NTNU – Trondheim
Norwegian University of
Science and Technology

Reliability assessment of subsea BOP control systems

Øyvind Sætre

Subsea Technology

Submission date:	June 2015
Supervisor:	Anne Barros, IPK
Co-supervisor:	Marvin Rausand, IPK Geir Ove Strand, IPK

Norwegian University of Science and Technology
Department of Production and Quality Engineering

NTNU – Trondheim
Norwegian University of
Science and Technology

Reliability assessment of subsea BOP control systems

Øyvind Korsvik Sætre

June 2015

MASTER THESIS

Department of Production and Quality Engineering

Norwegian University of Science and Technology

Supervisor 1: Professor Anne Barros

Supervisor 2: Professor Marvin Rausand

Supervisor 3: Geir Ove Strand

Preface

This master thesis was written during the spring of 2015. The thesis is carried out as a part of the Subsea Technology MSc at the Norwegian University of Science and Technology (NTNU), and concerns the reliability assessment of subsea BOP control systems.

Professor Marvin Rausand brought up the title, reliability assessment of subsea BOP control systems.

The reader is assumed to have basic knowledge about the petroleum industry and knowledge about safety reliability, equivalent to the books Rausand and Høyland (2004) and Rausand (2014).

Some of the definitions used in the report are from the International Electrotechnical Vocabulary (IEV) http://www.electroperdia.org. References to the vocabulary are given in the text as IEV xxx-yy-zz, where xxx refers to the chapter, and yy-zz is the number of the definition.

Trondheim, 2015-06-10

Øyvind Korsvik Sætre

Acknowledgment

This thesis could not have been carried out without the help and support of a few key individuals. Firstly I would like to thank my co-supervisor Marvin Rausand, professor at the department of production and quality engineering at NTNU, for dedicated help and support during the work. Also my other co-supervisor Geir Over Strand, PhD candidate - well drilling safety at NTNU, who always have been helpful with answering questions and providing competent input. Finally, I would like to thank my primary supervisor Anne Barros, professor in subsea reliability at NTNU, for valuable input in completing my report.

(Ø.K.S)

Summary

The subsea blowout preventer (BOP) and the BOP control system were the most important contributors to the Macondo accident in April 2010. A BOP is a large valve system used during the drilling phase; to seal, control, and monitor oil and gas wells. As a consequence of the Macondo accident, improved methods for reliability assessment of BOPs are now required.

Over the years, several subsea BOP reliability studies have been performed, where technical solutions and potential failures are thoroughly investigated. As a result of the information gained, both maintenance and reliability of the BOP systems have improved. Despite overall improvements, the BOP is still a main contributor to risk and downtime in the drilling phase. A deeper look into the reliability reports reveals the control system of the BOP as the root of the majority of failures.

Most subsea BOPs are equipped with a multiplex control system with a combination of electronics and hydraulics, used to operate the different functions of the BOP. Despite the high level of redundancy, several sections of the system are subject to critical system failures.

To prevent BOP failures, national regulations and standards have been developed in several countries. Most of the national requirements are similar, but there are also differences. These similarities and differences are illustrated in this study through a detailed comparison between the relevant regulations and standards in Norway and the United States, with respect to general-, design- and operational BOP requirements.

The main focus of this study is the multiplex subsea BOP control system. The potential critical failures of this system are identified and analyzed in a detailed failure mode, effects, and criticality analysis (FMECA). This analysis shows that the shuttle valve, the pod selector valve, the subsea accumulators, and the fluid reservoir are the most safety-critical parts of the control system.

The BOP control system has several redundant elements and these may be vulnerable to common-cause failures. The potential common-cause failures are examined in this study and found to have a significant influence on the reliability of the control system.

Improving current reliability assessments of subsea BOP control systems requires a thorough review of both the system and the previously used methods. In this study, a fault tree analysis is performed to reveal the relevant failure combinations. To improve reliability calculations provided by common fault tree analysis programs, a post-processing of the minimal cut sets in a spreadsheet (i.e., Excel) is proposed to cover the effect of common-cause failures. The method gives a more conservative and accurate approximation compared to the existing methods.

An event tree analysis is performed to cover the switching phases between the two pods, showing the time dependencies that can influence the consequences. This type of switching cannot be modeled in the fault tree, therefore, recommendations to apply the event tree analysis to similar situations to get a more accurate reliability estimate, is given.

For components such as the shear ram, a perfect function test cannot be conducted. In the performed analysis, no such components are evaluated. However, in an expanded analysis of the subsea BOP control system, such components will be involved, therefore, adding the contribution from the proof test coverage factor to components prone to imperfect testing, is recommended.

Sammendrag

Undervannsutblåsningsventilen (bedre kjent som BOP) og BOP kontrollsystemet var blant de utløsende faktorene i Macondo-ulykken april 2010. En BOP er et stort ventilsystem brukt under borefasen for å; forsegle, kontrollere og overvåke olje og gassbrønner. Som et resultat av Macondo-ulykken kreves nå forbedrede metoder for pålitelighetsanalyser av BOP'er.

Gjennom årene har flere pålitelighetsanalyser på undervanns BOP'er blitt utført, hvor tekniske løsninger og potensielle feil har blitt grundig undersøkt. Som et resultat har både vedlikeholdet og påliteligheten til BOP'er blitt forbedret. Til tross for en generell forbedring, er BOP'er fortsatt en av hovedårsakene bak risiko og nedetid i borefasen. Undersøkelser av pålitelighetsrapporter avslører kontrollsystemet til BOP'en som rotårsaken til flertallet av feilene.

Majoriteten av undervanns BOP'er er utstyrt med et multiplex kontrollsystem, som er en kombinasjon av elektronikk og hydraulikk, brukt til å operere de forskjellige funksjonene i BOP'en. Til tross for mye redundans, er systemet fortsatt utsatt for kritiske feil.

For å forhindre BOP feil, er nasjonale forskrifter og standarder utviklet i flere land. Flertallet av de nasjonale forskriftene er like, men forskjeller finnes. Likhetene og forskjellene er i oppgaven illustrert gjennom en detaljert sammenligning mellom relevante forskrifter fra Norge og Amerikas forente stater, med fokus på generelle-, utformings-, og operasjonelle BOP krav.

Hovedfokuset for denne oppgaven er det multiplexede undervanns BOP kontrollsystemet. De potensielle kritiske feilene i systemet er identifisert og analysert i en detaljert feilmode, effekter og kritikalitets analyse. Analysen viser at skyttelventilen, pod velgerventilen, undervannsakkumulatorene og væske reservoaret er de mest sikkerhetskritiske delene av kontrollsystemet.

BOP kontrollsystemet har flere redundante elementer som kan være utsatt for felles feil. Potensialet for felles feil er undersøkt i oppgaven og funnet til å ha en signifikant påvirkning på påliteligheten til systemet.

For å forbedre nåværende pålitelighetsvurderinger av undervanns BOP kontrollsystemer, kreves en grundig gjennomgang av både systemet og tidligere brukte metoder. I denne studien er en feiltreanalyse anvendt for å avsløre mulige feilårsaker. For å forbedre eksisterende feiltre kalkulasjoner, er en metode for å post-prosessere de minimale kutt setene i et regneark (dvs., Excel) foreslått for å ta høyde for bidraget fra felles feil.

En hendelsestreanalyse er utført for å dekke vekslingsfasen mellom to poder for å vise at tidsavhengighet kan dirkete påvirke konsekvensen. Denne typen veksling kan ikke bli modellert inn i et feiltre, derfor anbefales det å anvende et hendelsestre for liknende situasjoner for å oppnå et mer nøyaktig pålitelighets estimat.

For komponenter som skjæravstengeren kan ikke en perfekt funksjonstest utføres. I analysen er ingen slike komponenter evaluert. I en utvidet analyse av undervanns BOP kontrollsystemet vil slike komponenter bli involvert, derfor anbefales det å legge til bidraget fra sikker test dekningsfaktoren til komponenter utsatt for ufullkommen testing.

Contents

Chapter 1

Introduction

1.1 Background

The Macondo accident occurred on April 20th 2010, 11 people were killed, and approximately 4.9 million barrels of crude oil were spilled into the ocean. The accident caused the largest offshore oil spill ever, and the president of the United States declared it the biggest environmental catastrophe ever to occur in the country's history. The accident was caused by a blowout in the Macondo well, drilled by the Transocean-owned rig, Deepwater Horizon (DWH). The rig crew lost control of the situation and hydrocarbons emerged up to the drill floor, shortly after the hydrocarbons were ignited, eventually causing the DWH to sink.

Accident commissions later formed to investigate the event, pointed to the subsea blowout preventer (BOP) as one of the main reasons for the accident. The BOP is a safety critical system used to ensure safe drilling and well interventions. The main function of the BOP is to seal the well in the event of a blowout. In the aftermath of the DWH investigations reports, renewed focus was brought to the BOP, and enhanced BOP reliability assessments methods were demanded.

Several reports on the quantification of the subsea BOP reliability have been published over the years, especially by Per Holand. The reports are based on collection and analysis of rig specific failure data, and have resulted in a great amount of knowledge about BOP failures, failure causes, maintenance and testing. A recurring source of failure in several of the reports is the BOP control system.

To find the weaknesses in a system, such as the BOP control system, requires a great deal of work. Several master thesis have been written about BOP systems, but satisfactory methods for quantifying the subsea BOP control system are still lacking.

Quantification of the subsea BOP reliability has mostly been based on test intervals and estimated failure rates. In Klakegg (2012), the contribution from common cause failures (CCFs) are also taken into consideration, however, this analysis considers the entire BOP system. A potential improvement from the previous analyses could be to include the CCFs contribution in an analysis for the part of the BOP system where most failures occur, the control system.

Subsea BOP systems must comply with certain relevant standards and regulations. These are frequently updated and can vary depending on where the system is located. Designers and operators are therefore required to continually follow up the requirements for their present situation. For subsea BOPs, the most relevant guidelines and standards are for example, IEC-61511 (2011), IEC-61508 (2005), and NOG - 070 (2004).

The methods applied for quantifying the reliability are based on theoretical principles from reliability engineering, and the majority of these are covered in Rausand and Høyland (2004) and Rausand (2014). However, these theories may in some cases not be fully adequate.

To prevent accidents like the Macondo blowout, new/improved methods for complex safety critical systems, such as the subsea BOP system, must be developed. The main focus when applying such methods is to produce an accurate result as possible. This report takes a deeper look into the subsea BOP control system, and how its current reliability analyses can be enhanced.

1.2 Objectives

The main objectives of this study are:

1. Carry out and document a literature survey on the current status of the reliability performance of subsea BOP control systems (incl. regulations and standards) and to reveal the role of these systems in drilling accidents.

2. Become familiar with the design of a typical subsea BOP control system.

3. Perform a functional analysis of a subsea BOP control system and carry out a detailed FMECA for different operational modes/scenarios.

4. Carry out a reliability assessment of a subsea BOP control system.

1.3 Limitations

The report is limited to only considering the reliability of BOP control system designed for deepwater drilling. No human factors are considered and the scope ends when the shear ram is activated.

The emphasis of the reliability analysis lies in the methodology, rather than the detailed modeling of the subsea BOP control system.

1.4 Structure of the Report

The rest of the report is structured as follows. Chapter 2 gives a description of the subsea BOP control system. Chapter 3 discusses previous reliability studies and looks at potential failures in the subsea BOP control system. In chapter 4, an overview of regulations and standards are presented, as well as a comparison between Norwegian and United States regulations and standards. Chapter 5 discusses failures in the system and the potential contribution from CCFs. Chapter 6 provides an approach to quantify the subsea BOP control systems reliability, through post-processing the minimal cut sets from the fault tree analysis, and a discussion about the following result. In chapter 7, the report is summarized and concluded, and recommendations and ideas for further work are suggested.

Chapter 2

Subsea BOP Control System

The blowout preventer (BOP) control system is the brain of the subsea BOP system. It controls when the preventers are to close and open, with or without using primary rig power. The most essential parts of the system are the accumulators, the operating fluid, the high pressure piping to transport and direct fluid and the remote unit for controlling valves with the hydraulic unit (Goins and Sheffield, 1983). The main BOP components with a short description is shown in Fig. 2.1.

2.1 Multiplex Control System

A multiplex control system (MUX) is an electro-hydraulic system applied to control the functions of a subsea BOP. The MUX system is a replacement for the all-hydraulic system, previously used for subsea BOP applications. The basic layout of a MUX control system from topside to sea bottom is shown in Fig. 2.2.

The MUX system provides electrical power, hydraulic power, control signals and communication to the numerous BOP functions. It uses modems (modulator/demodulator) to send and receive signals to and from control computers, via copper wires. The cable goes from the rig and down along the riser to the BOP. The multi conductor cables carry the multiplexed signals in both directions. The power is provided by the Power and Communication Cabinets (A & B). Each cabinet has a dedicated uninterruptible power supply (UPS) delivering 230 VAC electrical power. It has the ability to power the BOP system for a minimum of two hours, should the main

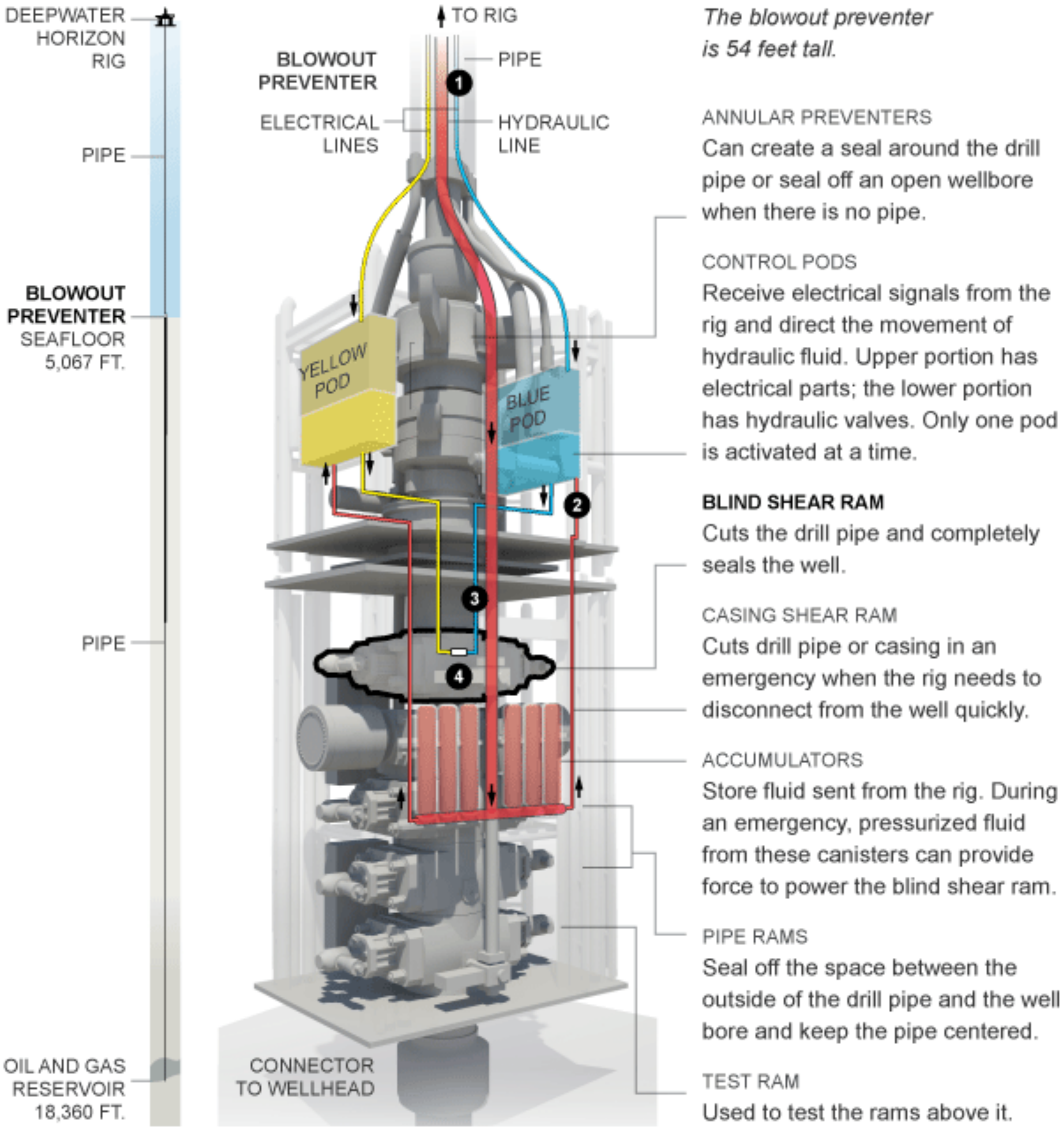

DEEPWATER HORIZON RIG
PIPE
BLOWOUT PREVENTER
SEAFLOOR 5,067 FT.
PIPE
OIL AND GAS RESERVOIR 18,360 FT.
TO RIG
BLOWOUT PREVENTER
PIPE
ELECTRICAL LINES
HYDRAULIC LINE
1
YELLOW POD
BLUE POD
2
3
4
CONNECTOR TO WELLHEAD
The blowout preventer is 54 feet tall.
ANNULAR PREVENTERS
Can create a seal around the drill pipe or seal off an open wellbore when there is no pipe.
CONTROL PODS
Receive electrical signals from the rig and direct the movement of hydraulic fluid. Upper portion has electrical parts; the lower portion has hydraulic valves. Only one pod is activated at a time.
BLIND SHEAR RAM
Cuts the drill pipe and completely seals the well.
CASING SHEAR RAM
Cuts drill pipe or casing in an emergency when the rig needs to disconnect from the well quickly.
ACCUMULATORS
Store fluid sent from the rig. During an emergency, pressurized fluid from these canisters can provide force to power the blind shear ram.
PIPE RAMS
Seal off the space between the outside of the drill pipe and the well bore and keep the pipe centered.
TEST RAM
Used to test the rams above it.

Figure 2.1: Typical configuration of a subsea BOP, from Grondahl (2015)

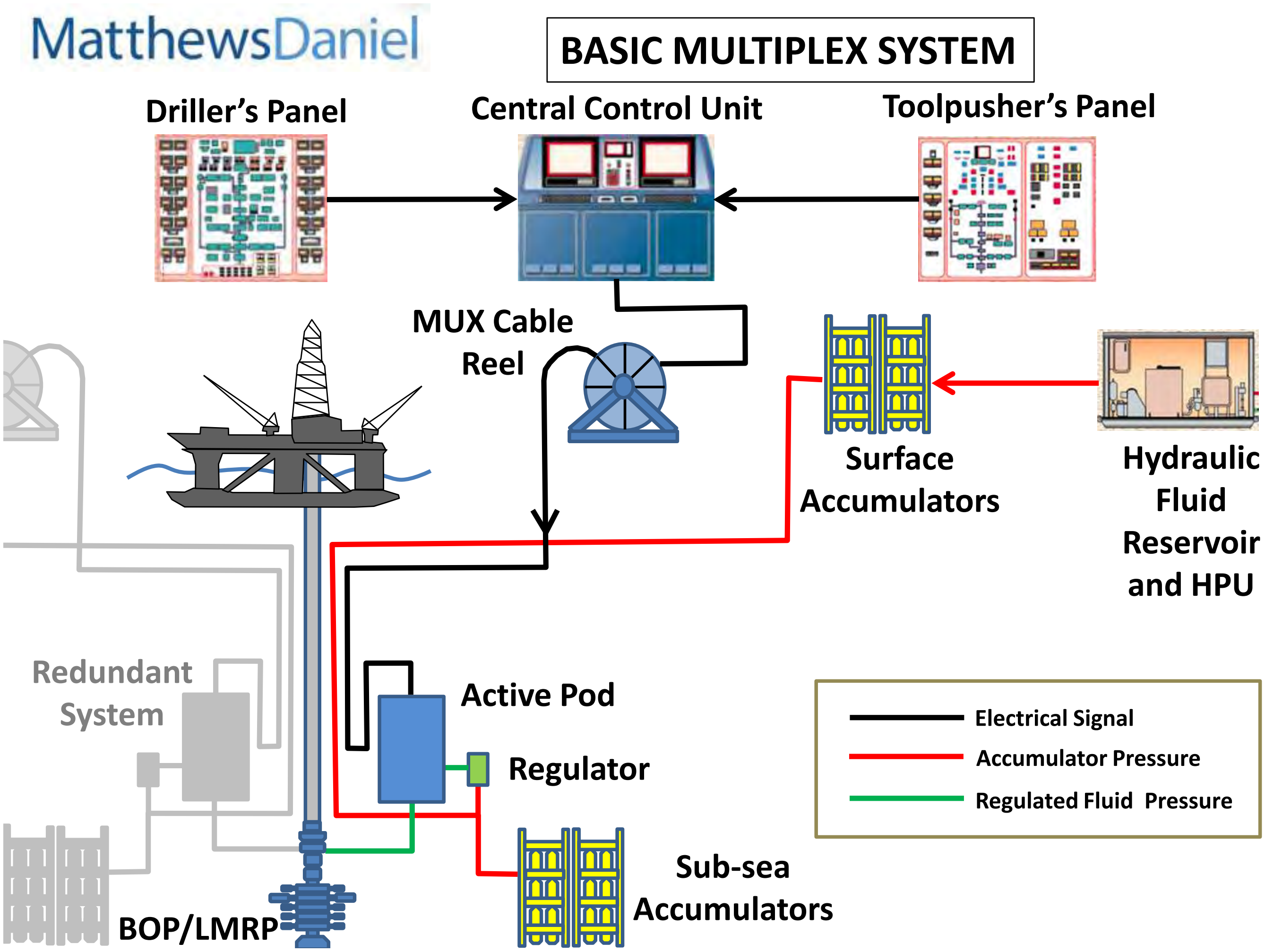


Figure 2.2: Basic MUX system, from Rees and Matthews (2011)

power be lost (Engineering Services LP, 2014).

The MUX control system is housed on the lower marine riser package (LMRP). Stingers connect the hydraulic control between the LMRP and the BOP stack. The stingers are located at the bottom of the LMRP and are extended to fit into recipients on the BOP side (stingers are shown in Fig. 2.4). When connection is made, each individual seal is activated by the corresponding stinger to prevent leakages.

