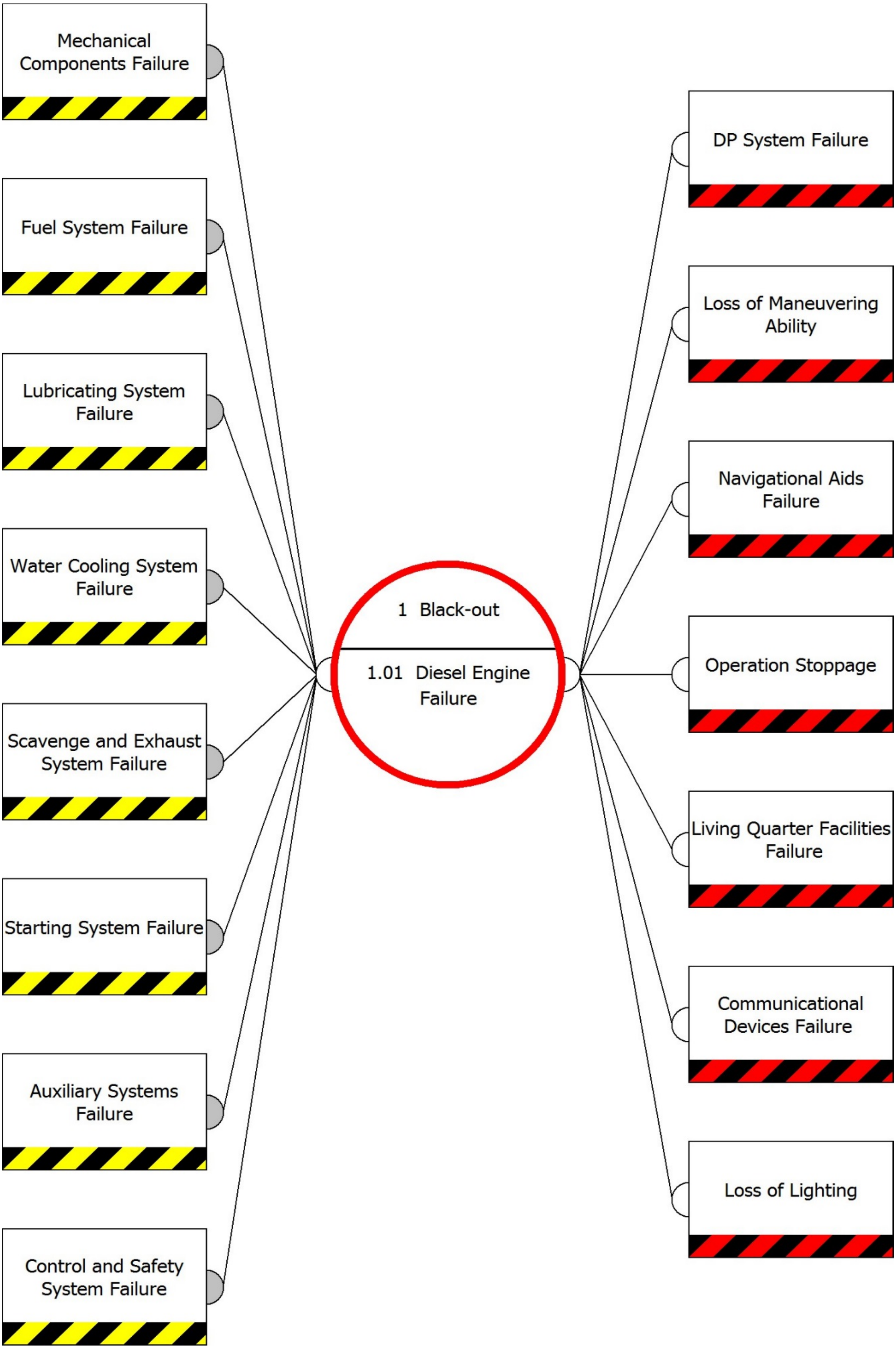


Appendix B: Bow-Tie Diagrams

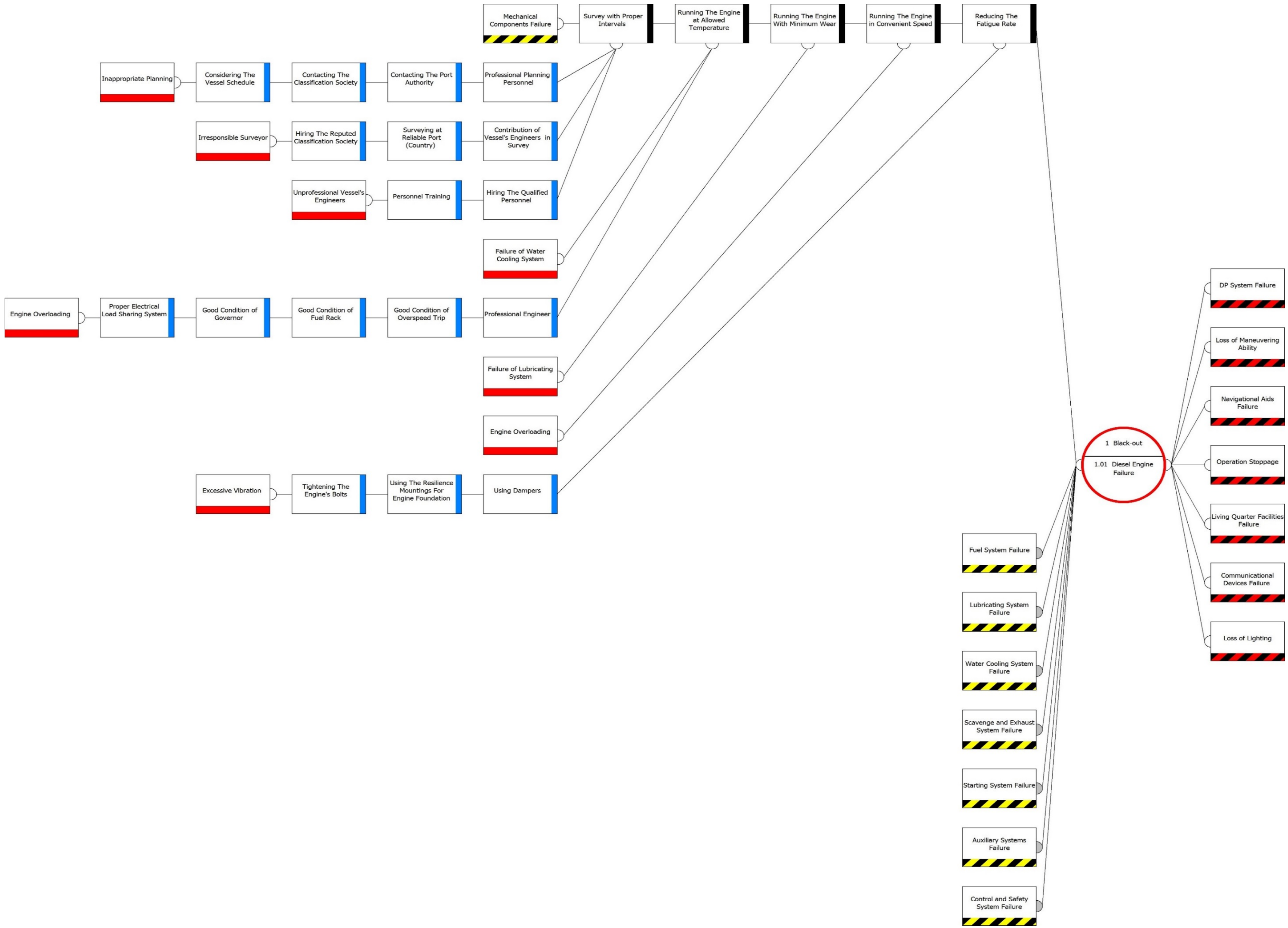
