



NTNU – Trondheim
Norwegian University of
Science and Technology

Improved methods for reliability assessments of safety-critical systems: An application example for BOP systems

Sondre Klakegg

Product Design and Manufacturing

Submission date: June 2012

Supervisor: Mary Ann Lundteigen, IPK

Co-supervisor: Håkon Husby, Det Norske Veritas
Håvard Brandt, Det Norske Veritas

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

MASTER THESIS
2012
for
stud. techn. Sondre Klakegg

IMPROVED METHODS FOR RELIABILITY ASSESSMENTS OF SAFETY-CRITICAL SYSTEMS: AN APPLICATION EXAMPLE FOR BOP SYSTEMS
(Forbedrede metoder for pålitelighetsvurdering av sikkerhetskritiske systemer: Med en utblåsningsventil (BOP) som anvendelseseksempel)

System reliability assessments provide important input to decision-making in relation to design-related issues as well as during operation and maintenance. The main purpose of a system reliability assessment is to provide realistic predictions of the future performance of the system, within the constraints of available data, operating conditions, and modeling capabilities. Special applications and operating conditions sometimes reveal inadequacies in current assessment methods. One such application is the blowout preventer (BOP), a safety-critical system that is used to ensure safe drilling and well interventions of oil and gas wells. The ability of the BOP system to function as a safety barrier depends on the ongoing operation, whether it is drilling, tripping-in, tripping-out, well logging, and so on. At the same time, the likelihood of demands to be handled depends on the same operations. An average estimate of the BOP's ability to function on demand is therefore not an adequate reliability parameter. A BOP system deviates from many other safety barrier systems since it does not have a fail-safe design (except for the choke and kill valves). Another deviation is due to the many different uses of the BOP and its components. Some of the components are operated more often than during the periodic proof tests. The usual formulas for reliability calculations based on periodic proof testing can therefore not be used directly.

In this master thesis, the main objective is to propose solutions to some of the challenges indicated above, using the BOP as an example. More specifically, the candidate shall:

1. *Give a presentation of a typical (standard) BOP system, its requirements and reliability challenges*
 - a. Describe and classify the main functions and the associated performance requirements of a BOP system.

- b. Identify and discuss the main operating situations of a BOP in light of the ability of the BOP to stop well kicks.
 - c. Identify recent BOP stack configurations and describe the pros and cons of these related to a standard BOP configuration.
2. *Suggest improved approaches to reliability assessment of BOP systems that can incorporate some of the above challenges*
- a. Carry out and document a literature survey on how reliability analyses of BOPs have been performed in the past, including the selection of reliability measure, and discuss the limitations of these approaches.
 - b. Discuss the implications and causes of common cause failures (CCFs) on the execution of BOP functions
 - c. Propose a new overall approach to risk and reliability assessment of a BOP system, which includes proposals for how to solve some of the identified challenges.
 - d. Identify related issues that need further research, and give recommendations for such research.

Within three weeks after the date of the task handout, a pre-study report shall be prepared. The report shall cover the following:

- An analysis of the work task's content with specific emphasis of the areas where new knowledge has to be gained.
- A description of the work packages that shall be performed. This description shall lead to a clear definition of the scope and extent of the total task to be performed.
- A time schedule for the project. The plan shall comprise a Gantt diagram with specification of the individual work packages, their scheduled start and end dates and a specification of project milestones.

The pre-study report is a part of the total task reporting. It shall be included in the final report. Progress reports made during the project period shall also be included in the final report.

The report should be edited as a research report with a summary, table of contents, conclusion, list of reference, list of literature etc. The text should be clear and concise, and include the necessary references to figures, tables, and diagrams. It is also important that exact references are given to any external source used in the text.

Equipment and software developed during the project is a part of the fulfilment of the task. Unless outside parties have exclusive property rights or the equipment is physically non-moveable, it should be handed in along with the final report. Suitable documentation for the correct use of such material is also required as part of the final report.

The student must cover travel expenses, telecommunication, and copying unless otherwise agreed.

If the candidate encounters unforeseen difficulties in the work, and if these difficulties warrant a reformation of the task, these problems should immediately be addressed to the Department.

The assignment text shall be enclosed and be placed immediately after the title page.

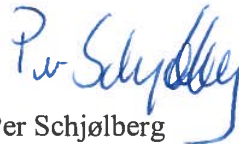
Deadline: June 11th 2012.

Two bound copies of the final report and one electronic (pdf-format) version are required.

Responsible supervisor at NTNU: Professor Mary Ann Lundteigen
Phone: 73 59 71 01
Mobile phone: 930 59 365
E-mail: mary.a.lundteigen@ntnu.no

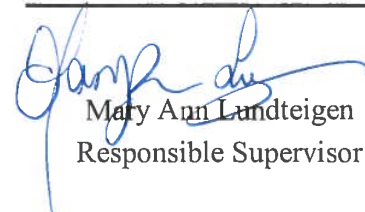
Supervisor at Energy Solutions: Consultant Håkon Husby
Business Risk Management Mobile phone: 936 30 449
E-mail: Hakon.Husby@dnv.com

**DEPARTMENT OF PRODUCTION
AND QUALITY ENGINEERING**



Per Schjølberg

Associate Professor/Head of Department



Mary Ann Lundteigen
Responsible Supervisor

Preface

This report documents my master thesis carried out during the spring of 2012. The thesis has been carried out as part of the Mechanical Engineering MSc program at the Norwegian University of Science and Technology (NTNU), and is concerned with reliability assessment of subsea drilling blowout preventers for deepwater application. The reader is assumed to be familiar with the terminology used in the NTNU course TPK4120 Safety and Reliability Analysis and/or the terminology used in Rausand and Hoyland (2004). The reader is also assumed to have knowledge of the basics concepts involved with drilling of hydrocarbon wells. It is further assumed that the reader has basic knowledge of the IEC61508 standard for functional safety of electric/electronic/programmable electronic safety-related systems.

Trondheim, 2012-06-11



Sondre Klakegg

Acknowledgments

This master thesis could not have been carried out without the invaluable help and support of a few key individuals. I would especially like to thank my primary supervisor Mary-Ann Lundteigen, professor at the Department of Production and Quality Engineering at NTNU, for dedicated help and support during the work. Also great thanks to Det Norske Veritas (DNV) representatives Håvard Brandt and Håkon Husby, who have been always helpful with answering questions and providing competent input. Thanks for Exprosoft AS representative Einar Molnes, for generously granting me a free version of the CARA FaultTree software tool for use in my master thesis. Finally I would like to thank all other DNV employees who have helped with my thesis work, and the organisation in general for their hospitality in providing me with an apartment and a workspace on their premises.

S.K.

Summary

The failure of the Deepwater Horizon drilling rig's blowout preventer has been pointed to as one of the main causes of the Macondo accident on April 10th 2010. The blowout preventer system is one of the most important safety barriers in a hydrocarbon well. The accident has created a demand for improved methods of assessing the reliability of blowout preventer systems. The objective of this master thesis is to propose improvements to current reliability assessment methods for complex safety critical systems such as the blowout preventer.

The report begins by presenting a typical subsea drilling blowout preventer system designed for deepwater application in exploration drilling, with a description of its main components and functions. The blowout preventer is also classified as a safety barrier in light of well barrier terminology in relevant standards.

A functional analysis of the blowout preventer system is presented next. Essential functions are defined, and performance criteria for these functions identified. An approach to classification of blowout preventer functions is also presented, before the report moves on to the analysis of four main operational situations to which the blowout preventer is exposed during the course of a typical drilling program, and whose characteristics have implications for the system's ability to act as a safety barrier.

The pros and cons of different widely used blowout preventer system configurations is also discussed. Three main types of configurations are mentioned in the report; the "modern" configuration, the "traditional" configuration and the Deepwater Horizon blowout preventer system configuration.

A literature survey which documents previous blowout preventer reliability studies performed by Per Holand on behalf of SINTEF is presented. An evaluation of the validity of the operational assumptions which have been made in these previous studies is also provided, such as assumptions regarding operational situations, failure input data, and several important assumptions regarding testing of blowout preventer systems. Regulations and guidelines which are relevant to blowout preventer reliability are also described here.

The report further discusses how the blowout preventer may fail, and which types of failure modes are considered critical from a safety perspective. Some theoretic principles behind common cause failures are presented, along with a discussion of how common cause failures should be included in reliability assessments of safety critical systems through an approach called the *PDS approach*. This is followed by a discussion of possible sources for common cause failures in the blowout preventer system.