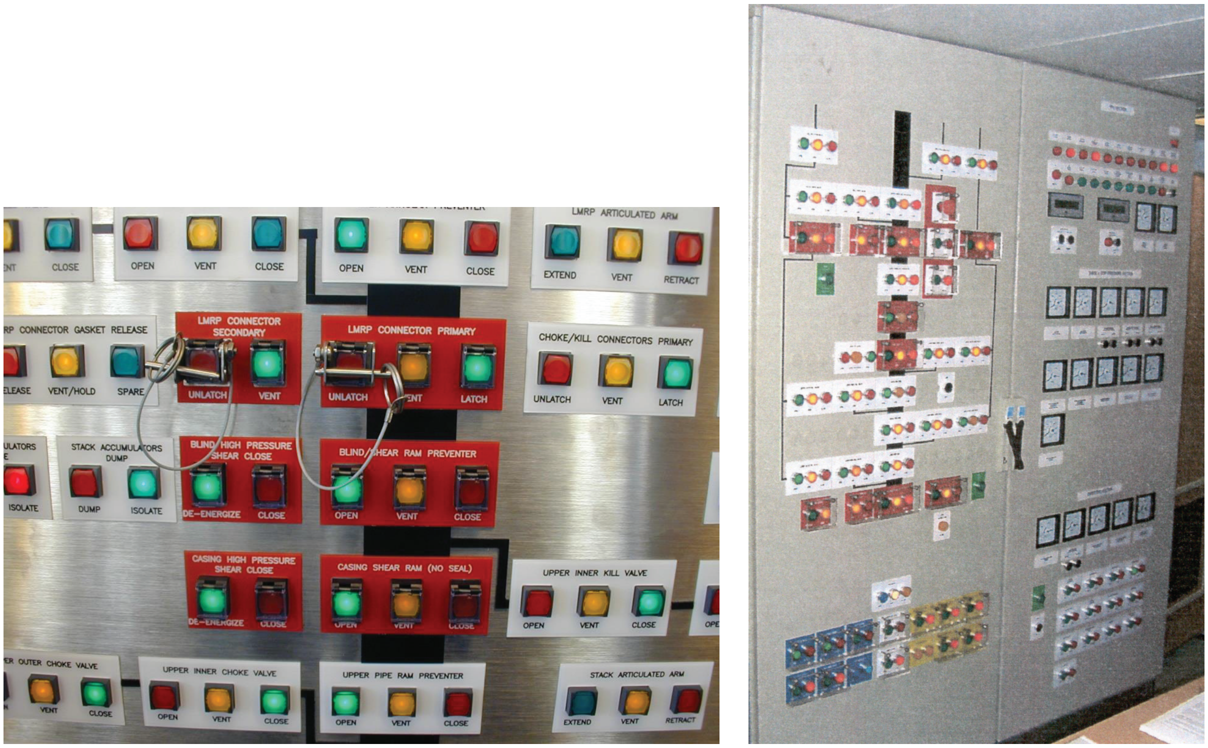


Figure 2.3: Driller's panel, from Imperial Oil and ExxonMobile (2009)

2.2 MUX Control Panels

Normally, three control panels controls the MUX system, driller's control panel (DCP), toolpusher's panel (TCP) and a remote panel. The DCP is located on the rig floor, while the TCP is on the bridge. They both contain a set of pushbuttons controlling the BOP functions. Functions of high criticality are often equipped with covers, seen in the left hand picture in Fig. 2.3. Alarms indicating abnormal fluid level, pressure and "read backs", are shown in the right hand side picture.

The remote control panel contains the same functions to operate the BOP, and can be done remotely from the hydraulic control manifold or the central processor. The panel is required to be explosion proof or air-purged and is normally placed in the toolpusher's quarters, or in similar nonhazardous areas (Hals and Molnes, 1984).

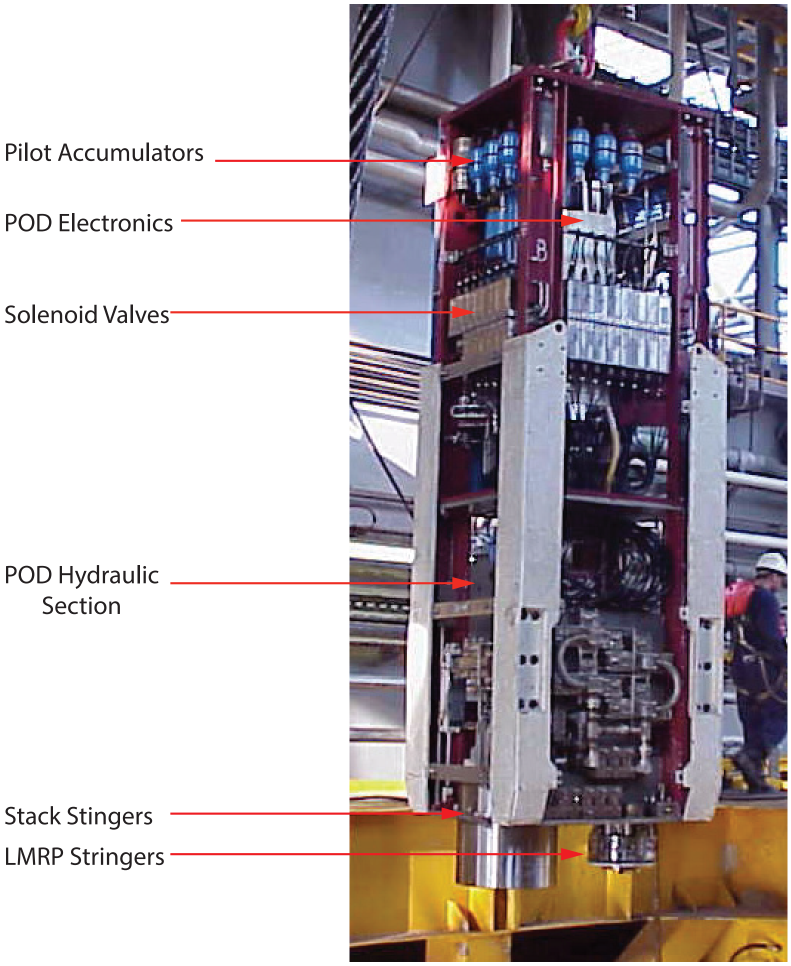


Figure 2.4: Complete pod with covers removed, adapted from Imperial Oil and ExxonMobile (2009)

2.3 MUX Control Pod

The MUX control pod is an electro-hydraulic valve control mounted on the LMRP. Normally there are two pods, but systems including three do exist. They are identical, interchangeable and can be installed in the blue or yellow position (see Fig. 2.1 for placement). Each pod consists of hydraulic pressure regulators, solenoid pilot valves, subsea electronic modules (SEMs), subsea transducer modules (STMs), hydraulic valves and hydraulic accumulators (Engineering Services LP, 2014). Both pods receive commands from the MUX and initiate solenoid valve actions; however, only one does it with hydraulic fluid, causing the effect of the other pod to be none. A pod without covers and named elements is shown in Fig. 2.4.

Both pods can perform all required functions on the BOP, making them redundant. However, a problem occurring in one of the pods will cause the system to be retrieved to the surface for repair. A major problem occurring during operations would cause the system control to be transferred to the other pod. Preparations for retrieving the riser and the LMRP, will immediately start. Situations where problems can be considered minor, may prevent the system from retrievement (Shanks et al., 2003).

An example of the control systems logic for an element closure in a subsea BOP is shown in Fig. 2.5. The hydraulic fluid is transported from the reservoir bank, through rigid and flexible conduit lines in the umbilical and ending in the conduit valve package (Drægebø, 2014). In the conduit valve package a pod selector directs the fluid to one of the pods. Before entering the pod, the fluid pressure is controlled/adjusted by a hydraulic regulator.

Each pod contains a low-pressure accumulator and a solenoid valve for each preventer. The generated low-pressure fluid is directed via a shuttle valve and into a pilot valve, opening for the high pressure fluid to go to the preventer(s) through hard lines.

An example of the process in Fig 2.5 could be: A situation requiring a BOP ram to close, a MUX signal would be sent from the central control unit to the pod for decoding. The decoded signal would notify the specific solenoid valve to open, causing the low-pressure hydraulic fluid to open the pilot valve. As a result, the pilot valve would shift and send stored high-pressurized hydraulic fluid from the accumulator to the BOP ram for closure.

2.4 Subsea Electronic Module

For each MUX control pod placed on the BOP, a corresponding subsea electronic module (SEM) is installed. The SEM is a sealed pressure vessel protecting the subsea electronics and batteries against the subsea environment. The SEM is internally redundant containing two programmable logical controllers (PLCs), two 9-volt battery packs and two automatic mode function/deadman cards (Engineering Services LP, 2014). The internally redundant systems are referred to as SEM A and SEM B. The inside of the pods, and the placement of the SEMs are displayed in Fig. 2.6.

During normal operations, a 230 VAC electrical power supply voltage feeds the two power supplies inside the SEM. The main control cable goes from the topside equipment and to an

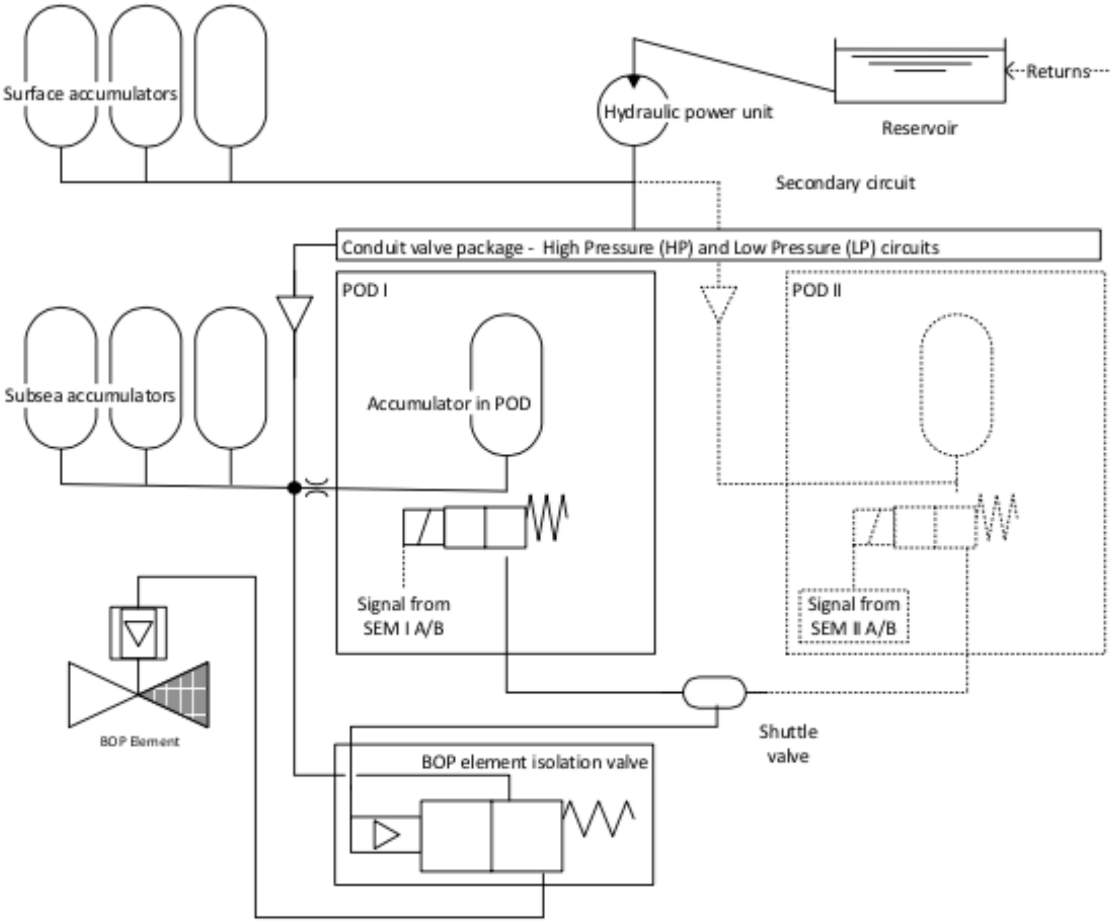


Figure 2.5: Example of a BOP element function electro-hydraulic control system principle, from Strand (2014)

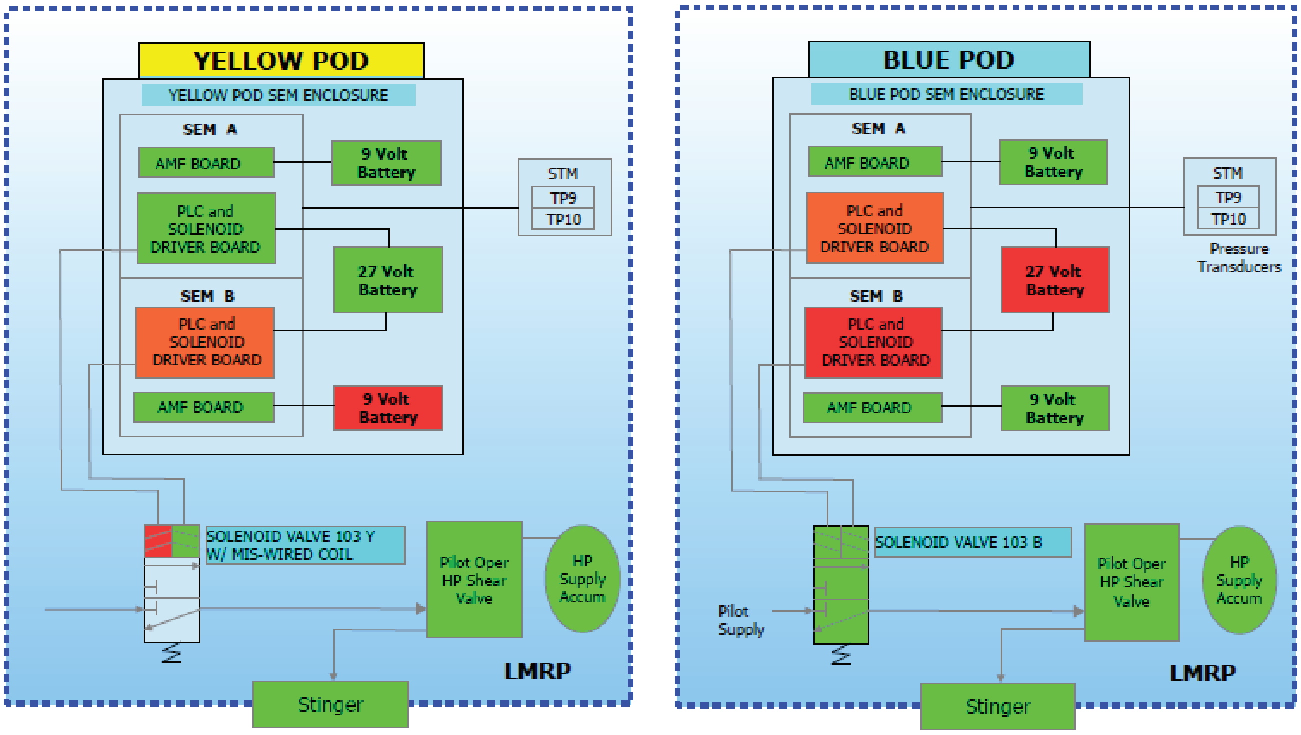


Figure 2.6: Inside of a POD, from Engineering Services LP (2014)

electrical connector mounted in the base plate on the pod. The power conductors are connected with the power supply, while signal conductors are connected to the MUX system modem. The modem controls both the uplink and downlink communication for the system. Analog data signals from pressure transducers and other sensors are digitally converted before transmitted to the surface. All-important values for pressure and voltage are monitored by this system. A SEM with and without housing is displayed in Fig. 2.7.

2.5 Solenoid Valve

In a subsea BOP application, a solenoid valve (SV) is a hydraulic valve activated by an electrical signal from the control system, which produces a pressure output by opening an internal valve (Engineering Services LP, 2014). Normally the SV is equipped with two redundant coils within its core. One or both coils can be energized by a 24/27 VDC power supply, causing actuation of a hydraulic valve.

Commands from the rig are sent through the MUX control system and converted by the

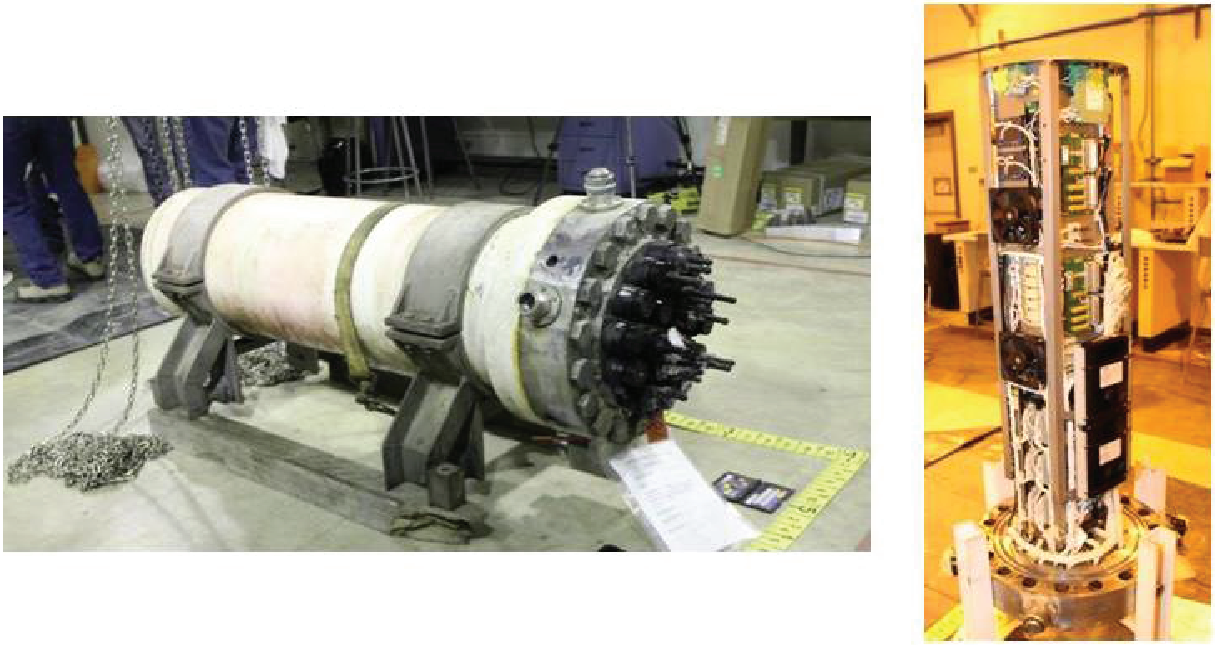


Figure 2.7: Example of a SEM with and without housing, from Engineering Services LP (2014)

SEMs to numerous actions, operating the BOP functions hydraulically. The electrical outputs from the SEMs are converted into hydraulic fluid actions, using the SV. When the SV is electrically energized, the magnetic forces in the coil pull the armature of the solenoid into the space within the coil and open the valve (Engineering Services LP, 2014). When the coil is deengergized, a spring pushes the armature back, closing the valve. In systems with redundant coils, activation of one coil is enough to actuate the solenoid. However, in the Macondo accident it came apparent how critical the polarity of the coils is. One of the coils was wired with opposite polarity, and the magnetic effect was canceled out. In this case the valve would not open, despite energizing both coils.

The hydraulic section of the SVs use sliding metal-to-metal, shear type seals, the same as the main BOP control valves (Cameron Controls). The SVs are arranged and installed in a way that makes them easily accessible from the outside of the MUX package (see Fig. 2.4).

The SVs need to endure pressure in the range of 3000 to 5000 psi, and temperatures down to 1.6 °C. As a result, the valves are enclosed in a heavy stainless steel housing (shown in Fig. 2.8) for protection. It also includes cable assemblies, allowing the SV to be plug-connected to the control system (Engineering Services LP, 2014).

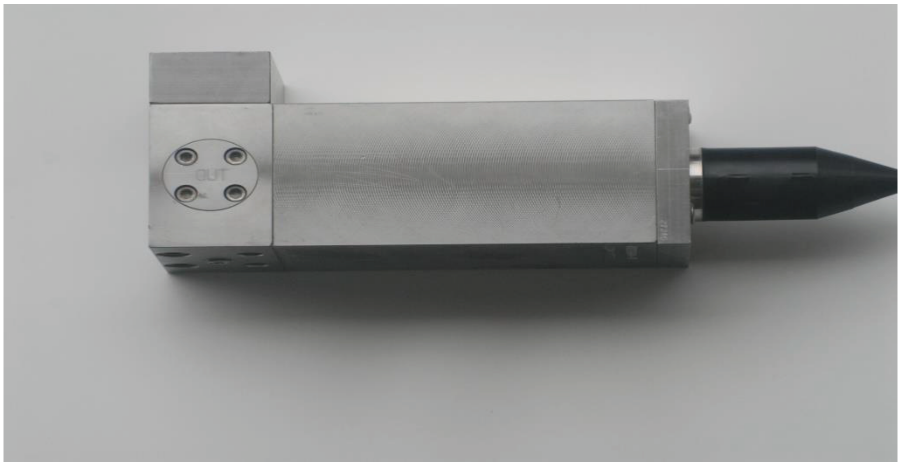


Figure 2.8: Typical BOP solenoid valve, from Engineering Services LP (2014)

2.6 Cable

Communication between the rig and a subsea BOP primarily goes through cable. There are two types of cables applied, hydraulic and MUX. The different cables each belong to one of the different control systems, the all hydraulic system and MUX system, which both holds advantages and disadvantages.

In a hydraulic cable, individual hydraulic lines represent all the BOP functions. The cable consists of numerous small hydraulic lines wrapped around a thick line for the hydraulic supply, going to the accumulators. The deeper the well, the longer it takes for the hydraulic system to activate the BOP functions. The hydraulic system is therefore not recommended for deep water drilling, as it also requires more hydraulic fluid and more pressure to be pumped.

In a MUX cable only electrical signals and power supplies are sent down to the control pods. The pods have PLCs to decode the signals, before forwarding the commands. The hydraulic fluid for the accumulators is sent via a separate line. The distance does not affect the multiplexed line and the pods will receive a command from the surface instantaneously. The MUX cables are most common nowadays for subsea BOP control systems. Compared to the all hydraulic they are costs reduced, size of lines are decreased and problems with retrieving and running large hose bundles are removed.

The MUX cables are stored on reels on the platform. The reels are equipped with slip rings, allowing circuitry to be maintained during reel rotation. The cable is normally equipped with

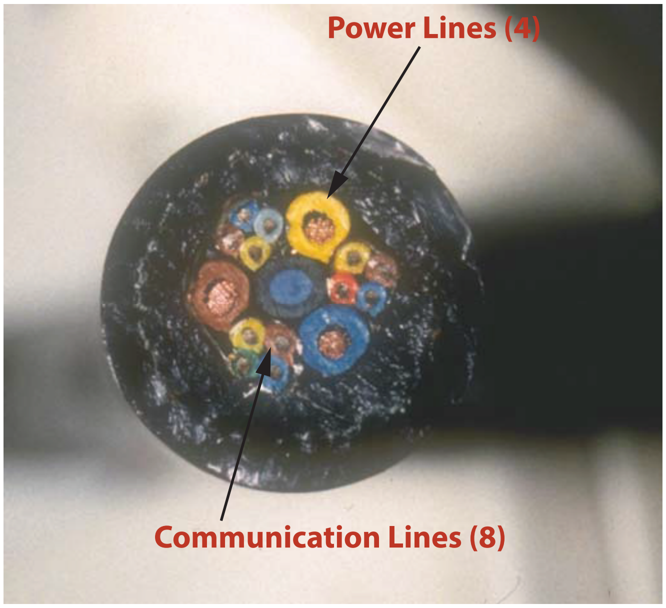


Figure 2.9: MUX cable, from Imperial Oil and ExxonMobile (2009)

four power supplies wires and 6-12 communication conductors. Typically, the cable has an outer diameter of 1-1/2" (Imperial Oil and ExxonMobile, 2009). A typical MUX cable is shown in Fig. 2.9.

2.7 Hydraulic Power Unit

The hydraulic power unit (HPU) mixes, monitors, stores hydraulic fluid and generates pressurized hydraulic fluid for BOP system control usage. The hydraulic fluid helps operate the numerous BOP functions and surface accumulators, going via regulators and manifolds.

The HPU pressure is normally in the range of 3000 to 5000 psi and is charged with three or four electric powered triplex pumps, with one typically connected to the emergency generator. The accumulators are charged with enough energy to operate all the BOP stack functions.

The fluid going through the system is a mixture of water and water-soluble oil, with a ratio ranging from 1:50 - 1:100. In cases where temperatures gets too low, glycol antifreeze is mixed into the fluid, preventing the lines from freezing (Hals and Molnes, 1984).

2.8 Accumulators

Requirements to having three different sets of accumulators in a MUX subsea BOP system is given:

1. Topside
2. On the LMRP
3. On the BOP stack

Normally, two accumulator banks provide pilot pressure to the pod pressure regulators. Each bank consisting of four small accumulators, see Fig. 2.4.