Bow-Tie Diagram B: DP System Failure



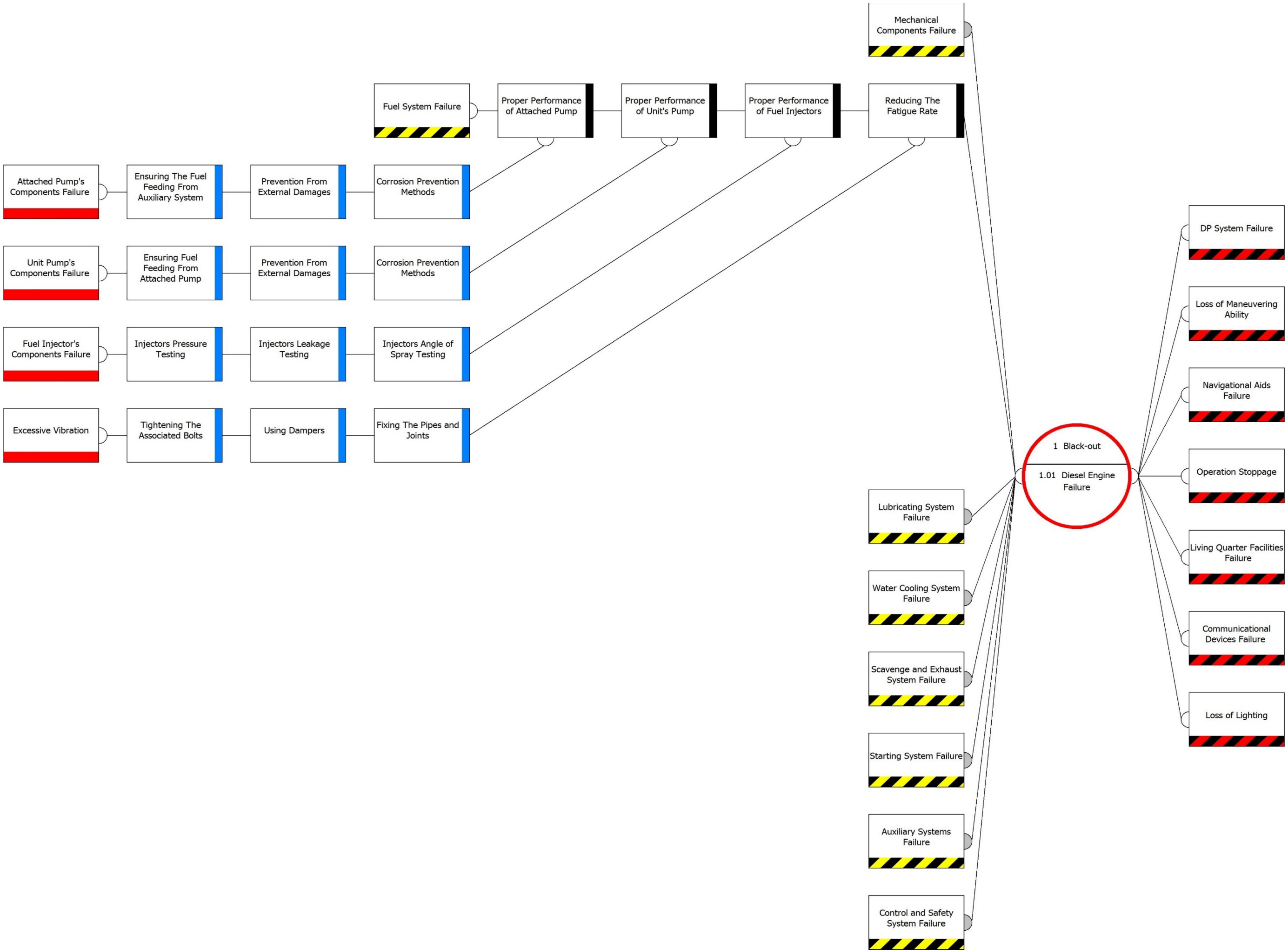
Bow-tie Diagram B.1: Diesel Engine Failure