As a suggestion towards how reliability assessments of blowout preventers can be improved, and

some of the identified reliability challenges solved, a reliability quantification method is presented. The method is based on post-processing of minimal cut sets from a fault tree analysis of the blowout preventer system, and produces more conservative and accurate approximations of the reliability than those produced through conventional methods. The method is also capable of taking into account common cause failures. The results from the calculations are presented and discussed.

Event trees are presented which illustrate the escalation of a well kick in two different operational situations are presented, along with a discussion of how event tree analysis may be used to improve the quality of blowout preventer reliability assessments, and the reliability of well barriers in general.

Finally, the conclusions from the thesis are provided. The main conclusions are summarized by three key findings. First, that the approach based on fault trees and post-processing of minimal cut sets can certainly be used to improve the quality of blowout preventer reliability estimates, and also provides a sound platform for including common cause failures in the analysis. Second, the failure modes of control system components contribute by far the majority of the unreliability of the blowout preventer system. And third, a test coverage factor should included in calculations in order to take into account failures that are unrevealed by function tests for certain key components in the blowout preventer system.

Sammendrag

Feil i boreriggen Deepwater Horizons utblåsningsventil har blitt pekt på som en av hovedårsakene til Macondo-ulykken som inntraff den 10. april 2010. Utblåsningsventilen er en av de viktigste barrierer ved leteboring i en olje- og gassbrønn. Macondo-ulykken har skapt en økt etterspørsel etter forbedrede metoder for å vurdere påliteligheten til komplekse, sikkerhetskritiske systemer slik som utblåsningsventiler. Målet med denne masteroppgaven er å fremlegge forslag til mulige forbedringer ved de nåværende metodene som brukes for å vurdere påliteligheten til utblåsningsventiler.

Rapporten begynner med å presentere en typisk utblåsningsventil designet for bruk under leteboring i dypvannsbrønner, og den beskrivelse av dens hovedkomponenter- og funksjoner. Utblåsningsventilen blir også klassifisert i lys av terminologi fra relevante standarder i forbindelse med brønnbarrierer.

Deretter presenteres en funksjonell analyse av utblåsningsventilen. Essensielle funksjoner blir definert, og ytelseskrav for disse funksjonene identifisert. En fremgangsmåte for klassifisering av utblåsningsventilers funksjoner blir også presentert, før rapporten går videre med en analyse av fire sentrale operasjonelle situasjoner som utblåsningsventilen blir utsatt for i løpet av et typisk boreprogram, og hvis egenskaper har innvirkning på systemets evne til å oppfylle sin funksjon som sikkerhetsbarriere.

Fordeler og ulemper ved ulike typer kjente konfigurasjoner for utblåsningsventiler blir også diskutert. Det skilles her mellom tre hovedkonfigurasjoner; den "moderne" konfigurasjonen, den "tradisjonelle" konfigurasjonen, og konfigurasjonen av utblåsningsventilen som var installert på Deepwater Horizon da denne var i ferd med å bore BPs Macondo-brønn.

Rapporten dokumenterer også et litteraturstudie som omfatter tidligere studier av påliteligheten til utblåsningsventiler, i all hovedsak utført av Per Holand på vegne av SINTEF. Gyldigheten til en rekke operasjonelle antagelser som er gjort i forbindelse med disse pålitelighetsstudiene, både i forhold til operasjonelle situasjoner, feildata, og en rekke viktige antagelser knyttet til testing av utblåsningsventiler, blir vurdert. Regler og retningslinjer som er relevante for utblåsningsventiler på norsk sokkel blir også beskrevet her.

Videre diskuteres det hvordan utblåsningsventilen kan feile, og hvilke typer feilmodi som bør anses som kritiske fra et sikkerhetsperspektiv. Enkelte teoretiske prinsipper angående fellesfeil blir presentert, sammen med en diskusjon som vedrører hvordan fellesfeil bør inkluderes i pålitelighetsvurderinger av utblåsningsventiler gjennom en metode som kalles *PDS-metoden*. Dette etterfølges av noen betraktninger angående mulige kilder til fellesfeil i utblåsningsventiler.

Som et forslag til hvordan gjeldende metoder for pålitelighetsvurdering av utblåsningsventiler kan forbedres, presenteres en kvantifiseringsmetode. Metoden er basert på post-prosessering av minimale kutt sett fra feiltreanalyse av utblåsningsventiler, hvor hovedpoenget er at metoden produserer mer nøyaktige og mer konservative estimater for påliteligheten enn det som oppnås ved hjelp av konvensjonelle metoder som f. eks å generere estimater automatisk ved hjelp av software-verktøy for feiltreanalyse. Et annet viktig poeng med metoden er at den er i stand til å ta hensyn til fellesfeil. Metoden blir anvendt på utblåsningsventilen, og resultatene fra utregningene blir presentert og diskutert.

Hendelsestrær som illustrerer en eskalert brønnkontrollsituasjon for to ulike operasjonelle situasjonene blir presentert, sammen med en diskusjon angående muligheten for å bruke analyse av hendelsestrær som en metode for å forbedre kvaliteten på pålitelighetsvurderinger av utblåsningsventiler, men også av brønnkontrollsystemer på generell basis.

Til slutt presenteres konklusjonene som kan trekkes fra arbeidet med diplomoppgaven. Konklusjonene kan oppsummeres av tre hovedfunn. Det første er at metoden basert på post-prosessering av minimale kutt sett fra feiltreanalyse definitivt kan brukes til å oppnå bedre estimater for påliteligheten til utblåsningsventiler, og er også et passende verktøy for å kunne inkludere fellesfeil i analysen på en god måte. Det andre hovedfunnet er at feil som stammer fra komponenter i kontrollsystemet bidrar klart mest til upåliteligheten i systemet. Det tredje og siste hovedfunnet er at en for å ta hensyn til feil som ikke avdekkes av funksjonelle tester av utblåsningsventilene bør inkludere en "dekningsfaktor" for ikke-perfekte tester av enkelte komponenter når man regner ut påliteligheten til disse.

Contents

Master Thesis Assignment	
Preface	iii
Acknowledgments	iv
Summary	v
Sammendrag på norsk	vii
1 Introduction	1
1.1 Background	1
1.2 Objectives	2
1.3 Limitations	3
1.4 Approach	4
1.5 Structure of the Report	5
2 BOP and drilling operations	6
2.1 BOP system description	6
2.1.1 Introduction	6
2.1.2 The main elements of a BOP system	6
2.2 Functional analysis of the BOP system	15
2.2.1 Introduction	15
2.2.2 The BOP as a well barrier	15
2.2.3 Essential BOP functions	16
2.2.4 BOP functional block diagram	17
2.2.5 Classification of BOP functions	18
2.3 BOP operational situations	20
2.3.1 Introduction	20
2.3.2 Analysis of four main operational situations	21
2.4 Recent BOP stack configurations	27
2.4.1 Introduction	27
2.4.2 Stack configurations	28

3 Literature survey	30
3.1 Literature on BOP reliability	30
3.1.1 Introduction	30
3.1.2 Previous BOP reliability studies	30
3.1.3 Operational assumptions	31
3.2 Regulations and guidelines	36
3.2.1 Introduction	36
3.2.2 Standards pertaining to BOP reliability	36
3.2.3 BOP testing regulations in the Norwegian Sector of the North Sea	37
4 BOP failures	40
4.1 Overview of all BOP failures	40
4.1.1 Introduction	40
4.1.2 Safety criticality of failures	40
4.1.3 Data sources	41
4.1.4 BOP system failure modes	41
4.2 Common cause failures	42
4.2.1 Introduction	42
4.2.2 Theoretic principles behind CCF modeling	43
4.2.3 CCF data sources	45
4.2.4 CCF in the BOP system	45
5 Reliability assessment model	46
5.1 Quantification of BOP reliability	46
5.1.1 Introduction	46
5.1.2 Background for the approach	47
5.1.3 Fault tree analysis of the BOP system	49
5.1.4 Event tree analysis	64
6 Summary and Recommendations for Further Work	65
6.1 Introduction	65
6.2 Summary and conclusions	65
6.3 Recommendations and ideas for further work	67
References	68
Appendices	70
A Acronyms	71

B	Fault Tree Analysis	74
B.1	Fault trees	74
B.2	Fault tree basic events	99
B.3	Minimal cut sets	104
C	Event trees	115
C.1	Event trees for Case B and C	115