The accumulators are precharged nitrogen bottles containing hydraulic fluid under pressure (Hawker, 2011). Each accumulator has a predefined pressure, dependent on the operating water depth. The charge pressure from the accumulator banks is controlled by "bleeding" and "feeding" short pulses from the controlling solenoid valves (Cameron Controls).

API 53 (2012) specifies time limits for executing each of the BOP functions, typically at 30, 40 or 60 seconds. The subsea accumulators can be considered batteries charged with hydraulic fluid, applied to fulfill the requirements. Should the umbilical be disconnected or broken, will the LMRP functions be activated either through remotely operated vehicle (ROV) operations or acoustic control.

Both for topside and stack mounted accumulators are the supply systems arranged in the same way. Charged to the right pressure and automatically recharged when the pressure drops too low. The blue and yellow control pods share the same accumulator, causing a leakage to affect both pods. To ensure that a failure on one pod does not affect the accumulator, the hydraulic supply system is equipped with accumulator isolation valves. Closing of the valves and regaining control topside will influence the closing time of each preventer severely.

Accumulators located subsea on the BOP stack is normally precharged up to 1200 psi, plus the hydrostatic pressure. Retrieving the accumulators requires the pressure to be bled off subsea, preventing the accumulators from bursting once they reach the surface or before.

The main contribution from the accumulators is to reduce the response time from the system, and absorb shock waves caused by high pressure and flow, as a result of function activation.

2.9 Programmable Logic Controller

A programmable logic controller (PLC) is an industrial computer that receives and interprets signals from the rig deck, and forwards commands. Normally, the subsea MUX PLCs communicate with computers on the rig and subsea, but can in emergency situations operate on its own (Engineering Services LP, 2014). During operations, the PLCs continually cycles through programmed inputs. All control computers react as predefined when receiving communications on the bus network.

2.10 Relay

A relay can be considered a small electrical switch, enabled by electric signals from the control system. It can have several different outputs and is normally used to control inputs to other logical devices or small power activations.

2.11 Subsea Transducer Module

Subsea transducer modules (STM) facilitate wiring and electronics to the temperature and pressure transmitters used in the MUX system in each pod.

2.12 Hose Bundles and Reels

The hydraulic hose bundles transport the fluid from the master control manifold and down to the blue and yellow control pods. Normally the supply line has an inner diameter (ID) of 1.0".

The hose bundles are connected to the master control manifold by jumper hoses and are mounted on big reels for storing and handling.

2.13 Typical Control Fluid

Fig. 2.10 shows a typical arrangement of a BOP control fluid circuit. The accumulator increases the fluid pressure to 3000-5000 psi, from thereon the fluid is sent via the pod selector valve and further down to one of the pods.

When the hydraulic control fluid is transported from the surface to the pods, a significant pressure drop occurs over the normally 1" ID cable. As a result, the flow rate from the surface accumulator is limited. The stack-mounted accumulators therefore assist with boosting the BOP open-/closing time response, to an acceptable level.

Should a fault occur or maintenance is required on one of the accumulators, total isolation from the circuit can be done with isolator pilot valves. Both surface and subsea accumulator valves gets blocked, isolating the accumulators from the line. They are brought back on the line when the isolator pilot valves are moved in the opposite direction.

The hydraulic manifold contains a flow meter for volumetric measuring of the control fluid. An accurate flow meter can record how much of the fluid volume is consumed by the subsea system, and indicate if something is wrong.

The initial pressure produced in the accumulator is too high for most BOP stack functions. As a result, pressure regulators are mounted on top of the pods. Normally a BOP control system consists of 2-3 regulators. One dedicated to regulate the pressure on the marine riser ball joint, one for the annular preventers and one for the ram preventers (Hals and Molnes, 1984).

In Fig. 2.10 the selector valve shows two potential sources controlling the pressure. With the selector valve in the UNIT position, the air regulator mounted on the master hydraulic manifold adjusts the pressure. When the selector is in the REMOTE position, the operator, through push buttons, controls the pressure. By energizing solenoid valves corresponding to the given command, adjustments through the air pilot regulator are made. A monitoring line for the subsea pressure is sent up to the pressure gauge on the manifold, and further directed to indicators in the driller's panel.

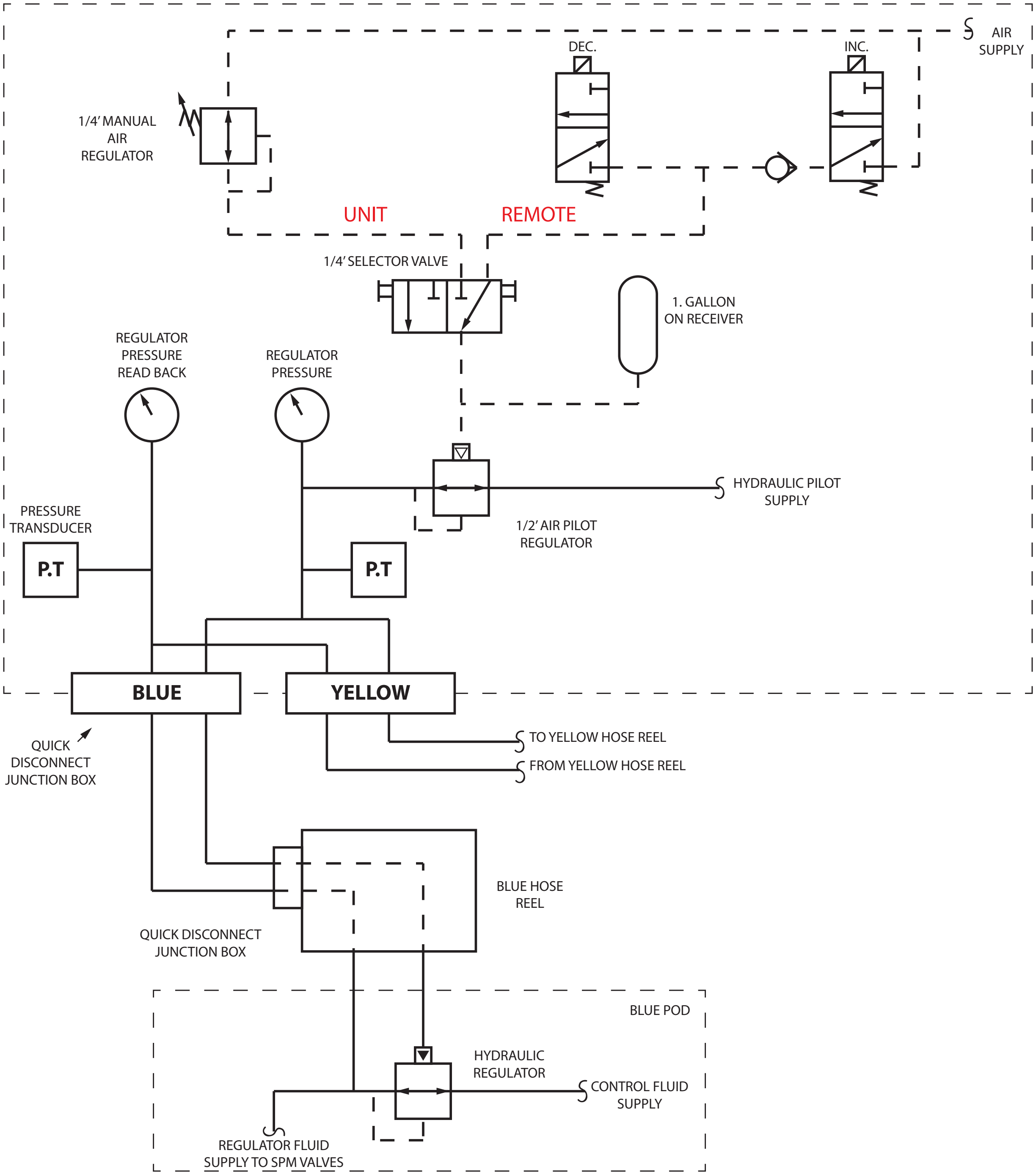


Figure 2.10: Typical control fluid pressure regulator circuit, from Hals and Molnes (1984)

Chapter 3

Reliability Review

There are two types of BOP failures considered important: (i) Failures that prevents the BOP from acting as a safety barrier or making the BOP unable to perform a safety function, and (ii) failures resulting in drilling stop and thereby causing economic losses.

The following review is conducted to highlight the significant contribution to downtime on subsea BOPs caused by the control system.

☞ **Reliability**: The ability of an item to perform a required function under stated environmental and operational conditions and for a stated period of time (IEV ref 192-01-24).

3.1 Introduction

This chapter reviews several reliability reports on subsea BOP equipment. The review is carried out to highlight critical BOP issues, and be an indicator to where greater focus regarding reliability for a subsea BOP system should be. The review is based on the three following study reports, assigned simpler names for readability:

- Study 1 - *Phase I DW*, examined the reliability of subsea BOPs applied in wells drilled in more than 400 meters water depth in Norway and Brazil, during 1992-1996. The study is further discussed and analyzed in Holand and Awan (2012) and Holand (1999).

- Study 2 - *Reliability of Subsea BOP Systems for Deepwater Application, Phase II DW*. It examines the reliability of subsea BOPs applied in wells drilled above 400 meters to more than 2000 meters water depth in the Gulf of Mexico (GOM), during 1997-1998. The study is further discussed and analyzed in Holland (1999).

- Study 3 - *Reliability of Deepwater Subsea BOP Systems and Well Kicks*. Looks at the reliability of subsea BOPs applied in wells drilled in more than 600 meters in the GOM, during 2007-2009. The study is further discussed and analyzed in Holand and Awan (2012).

3.2 BOP General Reliability

The studies introduces different expressions, the following are used frequently in this review.

- **BOP failure** can be a failure of a single component or a control system failure. A BOP failure does not necessarily lead to retrievement of the system, because of the redundancy in the system.

- **BOP days** are the total number of days from when the BOP is attached to the wellhead, until it is retrieved for the last time.

- **Mean time to failure (MTTF)** is the average time for the first failure of a component on the BOP. The MTTF is the inverse of the failure rate, for systems with constant failure rates.

- **Safety critical failures** can occur after the installation test of the subsea BOP is completed. The BOP acts as a well barrier, and failures are therefore critical. The importance of a failure depends on which part of the BOP system fails.

- **Hours lost** refer to the number of hours were drilling is suspended, caused by failures on equipment.

3.2.1 Mean Time To Failure

A comparison of the three studies with respect to MTTF and average downtime is shown in Tab. 3.1. It should be noted that the sources of information in the different studies differ. Study 1 and 2 uses daily drilling reports, whereas study 3 is based on the well activity reports. In the well activity reports, less critical failures with little downtime are often not reported, and will not show up in the comparison, making the analysis somewhat degraded. The most important results from the studies are listed below.

- In study 1, the MTTF was approximately 23 days, with an average downtime of 25 hours per failure.
- In study 2, the MTTF was approximately 34 days, with an average downtime of 31 hours per failure.
- In study 3, the MTTF was approximately 96 days, with an average downtime of 86 hours per failure.

Comparing study 1 and 2 reveals a slight difference. Study 2 has a higher MTTF, but the average downtime per failure is also higher.

In study 3, the differences from the two previous studies are much bigger. The MTTF has almost tripled, but the repair time for a component also increased significantly. The changed MTTF came as a result of improved equipment on the BOP. For the increased repair time, no explicit reason was given in the reports other than the effect of the increased water depth. Despite the increased pulling length, the downtime would most likely not be tripled. Other factors that may have contributed could be the increased complexity of the system, changed maintenance routines once the equipment already is pulled, bad weather or unavailability of spare parts.

3.2.2 BOP Downtime

☞ **BOP downtime**: The number of hours lost because of a failure on the BOP, regardless of the BOP being attached to the wellhead or not (Holand and Awan, 2012).

In study 1, the average downtime per BOP day was 1.08 hours. The biggest contribution to the downtime came from the control system and choke/kill line failures (MCS Kenny, 2013).

Table 3.1: BOP MTTF and average downtime, from Holand and Awan (2012) and Holand (1999).

Study	Location of Subsea BOPs	Period	No. of Wells	BOP-days	Total lost time (hrs)	No. of failures	MTTF (BOP-days)	Avg. downtime per failure (hr.)	Avg. downtime per BOP-day (hrs)
1	Brazil and Norway, wells drilled in water depth more than 400 m	1992 – 1996	144	3,191	3457.5	138	23.12	25.05	1.08
2	GOM, wells drilled in 400 m to more than 2000 m	1997 – 1998	83	4,009	3637.5	117	34.26	31.09	0.91
3	GOM wells drilled in water depth more than 600 m	2007 – 2009	259	15,056	13,448	156	96.51	86.21	0.89

In study 2, the average downtime per BOP day was 0.91 hours. In this study, the downtime was mainly caused by failures in the ram preventers. The preventers failed to open on three different occasions, this was not observed in early stages of BOP testing. The accident report concluded that it came as a result of new designs (MCS Kenny, 2013).

In study 3, the average downtime per BOP day was 0.89 hours, which was the lowest of all three studies. The main contribution to the down time came as a result of a failure occurring on the control system were only the LMRP needed to be retrieved. This caused the BOP stack to be left on the wellhead, avoiding major downtime.

3.2.3 BOP Failure Discussion

For a failure to be critical in terms of well control, the BOP must be an acting barrier. The BOP is first considered an acting barrier when attachment on the wellhead is made and the installation test is completed and accepted. All failures occurring on the BOP after installation are considered safety critical failures. The severity of a failure depends on which part of the systems is compromised.

The failure distribution of the different BOP studies is shown in Fig. 3.1. The average downtime per hour for the main components in the BOP are listed. The control system is likely to

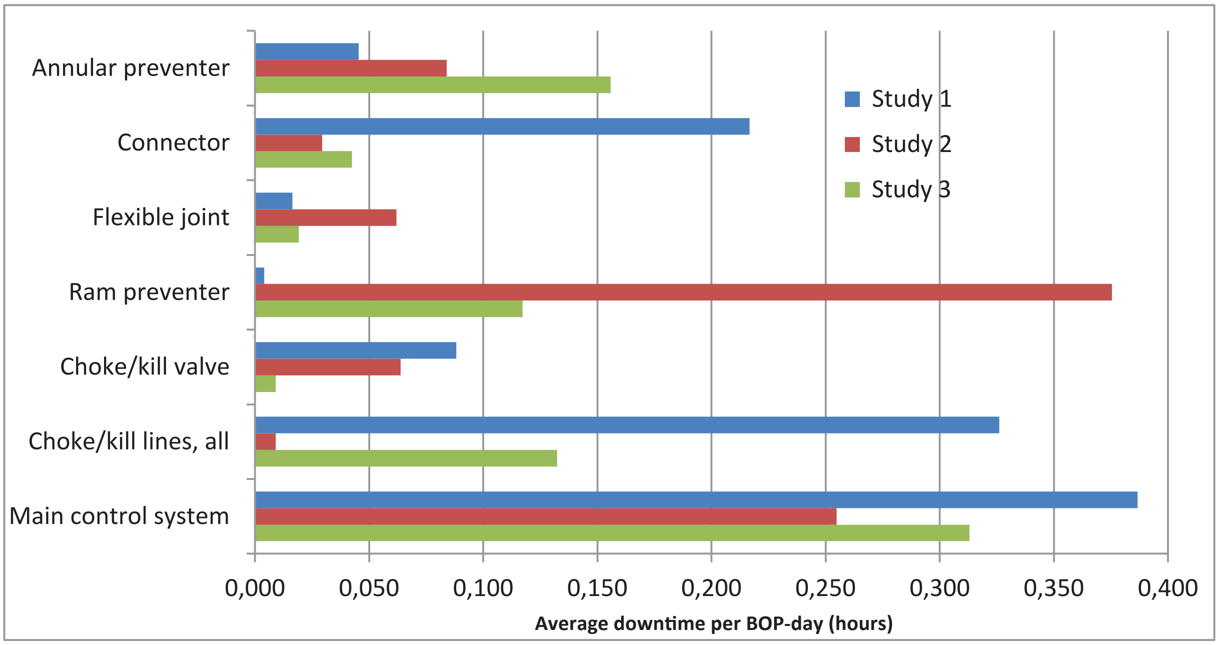


Figure 3.1: Comparison of BOP item specific downtime, from Holand and Awan (2012)

cause the most downtime in all three studies, with the exception of the ram preventers in study 2. The control system failures were revealed during function tests. However, a failure in the control system will most likely not compromise the well control, because of its redundancy.

A summary of the number of failures and the corresponding percentages for the main BOP components are shown in Tab. 3.2, revealing the subsea BOP control system as the biggest contributor to equipment failure in all studies. The failures are revealed by function tests performed every 7 days, as required by The Bureau of Safety and Environmental Enforcement (BSEE), title 30, part 250.449. Failure data from study 1 is restricted. Summing up Tab. 3.2, the most important values are:

- Study 1: 45% of all failures came from the control system.
- Study 2: 60 of the total 117 failures, 51%, came from the control system
- Study 3: 72 of the total 156 failures, 46%, came from the control system

The control system clearly dominates the failure rates in every study. However, the control systems include several components, making it more vulnerable to failures.

Table 3.2: Summary of BOP failures, from Holand and Awan (2012) and Holand (1999).

	Study number		
	1	**2**	**3**
BOP Components	**No. of Failures/percentage**		
Annular Preventer	-	12/ 10%	24/ 15%
Connector	-	10/ 8%	8/ 5%
Control System	45%	60/ 51%	72/46%
Choke & Kill Valve	-	13/ 11%	4/ 2.5%
Choke & Kill Lines, All	-	8/ 7%	17/ 11%
Ram Preventer	-	11/ 9%	23/ 15%
Flexible	-	1/ 0.08%	1/ 0.06%
Total	**138**	**117**	**156**

Table 3.3: MTTF of main BOP components, study 2 and 3, from Holand and Awan (2012) and Holand (1999).

	Study number	
	2	**3**
Component/ System	**MTTF Operating days/ failure**	
Annulars	334	627
Rams	364	655
Choke & Kill Valves	308	3,764
Choke & Kill Valves, All	501	886
Connectors	401	1,882
Control Systems	67	209
- Conventional	71	242
- MUX	46	198
Flexible Joint	4,009	15,056

MTTF for main subsea components during operating days is shown in Tab. 3.3. Note that every single component has an increased MTTF in study 3, compared to study 2, and for the control systems it has more than tripled. This comes as a result of development of technology and increased robustness on the different components. No MTTF data is available on study 1 in the public domain.

Failures that could not be assigned to the categories described in Tab. 3.2 or 3.3 have not been taken into account in this comparison.

3.3 Subsea BOP Control System Reliability

3.3.1 Control System Mean Time To Failure

In the different studies all three types of subsea BOP control systems are represented: Pilot hydraulic control system, pre-charged pilot hydraulic control system and multiplex control system (MUX).

The pilot signal is transmitted from the rig to the subsea control pods. The main differences between the systems are found in the pilot hydraulic control system where the pilot valves are activated directly by a pilot signal. The pre-charged pilot hydraulic system works the same way as the pilot hydraulic, only the pilot signal is given a pre-charged pressure, reducing the response time. For the MUX system, an electrical signal is transmitted to the pods instantaneously, allowing the subsea pilot valve to function immediately (Holand, 1999).

Study 1 and 2 was mainly dominated by pilot hydraulic or pre-charged pilot hydraulic systems. In study 3 the majority of rigs were equipped with MUX systems.

A comparison of the control systems MTTFs for the different studies is shown in Fig. 3.2. It can be seen that the MTTF in study 3 is increasingly larger compared to the previous two. Tab. 3.1 shows that significantly more BOP days are covered in study 3. It seems that the BOPs in general have improved compared to older studies. It should be noted that study 3 is based on well activity reports, whereas the two others are based on daily drilling reports, as mentioned earlier. This will have an effect on the calculated MTTF.

The MTTF for the MUX control systems and the conventional pilot control systems from study 3 are compared in Fig. 3.3. The differences between the systems are not significant, and similar results were found in the two other studies (Holand and Awan, 2012).

The average failure downtime for the different subsea BOP control systems in study 3 is shown in Fig. 3.4. The MUX system had approximately double the downtime, compared to the conventional. It should be noted that the MUX system was applied in deeper waters compared to the conventional. The increased downtime mainly came as a result of a few failures requiring a long repair time (Holand and Awan, 2012).