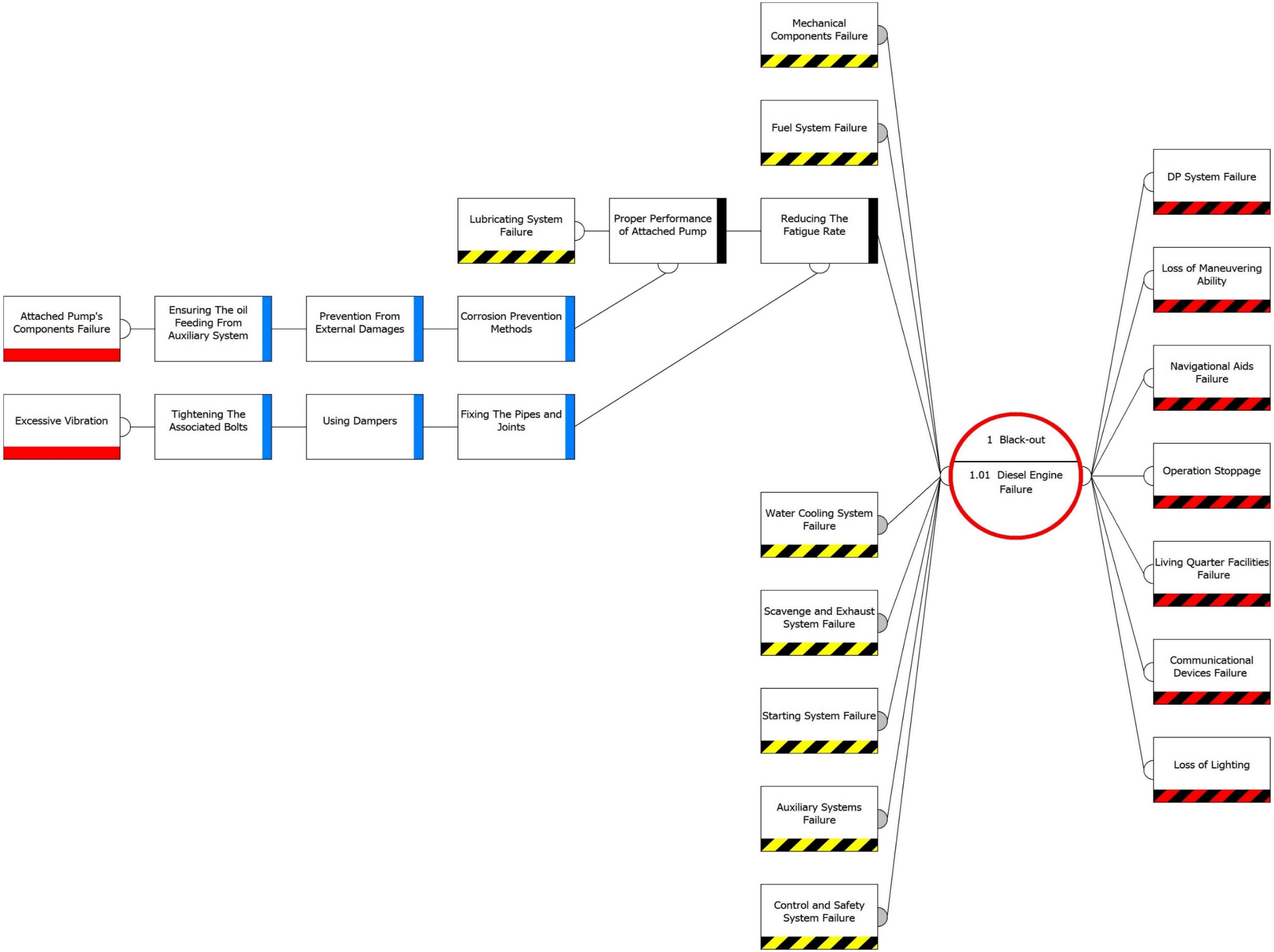
Bow-tie Diagram B.1.1: Mechanical Components Failure



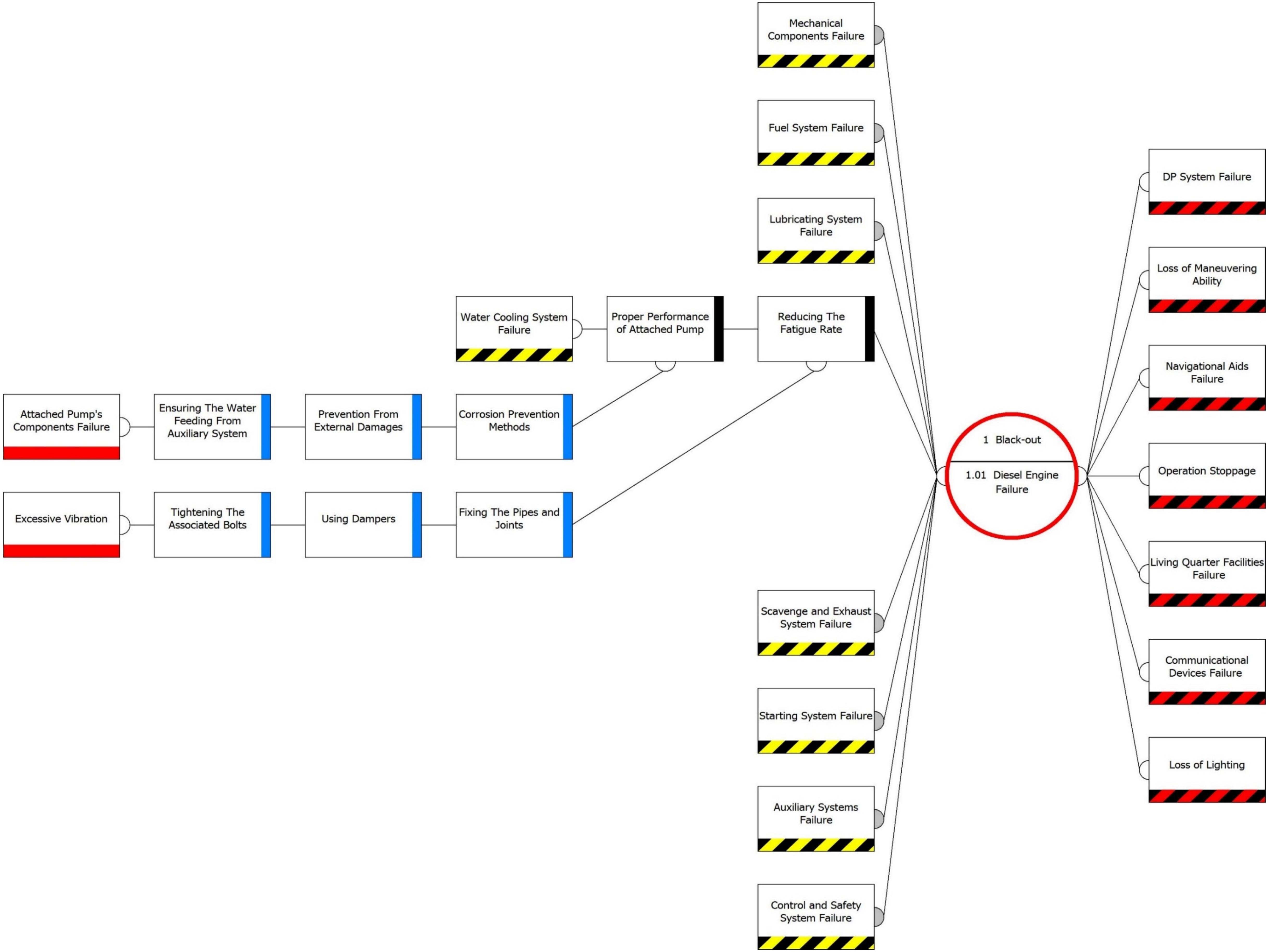