List of Figures

1.1	Master thesis approach (modified from Lundteigen (2009), p.21)	4
2.1	Typical configuration of a subsea drilling BOP system designed for deepwater application. Modified from OLF-070 (2004), page 85.	8
2.2	Simplified BOP control system.	12
2.3	BOP control system logic arrangement.	14
2.4	BOP essential functions, as specified in OLF-070 (2004).	16
2.5	Functional block diagram of the BOP system.	18
2.6	The four most common operational situations encountered by the BOP during a typical deepwater exploration drilling program.	22
2.7	RBDs illustrating available BOP functions in the base case.	24
2.8	Spacing of tool joints through wellbore annulus.	25
2.9	RBD of available BOP functions in Case B.	26
2.10	RBDs illustrating available BOP functions in the high pressure case.	27
5.1	Minimal cut A10, with two common cause component groups.	58

List of Tables

2.1	Inherent sub-functions and their functional requirements and classification for the overall primary BOP system function <i>Isolate well</i>	20
2.2	Three common BOP stack configurations.	28
3.1	Routine leak testing of drilling BOP and well control equipment. Source: D-010 (2004), p.157	38
4.1	Failure modes in the BOP system.	42
5.1	TOP event A minimal cuts.	53
5.2	TOP event B minimal cuts.	54
5.3	TOP event C minimal cuts.	54
5.4	TOP event D minimal cuts.	55
5.5	β -factors.	56
5.6	PFD calculation results for TOP Event A.	60
5.7	PFD calculation results for TOP Event B.	60
5.8	PFD calculation results for TOP Event C.	61
5.9	PFD calculation results for TOP Event D.	62

Chapter 1

Introduction

1.1 Background

The Macondo accident on April 20th 2010 caused the largest accidental offshore oil spill in the history of the petroleum industry. It has had devastating consequences, both economically and environmentally. The cause of the accident was a blowout from the BP licensed Macondo well, which was at the time being drilled by the Transocean-owned rig Deepwater Horizon (DWH). During the final stages of the drilling process, the rig crew lost control of the well and hydrocarbons were released onto the deck. After a short period of time, the hydrocarbons were ignited, and eventually the DWH rig sank. 11 men were killed during the explosion and subsequent fire, and a total of 4.9 million barrels of crude oil spilled into the sea.

The failure of the DWH blowout preventer (BOP) has been pointed to as one of the main causes of the accident. The BOP is one of the most important safety barriers between the rig and the hydrocarbons in the well. Thus, BOP reliability is a matter of vital importance in terms of ensuring safe operation during drilling of hydrocarbon wells. The Macondo accident has created a new level of interest into this area from the petroleum industry, and a demand for better methods of assessing the reliability of BOPs.

The industry uses reliability assessments to support decisions regarding the technical design and operation of safety critical systems. A reliability assessment will generally be performed in accordance with relevant standards and internal guidelines, such as IEC 61511 (2004), IEC 61508 (2010), and OLF-070 (2004). Methods for quantification of reliability of safety critical systems have been developed through application of theoretic principles from the reliability engineering discipline, most of which are presented in Rausand and Hoyland (2004). However, the specific features of a safety critical system and the conditions under which it operates may sometimes

reveal inadequacies in these assessment methods.

In the case of the BOP, there are important issues that must be taken into account, which have not been considered in previous reliability assessments. One of these issues is that the ability of the BOP to function as a safety barrier depends on the operational situation. Another issue is that, contradictory to most safety critical systems, the BOP has many components which are operated more often than during the periodic proof tests, because they are part of an operational function in addition to their application as a safety barrier function. Furthermore, the functional tests that are performed, are imperfect in the sense that some failures remain unrevealed by the tests. This means that the standard formulas for reliability calculations based on periodic proof tests cannot be directly applied to these components, or to the BOP as a whole. The same reliability calculations also include other assumptions regarding testing that do not necessarily hold for a BOP system.

Previous attempts to quantify the reliability of BOPs have largely been based on collection and analysis of rig-specific failure data. The studies carried out by Per Holand on behalf of SINTEF during the course of the 1980s and 1990s have resulted in important knowledge about a number of issues related to BOP reliability, such as failures and failure criticality towards both safety and downtime, failure causes, maintenance, test time consumption and the efficiency of various testing strategies (Holand, 1999), (Holand and Skalle, 2001). Based on testing intervals and estimated failure rates, quantitative techniques have been used to provide an estimate of the BOP reliability. However, when considering failures and failure causes, previous BOP reliability assessments have not considered the possible contribution from common cause failures (CCF). Along with the challenges described above, the inclusion of CCFs may serve as an important improvement to current reliability assessment methods.

To help prevent accidents such as the Macondo blowout from occurring in the future, the petroleum industry must find methods of improving the reliability of complex safety critical systems such as the BOP. However, in order to evaluate the reliability of such systems, an appropriate approach which gives accurate results must be developed. This master thesis is concerned with how the reliability of a complex safety critical system such as a BOP should be assessed, in order to respond to the inadequacies in current assessment methods described above.

1.2 Objectives

The main objective of this master thesis is to propose solutions for some of the challenges related to reliability assessments of a complex safety critical system such as the BOP. More specifically, the objectives are to:

- *Give a presentation of a typical (standard) BOP system, its requirements and reliability challenges*
 - Describe and classify the main functions and the associated performance requirements of a BOP system.
 - Identify and discuss the main operating situations of a BOP in light of the ability of the BOP to stop well kicks.
 - Identify recent BOP stack configurations and describe the pros and cons of these related to a standard BOP configuration.
- *Suggest improved approaches to reliability assessments of BOP systems that can incorporate some of the above challenges*
 - Carry out and document a literature survey on how reliability analyses of BOPs have been performed in the past, including the selection of reliability measure, and discuss the limitations of these approaches.
 - Discuss the implications and causes of common cause failures (CCFs) on the execution of BOP functions.
 - Propose a new overall approach to risk and reliability assessment of a BOP system, which includes proposals for how to solve some of the identified challenges.
 - Identify related issues that need further research, and give recommendations for such research.

1.3 Limitations

The most important limitation to the scope of this master thesis is that the only ability of to provide *initial closure of the annulus and/or well by the means of the BOP system* is considered. The report does not take into account reliability challenges related to e.g. internal closure of the drill string or kick killing. As a result, some subsystems/components, e.g. choke and kill lines, are only briefly described, and excluded from the reliability analysis.

This master thesis is limited towards the reliability of subsea BOPs designed for application in deepwater exploration drilling. It does not concern shallow water BOPs, development drilling BOPs, or workover/well intervention BOPs.

Finally, it should be noted that the emphasis of the reliability analysis is placed on application of reliability engineering methodology, rather than on the detailed modeling of the BOP system.

Some simplifications regarding the composition of the system have therefore been made.

1.4 Approach

The approach to the development of this thesis report is illustrated in Figure 1.1 below. The work has mainly consisted of two three activities; acquiring through relevant literature, detailed knowledge of the BOP system so as to be able to perform a qualified reliability assessment, followed by qualitative and quantitative analysis of the system reliability using proven methods from the reliability engineering discipline.

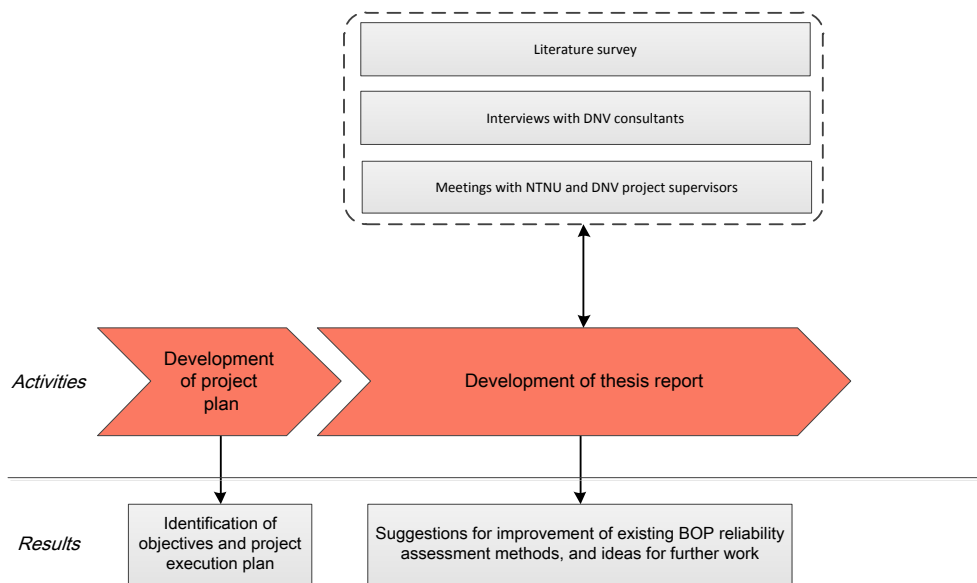


Figure 1.1: Master thesis approach (modified from Lundteigen (2009), p.21)

A preliminary study was first performed with the purpose of describing the objectives of the thesis, planning the activities which was to constitute the thesis work as well as a course schedule estimating the planned duration of each activity.