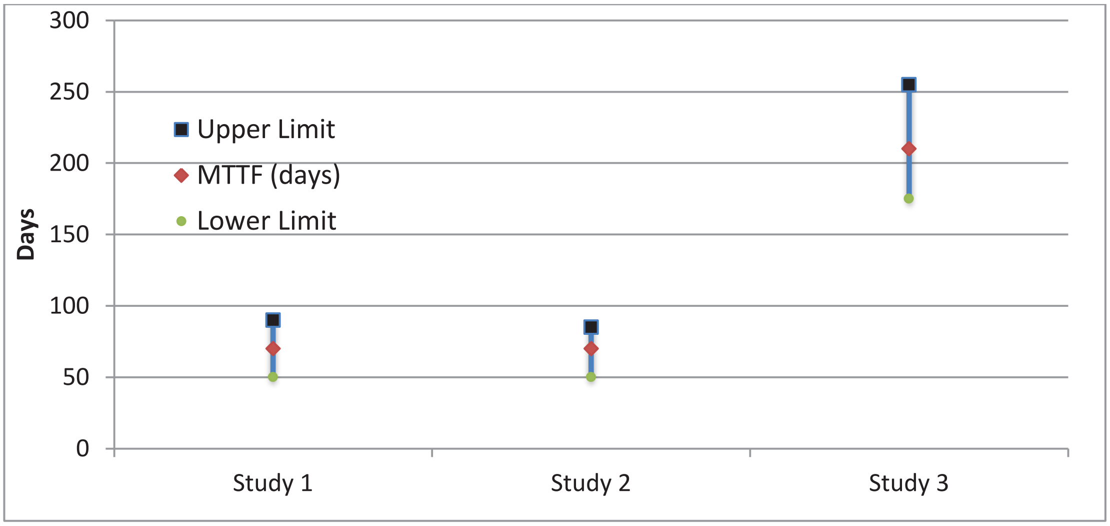


Figure 3.2: Control system MTTF, comparing study 1,2 and 3, with 90% confidence limits, from Holand and Awan (2012)

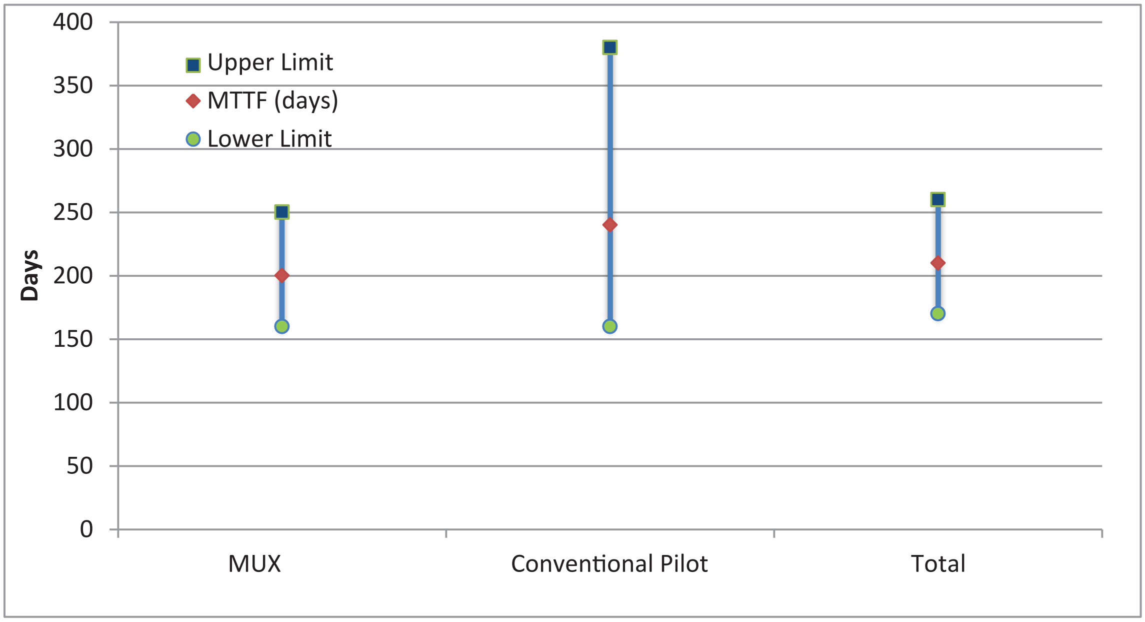


Figure 3.3: MTTF of BOP control system in Study 3, with 90% confidence limits, from Holand and Awan (2012)

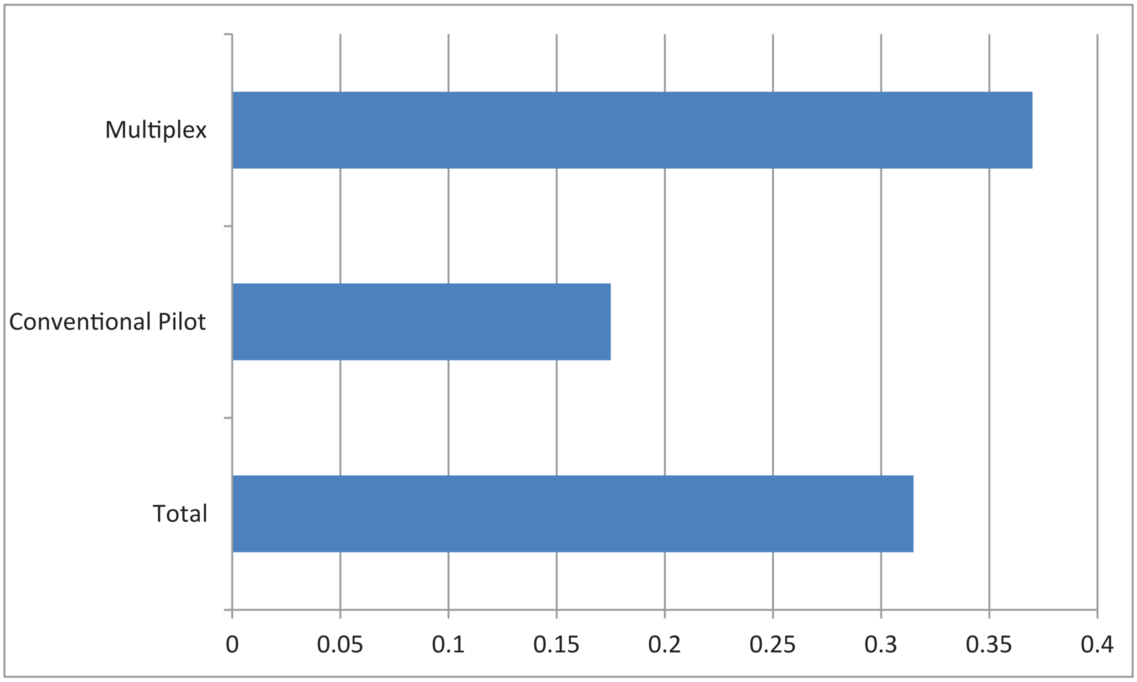


Figure 3.4: Average failure downtime per BOP day on different types of BOP control systems for Study 3, from Holand and Awan (2012)

3.3.2 Control System Failure Discussion

The majority of the control system failures were caused by failures of components in the control pods. For example, leakages in solenoid valves, leakage in subsea plate mounted (SPM) valves or malfunction in stack connector regulator (MCS Kenny, 2013).

The control system failures from study 2 are presented in Tab. 3.4. Failures marked "Unknown" are unspecified failures. Failures marked "Other", are failures specified in different categories than the ones in the table. Failures detected and resolved by switching to the back-up system, is marked with zero loss of time.

In the MUX control system, the dominating downtime came from loss of all functions in one pod, with an average downtime of 198.5 hours per failure. Only one incident of loosing function in both pods occurred during the study, leading to 2.5 hours without control of the BOP.

The control system failures for study 3 are presented in Tab. 3.5. The dominating downtime of the MUX control system came from loss of all functions in one pod, with an average downtime of 132.7 hours per failure.

The failure causing the most downtime in both studies are "Loss of all functions one pod".

Table 3.4: Control system failure distribution for study 2, from Holand (1999).

Type of Failure	**No. of failures**	**Total lost time (hrs)**	**Average Downtime - per BOP-day (hrs)**	**Days in Service (BOP-days)**
Multiplex Electro Hydraulic				
Loss of all functions both pods	1	2.5	2.5	
Loss of all functions one pod	1	189.5	189.5	
Loss of one function one pod	1	1	1	
Unknown	4	17.5	4.4	
Other	3	10	3.3	
All	**10**	**220.5**	**22.1**	**459**
Pre-charged pilot hydraulic				
Loss of all functions both pods	1	42.5	42.5	
Spurious operation of BOP function (s)	1	1.75	1.8	
Loss of several functions one pod	4	54.5	13.6	
Loss of one function one pod	4	14	3.5	
Unknown	2	7.5	3.8	
Other	4	18.5	4.6	
All	**16**	**138.5**	**8.7**	**552**
Pilot Hydraulic				
Spurious operation of BOP function(s)	2	57.5	28.8	
Loss of all functions one pod	6	173.5	28.9	
Loss of several functions one pod	1	135	135	
Loss of one function both pods	1	121.5	121.5	
Loss of one function one pod	8	33.5	4.2	
Loss of control of one topside panel	1	2	2	
Unknown	3	81	27	
Other	4	16	4	
All	**26**	**620**	**23.8**	**2,553**
Conventional Pilot, unknown if pre-charged or not				
Loss of all functions one pod	2	3.5	1.8	
Loss of several functions both pods	1	0	0	
Loss of several functions one pod	1	35.5	35.5	
Loss of one function one pod	2	1	0.5	
Unknown	2	2.25	1.1	
All	**8**	**42.25**	**5.3**	**445**

Table 3.5: Control system failure distribution for Study 3, from Holand and Awan (2012).

Type of Failure	**No. of failures**	**Total lost time (hrs)**	**Average Downtime - per BOP - day (hrs)**	**Days in Service (BOP-days)**
		Multiplex Electro Hydraulic		
Loss of all functions both pods	1	192	192	
Loss of all functions one pod	12	1592.5	132.7	
Loss of one function both pods	4	168	42	
Loss of one function one pod	10	576	57.6	
Loss of several functions one pod	1	0	0	
Unknown	19	1,108.5	58.3	
Other	5	330	41.3	
All	**55**	**3,967**	**72.1**	**10,942**
		Pilot Hydraulic		
Loss of all functions one pod	2	216	108	
Loss of one function both pods	2	0	0	
Loss of one function one pod	6	25	4.2	
Loss of several functions one pod	2	504	252	
Unknown	1	0	0	
Other	4	0	0	
All	**17**	**745**	**43.8**	**4,114**

The root cause of the failure is difficult to determine, but most likely it could come from loss of power, loss of hydraulic, dirt entering the system or a systematic error in the programming logic.

In all three studies, all functions in both pods failed in the control systems. This is a safety critical failure, as it leads to loss of control of the entire BOP.

Common for both studies is that only failures occurring in the system were documented, such that no indication to what other types of failures were tested for. As a result, Tab. 3.4 and 3.5 are not equal to each other, and a satisfactory comparison is much more difficult to conduct.

Chapter 4

Regulations and Standards

In the following chapter, only Norwegian and United States (U.S.) requirements for subsea BOPs are discussed, as they are the most relevant for this report.

4.1 American Requirements

4.1.1 BSEE

The Bureau of Safety and Environmental Enforcement (BSEE) provide regulations for design, operation and maintenance of subsea BOP systems in federal waters of the U.S. Gulf of Mexico (USGoM). Internationally, the BSEE regulations are considered the most recognized regulations (Strand, 2014). For guidance on how to fulfill the requirements, BSEE make references to important standards from the American Petroleum Institute (API), such as, API 53 (2012), API spec 16D (2005), and API spec 16A. Main design requirements from BSEE for a subsea BOP, with primary focus on the control system, are listed below (from §250.442).

The subsea BOP must:

- Have an operable dual-pod control system to ensure proper and independent operation of the BOP system
- Have an accumulator system to provide fast closure of the BOP components and to operate all critical functions in case of a loss of the power fluid connection to the surface

- Have two redundant BOP control panels whereof one panel on the drilling floor
- Have operational or physical barrier(s) on BOP control panels to prevent accidental disconnect functions
- Clearly label all control panels for the subsea BOP system

4.1.2 American Petroleum Institute

To fulfill the BSEE requirements concerning usage and design for subsea BOPs, API std 53 is applied. The standard is considered one of the most internationally recognized, concerning drilling. API spec 16D provides specific requirements to the design of the control system. Worth noticing is that API spec 16D does not mention safety integrity system (SIS) terminology, as opposed to NOG - 070 (2004), applied for the Norwegian continental shelf (NCS) (see. 4.2.3).

4.1.3 Function Testing

Despite that API std 53 is an extension of the BSEE requirements, differences can be found. Worth noticing is the test intervals for function testing of the control system. API std 53 states that function tests of the control system for a subsea BOP should be executed at least every 21 day (7.6.5.1.1), while BSEE set the requirement for every 14 day (§250.449). The test interval from BSEE should therefore be applied.

Reliability data collected by Sattler and Gallander (2010) shows that failures in the control systems are normally revealed by function tests. Sattler and Gallander (2010) states that through the use of simple function tests, a large percentage of the failures could be discovered. Meaning a high proof test coverage (PTC) can be obtained on the control system for a subsea BOP by performing full proof tests.

4.2 Norwegian Requirements

4.2.1 Petroleum Safety Authority

The Petroleum Safety Authority Norway (PSA) issues operation and maintenance regulations concerning design for subsea BOP systems in Norway. The PSA is equivalent to BSEE in the U.S. The PSA further refers to standards for fulfillment of the requirements. The most relevant standard for well drilling activities on the NCS is NORSOK D-001 (2012).

4.2.2 NORSOK D-001

In NORSOK D-001, descriptions of different requirements concerning drilling operations are given. The most important features are: functionality, design, installation, testing and equipment on both fixed installations and mobile offshore drilling unites (NORSOK D-001, 2012). Several similarities can be found between the NORSOK standards and the API standards, since both are built on the same basis. Still differences can be found, which are further discussed in 4.3.

4.2.3 NOG 070

NORSOK D-001 states that requirements for BOP control systems made in NOG-070 shall be met. NOG-070 is an application of IEC 61508 and IEC 61511 made by Norwegian Oil and Gas, for the Norwegian petroleum industry. The following safety integrity functions (SIFs) for a BOP control system are described in NOG-070:

1. Seal around drill pipe
2. Seal an open hole
3. Shear drill pipe and seal off well

In NOG-070, minimum safety requirements for the different functions are described with safety integrity levels (SILs). All three BOP functions above are given a SIL 2 requirement, meaning an average probability of failure on demand (PFD_{AVG}) in less than 1 per 100 failure.

In NORSOK D-001 only references to the SIF is made for the control system. The SIF only incorporates components going from the BOP control panels and down to the BOP accumulator isolation valves (Strand, 2014). While in NOG-070, the final elements are also included in the reliability assessment. As a result, the PFD_{AVG} increases. Therefore, obtaining a higher SIL requirement would be much harder following the NOG-070. The current system would have to be changed, and more rams in standard BOP assemblies would be required (NOG - 070, 2004).

4.3 Comparison

4.3.1 BSEE vs. PSA

To highlight the differences in requirements between Norway and U.S., a summary of regulations concerning subsea BOPs from BSEE and PSA is shown in Tab. 4.1. The comparison has a basis in BSEE regulations and related PSA regulations have been added.

Cases where the requirements are the same can be found. For example, both state that the best and safest technology should be applied, at all time. The similarities between the two are mostly found in requirements on a general level.

The major differences between the two regulations are the specificity. The PSA requirements focus mainly on the system on a general level, whereas the BSEE is much more specific in regard to equipment and personnel.

The PSA mostly emphasizes that dangerous situations needs to be avoided, whereas in the BSEE specific demands to equipment and personnel are given to prevent dangerous situations from happening.

4.3.2 NORSOK vs. API

This comparison takes a deeper look at the control system for subsea BOPs.

Both API and NORSOK issues several standards. Comparing them up to one and other can be difficult since non of them are equal to each other. Therefore, a comparison has been made with a basis in NORSOK D-001 and equivalent requirements from API std 53 and API spec 16D.

NORSOK D-001 describes the requirements to the control system much like what is done in

Table 4.1: Comparison of the BSEE and the PSA requirements for subsea BOPs.

BSEE (USA, USGoM OCS)	PSA (Norway, North Sea)
General Principles	
30 CFR §250.401 - Use the best available and safest drilling technology - Have a person onsite during drilling operations that are trained to fulfill all responsibilities - Use and maintain equipment and materials necessary to ensure the safety - Ensure that the toolpusher, operator's representative, or a member of the drilling crew maintains continuous surveillance on the rig floor	*Activities regulations: Section 85 - Well Barriers* - During drilling and well activities, there shall be tested well barriers with sufficient independence - If a barrier fails, activities shall not be carried out in the well other than those intended to restore the barrier
Design	
30 CFR 250.440-451 - At least four remote-controlled BOP preventers/rams: At least one annular preventer, two pipe rams, and one blind-shear rams, capable of shearing any drill pipe (including workstring and tubing) - A dual-pod control system ensuring independent operation of the BOP system - Accumulators providing fast closure of the BOP components and to operate all critical functions in case of a loss of the power fluid connection to the surface - Working-pressure rating of each BOP component must exceed maximum anticipated surface pressures - Subsea BOP stack equipped with ROV intervention capability - Operational or physical barrier(s) on BOP control panels to prevent accidental disconnect functions - Clearly label all control panels for the subsea BOP system - At least two BOP control stations. One on the drilling floor, the other located easy accessible away from the drilling floor - A choke and a kill line on the BOP stack. Each line must be equipped with two full-opening valves, both valves in each line must be remote-controlled	*Facilities regulations: Section 48 - Well barriers* - Shall be designed such that well integrity is ensured and the barrier functions are safeguarded during the well's lifetime. - Prevent influx or outflow to the environment - Shall be designed such that their performance can be verified *Facilities regulations: Section 49 – Well control equipment* - Be designed and capable of activation such that it ensures both barrier integrity and well control - Have remote-controlled valves with mechanical locking mechanisms in the closed position - Floating facilities shall have an alternative activation system for activating critical functions on the BOP in the event of an evacuation
Operation	
30 CFR 250.442 - Install the BOP system before drilling below the surface casing, unless other requirements are given by the District Manager - Constantly have ROV crew available when the BOP is deployed, as an option for use during intervention - Before removing the marine riser, displace the fluid in the riser with seawater	

Maintenance	
30 CFR 250.446-449 - Conduct a weekly well-control drill with each drilling crew - Visually inspect the subsea BOP system and marine riser at least once every 3 days - Maintain and inspect the BOP system to ensure that the equipment functions properly - Stump test the subsea BOP system before installation. Perform the initial subsea BOP test on the seafloor within 30 days of the stump test - Alternate tests between control stations and pods - Pressure test the blind or blind-shear ram BOP during stump tests and at all casing points - The interval between any blind or blind-shear ram BOP pressure tests may not exceed 30 days - Function test annular and ram BOPs every 7 days between pressure tests - Document all test results and make them available to BSEE upon request *30 CFR 250.451* - BOP control station or pod that does not function properly, suspend further drilling operations until that station or pod is operable - If activated blind shear ram or casing shear ram and sheared pipe or casing, correct problem, and conduct a full pressure test of the BOP stack	*Activities regulations: Section 45* - The responsible party shall ensure that facilities or parts thereof are maintained, so that they are capable of carrying out their intended functions in all phases of their lifetime *Activities regulations: Section 47* - Fault modes that may constitute a health, safety or environment risk, cf. Section 46, shall be systematically prevented through a maintenance programme - This programme shall include activities for monitoring performance and technical condition, which ensure identification and correction of failure modes that are under development or have occurred

API std 53, while API spec 16D is much more oriented on the details of the system. References to API spec 16D can therefore be found in NORSOK D-001. For example: "Color configuration shall follow API Spec 16D for subsea and dry BOPs".

Despite the high level of details in API spec 16D, some additional requirements have been made in the Norwegian regulations, compared to the two U.S. standards.

Most requirements from NORSOK D-001 are covered in the API standards, but a few exceptions can be found, see Tab. 4.2. NORSOK D-001 requires activation of the BOP from at least three different locations, while API only requires two. NORSOK D-001 requires all electrical equipment to be EX [1] proof and have a UPS, whereas API only present requirements for the UPS. The last major difference between the standards is that the failure of one activation panel, shall not affect activation on the remaining panels. No such requirements could be found in the two API standards.

Differences between the standards are small, and the API covers a great deal of areas. Still

[1] EX is short for explosion

some supplements have been added by the Norwegian government worth noticing.

Table 4.2: Comparison of NORSOK vs API for control systems.

NORSOK (Norway, North Sea)	API (USA, USGoM OCS)
NORSOK D-001 - 6.42.1 It shall be possible to activate the BOP from at least three (3) locations on the facility: - one activation panel at the driller's position; - independent activation panel in a safe accessible area, reference clause 5.2 design outline 4th section; - activated directly on the main unit (except multiplex systems which require a 3rd remote control).	*API std 53 - 7.3.14.3* -One control station location shall provide easy accessibility for the drill crew. *API std 53 - 7.3.14.4* -The other control station shall be placed away from the rig floor to provide safe access for functioning the BOPs during an emergency well control event.
NORSOK D-001 - 6.42.1 Control panels shall clearly indicate (e.g. by means of lights for remote panel) whether the functions are in open or closed position.	*API Spec 16D - 5.2.5.4* Panel lamps (or other means of visual indication) used to indicate function status shall track the position of the hydraulic control valves. Red, amber and green shall be used as standards colors for control panel indicator lights (or displays)
NORSOK D-001 - 6.42.1 The control panels shall be equipped with a securing device against unintentional operation of essential functions (e.g. shear ram, riser connection).	*API Spec 16D - 5.2.5.5* A transparent safety cover or other lock-out means that does not obstruct visibility of function status shall be employed to avoid unintended operation for critical equipment.
NORSOK D-001 - 6.42.1 All electrical equipment related to activate the BOP/diverter shall be supplied by UPS and Ex proof.	*API Spec 16D - 5.4.2* Electrical power (excludning the pump system) shall be supplied from one or more uninterruptable power supplies with backup battery capacities to operate the control for at least 2 hours.
NORSOK D-001 - 6.42.1 Failure of one activation panel shall not effect activation from remaining panels.	
NORSOK D-001 - 6.42.2 When calculating additional accumulator capacity for subsea BOPs, corrections shall be made for hydrostatic pressure of the relevant sea water column, as well as for sea temperature.	*API std 53 - 7.3.11.4* The manufacturer-supplied control system surface base pressure, adjusted for water depth and operating temperature, shall be used as required. Documentation of the measurement and adjustment shall be retained at the rig site.

Chapter 5

Subsea BOP Control System Failures

5.1 Failure Assessment

When estimating the reliability of a safety critical system, such as the subsea BOP control system, a process for identifying potential failures in the system should be conducted through the use of familiarization and functional analyses. The best approach is to apply a qualitative analysis such as hazard and operability study (HAZOP), hazard identification (HAZID) or failure mode, effects and criticality analysis (FMECA) (Drægebø, 2014). Ideally, the analysis should involve personnel from several different disciplines with expert/extensive knowledge about the system.

5.1.1 Safety Critical System

When analyzing the subsea BOP control system, failures that can prevent the system from performing its intended safety function or process demands, are the events of highest importance. Both these are classified as dangerous undetected (DU) failures. In the analysis for the subsea BOP control systems, only DU-failures are considered.

It should be noted that a conventional safety critical system is not normally operated without a process demand. However, the BOP system differs from this, as some functions are operated during normal operation. Annular preventers, for example, are closed for stripping of the drill pipe (Klakegg, 2012). A critical failure preventing activation of such an operation, will be discovered during normal mode, without a process demand. The analysis calculations presumes that all failures are detected in proof tests, hence, this will in some cases not be true for the subsea BOP control system. However, the effect of the deviation will not be significant, and the assumption that the BOP system is a safety critical system can therefore be recognized.

5.1.2 Sources of Data

The quantitative analyses are based on failure rates and test intervals (τ) for relevant components in the subsea BOP control system. The main sources of data are Holand and Awan (2012), Holand (1999), Håbrekke et al. (2013) and previous master thesis work form Klakegg (2012) and Drægebø (2014). Not all components in the analysis are covered in the data sources; as a result, some components have "expert judgment" failure rates.

5.1.3 BOP Control System Failure Modes

Based on the previous studies, some of the typical failure modes that can cause DU-failures in a subsea BOP control system are listed below.

- Leakage in pod selector valve
- Blue/yellow pod, SEM A/B fail to activate solenoid valve
- Topside control panels PLCs fail to signal pods
- Loss of communication with pods, because of failure in MUX cable
- Loss of hydraulic fluid in pods, because of leakage in hydraulic lines

In addition to these typical failure modes, common cause failures (CCFs) for the system should also be identified. The next section gives a brief introduction to CCF theory, the effect of CCF on the subsea BOP control system and how to include CCF in a reliability assessment of the system.

5.2 Common Cause Failures

Safety critical systems are often equipped with a high level of redundancy, and the subsea BOP control system is no exception. Redundancy is integrated into safety critical systems to enhance its reliability (Lundteigen and Rausand, 2007). In the BOP system, redundancy ensures functional safety in the event of a kick.

Before quantifying the reliability of redundant safety critical systems, categorizing potential failures must be done. Failures are mainly divided into either random hardware- or systematic failure. Random hardware failure are caused by natural stressors and are considered independent failures, such that a component failure in a system is not assumed to influence the other components failure rates, normally called aging failure (Hauge et al., 2013). Systematic failures may come as a result of failures related to operation, excessive stress or installation, making components in the same system potentially dependent (Hauge et al., 2013). Systematic dependent failures will in most cases lead to CCFs, meaning, more than one component failing by the same cause, within a given period. CCFs can potentially reduce the effect of redundancy in a safety critical system (Rausand, 2014).

For redundant systems, such as the subsea BOP control system, the potential impact from CCFs with regard to system reliability, is huge. Identification of potential CCFs and necessary measures to prevent the failures from occurring, are extremely important before the system can be installed (Rausand and Høyland, 2004).

5.2.1 CCF Modeling Theory

The term CCF has been discussed for a long time, and still no general definition has been accepted, meaning, people within different sectors have different opinions of what CCFs are (Rausand, 2014). IEC-61508 (2005) defined CCF as: *"failure, that is the result of one or more events, causing concurrent of two or more separate channels in a multiple channel system, leading to system failure"*. In the nuclear power industry CCF is defined as: *“a dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause”.*

Simultaneous is an important expression to understand when categorizing failures as CCFs.