Bow-Tie Diagram B.1.2: Fuel System Failure



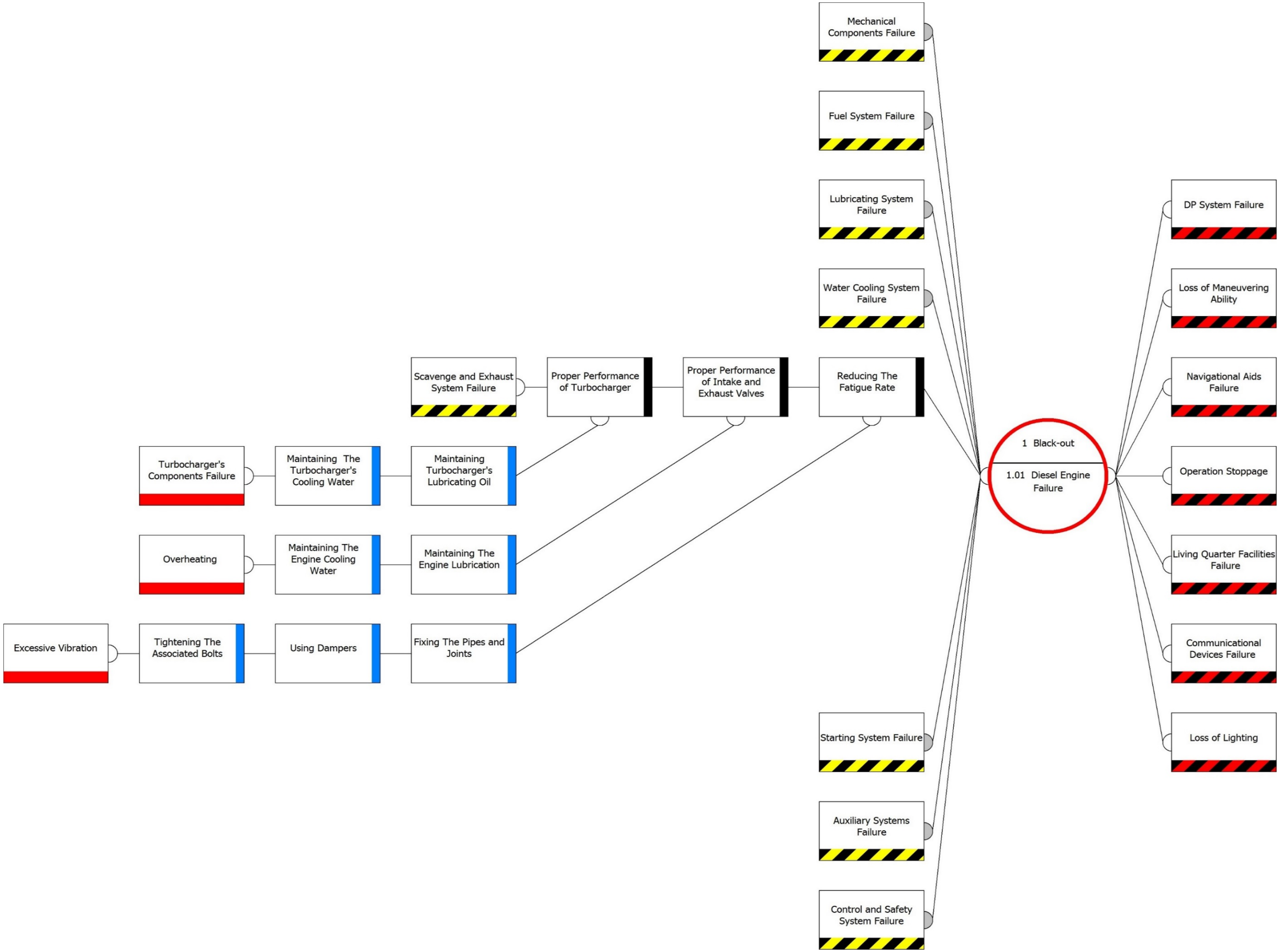
Bow-Tie Diagram B.1.3: Lubricating System Failure



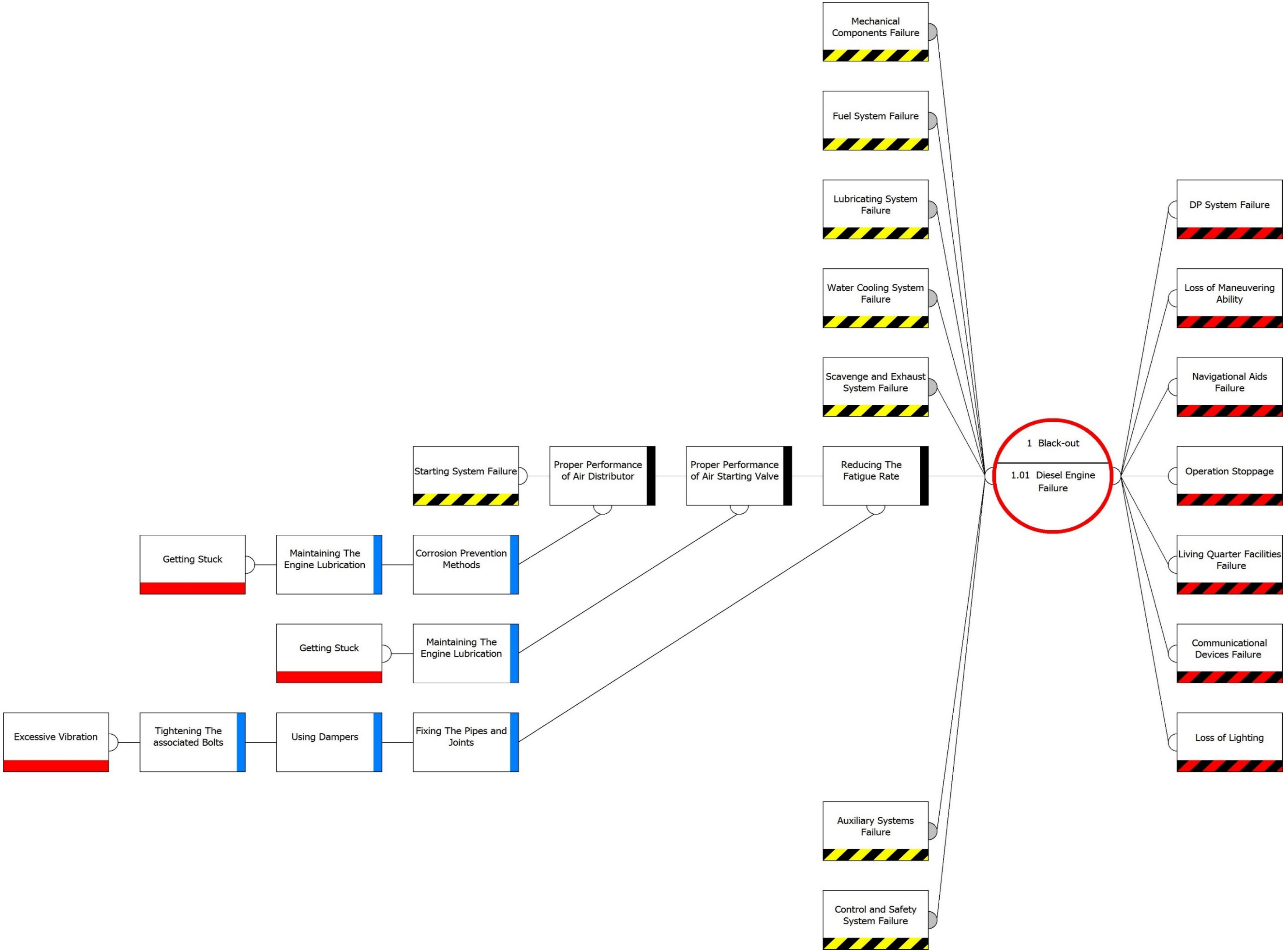
Bow-Tie Diagram B.1.4: Water Cooling System Failure