The literature survey performed in the fall of 2011 in relation to a project assignment regarding the same topic was continued, with the objective of finding information on how different operational situations and stack configurations affect the ability of the BOP to act as a safety barrier, to review some of the operational assumptions made in previous BOP reliability studies, and to gain knowledge about theoretic principles and methodology regarding modeling of common cause failures.

A thorough qualitative analysis of four common operational situations was performed, which resulted in important knowledge of how these affect the BOP system's ability to act as a safety

barrier in a well control situation. The analysis of operational situations was carried out partly with help from experts from within DNV, who provided useful input regarding both technical, operational and reliability aspects.

The results from the qualitative system analysis was then used as a basis for establishing a suggested approach to BOP reliability assessment based on fault tree and event tree models of the system.

1.5 Structure of the Report

The rest of the report is structured as follows. Chapter 2 gives a description and functional analysis of the BOP system, as well as an analysis of different operational situations the BOP is exposed to. Chapter 3 documents the literature survey, discussing previous reliability studies as well presenting the regulations and guidelines which are relevant to BOP systems. In Chapter 4, an overview of BOP failures considered in the following quantitative analysis is presented. Chapter 4 also describes the some theoretic principles regarding CCF, as well as the methodology through which CCF has been modeled in the quantitative analysis of the BOP system. In Chapter 5, an approach to quantification BOP reliability through post-processing of minimal cut sets from fault tree analysis is suggested, and the calculated results discussed. Finally, the thesis is summarized and concluded in Chapter 6, and recommendations and ideas for further research are suggested.

Chapter 2

BOP and drilling operations

2.1 BOP system description

2.1.1 Introduction

The subsea BOP system is located between the wellhead and the riser in a subsea drilling system. It is designed to assist in well control and be able to rapidly shut in the well in the event of unexpected influx of formation fluids into the wellbore. The primary function of the BOP is to act as the final safety barrier in the case that well control is lost. In addition, the BOP is used for a range of routine operational tasks, such as the testing of casing pressure and formations strength (BP, 2010). This section contains a description of a typical deepwater drilling BOP system, its components and its functions.

2.1.2 The main elements of a BOP system

The three main elements comprising a BOP system are the lower marine riser package (LMRP), the BOP stack and the control system. In the following, the main components in these subsystems are described.

The BOP system consists of ram and annular type preventers, the valves and piping that used to supply the preventers with hydraulic fluid, and the choke and kill valves and lines used to maintain pressure control in the well. All actuating devices are hydraulically operated, and are activated by human interaction from topside control panels. A typical drilling BOP system designed for deepwater application is equipped with five to six ram type preventers, and either one or two annular type preventers:

- The annular preventers are designed to seal the wellbore by closing around the drill pipe on a range of tubular dimensions when the drillstring is running through the BOP.
- Pipe rams are designed to close and seal around the drill pipe.
- Blind shear rams (BSR) are designed to close and seal the wellbore, shearing the drillstring if it is running through the BOP.
- Casing shear rams (CSR) are designed to shear the casing and drillstring without sealing the wellbore.

A typical configuration of a subsea BOP system is shown in Figure 2.1. This configuration has two shear rams, a feature which is becoming increasingly widespread in modern deepwater BOP design as an attempt to increase the redundancy in the system, and thereby the reliability. Although a number of variations to this stack configuration are used throughout the world, this is considered the most relevant type of configuration for future applications, and it is thus used as the basis for the analysis in this report. An overview of the most common BOP stack configurations and the pros and cons of these is described in Section 2.4.

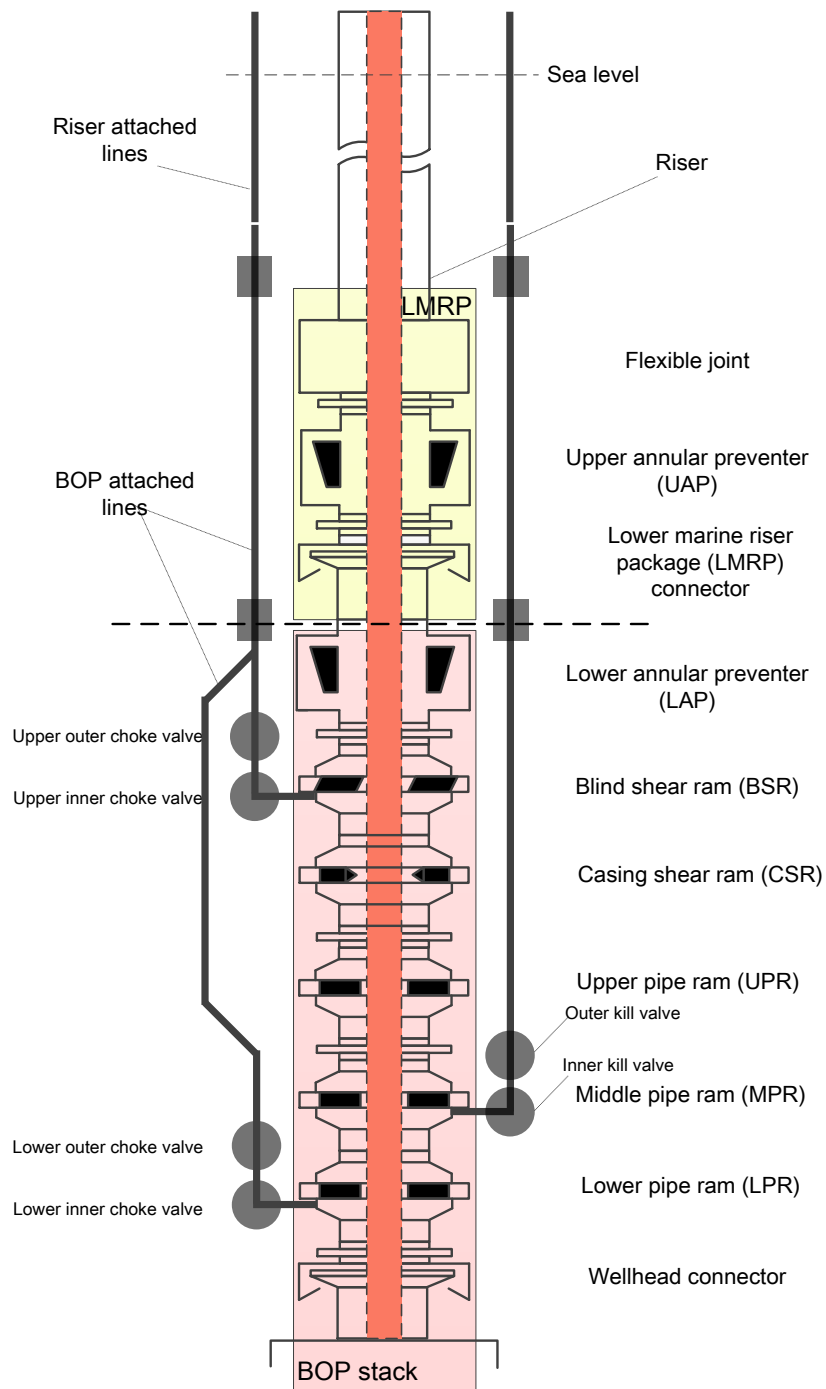


Figure 2.1: Typical configuration of a subsea drilling BOP system designed for deepwater application. Modified from OLF-070 (2004), page 85.

The lower marine riser package (LMRP)

Flexible joint

Due to lateral movements of the drilling rig during drilling, a flexible joint is installed as the uppermost component of the LMRP. The flexible joint is normally designed to compensate for up to 10 degrees angular deflection of the marine drilling riser from the vertical axis of the BOP.

Annular preventer

Annular preventers, often simply denoted *annulars*, are used to seal around drill pipe or tubular, and are located in the upper part of the BOP system, often on the LMRP. The annular preventer consists of a large internally reinforced rubber packing ring enclosed in a steel housing, which can seal around virtually any anticipated tubular diameter (Holand, 1985). An annular is normally the first preventer to be shut if a kick is detected. Annular preventers are positioned above the ram preventers, because they generally have lower working pressure ratings (5 000 psi) than those of the ram type preventers (15 000 psi) (Transocean, 2011).