There can be a distinct dependency between failures, even though they do not occur at the exact same time (Hokstad and Rausand, 2008). In Stamatelatos and Dezfuli (2011), a CCF event is defined as multiple failures occurring during the same mission. The mission is dependent on what type of industry the system is within. For example, in the aviation industry, a CCF event would be if multiple failures occurred during a flight. For a subsea BOP control system, the mission time is equal to the periodic testing time. Hokstad and Rausand (2008) state that if multiple failures occur on redundant components within the test interval (τ), it can be classified as CCFs. The test intervals can vary in the range of hours to a year, making it more complex to decide if failures in the same system are independent or CCFs.

5.2.2 Modeling Common Cause

Rausand (2014) implies that there exists a cause-effect relationship between the CCF event and a certain cause. However, this is rarely reflected in most CCF models, and is in several cases difficult to identify, and yet quantify. Causes of CCFs that can be identified, should explicitly be modeled into, for example, a reliability block diagram (RBD) or with a fault tree analysis (FTA) (Rausand and Høyland, 2004). Explicit modeling, even with low quality input data, is considered more accurate compared to CCF modeling with implicit data (Rausand and Høyland, 2004). Lundteigen and Rausand (2009) state that by applying the explicit approach to systems with several types of common cause, such as the subsea BOP control system, may lead to large and complex fault trees. The increased complexity may cause events to be overlooked or included in multiple places. By applying the implicit approach the fault tree is kept simple and the CCFs are based on the minimal cut sets (Lundteigen and Rausand, 2009). The analysis in this report will therefore be using implicit modeling of CCFs for the BOP control system.

Beta Factor Model

The beta-factor model is most commonly used, and recommended in IEC-61508 (2005) and IEC-61511 (2011), for implicit modeling of CCFs for safety critical systems. The model assumes that of all the failures in the system, a fraction is CCF. This fraction value is assigned to beta, β. An occurring CCF assumes that all components in that group will fail as a result of the same cause

(Lundteigen and Rausand, 2009). The contribution to the system from independent DU-failures are expressed as $(1-\beta)\lambda_{DU}$, while failures from CCFs are expressed as $\beta\lambda_{DU}$.

A weakness in the beta-factor model is that voted configurations are not taken into account. Meaning, CCFs are expected where not all redundant independent components fail, in systems such as, *1-out-of-3* and *2-out-of-3* (Lundteigen and Rausand, 2009). The PDS method adds a correction factor taking this into account, and Hauge et al. (2013) argue for its use. In this report the beta-factor model is preferred, easy to understand, the β parameter is easy to interpret and it provides an adequate result.

5.2.3 CCF Data Sources

When quantifying the beta-factor, relevant and updated failure data for CCFs are important. However, access to such data is limited, therefore other methods must be applied. In Rausand (2014) the IEC 61508 method is mentioned, which consists of 37 relevant questions, used to quantify the β-values. Still a satisfactory quantification is hard to perform with limited time and knowledge.

5.2.4 Potential CCFs in Subsea BOP Control Systems

As described earlier in chapter 2, the subsea BOP control system consists of several subsystems with identical and redundant components that can be exposed to CCFs, for example, SEMs, PLCs, MUX cables, hydraulic cables, pod accumulator isolation valves, shuttle valves and solenoid valves in each pod. To further determine what type of CCFs these components can be exposed to, an analysis, typically FMECA or HAZOP should be performed.

Chapter 6

Analysis

The report has, so far, given a general description of the subsea BOP control system, with key functions and system boundaries. Previous studies have been evaluated and discussed. The most relevant failure modes for subsea BOP control systems have been presented along with the potential contribution from CCFs. Based on previous chapters, an approach to quantifying the reliability by conducting an FMECA followed by an FTA, is made.

6.1 FMECA

An FMECA involves reviewing numerous components, assemblies and subsystems to identify the potential causes and effects of failures, and are often the first item of a systems reliability study (Rausand and Høyland, 2004). Ideally, the FMECA should be performed in close cooperation with the design team and is based on detailed knowledge about the system and its components (Rausand, 2014). However, for this analysis there is limited access to such personnel, and potential failure modes or consequence may have been overlooked. The focus of the analysis lies therefore in the method of it.

Data Sources

The analysis performed is based on the system description of the subea BOP control systems in chapter 2, the reliability study performed in chapter 3 involving studies such as Holand and Awan (2012) and Holand (1999), and previous master thesis work from Drægebø (2014) and

Table 6.1: Potential failure modes in a subsea BOP control system

Comp. number	Component	Failure number	Some potential failures
		Sub-function 1: BOP control functions	
1.1	Power supply unit (topside)	F-1.1.1 F-1.1.2	Transmission failure Erratic output
1.2	Control panels (topside)	F-1.2.1	Erratic output
1.3	Electric power from back-up battery	F-1.3.1	Insufficient power
1.4	Batteries in pods	F-1.4.1	Insufficient power
1.5	MUX cable reel	F-1.5.1	Transmission failure
1.6	CCU	F-1.6.1 F-1.6.2 F-1.6.3 F-1.6.4	Control/ signal failure Erratic output Fail to function on demand Spurious activation
1.7	Pod selector valve	F-1.7.1	Fail to move
1.8	Blue/ yellow pod	F-1.8.1	Unable to deliver hydraulic power
1.9	Solenoid valve	F-1.9.1	Fail to move
1.10	SPM valve	F-1.10.1	Fail to open/ close
1.11	Shuttle valve	F-1.11.1	Fail to move (stuck in position)
1.12	Choke and kill valve	F-1.12.1 F-1.12.2 F-1.12.3	Fail to open/ close External leakage Internal leakage
		Sub-function 2: Power supply	
2.1	Subsea accumulator	F-2.1.1 F-2.1.2	Internal leakage Burst bladder
2.2	Fluid reservoir	F-2.2.1 F-2.2.2 F-2.2.3	Containment of reservoir Too low volumetric capacity Reservoir plugged
2.3	HPU	F-2.3.1	Hydraulic pump failure
2.4	Hydraulic line from HPU to BOP	F-2.4.1 F-2.4.2 F-2.4.3	Plugged/ choked line External leakage Internal leakage
2.5	Regulator valve	F-2.5.1	Fail to move
2.6	Pod isolation valve	F-2.6.1	Fail to open/ close
2.7	Hydraulic lines on BOP stack	F-2.7.1	Internal leakage

Klakegg (2012). The subsea BOP control system is broken down to approximately 30 components, which will be further analyzed.

Subsea BOP Control Systems FMECA

All the analyzed components and some of the failure modes considered most important for this analysis are identified and assigned an identification number in Tab. 6.1. The corresponding FMECA sheets are given in Appendix B.1.

The criticality is divided into three different classes in the analysis:

- *P*: Production loss
- *E*: Environmental impact
- *S*: Safety of personnel

For each of the consequence classes the criticality is ranked with different colors, green meaning acceptable risk, yellow meaning tolerable risk and red meaning critical risk.

Most of the components within the BOP control functions are assigned with an acceptable criticality level, mainly as a result of redundancy. A failure occurring on one of the pods should lead to retrievement of the system, however, the production loss class is still marked acceptable for such components, because the pods will not be retrieved until next scheduled maintenance. Component failures considered most critical for the sub-system are the CCU, pod selector valve and shuttle valve. A CCU failure has the option of acoustic back-up control or ROV, to operate the BOP. Failures in the pod selector valve or shuttle valve are both marked critical, because a failure in either of these would lead to loss of control of the BOP.

For components within the power supply sub function, are the subsea accumulators, fluid reservoir, hydraulic lines on the BOP stack and hydraulic line from HPU to BOP, all considered most critical in the system. A failure in the subsea accumulator would not directly lead to loss of control because of redundant bottles and overcharging, however a potentially dangerous situation could occur. A reservoir with low fluid levels is dangerous for personnel, but also easier to detect compared to failures on the sea bottom. The potential of hydraulic lines failing to deliver hydraulics are dangerous, however increased storage in the accumulators and pod redundancy limits the potential risk.

6.2 Fault Tree Analysis

6.2.1 Theory Behind Approach

Relationship to Safety Instrumented Functions

Before quantifying the reliability of a subsea BOP control system, linking it against a well know regulatory requirement, based on probabilistic formulas, is most ideal. As a result, better understandability and verification of the system can be achieved. An example of such a system is the safety integrity level (SIL), defined below.

☞ **SIL**: Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems (IEC-61511, 2011).

Applying SIL to the subsea BOP control system requires compliance with the definition of safety-instrumented systems (SIS), which governs one or more safety instrumented functions (SIFs). The SIS consists of at least three subsystems, sensors(s), logic solver(s) and final element(s) (Rausand, 2014). Categorizing the subsea BOP control system underneath the SIS definition can to some degree be considered accurate. However, a SIS is mainly intended for dedicated safety systems that automatically respond to a process demand through the use of SIFs. The BOP system does not respond to process demands automatically, but relies on personnel's knowledge and physical interaction to activate such functions. Also, the BOP functions are part of the normal operation, and not only dedicated to the role as safety barrier, like the SIS (Klakegg, 2012). Applying the SIS definition directly to the subsea BOP control system can therefore not be done.

Despite inaccuracies between the BOP systems and the SIS definition, is the BOP reliability commented in SIL methodology in NOG - 070 (2004) (mentioned shortly in chapter 4.2.3). NOG-070 recommends that the required PFD/SIL level for each well should be calculated, and tolerable risk levels be set as part of the application process for consent to exploration and development drilling. A SIL 2 requirement is set for both isolation of the well and closing of the blind shear ram. Worth noticing is that no recommendations has been given to the actual shearing of the pipe (Klakegg, 2012).

Systems within SIS terminology can be divided into two groups related to operation, continuous/high demand mode, or low demand mode. Continuous/high demand is calculated through the average probability of dangerous failures per hour (PFH), while low demand mode, uses the average probability failure on demand (PFD). The system in question must be calculated using one of these methods, to comply with SIL levels. IEC-61508 (2005) states that the BOP should be considered as operating in a low demand mode of operation, meaning the BOP system should be expressed by the average PFD of the SIF.

Model Selection

To quantify the PFD for the functions in the subsea BOP control system, a reliability analysis method must be applied. Several different methods are available, and in Rausand (2014), seven different approaches are recommended. IEC 61508 and IEC 61511 suggest for this type of analysis either fault tree analysis (FTA), reliability block diagrams (RBD), or Markov methods, should be applied. The CCF contribution must also be accounted for in the analysis. Lundteigen and Rausand (2009) recommend the use of FTA or RBD for complex systems, such as the subsea BOP control system.

FTA modeling focuses on the failure of a function, rather than the achievement of one. The FTA model makes it easier to identify failures that are not directly linked to a component function, and is considered intuitive and structured compared to RBD and Markov methods (Lundteigen and Rausand, 2009).

RBD models often resemble the physical structure of the system, because of the similarities between the block sequencing and the systems activation of components. Modeling of the RBD is based on how functions are achieved, rather than the failure of it, as in FTA. Lundteigen and Rausand (2009) describe this as a possible strength, but also a weakness, because functions installed (or should be installed) to protect the main system function may easily be forgotten. As opposed to the physical structure, the RBD may include the same component in different sections of the model, if the component is part of several functions. This may confuse personnel unfamiliar with reliability modeling (Lundteigen and Rausand, 2009).

The Markov methods have the ability to model systems who frequently switch between different operational modes, and can be used to analyze repairable systems with complex repair strategies (Rausand and Høyland, 2004). However, the number of system states increases exponentially with the number of components, making systems with moderate complexity difficult to comprehend (Lundteigen and Rausand, 2009).

The subsea BOP control system is a large and complex system, considering both design and operations and maintenance. The frequency of different operational situations is relatively low, making the Markov methods less suitable. RBDs can be a sufficient tool for modeling parts of the system, for example, when reviewing the effect of redundancy in different operational situations (Klakegg, 2012). When conducting reviews of the system, close involvement with design engineers and operators are extremely important. The FTA provides an intuitive and structured analysis on the whole system, based on the potential failures. It has a structured design and is easy to understand for personnel without a reliability background. Based on this, the FTA is preferred for the reliability assessment of the subsea BOP control system.

6.2.2 Fault Tree Analysis of the Subsea BOP Control System

Conservative PFD approximation

Analyses previously discussed in the report have all used FTA programs to calculate the PFD of the systems. The calculations are in most cases influenced by lack of data, causing approximations to be made. Approximations used must be conservative, so that the "actual" PFD is lower than the one calculated (Lundteigen and Rausand, 2009). Studies such as Holand and Awan (2012) and Holand (1999), uses the FTA software tool Cara FaultTree to model and calculate the top event probabilities. The programs weakness, along with other similar FTA programs, is that it produces non-conservative values, meaning inaccurate PFD approximations (Lundteigen and Rausand, 2009).

In Lundteigen and Rausand (2009), an alternative approach for producing non-conservative and more accurate estimates of the PFD is presented. The approach is based on post-processing minimal cut sets, and has the ability to include CCFs. Further it will be shown how the approach presented by Lundteigen and Rausand (2009) can be applied to produce conservative PFD estimates, including CCFs, for the subsea BOP control system.

Consider a fault tree for a specified TOP event, constructed and identified with m minimal cut sets $\{MC_1, MC_2, ..., MC_m\}$. Let $PDF_{j,i}$ denote the (average) PFD of a component i in minimal cut set j, for j = 1,2,...,m. Minimal cut j of order m_j is a $1-out-of-m_j$ voted structure, and only fails ones all m_j components are in a failed state, at the same time. When all components are independent in the minimal j, the PFD of the minimal cut is normally calculated by (Lundteigen and Rausand, 2009):

$$PFD_{MC_j} \approx \prod_{i=1}^{m_j} PFD_{j,i} \tag{6.1}$$

Several software tools uses (6.1), including Cara FaultTree, for calculating the PFD of a minimal cut, however, the result is not accurate (Dutuit et al., 2008). Due to the well known Schwartz' inequality saying that *"the average of a product is not equal to the product of averages"* (Lundteigen and Rausand, 2009). Equation 6.1 is therefore categorized as a non-conservative approximation.

The average $PFD_{j,i}$, for a single component i in minimal cut j, periodically tested and has a constant DU failure rate, can be calculated as (Rausand and Høyland, 2004):

$$PFD_{j,i} = \frac{1}{\tau}\int_0^{\tau}(1-exp(-\lambda_{DU,j,i}\cdot t))dt \approx \frac{\lambda_{DU,j,i}\cdot\tau}{2} \tag{6.2}$$

Equation 6.2 gives a conservative PFD approximation, and is considered to produce adequate results when (Rausand and Høyland, 2004):

- $\lambda_{DU,j,i}\cdot\tau < 10^{-2}$ Approximation might be to conservative for higher values (Lundteigen and Rausand, 2009).
- Detection of a DU failure stops the operation and is not resumed until the failure has been repaired.
- The functional test is perfect, meaning, all DU failures are revealed during testing.

The subsea BOP control system fulfills the two first conditions; the third is not fully obtained because of the shear ram. A perfect test cannot be conducted on the shear ram, only an imperfect functional test can be performed. To account for this, the term proof test coverage factor (PTC) is introduced in Rausand (2014).

Including the PTC when calculating the PFD_{MC_j} accounts for the fraction (1-PTC) of all DU-failures that are left unrevealed after the function test. Failures left undetected by weekly functional tests, can normally not be revealed until the systems gets a complete overhaul ($\tilde{\tau}$). For a single channel, such as the shear ram, the PFD for the component failure mode will be (Rausand, 2014):

$$PFD_{avg} \approx \frac{PTC \cdot \lambda_{DU}\tau}{2} + \frac{(1-PTC)\lambda_{DU}\tilde{\tau}}{2} \tag{6.3}$$

Rausand (2014) makes references to studies based on SINTEF reports, showing the PTC has a high order of magnitude on the systems. Therefore, it is argued that the PTC shall be included in the PFD calculation for the subsea BOP control system, for components exposed to such failures.

The PFD_{MC_j} for a minimal cut *j* with m_j independent components and a test interval τ, can be expressed as following (Lundteigen and Rausand, 2009):

$$\begin{aligned} PFD_{MC_j} &= \frac{1}{\tau}\int_0^{\tau}\prod_{i=1}^{m_j}(1-exp(-\lambda_{DU,j,i}\cdot t))dt \\ &\leq \frac{1}{\tau}\int_0^{\tau}\prod_{i=1}^{m_j}(\lambda_{DU,j,i}\cdot t)dt \\ &= \frac{\left(\prod_{i=1}^{m_j}\lambda_{DU,j,i}\right)\cdot\tau^{m_j}}{m_j+1} \\ &= \frac{\left(\bar{\lambda}_{DU,j}\cdot\tau\right)}{m_j+1} \end{aligned} \tag{6.4}$$

where

$$\bar{\lambda}_{DU,j} = \left(\prod_{i=1}^{m_j}\lambda_{DU,j,i}\right)^{\frac{1}{m_j}} \tag{6.5}$$

is the geometric mean of the m_j failure rates, in the minimal cut *j*.

To better compare the conservative with non-conservative approximations, a minimal cut *j* consisting of two independent components with the same failure rate, $\lambda_{DU,j}$, is inserted into the formulas. Combining (6.1) and (6.2) gives $PFD_{MC_j} = (\lambda_{DU,j}\cdot\tau)^2/4$. While inserting the failure rates into (6.4) gives $PFD_{MC_j} = (\lambda_{DU,j}\tau)^2/3$, showing that the non-conservative is 25 % lower than the conservative. The percentage increases with the order m_j, of minimal cut sets. Meaning the result of the PFD approximations achieved in the FTA tools calculations can be greatly improved by post-processing the minimal cut sets using the approach presented in Lundteigen and Rausand (2009).

Fault Tree Development

Development of the fault tree should ideally be done in close cooperation with design engineers and operators of the BOP system. This type of personnel has not been available when writing the report, but input from experienced personnel at SINTEF has strengthened the analysis. Still, it should be noted that due to limited experience with the system, critical failures might have been overlooked or incorrectly included in the fault tree.

The scope of the analysis starts after the push button has been activated, and ends when the shear ram is activated. Meaning human factors and the shearing ability of the shear ram is not considered.

The TOP event in the FTA relates to the control system's ability to close the shear ram upon request. The fault trees can be found in Appendix C.1 and the corresponding basic events are listed in Appendix C.2. The failure rates for the basic events are mostly based on Holand and Awan (2012) and Håbrekke et al. (2013), with a few exceptions where "expert judgment" has been used.

Minimal Cut Sets

The minimal cut sets of the fault tree are generated by the Cara FaultTree program. All orders of the cut sets are considered due to the potential contribution from the beta-factor. However, the highest order of cut sets is 4. All the minimal cut sets are imported into Excel for further calculation, and can be found in Appendix C.3.

Identification of Common Cause Component Groups

For each minimal cut set MC_j, it must be determined whether the components are dependent or independent. This is done by looking for common root causes and coupling factors in each of the minimal cut sets (Lundteigen and Rausand, 2009). Components in the subsea BOP control system that are dependent and share the same common failure cause, are included in the same common cause component group $CG_{j,v}$, for $j = 1,2,...,m$ and $v = 1,2,...,r_j$, where r_j is the number of different common cause component groups in minimal cut MC_j (Lundteigen and Rausand, 2009). In cases where a minimal cut set contains a single common cause component group, the index v may be omitted from the notation. Each $CG_{j,v}$ is assigned a corresponding beta factor, $\beta_{j,v}$.

The identified common cause groups in the events are marked in bold in the table for the minimal cut sets, found in Appendix C.3. Cut sets where identical components in different systems are marked as common cause, is a result of exposure to failures such as similar design and material, same power line and/or prone to same stressors such as temperature, vibration and pressure. Other common cause groups are mainly a result of common electric and/or hydraulic source.

Quantifying $\beta_{j,v}$ for $CG_{j,v}$

Preferably the β-values should be quantified using plant specific conditions, applying specially developed checklists (Lundteigen and Rausand, 2009). Due to somewhat limited knowledge about the subsea BOP control system, the preferred approach is a combination of finding data in the NOG - 070 (2004) and expert judgment. β-values for the SEMs and PLCs are found in the NOG - 070 (2004), while the rest of the values are based on expert judgment. The β-values are listed in Tab. 6.2.

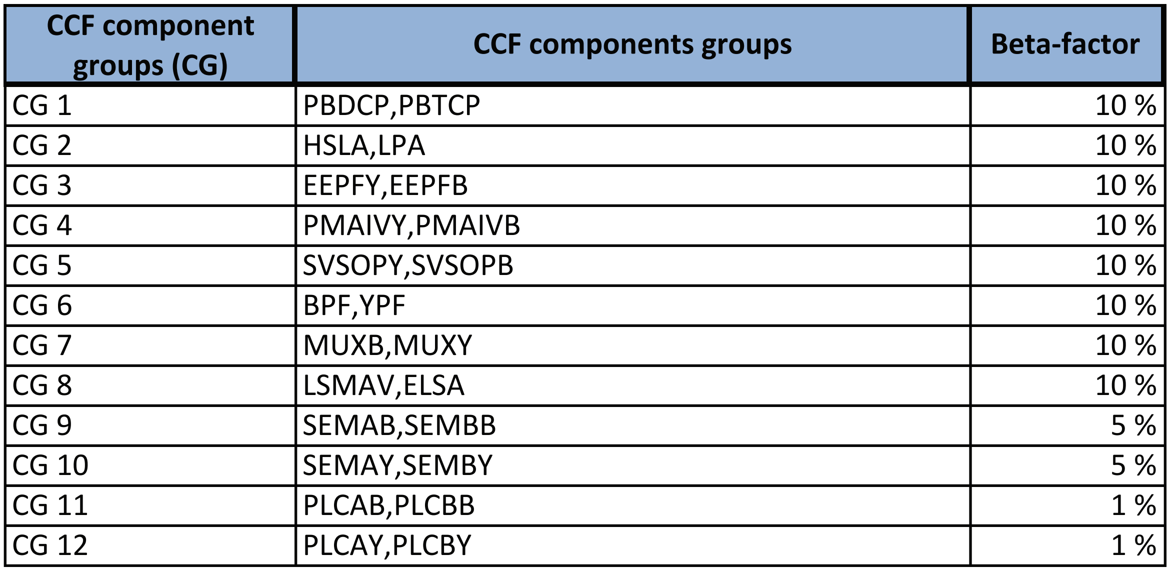
PFD Calculations

PFD calculation of the system is performed based on the generated minimal cut sets and the identified common cause component groups. The methods for calculating the different minimal cut sets in the subsea BOP control system are based on theory presented in Lundteigen and Rausand (2009).

Calculating the PFD_{MC_j} is influenced by the following (Lundteigen and Rausand, 2009):

1. The order m_j of the minimal cut

Table 6.2: β-factor values



CCF component groups (CG)	CCF components groups	Beta-factor
CG 1	PBDCP,PBTCP	10 %
CG 2	HSLA,LPA	10 %
CG 3	EEPFY,EEPFB	10 %
CG 4	PMAIVY,PMAIVB	10 %
CG 5	SVSOPY,SVSOPB	10 %
CG 6	BPF,YPF	10 %
CG 7	MUXB,MUXY	10 %
CG 8	LSMAV,ELSA	10 %
CG 9	SEMAB,SEMBB	5 %
CG 10	SEMAY,SEMBY	5 %
CG 11	PLCAB,PLCBB	1 %
CG 12	PLCAY,PLCBY	1 %

2. Whether or not the components of the minimal cut are identical

3. Whether or not the components of the minimal cut are dependent

4. Whether or not the components of the minimal cut are tested simultaneously

The analysis considers all orders of cut sets, but only cut sets to the order 4 were generated by the analysis. In chapter 4 it was stated that the pods should be tested every 14 day, meaning, one pod was tested every 7 day. However, the reliability data applied in the analysis is for testing every 7 day. Therefore, it is presumed that all components in the system are tested simultaneously.