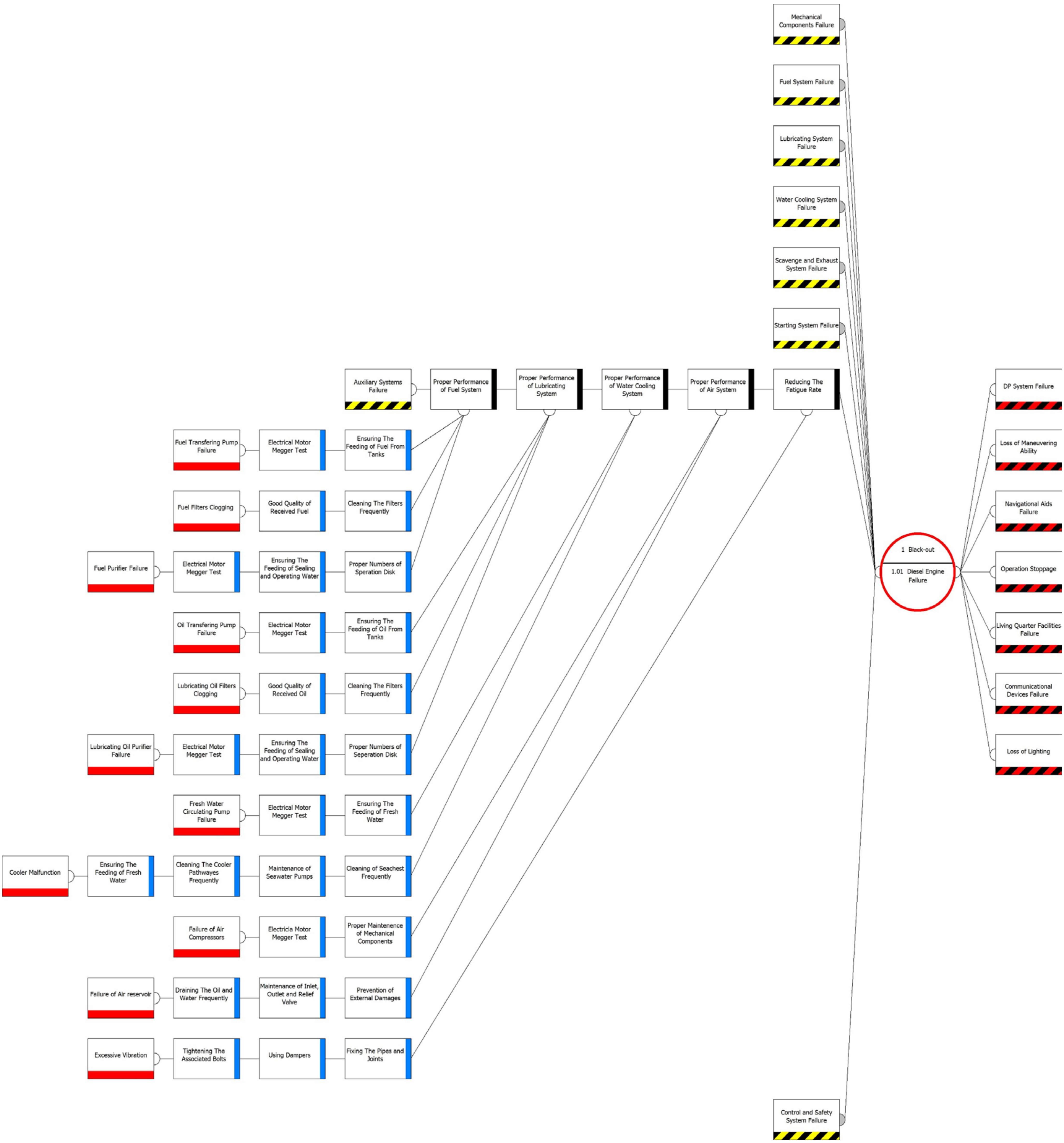
Bow-Tie Diagram B.1.5: Scavenge and Exhaust System Failure