Annulars are also the most frequently used function outside of well control situations, e.g. for *stripping* purposes. The concept of stripping is further detailed in Section 2.3. Failure of the annular preventer function in a well control situation will lead to a loss of both flexibility and redundancy in the BOP system.

Control pods

One electro-hydraulic subsea control pod is installed on either side of the LMRP assembly. The two control pods, often denoted the blue and yellow pods, are identical, redundant modules dedicated to providing function control and communication between the subsea LMRP and BOP stack components and the topside control system interfaces. A back-up pod named the white pod is often held on the rig.

All subsea BOP functions are activated via the two control pods. Ensuring the reliability of the control pods is therefore extremely important from a safety perspective.

LMRP connector

The LMRP connector is a hydraulic connector providing the connection between the bottom of the LMRP and the top of the BOP stack. The connector allows for the LMRP together with the rest of the marine drilling riser to be separated from the BOP stack while the well remains shut in by the BOP. This permits disconnection of the LMRP and riser for retrieval of the control pods to the surface for repair, and in the event that rig dynamic-position station keeping is lost (BP, 2010).

The BOP stack

Blind shear ram (BSR)

The blind shear ram is fitted with ram blocks that are capable of cutting through the drillpipe, and rubber sealing elements which also enables it to seal off the well after the drill pipe has been severed. The intended function of the BSR is to completely seal off the well in the event that the BOP fails to successfully mitigated the well control situation through its non-destructive functions. Activating the BSR is a last-resort option in case of emergency, since the cost impact from severing the drill pipe will be huge both in terms of equipment damage and rig downtime.

The BSR is the only ram in the BOP stack which is capable of both shearing the drill pipe *and* sealing off the well. In an escalated well control situation, failure of the BSR to deliver its intended function will likely lead to complete loss of well control, and a blowout through the wellbore annulus and/or drill pipe. Ensuring that the BSR is reliable is therefore very important from a safety perspective.

Casing shear ram (CSR)

The CSR is similar to the blind shear ram, but its design is more focused towards shearing capability. The CSR is not equipped with rubber sealing elements, but is a larger ram equipped with more powerful cutting blades than the BSR. The CSR is designed to cut through the heaviest drill pipe and casing.

In cases where the geometry or material properties of the drill pipe or casing exceeds the shearing capability of the BSR, the CSR is critical if the well control situation is allowed to escalate to a scenario where the drill pipe or casing must be sheared.

Pipe rams

A pipe ram is designed to close and seal the wellbore annulus on a specified range of tubular diameters. A few variations of pipe ram design principles exist, but the main types used are:

- *Standard (fixed) pipe rams*: Capable of sealing on a specified pipe O.D. tolerance.
- *Variable bore rams (VBR)*: A more flexible ram capable of sealing on most of the tubular dimensions which are anticipated in a typical drilling program.

This report bases its analysis on a BOP configuration with three pipe rams; two fixed pipe rams and one variable bore ram, which is considered the most common configuration for deepwater drilling BOPs at the present time. The upper and lower pipe rams are here specified as fixed rams, while the middle pipe ram is considered to be a VBR. The tubular dimensional interval around which each ram is capable of closing has implications for the BOP system's redundancy when different operational conditions are present. These implications and their effect on the reliability of the system are further detailed in Section 2.3

Wellhead connector

The wellhead connector is a hydraulically actuated connector which provides the connection between the bottom of the BOP stack and the top of the subsea wellhead housing.

Choke and kill lines and valves

The main function of the choke and kill lines and valves is to circulate out a kick or kill a well. During well control operations, the fluid under pressure in the wellbore flows out of the well through the choke line to the choke, reducing the fluid pressure to atmospheric pressure (Schlumberger). The choke and kill lines exit the subsea BOP stack and then run along the outside of the drilling riser to the surface (Schlumberger).

The valves are designed with a fail-safe "close" hydraulic operation, implying that they will close by spring action when the opening pressure on the valves is released.

The choke line usually has two outlets; between the MPR and UPR, and between the UPR and BSR. The kill line is usually connected to the BOP stack between the LPR and MPR.

Note: *This report does not concern kick killing operations, and the reliability of choke and kill lines is therefore not considered.*

BOP stack mounted accumulators

A typical BOP stack is equipped with eight accumulator bottles which are used for high-pressure closing of the BOP functions. The accumulator bottles store pressurized hydraulic fluid which is supplied from the hydraulic fluid supply lines that run from the topside hydraulic power unit (HPU), down along the riser to the subsea BOP components.

The main objective of the accumulators is to provide the BOP functions with closing force in terms of a pre-charge of hydraulic pressure, allowing them to close rapidly upon demand. The accumulators provide a significant decrease in the closing time for a BOP function (Holand, 1997). The supply system is arranged so that the accumulator bottles; both topside and stack mounted ones, are charged to the required pressure, and then automatically recharged when the stored fluid is depleted by activation of BOP functions. The accumulator bottles are common for the blue and yellow control pods, meaning that a leak in the accumulators will affect both pods. However, the hydraulic supply system is equipped with accumulator isolation valves topside, in each pod and on the BOP stack. The accumulator isolation valves can be closed and the BOP's functions operated directly from the HPU. This will however have a significant impact on the closing time for each preventer.

The BOP control system

Most of the components described above; the annular and ram type preventers, the valves and the connectors, are hydraulically actuated. The different BOP functions are governed by an electro-hydraulic control system called a multiplexed (MUX) control system, consisting of both electrical/electronic and hydraulic components. The control system components are located both topside and subsea. In this section, a detailed description of the BOP control system is presented. Figure 2.2 gives a simplified overview of the BOP control system.

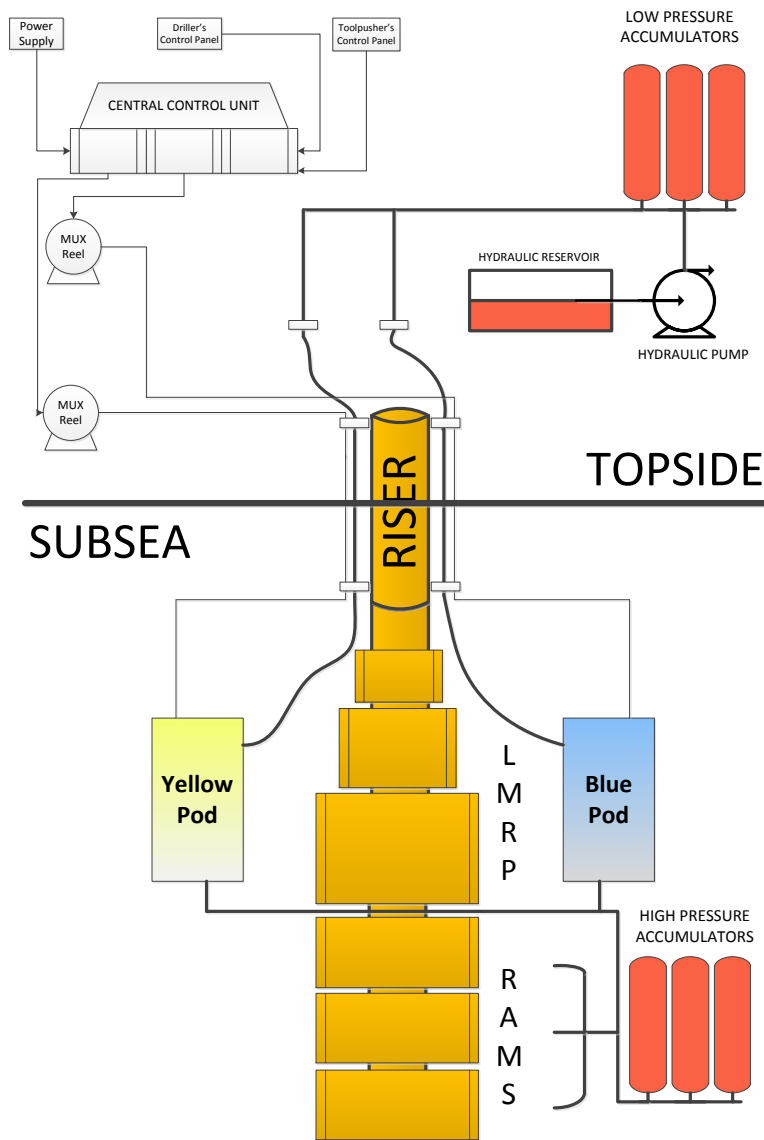


Figure 2.2: Simplified BOP control system.