Minimal cut sets with only independent components are calculated using (6.4) and (6.5), directly.

Considering minimal cut j, where the components are identical and dependent, the PFD_{MC_j} can be calculated from (Lundteigen and Rausand, 2009):

$$PFD_{MC_j} \approx \frac{\left((1-\beta_j)\lambda_{DU,j}\cdot\tau\right)^{m_j}}{m_j+1} + \frac{\beta_j\lambda_{DU,j}\cdot\tau}{2} \tag{6.6}$$

Components in a minimal cut set that are non-identical, can still be exposed to the same CCF, such as vibrations, temperature increase or pressure increase. Lundteigen and Rausand (2009) state that this must be cared for when applying the beta factor model for calculating

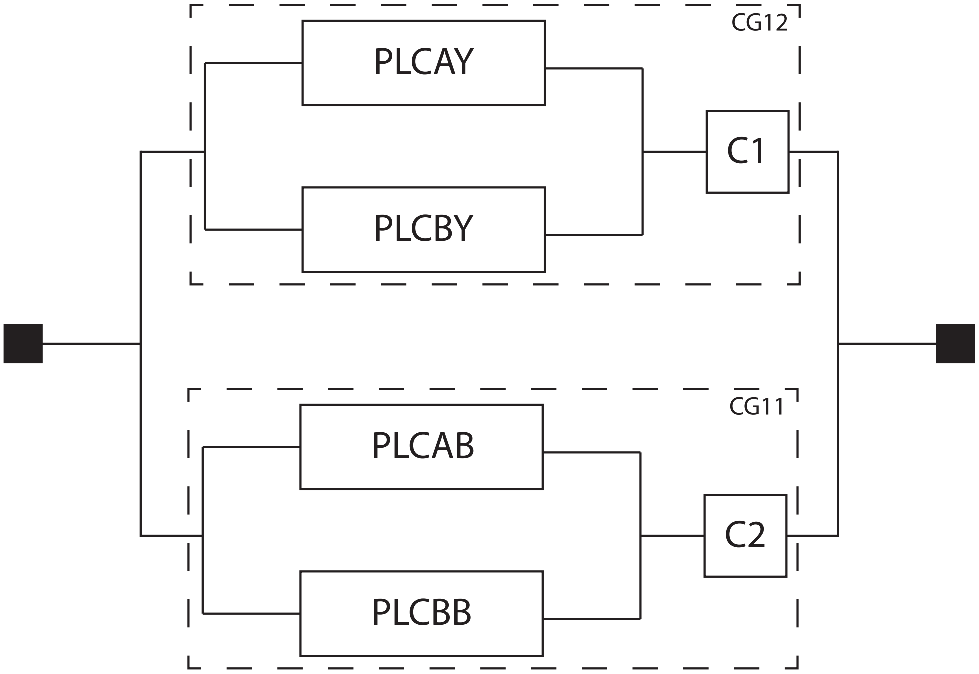


Figure 6.1: Minimal cut 115, with two common cause component groups

the CCFs contribution. To overcome the problem, Lundteigen and Rausand (2009) purpose to define the beta-factor to be a fraction of the lowest component failure rate, as this rate limits how often components fails simultaneously in a parallel structure.

The PFD_{MCj} for a minimal cut with dependent, non-identical components all belonging to the same common cause component group, based on this approach, becomes (Lundteigen and Rausand, 2009):

$$PFD_{MCj} \approx \frac{\left[(1-\beta_j)\bar{\lambda}_{DU,j} \cdot \tau\right]^{m_j}}{m_j+1} + \beta_j \cdot \lambda_{DU,j}^{\min} \cdot \frac{\tau}{2} \tag{6.7}$$

where

$$\lambda_{DU,j}^{\min} = \min\{\lambda_{DU,j,i}\} \tag{6.8}$$

is the lowest DU failure rate in MC_j

For minimal cut sets consisting of more than one common cause component group, or includes both independent and dependent components, (6.6) or (6.7) cannot be applied. This situation, with a basis in the analysis, is illustrated in Fig. 6.1, showing the minimal cut set with two common cause component groups, CG 11 and CG 12, each with two components. The CCFs

(C_1 and C_2) are included as "virtual" components, in series with the parallel structure.

The remaning components in the MC_j, are the independent components, marked H_j (Lundteigen and Rausand, 2009). The order of H_j is denoted by $k_j^{(I)}$, and the order of $CG_{j,v}$ by $k_{j,v}^{(C)}$ (Lundteigen and Rausand, 2009). Components in H_j have failure rates $\lambda_{DU,i}^{(I)}$ for $i = 1,2,...,k_{j,v}^{(C)}$ and the components in $CG_{j,v}$ have $\lambda_{j,v,l}$ for $v = 1,2,...,r_j$ and $l = 1,2,...,k_{j,v}^{(C)}$ (Lundteigen and Rausand, 2009). For the minimal cut in Fig. 6.2, $k^{(I)} = 0$, $r = 2$, $k_1^{(C)} = 2$ and $k_2^{(C)} = 2$.

Following the approach from Lundteigen and Rausand (2009), the PFD_{MCj} of the virtual cut set with the lowest order in a minimal cut set, containing more than one common cause component group and/or both dependent and independent components, can be expressed as following:

$$PFD_{MCj}^{(I)} \approx \frac{\left(\prod_{i=1}^{k_j^{(I)}} \lambda_{j,i}^{(I)} \cdot \prod_{v=1}^{r_j} \beta_{j,v} \cdot \lambda_{DU,j}^{\min,v}\right) \tau^{k_j^{(I)} r_j}}{k_j^{(I)} + r_j + 1} \tag{6.9}$$

where $\lambda_{DU,j}^{\min,v}$ is the lowest failure rate in $CG_{j,v}$ in minimal cut MC_j.

To better understand (6.9), an example of the MC 115, shown in Fig. 6.1, can be applied. The minimal cut sets consists of the following virtual cuts: {C1, C2}, {C1, PLCAB, PLCBB}, {C2, PLCAY, PLCBY} and {PLCAB, PLCBB, PLCAY, PLCBY}. In this example, the failure rate and β-factor is the same for all the components, making it easier to simplify the equations. {C1, C2} has the lowest order, and the following values can be determined: $k^{(I)} = 0$, $r = 2$, $k_1^{(C)} = 2$ and $k_2^{(C)} = 2$, the PFD for the cut is then:

$$PFD_{MC}^{(1)} \approx \frac{\beta^2 \lambda_{DU}^2 \cdot \tau^2}{3} \tag{6.10}$$

The PFD for the remaning cut sets are found using the same method as above, based on the approach in Lundteigen and Rausand (2009).

$$PFD_{MC}^2 = PFD_{MC}^3 \approx \frac{(1-\beta)^2 \lambda_{DU}^2 \beta \lambda_{DU} \cdot \tau^3}{4} \tag{6.11}$$

$$PFD_{MC}^4 \approx \frac{(1-\beta)^2 \lambda_{DU}^2 (1-\beta)^2 \lambda_{DU}^2 \cdot \tau^4}{5} \tag{6.12}$$

This approach is used for calculating cut sets consisting of both several common cause components and for cut sets consisting of both common cause components and independent components, in the subsea BOP control system.

Calculation of the PFD_{MCj} of a minimal cut j, can be done using the "upper bound approximation" (Lundteigen and Rausand, 2009).

$$PFD_{MCj} \approx 1 - \prod_{i=1}^{n} \left(1 - PFD_{MCj}^{(k)}\right) \tag{6.13}$$

where n is the number of virtual cuts in MC_j

Calculate system PFD_{SIF}

The PFD_{SIF} for the top event is calculated in Appendix C.3 using (6.14), meaning the probability that the subsea BOP control system is unable to activate the shear ram upon demand. The PFD for each of the minimal cut sets have been calculated using Excel and applying the formulas described earlier.

$$PFD_{SIF} \approx 1 - \prod_{j=1}^{m} \left(1 - PFD_{MCj}\right) \tag{6.14}$$

Discussion

The calculated PFD_{SIF} using conservative values and considering the contribution from CCF is approximately $7.66 \cdot 10^{-4}$, the calculations generated by Cara FaultTree, gives a value of $4.15 \cdot 10^{-4}$. Meaning, the manually calculated result is almost doubled compared to Cara FaultTree.

The calculations show the biggest contribution comes from a variety of different components, such as the shuttle valve, manifold regulator and different electric failures. The solenoid valves, PLCs and SEMs have much smaller contributions, and can almost be neglected from the calculations. Comparing the result to other reports such as Holand and Awan (2012) is difficult, older reports are based on the entire BOP system, while in this analysis the focus lies only within the control system, and the corresponding components.

The results clearly show the importance of using conservative PFD approximations. For cut sets consisting of one or more components, the PFD_{MCj} has significantly increased, using the methods described in Lundteigen and Rausand (2009). The contribution from the CCFs is also substantial. However, the biggest influence is mainly on cut sets consisting of components with low failure rates, hence having a relativity small impact on the system.

6.3 Event Tree

Introduction

The fault tree model provides a "static" picture of the system during a specified time in a specified condition. It shows numerous paths consisting of different events, potentially leading to system failures. The weakness in an FTA is that the sequence of the events does not affect the analysis.

An event tree analysis (ETA) provides a more "dynamic" model of the system. The event tree is a logic tree diagram; it starts with an initiating event (e.g., a kick) and provides a systematic coverage of the time sequence of event propagation to its potential outcomes or consequences (e.g., a blowout) (Rausand and Høyland, 2004). In this section, a brief discussion is made about how an ETA can strengthen the reliability assessment of the subsea BOP control system

Event Tree Analysis on Crucial Systems

The ETA method is a great supplement for gaining a wider perspective of the risk picture and potentially dangerous situations escalating during well control. However, conducting a full ETA on a system is both time consuming and often requires new elements in well control to be included, for example, the mud column. Therefore, only a small part of the subsea BOP control system is considered to highlight the shortcomings of the FTA.

A simplified event tree of a shear ram activation is shown in Fig. 6.2. The ETA considers the potential outcome of a failed pod activation, and the time duration before the redundant pod is activated (unless that one also fails to activate). The duration of time from blue pod activation and yellow pod activation, is marked *x*. This event takes approximately 2-3 minutes, and will have a direct influence on the consequence. However, this is not possible to model in a fault tree.

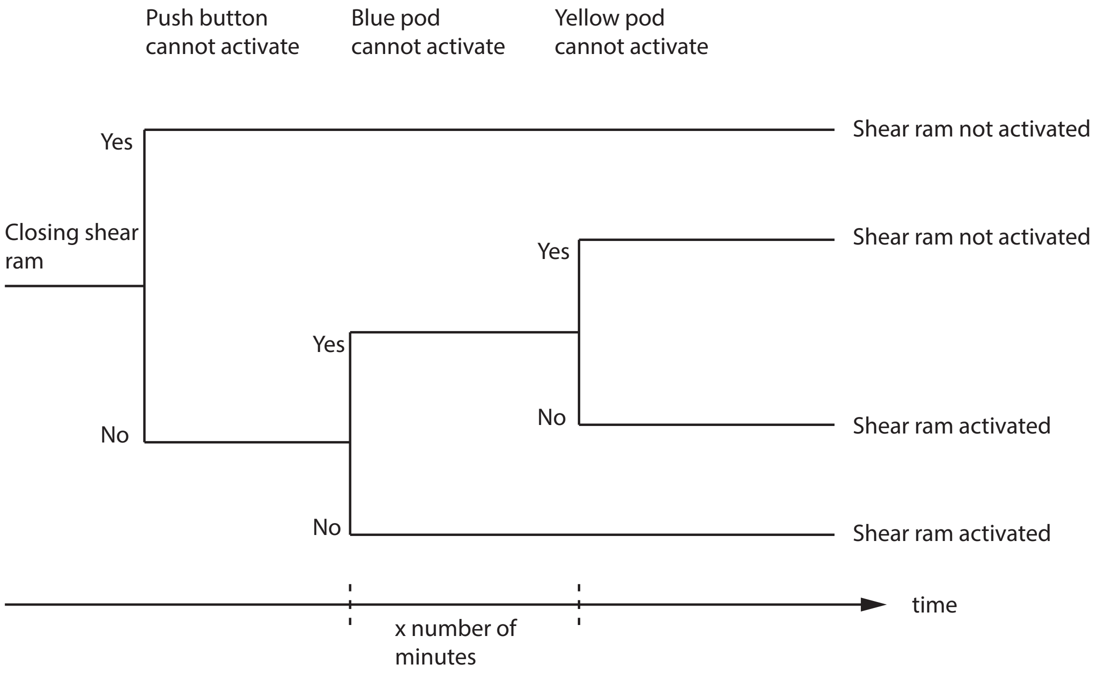


Figure 6.2: Event tree of pod activation

Applying ETA on specific parts of the system will strengthen the analysis, however, it is both time consuming and requires the scope of the analysis to be substantially widen.

Chapter 7

Summary and Recommendations for Further Work

7.1 Summary and Conclusions

The Macondo accident reports identified the BOP and its control system as main causes of the accident. As a consequence of this accident, improved methods for BOP reliability assessments are now required.

Several reliability assessment studies are discussed in this report, and all of these points to the subsea BOP control system as the main contributor to critical BOP failures.

The relevant regulations and standards in Norway and the United States have been compared as part of this study. They are rather similar, but there are also differences, especially when it comes to specificity. PSA gives requirements on a general level, whereas BSEE provides much more specific details with regards to equipment and personnel. Regarding standards, NORSOK D-001 mostly contains the same requirements as API 53 and API spec 16D, but differences such as BOP activation required from three different places, and all electrical equipment is required to be EX-proof and have access to a UPS, could be found.

To identify potentially critical failures in the subsea BOP control system a detailed FMECA has been performed, and revealed that the shuttle valve, the pod selector valve, the subsea accumulators and the fluid reservoir were the most safety critical components in the system.

The potential contribution from CCFs was examined and found relevant for the analysis of the control system.

To improve current reliability assessments methods of the subsea BOP control system, a thorough review of both the system and previously used methods was required. Relevant failure modes and potential failures were identified using the FTA. To improve reliability calculations, a method based on post-processing of the minimal cut sets generated in the FTA, was purposed. The method gave a more conservative and accurate approximation, and the calculated result almost doubled, compared to the conventional method. The contribution from CCFs was also implemented.

The ETA was performed to cover the switching phases between the two pods, showing the time dependencies that can influence the consequences. This type of switching cannot be modeled in the fault tree, therefore, recommendations to apply the ETA to similar situations to get a more accurate reliability estimate is given.

For components such as the shear ram, a perfect function test cannot be performed. In the analysis, no such components are evaluated. However, in an expanded analysis of the subsea BOP control system, such components will be involved, therefore, it is recommended to add the contribution from PTC to components with imperfect testing.

7.2 Discussion

Neglecting human factors from the analysis is not ideal, in the event of a kick, an essential part of the operation is for humans to detected and act, before the control system takes over. Ignoring the human factors makes the result in the analysis some what degraded, however, modeling and quantification of human factors can be difficult. The effects of human factors in well integrity are discussed in Vignes (2011).

The majority of data used in the calculations may be outdated, as a result of limited access to updated data. The preliminary results from an ongoing SINTEF study shows a significantly higher beta-value compared to old reports. The old values are based on detection of dangerous detected failures by using diagnostic tests; however, in the analysis only DU-failures are considered. A higher contribution from the beta-factors can therefore be argued for.

The transition between pods is not fully accounted for in the analysis. In Rausand and Høyland (2004) the term *imperfect switching* is introduced, where the probability of switching between two redundant components is quantified. This contribution is not present in the analysis, and may have an impact on the calculations.

7.3 Recommendations for Further Work

The study is carried out within a limited period of time and recommendations to explore the conclusions of this report further, is given. Recommended tasks for making better conclusions are described below.

7.3.1 Proof Test Coverage

In an expanded analysis of a subsea BOP, components prone to imperfect tests are likely to be included. Calculating the PFD contribution from these components using the same methods applied for components with perfect proof tests will be wrong. Therefore, recommendations are given to add the contribution from the proof test coverage factor, for such components.

7.3.2 Event Tree Model

To strengthen the reliability analysis for the subsea BOP control system, it is recommended to expand the scope of the analysis and include event tree modeling.

7.3.3 Common Cause Failures

Performing a deeper analysis on potential common cause failures in the subsea BOP control system could expose more components prone to common cause failures, and strengthen the analysis.

7.3.4 Three Pods

Cameron has a control system containing three pods. A comparison between the conventional two pod system and the three pod system could provide useful knowledge about advantages and disadvantages between the systems, and give recommendations to future subsea BOP control systems.

Appendix A

Acronyms

API American Petroleum Institute

BOP Blowout Preventer

BSEE The Bureau of Safety and Environmental Enforcement

CCF Common Cause Failure

CCU Central Control Unit

DCP Driller's Control Panel

DU Dangerous Undetected

DWH Deepwater Horizon

EX Explosion

FMECA Failure Mode, Effects and Criticality Analysis

FTA Fault Tree Analysis

GOM Gulf of Mexico

HAZID Hazard Identification

HAZOP Hazard and Operability

HPU Hydraulic Power Unit

ID Inner Diameter

LMRP Lower Marine Riser Package

MTTF Mean time to failure

MUX Multiplex

NCS Norwegian Continental Shelf

NOG Norwegian Oil and Gas Association

PFD Probability of Failure on Demand

PFH Probability of Dangerous Failures per Hour

PLC Programmable Logical Controller

PSA Petroleum Safety Authority Norway

PTC Proof Test Coverage

RAMS Reliability, availability, maintainability, and safety

RBD Reliability Block Diagram

ROV Remotely Operated Vehicle

SEM Subsea Electronic Module

SIF Safety Integrity Function

SIL Safety Integrity Level

SIS Safety Instrumented System

STM Subsea Transducer Module

SV Solenoid Valve

TCP Toolpusher's Control Panel

UPS Uninterruptible Power Supply

U.S. United States

Appendix B

FMECA Sheets

B.1 FMECA

Sub-function 1: BOP control functions													
Description of unit				**Description of failure**				**Effect of failure**					
Comp. No	*Component*	*Function*	*Operational mode*	*Failure mode*		*Failure cause or mechanism*	*Detection of failure*	*On the subsystem*	*On the system function*	*Risk reducing measures/ safeguard*	*Criticality*		
											P	*E*	*S*
1.1	Power supply unit (topside)	Deliver power to el. panels and CCU	Avaliable at all times	F-1.1.1	Transmission failure	Failed electrical cable	Testing/ operation	No direct effect	No direct effect, because of safeguard	Frequent testing. Redundancy: Back-up battery	🟩	🟩	🟩
				F-1.1.2	Erratic output	Mechanical/ electrical failure		No electrical output			🟩	🟩	🟩
1.2	Control panels (topside)	Sends activation signals to CCU	Avaliable at all times	F-1.2.1	Erratic output	Electric failure	Testing/ operation	Pods will not recieve activation signal	Pods wil not activate, use secondary control system to activate BOP	Frequent testing and inspection. Redundancy: Have at least two separate panels	🟩	🟩	🟩
						Failure in MUX cable					🟩	🟩	🟩
1.3	Electric power from back-up battery	Deliver power to el. panels and CCU as back-up	Standby	F-1.3.1	Insufficient power	Failed electrical cable	Testing/ operation	No direct effect	No direct effect, because of redundancy	Maintenace/ operational routines. Redundancy: Main power is the primary source of power	🟩	🟩	🟩
						Battery empty					🟩	🟩	🟩
1.4	Batteries in pods	Enable pods to convert el. signals to hydraulic	Avaliable at all times	F-1.4.1	Insufficient power	Thermal variations	Testing/ operation	Solenoid valves would not function	Rams could not be activated in an emergency	Maintenance/ operational routines. Redundancy: Batterie in other pod and acoustic back-up system	🟩	🟩	🟩
						Corrosion					🟩	🟩	🟩
						Obsolete battery					🟩	🟩	🟩
1.5	MUX cable reel	Transefer electric comm. signals from CCU to subsea pod	Avaliable at all times	F-1.5.1	Transmission failure	Worn cable	Testing/ operation	Not able to initiate BOP functions	Commands from control panels cannot initiate BOP functions	Maintenance/ operational routines. Redundancy: Other MUX cable can be applied	🟩	🟩	🟩
						Short circuit					🟩	🟩	🟩
						No signal sent from electric panel					🟩	🟩	🟩

Description of unit				Description of failure				Effect of failure					
Comp. No	*Component*	*Function*	*Operational mode*	*Failure mode*		*Failure cause or mechanism*	*Detection of failure*	*On the subsystem*	*On the system function*	*Risk reducing measures/ safeguard*	*Criticality*		
											P	*E*	*S*
1.6	CCU	Send/recieve comm. signals Monitoring	Avaliable at all times	F-1.6.1	Control/signal failure	Mechanical/ electrical failure	Testing/ operation	Routing failure of electrical signals	BOP functions will not be activated	Frequent testing. Redundancy: ROV operation and acoustic back-up control system	🟨	🟩	🟨
				F-1.6.2	Erratic output	Mechanical/ electrical failure.		Routing failure of electrical signals			🟨	🟩	🟨
				F-1.6.3	Fail to function on demand	Mechanical/ electrical failure. Worn cables		No signal output			🟩	🟩	🟩
				F-1.6.4	Spurious activation	Mechanical/ electrical failure. Worn cables		Routing failure of electrical signals			🟨	🟩	🟨
1.7	Pod selector valve	Deliver power to el. panels and CCU as back-up	Avaliable at all times	F-1.7.1	Fail to move	Mechanical failure	Monitoring of valve position	Hyraulic fluid wrongly routed	If failure in a pod and trying to route hydraulic fluid away from it, no BOP function will be executed.	Maintenace/ operational routines. Regulary testing	🟥	🟩	🟥
						Obstruction							
						Corrosion							
1.8	Blue/ Yellow pods	Direct hydraulic fluid and operate the BOP	Avaliable at all times	F-1.8.1	Unable to deliver hydraulic power	SEM does not work	Testing/ operation		BOP will not activate, use different pod	Frequent testing, change damaged parts during maintenance, always have a pod working	🟩	🟩	🟩
						High pressure valve does not open							
						Solenoid valve do not activate							
1.9	Solenoid valve	Convert electrical signals into hydraulics	Avaliable at all times	F-1.9.1	Fail to move	Mechanical/ electrical failure.	Testing/ operation	Can no longer operate the solenoid valves from control panel	Still possible to operate the BOP functions manually	Maintenance/ operational routines. Regulary function testing of the BOP	🟩	🟩	🟩
						Obstruction							
						Corrosion							

Description of unit				Description of failure				Effect of failure					
Comp. No	Component	Function	Operational mode	Failure mode		Failure cause or mechanism	Detection of failure	On the subsystem	On the system function	Risk reducing measures/ safeguard	Criticality		
											P	E	S
1.10	SPM valve	Convert electrical signals into hydraulics	Avaliable at all times	F-1.10.1	Fail to open/close. Fail between positions	Mechanical failure, stuck, corrosion, worn/ degraded parts, hydraulic leakage.	Monitoring using flowmeter and pressure transmitter. Testing/ operation	SPM valve will not open/ close, will cause delay in the hydraulic system	No mediate effect, because of redundant SPM valves	Maintenace/ operational routines. Regulary testing. Redundancy: Have redundant SPM valve	🟩	🟩	🟩
1.11	Shuttle valve	Transfer hydraulics to BOP functions	Avaliable at all times	F-1.11.1	Fail to move	Mechanical failure Corrosion, due to exposure	Monitoring of valve position	Shuttle valve cannot move	Redundancy on shear rams will be lost, worst case no shearing	Maintenace/ operational routines. Regular function testing of BOP	🟥	🟩	🟥
1.12	Choke and kill valve	Testing BOP functions (Well killing is outside scope)	Avaliable at all times	F-1.12.1	Fail to open/close	Mechanical failure, corrosion, plugged line	Monitoring/ Testing procedures	Unable to perform testing as planned	No mediate effect, because of redundancy	Redundancy: Other ckoke and kill valve	🟩	🟩	🟩
					External leakage	Worn/degraded parts					🟩	🟩	🟩
					Internal leakage	Worn/degraded parts					🟩	🟨	🟩