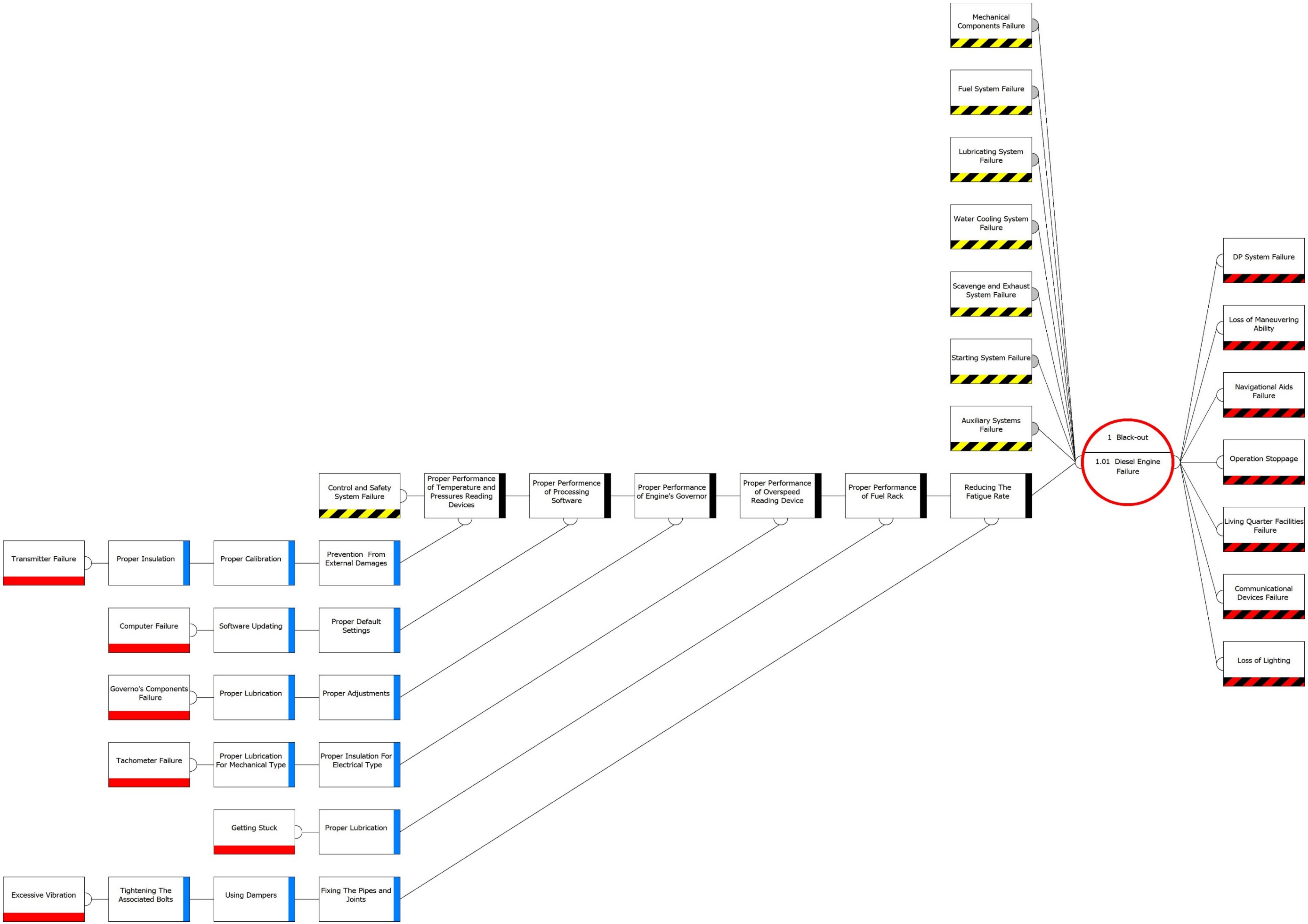
Bow-Tie Diagram B.1.6: Starting System Failure



Bow-Tie Diagram B.1.7: Auxiliary Systems Failure



Bow-Tie Diagram B.1.8: Control and Safety System Failure



Bow-Tie Diagram B.2: Power Generation System Failure