Topside interface control panels

The main topside components of an MUX BOP control system are the control panels and electric/hydraulic supply utilities. Each BOP function must be activated manually by pressing push buttons on the control panels. There are normally two such control panels on a rig floor; the driller's control panel (DCP) and the toolpusher's control panel (TCP), equipped with multiple push-buttons for activation of the different BOP functions. Each of the control panels can be operated on two separate, independent control networks run by two programmable logic solvers (PLC). The control panels also display all available information regarding the condition of the BOP system, e.g. flow and pressure levels in the wellbore, accumulator pressure levels and mud volumes pumped.

Power supply

Electric power is supplied from an uninterruptable power supply unit. A central control unit (CCU) distributes the electric current to the various topside components; the control panels and the power and communications cables. Signals sent from the control panels are transmitted from the rig surface to the subsea control pods by the means of power/communications cables often called MUX cables. These cables are stored in dedicated blue and yellow control pod MUX reels on the rig floor, and run down along the riser in two sets of lines, one to each of the subsea control pods.

Hydraulic fluid supply

Figure 2.3 below shows the logic arrangement of the BOP's hydraulic fluid supply system. Hydraulic fluid is supplied from a reservoir connected to an HPU. A pod selector valve directs the fluid towards either of the two pods, depending on which is selected by the operator to be the active one. From here, the fluid is transported down along the riser via rigid and flexible conduit lines to the LMRP. The fluid is further directed through the active pod to the subsea accumulators and the preventers via hard lines.

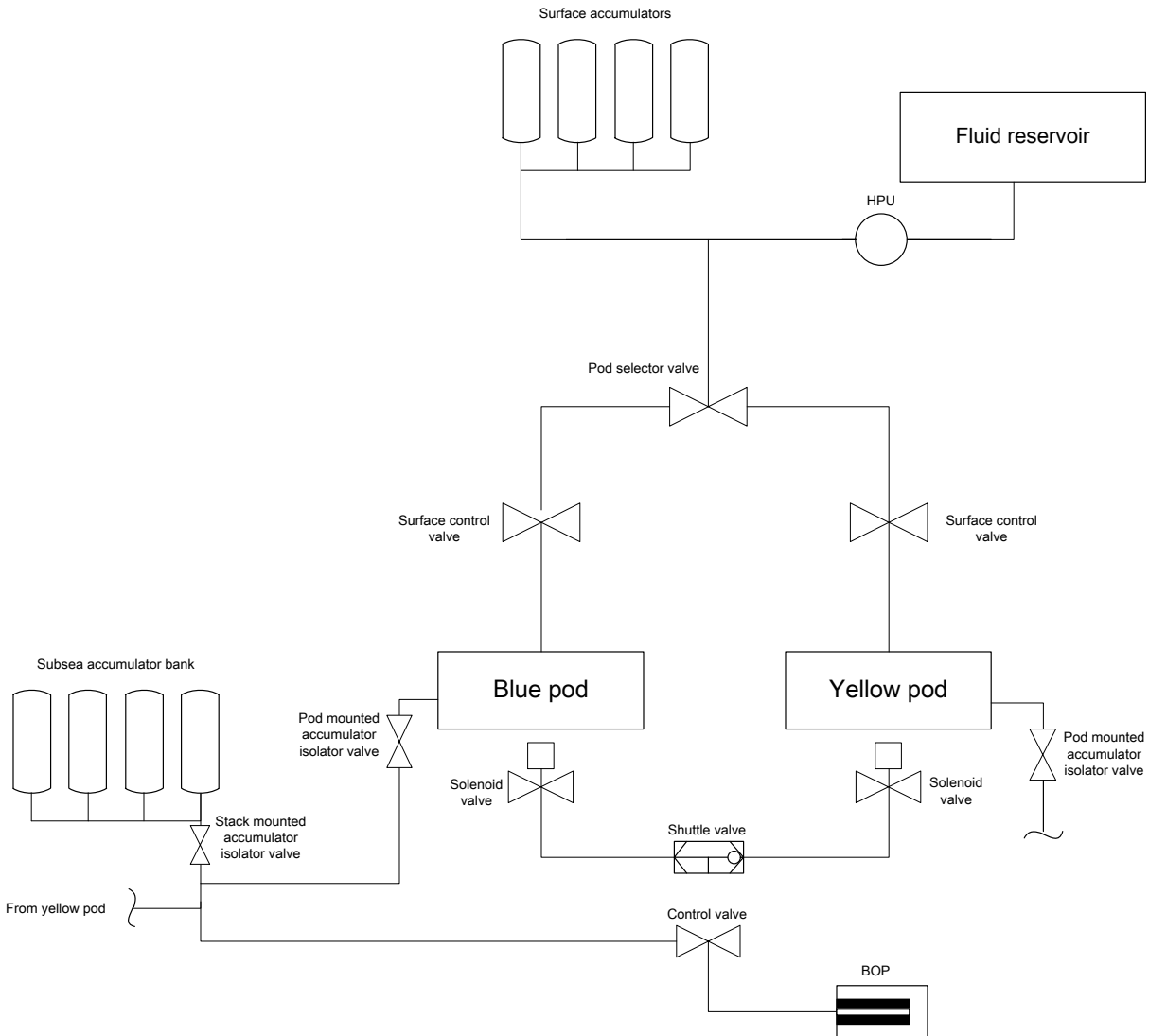


Figure 2.3: BOP control system logic arrangement.

Control pods and electronic communications

A subsea electronic module (SEM) housing is located in each control pod. The SEM housing contains two SEMs, A and B, which are identical, redundant components. The operator chooses which pod and SEM is the active one. When e.g. the blue pod - SEM A is the active component, the hydraulic fluid supply from the surface is automatically directed accordingly. The most important function of the SEM is to energize the solenoid valves dedicated to each preventer. If say, the upper annular is activated through the blue pod - SEM A, the solenoid valve in the blue pod belonging to the upper annular is energized by SEM A, opening the valve such that a pilot hydraulic signal is sent to the hydraulic control valve belonging to that function. The hydraulic control valve is thus opened and allows high pressure fluid to flow from the accumulator bottles and through the designated shuttle valve, finally closing the annular preventer. The SEM is also

the provider of the BOP status information displayed on the control panels.

2.2 Functional analysis of the BOP system

2.2.1 Introduction

Having described the relevant systems, subsystems and components of the BOP system and how these are connected, the focus is now directed towards BOP functions; their properties, their performance requirements and reliability challenges related to them. First, a short description of well barriers and how the BOP should be viewed as a barrier in light of the terminology in D-010 (2004) is given.

2.2.2 The BOP as a well barrier

The NORSOK standard (D-010, 2004) specifies requirements and guidelines pertaining to well integrity during drilling activities and operations. (D-010, 2004) states the requirement for the number of well barriers present during well activities in the Norwegian Sector of the North Sea (NSNS):

"There shall be two well barriers available during all well activities and operations (...), where a pressure differential exists that may cause uncontrolled outflow from the borehole/well to the external environment."

A typical exploration program obviously falls under this requirement. Hence there must always be at least two well barriers present during drilling operations, a *primary* and a *secondary* well barrier. The hydrostatic pressure exerted by the fluid column of drilling mud is defined in D-010 (2004) as the primary well barrier. The BOP system thus constitutes one of the secondary well barriers. Other secondary well barriers include the casing, casing cement and the wellhead (D-010, 2004).

According to Sklet (2006), an *active* barrier is *"a barrier that is dependent on the actions of an operator, a control system, and/or some energy sources to perform its function."* With the exclusion of some support functions such as the pressure and flow level measurement, the BOP performs most all of its function upon demand from an operator through electronic and hydraulic energy sources governed by a control system. Hence, the BOP system should be viewed as an *active* well barrier.

2.2.3 Essential BOP functions

The most essential functions of a BOP system are the prevention of blowouts and the prevention of well leaks, i.e. the ability to shut in or *isolate* the well. In the following, the function *Isolate well* will be defined as the a *safety instrumented function* (SIF) performed by the BOP system. The concept of safety instrumented functions is further detailed in Chapter 5. The BOP is designed to be able to fulfill the SIF in a variety of ways, depending on the nature of the process demand and on operational conditions present when the process demand takes place.

OLF-070 (2004) specifies three essential functions in terms of the BOP's ability to act as a safety barrier. Together, these three sub-functions must fulfill the requirements for the BOP as a well barrier. The three essential BOP functions are listed below, and illustrated in Figure 2.4.