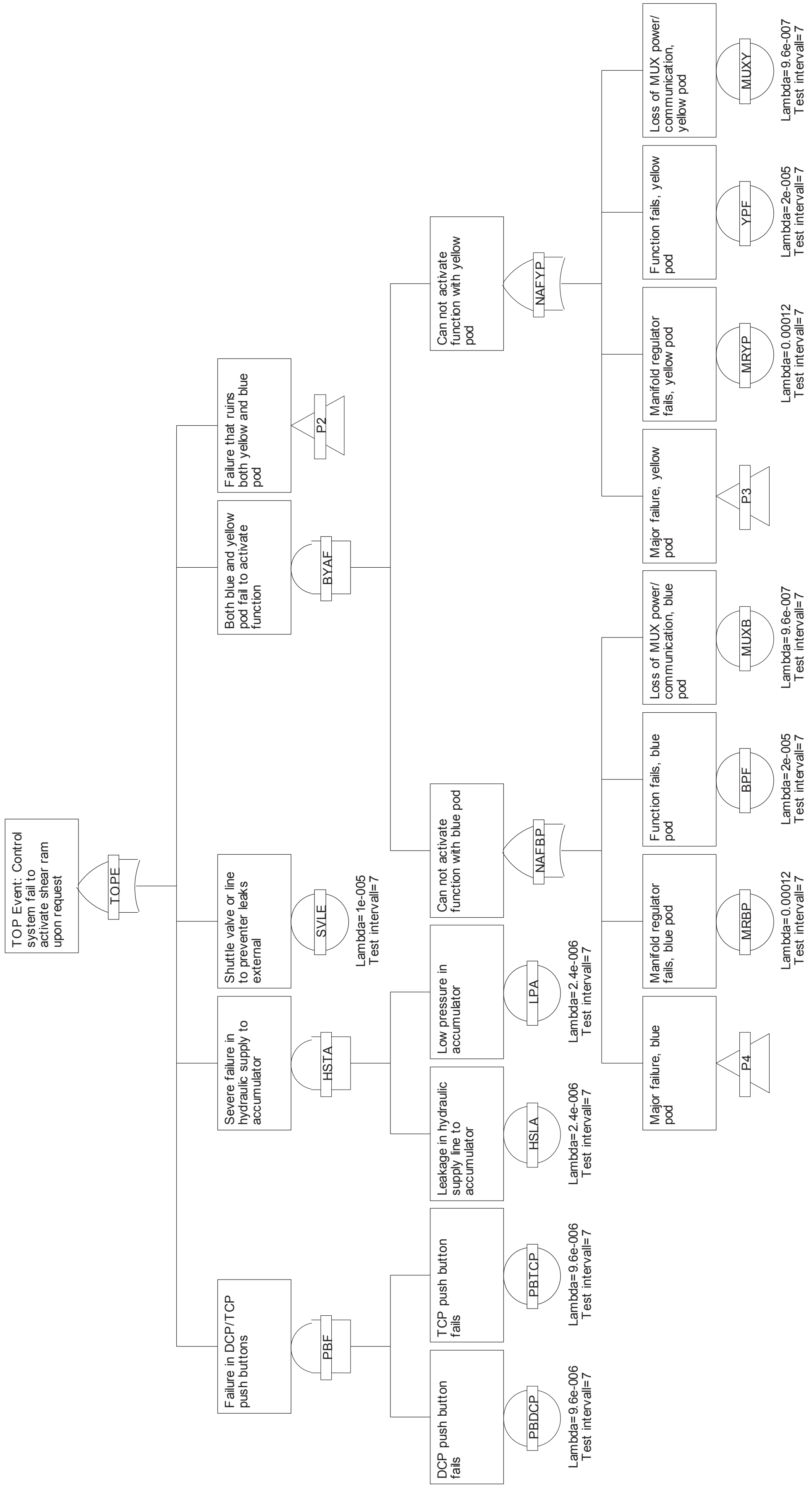
Sub-function 2: Power Supply													
Description of unit				**Description of failure**				**Effect of failure**					
Comp. No	*Component*	*Function*	*Operational mode*	*Failure mode*		*Failure cause or mechanism*	*Detection of failure*	*On the subsystem*	*On the system function*	*Risk reducing measures/ safeguard*	*Criticality*		
											P	*E*	*S*
2.1	Subsea accu-mulators	Store hydraulic fluid, provide high pressure to BOP functions	Avaliable at all times	F-2.1.1	Internal leakage	Mechanical damage. Poor quality on accumulator valve	Regular testing of BOP functions	Accumulator capacity is reduced/ lack of pressure/ does not function	No mediate effect, because of redundancy. BOP functions will work because of overcapacity	Regular function test of BOP functions and leak testing. Redundancy: Bottles are charged more than what is needed.	🟨	🟩	🟨
				F-2.1.1	Burst bladder	Wear due to aging. Damage on valve in bottom of baldder		Lack of pressure/ Gas in system/ Affected bladder will not function	Som reduced capacity. BOP functions will work because of overcapacity. Particles from bursted baldder can enter the hydraulic system		🟨	🟩	🟨
2.2	Fluid reservoir	Deliver hydraulic fluid	Avaliable at all times	F-2.2.1	Containment of reservoir	Reservoir cover degraded, causing the reservoir to be contaminated by dirt	Maintenace procedured/ Sampling of fluid to operations	Fluid quality is degraded, damages valves	Pumps clogging. Fine particles passing through, causing wear on pumps	Installing stainers will reduce number of large particles.	🟩	🟩	🟨
				F-2.2.2	Too low volumetric capacity	Failure in level transmitter. Capacity of reservoir is to small	Visual inspection. Level transmitter	Empty tank or overflown if more fluid is in the system, than capacity	Potentail spilling fluid to the environment	Maintenance/ operational routines. Low level alarm. Environmently friendly fluid	🟩	🟩	🟨
				F-2.2.3	Reservoir plugged	Too small or clogged went on the hydraulic reservoir	Visual inspection. Level transmitter	Leakage of hydraulic fluid	No mediate effect, because of safeguards	Accumulators store enough energy to secure BOP operations	🟩	🟩	🟨

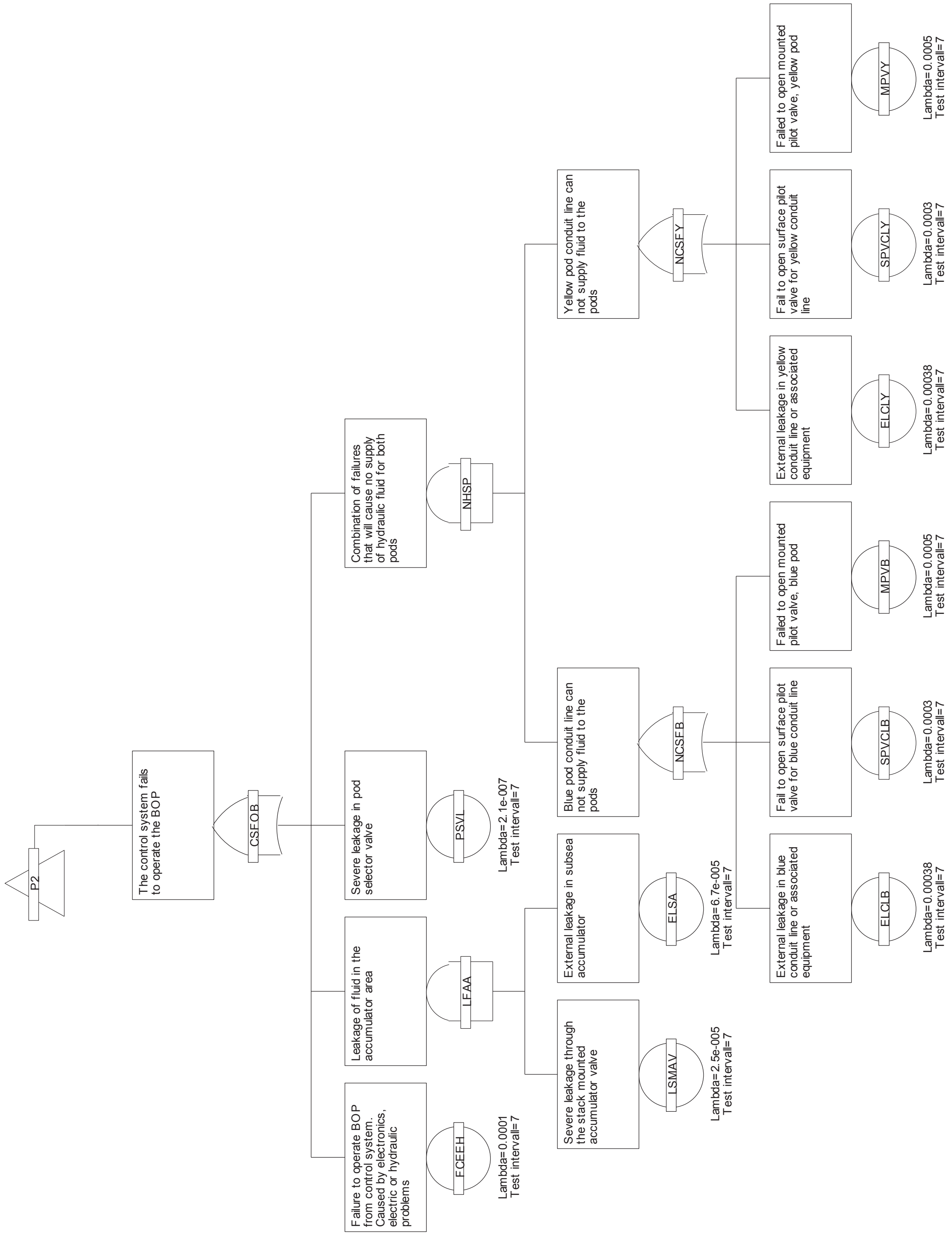
Description of unit				**Description of failure**				**Effect of failure**					
Comp. No	*Component*	*Function*	*Operational mode*	*Failure mode*		*Failure cause or mechanism*	*Detection of failure*	*On the subsystem*	*On the system function*	*Risk reducing measures/ safeguard*	*Criticality*		
											P	*E*	*S*
2.3	HPU	Deliver hydraulics	Avaliable at all times	F-2.3.1	Hydraulic pump failure	Mechanical/ electrical failure Quality of electrical motor in pump	Pumps are monitored with alarms	Pumps are not running	System will still function because of redundancy	Maintenance/ operational routines Redundancy: Extra pumps and accumulator banks	🟩	🟩	🟩
2.4	Hydraulic line from HPU to BOP	Deliver hydraulics	Avaliable at all times	F-2.4.1	Plugged/ choked line	Mechanical failure. Contamination of fluid	Pumps running excessivly Alarm indication Visual inspection	Spill to environment	Potential loss of individual BOP functions	Maintenace/ operational routines. Low level alarms Environmental fluid	🟨	🟩	🟩
				F-2.4.2	External leakage	External forces Vibration Failure in fittings gaskets, etc.		Reduced fluid delivery Spill to environment	Loos all hydraulic fluid. Loss of BOP functions		🟨	🟨	🟩
				F-2.4.3	Internal leakage	External forces Vibration Failure in fittings gaskets, etc.		Reduced fluid delivery	No qonsequence because of redundancy		🟨	🟩	🟩
2.5	Regulator valve	Regulate hydraulics	Avaliable at all times	F-2.5.1	Fail to move	Mechanical/ electrical failure Corrosion Failure in solenoid valve	Testing/ operation/ pressure trasmitters	Regulators cannot be operated from panels	No direct qonsequence due to redundancy	Maintenace/ operational routines. Can me operated manually or be bypassed	🟩	🟩	🟩
2.6	POD isolation valve	Regulate hydraulics	Avaliable at all times	F-2.6.1	Internal leakage	Mechanical, corrosion failure	Testing/ operation	Unable to perform BOP functions	Leakage to the environment	Monitoring of valve, flow meter and pressure transmitters	🟩	🟩	🟩
2.7	Hydraulic lines on BOP stack	Transfer hydraulic fluid	Avaliable at all times	F-2.7.1	Internal leakage	Mechanical, corrosion failure	Testing/ operation	Unable to perform BOP functions	Leakage to the environment	Monitoring of valve, flow meter and pressure transmitters	🟨	🟨	🟨

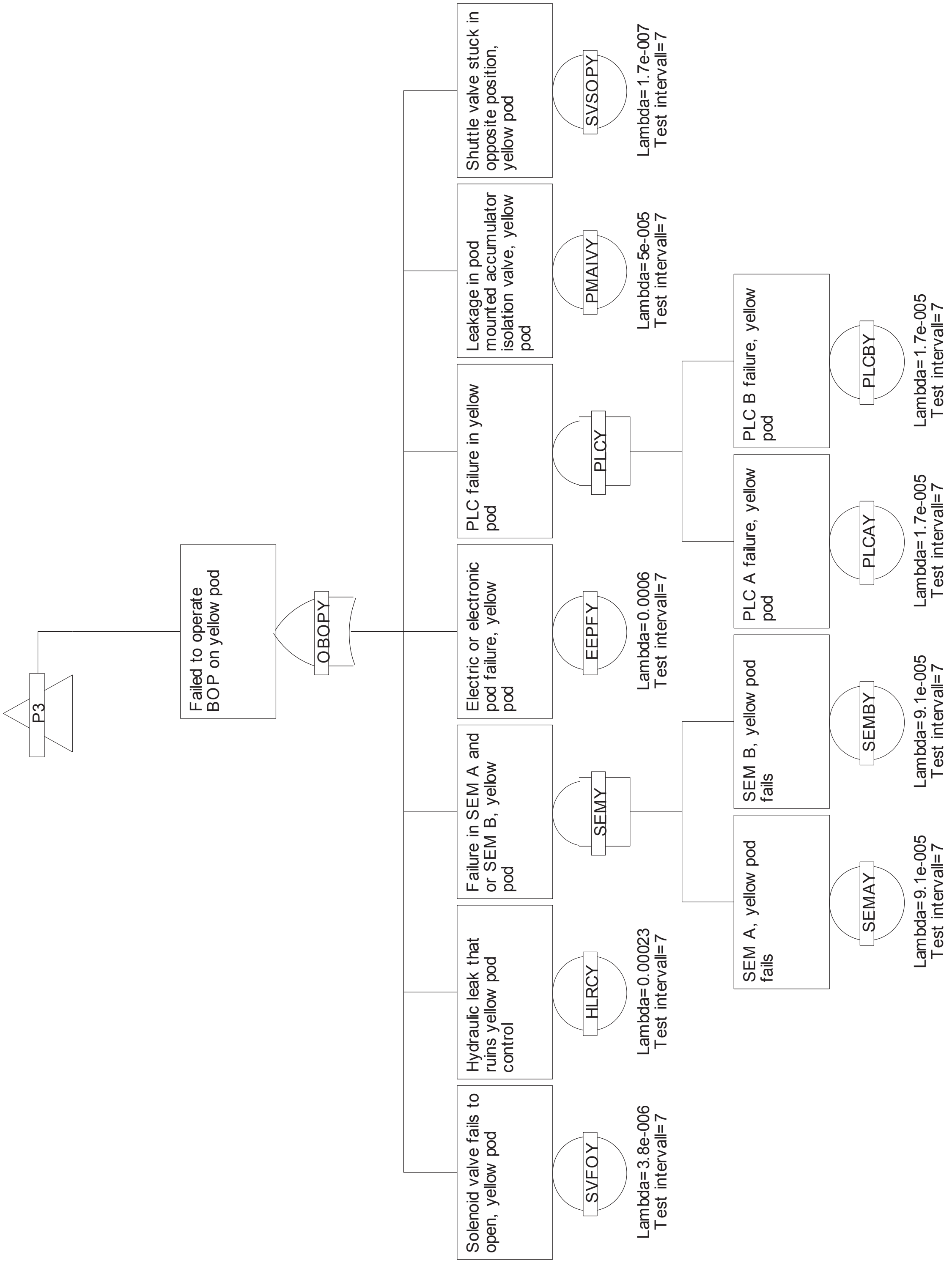
Appendix C

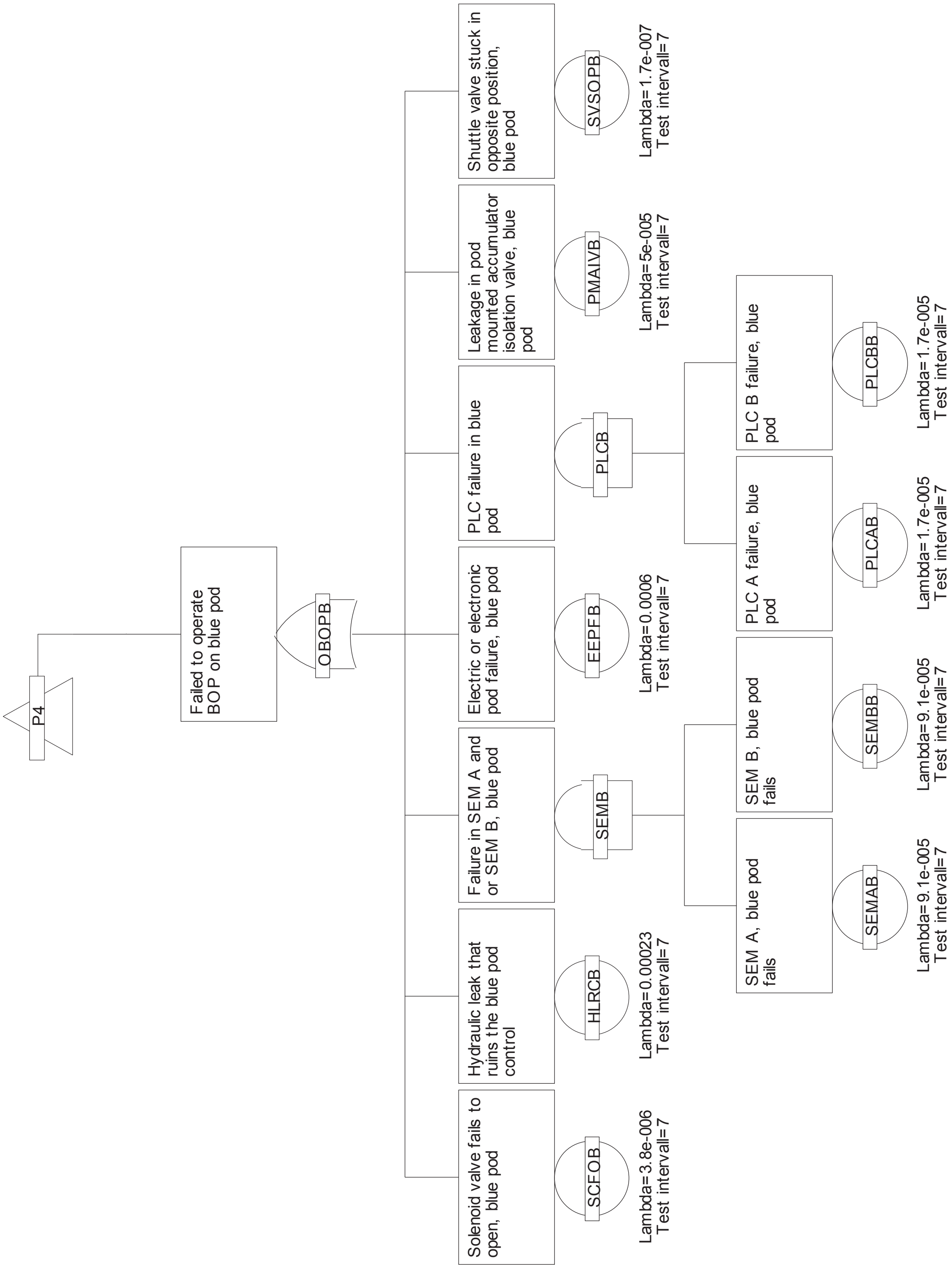
Fault Tree Analysis

C.1 Fault Tree


TOP Event: Control system fail to activate shear ram upon request
TOPE
Failure in DCP/TCP push buttons
PBF
Severe failure in hydraulic supply to accumulator
HSTA
Shuttle valve or line to preventer leaks external
SVLE
Lambda=1e-005
Test intervall=7
Both blue and yellow pod fail to activate function
BYAF
Failure that ruins both yellow and blue pod
P2
DCP push button fails
PBDCP
Lambda=9.6e-006
Test intervall=7
TCP push button fails
PBTCP
Lambda=9.6e-006
Test intervall=7
Leakage in hydraulic supply line to accumulator
HSLA
Lambda=2.4e-006
Test intervall=7
Low pressure in accumulator
LPA
Lambda=2.4e-006
Test intervall=7
Can not activate function with blue pod
NAFBP
Can not activate function with yellow pod
NAFYP
Major failure, blue pod
P4
Manifold regulator fails, blue pod
MRBP
Lambda=0.00012
Test intervall=7
Function fails, blue pod
BPF
Lambda=2e-005
Test intervall=7
Loss of MUX power/ communication, blue pod
MUXB
Lambda=9.6e-007
Test intervall=7
Major failure, yellow pod
P3
Manifold regulator fails, yellow pod
MRYP
Lambda=0.00012
Test intervall=7
Function fails, yellow pod
YPF
Lambda=2e-005
Test intervall=7
Loss of MUX power/ communication, yellow pod
MUXY
Lambda=9.6e-007
Test intervall=7


P2
The control system fails to operate the BOP
CSFOB
Failure to operate BOP from control system. Caused by electronics, electric or hydraulic problems
FCEEH
Lambda=0.0001
Test intervall=7
Leakage of fluid in the accumulator area
LFAA
Severe leakage through the stack mounted accumulator valve
LSMAV
Lambda=2.5e-005
Test intervall=7
External leakage in subsea accumulator
ELSA
Lambda=6.7e-005
Test intervall=7
Severe leakage in pod selector valve
PSVL
Lambda=2.1e-007
Test intervall=7
Combination of failures that will cause no supply of hydraulic fluid for both pods
NHSP
Blue pod conduit line can not supply fluid to the pods
NCSFB
External leakage in blue conduit line or associated equipment
ELCLB
Lambda=0.00038
Test intervall=7
Fail to open surface pilot valve for blue conduit line
SPVCLB
Lambda=0.0003
Test intervall=7
Failed to open mounted pilot valve, blue pod
MPVB
Lambda=0.0005
Test intervall=7
Yellow pod conduit line can not supply fluid to the pods
NCSFY
External leakage in yellow conduit line or associated equipment
ELCLY
Lambda=0.00038
Test intervall=7
Fail to open surface pilot valve for yellow conduit line
SPVCLY
Lambda=0.0003
Test intervall=7
Failed to open mounted pilot valve, yellow pod
MPVY
Lambda=0.0005
Test intervall=7


P3
Failed to operate BOP on yellow pod
OBOPY
Solenoid valve fails to open, yellow pod
SVFOY
Lambda=3.8e-006
Test intervall=7
Hydraulic leak that ruins yellow pod control
HLRCY
Lambda=0.00023
Test intervall=7
Failure in SEM A and or SEM B, yellow pod
SEMY
SEM A, yellow pod fails
SEMAY
Lambda=9.1e-005
Test intervall=7
SEM B, yellow pod fails
SEMBY
Lambda=9.1e-005
Test intervall=7
Electric or electronic pod failure, yellow pod
EEPFY
Lambda=0.0006
Test intervall=7
PLC failure in yellow pod
PLCY
PLC A failure, yellow pod
PLCAY
Lambda=1.7e-005
Test intervall=7
PLC B failure, yellow pod
PLCBY
Lambda=1.7e-005
Test intervall=7
Leakage in pod mounted accumulator isolation valve, yellow pod
PMAIVY
Lambda=5e-005
Test intervall=7
Shuttle valve stuck in opposite position, yellow pod
SVSOPY
Lambda=1.7e-007
Test intervall=7


P4
Failed to operate BOP on blue pod
OBOPB
Solenoid valve fails to open, blue pod
SCFOB
Lambda=3.8e-006
Test intervall=7
Hydraulic leak that ruins the blue pod control
HLRCB
Lambda=0.00023
Test intervall=7
Failure in SEM A and or SEM B, blue pod
SEMB
SEM A, blue pod fails
SEMAB
Lambda=9.1e-005
Test intervall=7
SEM B, blue pod fails
SEMBB
Lambda=9.1e-005
Test intervall=7
Electric or electronic pod failure, blue pod
EEPFB
Lambda=0.0006
Test intervall=7
PLC failure in blue pod
PLCB
PLC A failure, blue pod
PLCAB
Lambda=1.7e-005
Test intervall=7
PLC B failure, blue pod
PLCBB
Lambda=1.7e-005
Test intervall=7
Leakage in pod mounted accumulator isolation valve, blue pod
PMAIVB
Lambda=5e-005
Test intervall=7
Shuttle valve stuck in opposite position, blue pod
SVSOPB
Lambda=1.7e-007
Test intervall=7

C.2 Basic Events

The basic events for the fault tree are listed on the next page. Failure rates marked with green been derived from Holand and Awan (2012). Those failure rates marked with red is derived from Håbrekke et al. (2013), and those marked with yellow are "expert judgment"

Basic event	Failure mode description	Failure rate per day	Test intervall (Days)
PBDCP	DCP push button fails	9.60E-06	7
EEPFB	Electric or electronic pod failure, blue pod	6.00E-04	7
EEPFY	Electric or electronic pod failure, yellow pod	6.00E-04	7
ELCLB	External leakage in blue conduit line or associated equipment	3.80E-04	7
ELSA	External leakage in subsea accumulator	6.70E-05	7
ELCLY	External leakage in yellow conduit line or associated equipment	3.80E-04	7
SPVCLB	Fail to open surface pilot valve for blue conduit line	3.00E-04	7
SPVCLY	Fail to open surface pilot valve for yellow conduit line	3.00E-04	7
MPVB	Failed to open mounted pilot valve, blue pod	5.00E-04	7
MPVY	Failed to open mounted pilot valve, yellow pod	5.00E-04	7
FCEEH	Failure to operate BOP from control system. Caused by electronics, electric or hydraulic problems	1.00E-04	7
BPF	Function fails, blue pod	2.00E-05	7
YPF	Function fails, yellow pod	2.00E-05	7
HLRCB	Hydraulic leak that ruins the blue pod control	2.30E-04	7
HLRCY	Hydraulic leak that ruins yellow pod control	2.30E-04	7
HSLA	Leakage in hydraulic supply line to accumulator	2.40E-06	7
PMAIVB	Leakage in pod mounted accumulator isolation valve, blue pod	5.00E-05	7
PMAIVY	Leakage in pod mounted accumulator isolation valve, yellow pod	5.00E-05	7
MUXB	Loss of MUX power/ communication, blue pod	9.60E-07	7
MUXY	Loss of MUX power/ communication, yellow pod	9.60E-07	7
LPA	Low pressure in accumulator	2.40E-06	7
MRBP	Manifold regulator fails, blue pod	1.20E-03	7
MRYP	Manifold regulator fails, yellow pod	1.20E-03	7
PLCAB	PLC A failure, blue pod	1.68E-05	7
PLCAY	PLC A failure, yellow pod	1.68E-05	7
PLCBB	PLC B failure, blue pod	1.68E-05	7
PLCBY	PLC B failure, yellow pod	1.68E-05	7
SEMAY	SEM A, blue pod fails	9.10E-05	7
SEMAB	SEM A, yellow pod fails	9.10E-05	7
SEMBB	SEM B, blue pod fails	9.10E-05	7
SEMBY	SEM B, yellow pod fails	9.10E-05	7
PSVL	Severe leakage in pod selector valve	2.08E-07	7
LSMAV	Severe leakage through the stack mounted accumulator valve	2.50E-05	7
SVLE	Shuttle valve or line to preventer leaks external	1.00E-05	7
SVSOPB	Shuttle valve stuck in opposite position, blue pod	1.67E-07	7
SVSOPY	Shuttle valve stuck in opposite position, yellow pod	1.67E-07	7
SCFOB	Solenoid valve fails to open, blue pod	3.84E-06	7
SVFOY	Solenoid valve fails to open, yellow pod	3.84E-06	7
PBTCP	TCP push button fails	9.60E-06	7

C.3 Minimal Cut Sets

Cara FaultTree generated the minimal cut sets. The basic event marked in bold indicates a common cause component relationship. At the end of the table, the PFD_{SIF} for the TOP event can be found.

ID	Minimal cuts j	Non-cons. PFD w/out CCF	Cons. PFD w/out CCF	Cons PFD w/ CCF	1-PFD
MC 1	{FCEEH}	-	3.50E-04	-	0.9996500000000
MC 2	{PSVL}	-	7.28E-07	-	0.9999992720000
MC 3	{SVLE}	-	3.50E-05	-	0.9999650000000
MC 4	**{PBDCP,PBTCP}**	1.13E-09	2.26E-09	3.36E-06	0.9999966381711
MC 5	**{HSLA,LPA}**	6.48E-07	1.41E-10	8.40E-07	0.9999991598857
MC 6	{SVFOY,SCFOB}	1.81E-10	3.61E-10	-	0.9999999996387
MC 7	{HLRCY,SCFOB}	1.81E-10	3.61E-10	-	0.9999999996387
MC 8	{EEPFY,SCFOB}	2.82E-08	5.64E-08	-	0.9999999435520
MC 9	{PMAIVY,SCFOB}	2.35E-09	4.70E-09	-	0.9999999952968
MC 10	{SVSOPY,SCFOB}	7.84E-12	1.57E-11	-	0.9999999999843
MC 11	{MRYP,SCFOB}	5.64E-08	1.13E-07	-	0.9999998871040
MC 12	{YPF,SCFOB}	9.41E-10	1.88E-09	-	0.9999999981184
MC 13	{MUXY,SCFOB}	4.52E-11	9.03E-11	-	0.9999999999097
MC 14	{SVFOY,HLRCB}	1.08E-08	2.16E-08	-	0.9999999783616
MC 15	{HLRCY,HLRCB}	6.48E-07	1.30E-06	-	0.9999987039500
MC 16	{EEPFY,HLRCB}	1.69E-06	3.38E-06	-	0.9999966190000
MC 17	{PMAIVY,HLRCB}	1.41E-07	2.82E-07	-	0.9999997182951
MC 18	{SVSOPY,HLRCB}	4.70E-10	9.39E-10	-	0.9999999990606
MC 19	{MRYP,HLRCB}	3.38E-06	6.76E-06	-	0.9999932380000
MC 20	{YPF,HLRCB}	5.64E-08	1.13E-07	-	0.9999998873000
MC 21	{MUXY,HLRCB}	2.70E-09	5.41E-09	-	0.9999999945904
MC 22	{SVFOY,EEPFB}	2.82E-08	5.64E-08	-	0.9999999435520
MC 23	{HLRCY,EEPFB}	1.69E-06	3.38E-06	-	0.9999966190000
MC 24	**{EEPFY,EEPFB}**	4.41E-06	8.82E-06	2.17E-04	0.9997828558000
MC 25	{PMAIVY,EEPFB}	3.67E-07	7.35E-07	-	0.9999992651176
MC 26	{SVSOPY,EEPFB}	1.23E-09	2.45E-09	-	0.9999999975495
MC 27	{MRYP,EEPFB}	8.82E-06	1.76E-05	-	0.9999823600000
MC 28	{YPF,EEPFB}	1.47E-07	2.94E-07	-	0.9999997060000
MC 29	{MUXY,EEPFB}	7.06E-09	1.41E-08	-	0.9999999858880
MC 30	{SVFOY,PMAIVB}	2.35E-09	4.70E-09	-	0.9999999952968
MC 31	{HLRCY,PMAIVB}	1.41E-07	2.82E-07	-	0.9999997182951
MC 32	{EEPFY,PMAIVB}	3.67E-07	7.35E-07	-	0.9999992651176
MC 33	**{PMAIVY,PMAIVB}**	3.06E-08	6.12E-08	1.75E-05	0.9999824532034
MC 34	{SVSOPY,PMAIVB}	1.02E-10	2.04E-10	-	0.9999999997958
MC 35	{MRYP,PMAIVB}	7.35E-07	1.47E-06	-	0.9999985302352
MC 36	{YPF,PMAIVB}	1.22E-08	2.45E-08	-	0.9999999755039
MC 37	{MUXY,PMAIVB}	5.88E-10	1.18E-09	-	0.9999999988242
MC 38	{SVFOY,SVSOPB}	7.84E-12	1.57E-11	-	0.9999999999843
MC 39	{HLRCY,SVSOPB}	4.70E-10	9.39E-10	-	0.9999999990606
MC 40	{EEPFY,SVSOPB}	1.23E-09	2.45E-09	-	0.9999999975495
MC 41	{PMAIVY,SVSOPB}	1.02E-10	2.04E-10	-	0.9999999997958
MC 42	**{SVSOPY,SVSOPB}**	3.40E-13	6.81E-13	5.83E-08	0.9999999416544

MC 43	{MRYP,SVSOPB}	2.45E-09	4.90E-09	-	0.9999999950990
MC 44	{YPF,SVSOPB}	4.08E-11	8.17E-11	-	0.9999999999183
MC 45	{MUXY,SVSOPB}	1.96E-12	3.92E-12	-	0.9999999999961
MC 46	{MRBP,SVFOY}	5.64E-08	1.13E-07	-	0.9999998871040
MC 47	{MRBP,HLRCY}	3.38E-06	6.76E-06	-	0.9999932380000
MC 48	{MRBP,EEPFY}	8.82E-06	1.76E-05	-	0.9999823600000
MC 49	{MRBP,PMAIVY}	7.35E-07	1.47E-06	-	0.9999985302352
MC 50	{MRBP,SVSOPY}	2.45E-09	4.90E-09	-	0.9999999950990
MC 51	{MRBP,MRYP}	1.76E-05	3.53E-05	-	0.9999647200000
MC 52	{MRBP,YPF}	2.94E-07	5.88E-07	-	0.9999994120000
MC 53	{MRBP,MUXY}	1.41E-08	2.82E-08	-	0.9999999717760
MC 54	{BPF,SVFOY}	9.41E-10	1.88E-09	-	0.9999999981184
MC 55	{BPF,HLRCY}	5.64E-08	1.13E-07	-	0.9999998873000
MC 56	{BPF,EEPFY}	1.47E-07	2.94E-07	-	0.9999997060000
MC 57	{BPF,PMAIVY}	1.22E-08	2.45E-08	-	0.9999999755039
MC 58	{BPF,SVSOPY}	4.08E-11	8.17E-11	-	0.9999999999183
MC 59	{BPF,MRYP}	2.94E-07	5.88E-07	-	0.9999994120000
MC 60	**{BPF,YPF}**	4.90E-09	9.80E-09	7.01E-06	0.9999929920620
MC 61	{BPF,MUXY}	2.35E-10	4.70E-10	-	0.9999999995296
MC 62	{MUXB,SVFOY}	4.52E-11	9.03E-11	-	0.9999999999097
MC 63	{MUXB,HLRCY}	2.70E-09	5.41E-09	-	0.9999999945904
MC 64	{MUXB,EEPFY}	7.06E-09	1.41E-08	-	0.9999999858880
MC 65	{MUXB,PMAIVY}	5.88E-10	1.18E-09	-	0.9999999988242
MC 66	{MUXB,SVSOPY}	1.96E-12	3.92E-12	-	0.9999999999961
MC 67	{MUXB,MRYP}	1.41E-08	2.82E-08	-	0.9999999717760
MC 68	{MUXB,YPF}	2.35E-10	4.70E-10	-	0.9999999995296
MC 69	**{MUXB,MUXY}**	1.13E-11	2.26E-11	3.36E-07	0.9999996639817
MC 70	**{LSMAV,ELSA}**	1.37E-10	2.74E-10	5.85E-08	0.9999999415072
MC 71	{ELCLB,ELCLY}	1.77E-06	3.54E-06	-	0.9999964622000
MC 72	{ELCLB,SPVCLY}	1.40E-06	2.79E-06	-	0.9999972070000
MC 73	{ELCLB,MPVY}	2.33E-06	4.66E-06	-	0.9999953450000
MC 74	{SPVCLB,ELCLY}	1.40E-06	2.79E-06	-	0.9999972070000
MC 75	{SPVCLB,SPVCLY}	1.10E-06	2.21E-06	-	0.9999977950000
MC 76	{SPVCLB,MPVY}	1.84E-06	3.68E-06	-	0.9999963250000
MC 77	{MPVB,ELCLY}	2.33E-06	4.66E-06	-	0.9999953450000
MC 78	{MPVB,SPVCLY}	1.84E-06	3.68E-06	-	0.9999963250000
MC 79	{MPVB,MPVY}	3.06E-06	6.13E-06	-	0.9999938750000
MC 80	{SVFOY,**SEMAB,SEMBB**}	1.36E-12	2.73E-12	2.88E-10	0.9999999997122
MC 81	{HLRCY,**SEMAB,SEMBB**}	8.17E-11	1.63E-10	1.72E-08	0.9999999827598
MC 82	{EEPFY,**SEMAB,SEMBB**}	2.13E-10	4.26E-10	4.50E-08	0.9999999550255
MC 83	{PMAIVY,**SEMAB,SEMBB**}	1.77E-11	3.55E-11	3.75E-09	0.9999999962527
MC 84	{SVSOPY,**SEMAB,SEMBB**}	5.92E-14	1.18E-13	1.25E-11	0.9999999999875
MC 85	{MRYP,**SEMAB,SEMBB**}	4.26E-10	8.52E-10	8.99E-08	0.9999999100510
MC 86	{YPF,**SEMAB,SEMBB**}	7.10E-12	1.42E-11	1.50E-09	0.9999999985009
MC 87	{MUXY,**SEMAB,SEMBB**}	3.41E-13	6.82E-13	7.20E-11	0.9999999999280

MC 88	{SVFOY,**PLCAB,PLCBB**}	4.65E-14	9.29E-14	1.06E-11	0.9999999999894
MC 89	{HLRCY,**PLCAB,PLCBB}**	2.78E-12	5.57E-12	6.37E-10	0.9999999993634
MC 90	{EEPFY**,PLCAB,PLCBB**}	7.26E-12	1.45E-11	1.66E-09	0.9999999983394
MC 91	{PMAIVY,**PLCAB,PLCBB**}	6.05E-13	1.21E-12	1.38E-10	0.9999999998616
MC 92	{SVSOPY,**PLCAB,PLCBB**}	2.02E-15	4.03E-15	4.61E-13	0.9999999999995
MC 93	{MRYP,**PLCAB,PLCBB**}	1.45E-11	2.90E-11	3.32E-09	0.9999999966787
MC 94	{YPF,**PLCAB,PLCBB**}	2.42E-13	4.84E-13	5.54E-11	0.9999999999446
MC 95	{MUXY,**PLCAB,PLCBB**}	1.16E-14	2.32E-14	2.66E-12	0.9999999999973
MC 96	{**SEMAY,SEMBY**,SCFOB}	1.36E-12	2.73E-12	2.88E-10	0.9999999997122
MC 97	{**PLCAY,PLCBY**,SCFOB}	4.65E-14	9.29E-14	1.06E-11	0.9999999999894
MC 98	{**SEMAY,SEMBY**,HLRCB}	8.17E-11	1.63E-10	1.72E-08	0.9999999827598
MC 99	{**PLCAY,PLCBY**,HLRCB}	2.78E-12	5.57E-12	6.37E-10	0.9999999993634
MC 100	{**SEMAY,SEMBY**,EEPFB}	2.13E-10	4.26E-10	4.50E-08	0.9999999550255
MC 101	{**PLCAY,PLCBY**,EEPFB}	7.26E-12	1.45E-11	1.66E-09	0.9999999983394
MC 102	{**SEMAY,SEMBY,**PMAIVB}	1.77E-11	3.55E-11	3.75E-09	0.9999999962527
MC 103	{**PLCAY,PLCBY**,PMAIVB}	6.05E-13	1.21E-12	1.38E-10	0.9999999998616
MC 104	{**SEMAY,SEMBY**,SVSOPB}	5.92E-14	1.18E-13	1.25E-11	0.9999999999875
MC 105	{**PLCAY,PLCBY**,SVSOPB}	2.02E-15	4.03E-15	4.61E-13	0.9999999999995
MC 106	{MRBP,**SEMAY,SEMBY**}	4.26E-10	8.52E-10	8.99E-08	0.9999999100510
MC 107	{MRBP,**PLCAY,PLCBY**}	1.45E-11	2.90E-11	3.32E-09	0.9999999966787
MC 108	{BPF,**SEMAY,SEMBY**}	7.10E-12	1.42E-11	1.50E-09	0.9999999985009
MC 109	{BPF,**PLCAY,PLCBY**}	2.42E-13	4.84E-13	5.54E-11	0.9999999999446
MC 110	{MUXB,**SEMAY,SEMBY**}	3.41E-13	6.82E-13	7.20E-11	0.9999999999280
MC 111	{MUXB,**PLCAY,PLCBY**}	1.16E-14	2.32E-14	2.66E-12	0.9999999999973
MC 112	{[**SEMAY,SEMBY],[SEMAB,SEMBB]**}	1.03E-14	3.29E-14	3.46E-10	0.9999999996541
MC 113	**{[PLCAY,PLCBY],[SEMAB,SEMBB]}**	3.51E-16	1.12E-15	1.27E-11	0.9999999999873
MC 114	**{[SEMAY,SEMBY],[PLCAB,PLCBB]}**	3.51E-16	1.12E-15	1.27E-11	0.9999999999873
MC 115	**{[PLCAY,PLCBY],[PLCAB,PLCBB]}**	1.20E-17	3.83E-17	4.72E-13	0.9999999999995
				PFDsif	7.66E-04

Bibliography

API 53 (2012). *Blowout Prevention Equipment Systems for Drilling Wells.* American Petroleum Institute, Washington DC.

API spec 16D (2005). *Specification for Control Systems for Drilling Well Control Equipment and Control Systems for Diverter.* American Petroleum Institute, Washington DC.

Cameron Controls. *Multiplex Drilling Control Systems - Control Pod.* Cameron Controls, Houston, Texas.

Drægebø, E. (2014). Reliability analysis of blowout preventer systems. Master's thesis, NTNU, Trondheim, Norway.

Dutuit, Y., Rauzy, A., and Signoret, J.-P. (2008). A snapshot of methods and tools to assess safety integrity levels of high-integrity protection systems. *Part O: Journal of Risk and Reliability 222(3) (2008b) 371–379. Bordeaux, Talence, France.*

Engineering Services LP (2014). Deepwater horizon RBS 8D BOP MUX control system report. *To the U. S. Chemical Safety and Hazard Investigation Board, Huston, Texas.*

Goins, W. and Sheffield, R. (1983). *Blowout prevention - Practical drilling technology; 1.* Houston: Gulf Publishing Company.

Grondahl, M. (2015). http://www.nytimes.com/interactive/2010/06/21/us/20100621-bop.html?_r=0. New York Times.

Hals, T. and Molnes, E. (1984). *Reliability of Subsea BOP Systems - Phase II Control Systems.* SINTEF STF18 F84516, Trondheim, Norway.

Hauge, S., Kråkenes, T., Hokstad, P., Håbrekke, S., and Jin, H. (2013). *Reliability Prediction Method for Safety Instrumented Systems*. SINTEF, Trondheim, Norway.

Hawker, D. (2011). *Blow Out Prevention & Well Control (Version 2.1)*. Datalog, Anca Maria Anistoroae.

Hokstad, P. and Rausand, M. (2008). Common cause failure modeling: Status and trends. *Chapter 39 in Handbook of Performability Engineering, Trondheim, Norway*.

Holand, P. (1999). Reliability of subsea bop systems for deepwater application, phase II DW. Technical report, SINTEF, Trondheim, Norway.

Holand, P. and Awan, H. (2012). Reliability of deepwater subsea bop systems and well kicks. Technical report, Exprosoft, Trondheim, Norway.

Håbrekke, S., Hauge, S., and Onshus, T. (2013). *Reliability Data for Safety Instrumented Systems - PDS Data Handbook - 2013 Edition*. SINTEF, Trondheim, Norway.

IEC-61508 (2005). *Functional safety of electrical/electronic/programmable electronic safety-related systems*. International Electrotechnical Commision, Oslo, Norway.

IEC-61511 (2011). *Functional safety: Safety instrumented systems for the process industry sector*. International Electrotechnical Commision, Oslo, Norway.

Imperial Oil and ExxonMobile (2009). Appendix d - offshore drilling well control.

Klakegg, S. (2012). Improved methods for reliability assessments of safety- critical systems: An application example for bop systems. Master's thesis, NTNU, Trondheim, Norway.

Lundteigen, M. A. and Rausand, M. (2007). Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *Journal of Loss Prevention in the Process Industries 20 (2007) 218–229, Trondheim, Norway*.

Lundteigen, M. A. and Rausand, M. (2009). Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and a case study. *International Journal of Reliability, Quality and Safety Engineering Vol. 16, No. 2 187–212, Trondheim, Norway*.

MCS Kenny (2013). Assessment of BOP stack sequencing, monitoring and kick detection technology. *BSEE, Final Report 02 - BOP Monitoring and Acoustic Technology, Huston, Texas.*

NOG - 070 (2004). *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry.* Norwegian Oil and Gas Association, Sandnes, Norway.

NORSOK D-001 (2012). *Drilling facilities.* Standards Norway, Lysaker, Norway.

Rausand, M. (2014). *Reiability of Safety-Critical Systems: Theory and Applications.* Wiley, Hoboken, NJ.

Rausand, M. and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications.* Wiley, Hoboken, NJ, 2nd edition.

Rees, A. and Matthews, D. (2011). Blowout preventer stack and control systems. In *Lillehammer Energy Claims Conferance.*

Sattler, J. and Gallander, F. (2010). Just how reliable is your BOP today? results from a JIP, US GOM 2004- 2006. *Presented at the IADC/SPE Drilling Conference and Exhibition, New Orleans, 4 February.*

Shanks, E., Dykes, A., Quilici, M., and Pruitt, J. (2003). Deepwater BOP control systems - a look at reliability issues. *Offshore Technology Conference, Huston, Texas.*

Stamatelatos, M. and Dezfuli, H. (2011). *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners.* NASA, NASA Headquaters, Washington, DC.

Strand, G. O. (2014). Critical safety unavailability of subsea blowout preventer systems. Technical report, NTNU, Trondheim, Norway.

Vignes, B. (2011). *Contribution to well integrity and increased focus on well barriers from a life cycle aspect.* PhD thesis, Faculty of Science and Technology University of Stavanger.