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

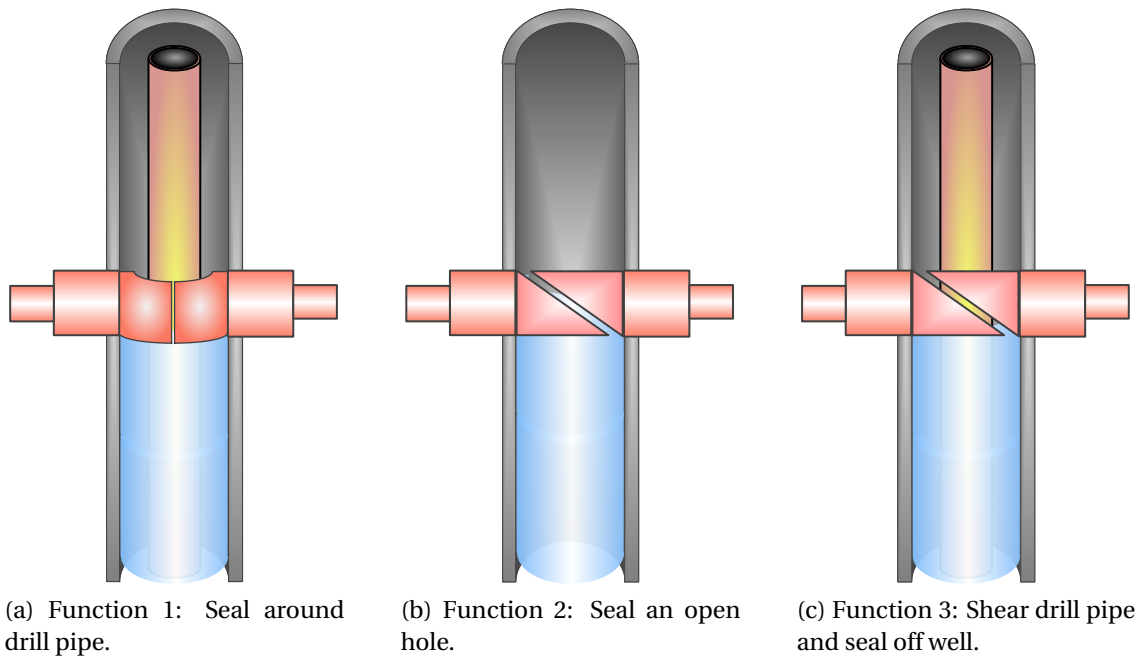


Figure 2.4: BOP essential functions, as specified in OLF-070 (2004).

Function 1 is the most frequently used function. In the event of a well kick, the most common initial response of the operator on the rig floor is to close the annular preventer and/or one of the pipe rams, thus sealing the wellbore annulus around the drill pipe.

Function 2 involves closing the blind shear ram on an open hole, sealing off the well. As implied, *Function 2* will only be relevant in a scenario where the drill pipe is not running through the BOP.

Note: *It is claimed by manufacturers that the annular preventers can be used to seal on an open hole. However, according to Holand (1997) this is rarely done and no reliability data exist for such application of annular preventers. Closing the annular preventer on an open hole is therefore not considered as a valid means of sealing the well when the drill pipe is not running through the BOP, and thus the effect of this operation is not included in the further analysis.*

Function 3 is intended as the "last line of defense" in a scenario where control of the well is lost. The operator will be very reluctant to resort to this function, because of the huge cost impact of shearing the drill pipe. *Function 3* can only be fulfilled by closing one or more of the shear rams. The blind shear ram will shear the drill pipe and seal off the well. In deepwater drilling however, the contribution to wellbore pressure from the hydrostatic pressure exerted by the mud column is significant and has large implications on the BOP's ability to seal. The CSR is therefore often closed previous to the BSR in a demand situation to decrease the pressure against which the BSR must close. Shearing ram sealing capability is further discussed in Section 2.3.

Note: *In a well control situation, the hydrocarbons may travel up the wellbore annulus or up through the drill pipe. Preventing hydrocarbons from reaching the surface may therefore also involve closing the drill pipe internally by the means of what is called the "internal BOP" (IBOP), or stabbing/kelly valve. This report only concerns the closing of the annular and ram preventers in response to a kick, and does not consider internal closing of the drill pipe.*

2.2.4 BOP functional block diagram

The structural and functional interrelationships in the BOP system can be illustrated by a *functional block diagram* (Rausand and Hoyland, 2004). A functional block diagram of the BOP system is shown in Figure 2.5 below.

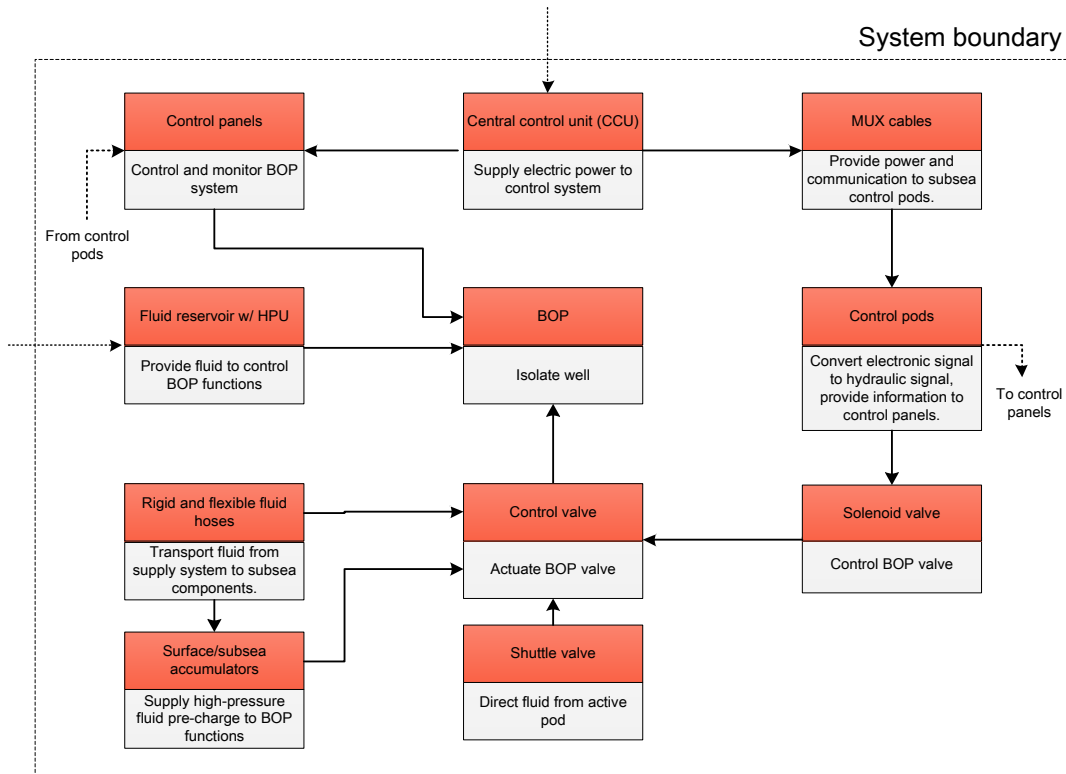


Figure 2.5: Functional block diagram of the BOP system.

The functional block diagram gives a clear view of the functions in the the system, and how these must interface in order to achieve the overall function *Isolate well*, by closing one or more of the preventers (i.e. performing one or more of the Functions 1, 2 or 3 defined above). Each functional block represents function in the system, with inherent sub-functions. In order to be able to identify all potential failures, one should have an unambiguous understanding of the various functions of each functional block, and the performance criteria related to each of these functions (Rausand and Hoyland, 2004). A *functional requirement* is a specification of the performance criteria related to a function (Rausand and Hoyland, 2004). As an example, the function *Provide fluid to control BOP functions* may be translated to a functional requirement for the HPU to supply fluid with output pressure 1500 psi.

2.2.5 Classification of BOP functions

The BOP system is a complex system with a high number of required functions. However, in terms of safety criticality for the purpose of reliability performance analysis, not all functions will have the same importance and relevance to the analysis. A useful activity may therefore be to classify the functions according to their role in the system. Rausand and Hoyland (2004)

suggest the following method for classifying the functions in a system:

1. 1. *Essential functions*: The functions required to fulfill the intended purpose of the functional block. In the functional block diagram in Figure 2.3, the essential BOP functions are the descriptions on each functional block, e.g. one essential function is the ability of the CCU to *Supply electric power to control system*.
2. 2. *Auxiliary functions*: The functions required to support the essential functions. An auxiliary function may be less obvious and more difficult to identify, but can be equally important as the essential function it supports. An auxiliary function of the CCU power supply functional block in Figure 2.3 is to *Transform current*, such that the CCU supplies the control system with the correct voltage.
3. 3. *Protective functions*: The functions intended to protect people, equipment and the environment. An example of a protective function in the BOP system is overpressured cabinets housing the PLCs in order to ensure that these critical components are isolated in the event of a gas leak.
4. 4. *Information functions*: The functions dedicated to providing information about the system. Typical information functions include condition monitoring, pressure and flow meters, alarms, and so forth. The BOP control system function has a number of inherent information functions which are used to monitor its condition. One example an information function in the BOP system is pressure gauges reporting the pressure levels in the subsea accumulator bottles.

Table 2.1 is a description of the overall BOP function *Isolate well*, its sub-functions with related functional requirements, as well as a classification of each sub-function according to the method presented above.

BOP - "Isolate well"			
Sub-functions	Sub-sub-functions	Functional requirements	Class
Seal around drill pipe	Close annular	Annular must be able to seal around any anticipated tubular dimension in the wellbore within wellbore pressures up to 5 000 psi.	Essential
	Close fixed pipe ram	Fixed pipe ram must be able to seal around drill pipe with 5" drill pipe within wellbore pressures up to 15 000 psi.	
	Close variable bore ram	Variable bore ram must be able to seal around tubular dimensions ranging from 3.5"-6 7/8" O.D within wellbore pressures up to 15 000 psi.	
Seal an open hole	Close blind shear ram	BSR must close and seal off well within wellbore pressures up to 18 000 psi.	Essential
Shear drill pipe and seal off well	Close blind shear ram	BSR must be able to shear drill pipe or tubular on wellbore pressures up to 18 000 psi. BSR must seal off well against wellbore pressures up to 18 000 psi.	Essential
	Close casing shear ram	CSR must be able to shear the heaviest drill pipe and casing against wellbore pressures up to 18 000 psi.	

Table 2.1: Inherent sub-functions and their functional requirements and classification for the overall primary BOP system function *Isolate well*.

As indicated in Table 2.1 above, the function *Isolate well* can be accomplished by three sub-functions. One sub-function, e.g. *Seal around drill pipe* can be accomplished by three sub-sub-functions, which each involve closing a preventer around whatever drill pipe or tubular is running through the BOP, e.g. *Close annular*. These are the essential sub-sub-functions of each sub-function, and may be further broken down in terms of the auxiliary, information and interface functions contributing to their fulfillment. Development of similar functional overviews for each function may serve as a useful tool for familiarizing the system before attempting to assess its reliability.

2.3 BOP operational situations

2.3.1 Introduction

During the course of an exploration drilling program, the BOP will be exposed to different operational situations, and the conditions under which it operates are far from constant. These conditions have a significant effect the BOP's ability to perform the functions described in the previous sections.

Drilling an exploration well is a stepwise procedure during which the BOP will spend most of the time on the wellhead, but it can also be located on the rig, be traveling down the wellbore

(*tripping in*), or be traveling up the wellbore (*tripping out*). The O.D. of the drill pipe or tubular which is running through the BOP when it is on the wellhead will also vary, depending on what operation is carried out or which stage the drilling program has reached. Furthermore, the pressure inside the wellbore will not be constant. The ability of the BOP to act as a safety barrier depends on all of these variables, and the conditions that apply to each situation will have consequences for the reliability. The implications from exposure to different operational situations should therefore be treated carefully in a BOP reliability assessment.

2.3.2 Analysis of four main operational situations

The objective of this section is to analyse the effect on BOP reliability from the four most important operational situations encountered by a subsea drilling BOP during the course of a typical deepwater exploration drilling program. These four cases are listed below, and followed by a discussion of their effect on BOP ability to seal the well in the event of a kick by performing one of the three OLF-070 (2004) essential functions presented in Section 2.2.3.

- **Case A: Base case.** Both annulars and all of the pipe rams can seal around drill pipe or tubular, the CSR can shear the pipe or tubular and the BSR can shear the drill pipe and seal the off the well.
- **Case B: Large/small drill pipe or tubular O.D.** Only the annular preventers and the VBR can seal around the drill pipe, due to the O.D. of the pipe or tubular running through the BOP. The BSR and CSR are still considered to have the same shearing and sealing capabilities.
- **Case C: High wellbore pressure.** Only the UPR, MPR and LPR can seal around the drill pipe or tubular. The annular preventers cannot be operated because the wellbore pressure exceeds the their pressure rating. The CSR can shear the drill pipe, and the BSR can subsequently seal off the well against the open hole pressure.
- **Case D: Open wellbore.** The drill pipe is not running through the BOP. All annular BOP sealing functions are unavailable. Only the BSR can be used to seal off the well.

Figure 2.6 illustrates how the each of the above cases A, B, C and D will affect the system redundancy of the BOP.

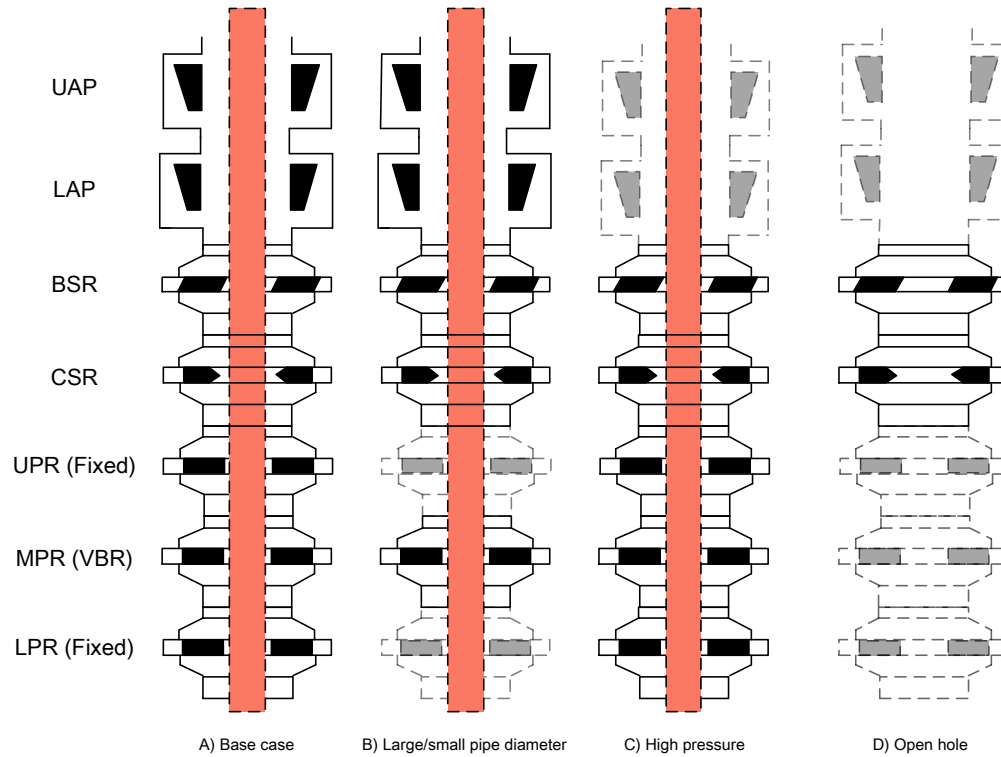


Figure 2.6: The four most common operational situations encountered by the BOP during a typical deepwater exploration drilling program.

Case A: Base Case

Case A represents the largest proportion of a typical drilling program. In the study performed by Holand, a total of 48 kicks were recorded, where 85.4 percent of these occurred in a situation where Case A applied (Holand and Skalle, 2001). Case A is therefore considered the *base case*. In this situation, both annulars and all of the ram preventers can be operated.

When the drill pipe is running through the BOP, successfully closing in a kick will require the BOP to either seal around the pipe or seal off the well entirely. The preferred operation is obviously to seal around the drill pipe as opposed to sealing off the well entirely, since the latter implies shearing the drill string and thereby incurring huge downtime and material costs and possibly losing the well completely. Consequently, the operator will first attempt to execute *Function 1*, by choosing to close one of the annular preventers.

Annular vs. pipe ram stripping capabilities

Closing the annular, as opposed to a pipe ram, is the more desirable choice in a well control situation primarily because of its *stripping* capabilities. Stripping refers to the act of lowering drill pipe into the wellbore when the BOP is closed and pressure is contained in the well (Schlum-

berger). The purpose of stripping is to lower the drill pipe to the bottom of the wellbore, as kick killing operations should always be conducted with the drill pipe fully lowered (Schlumberger).

When the annular is closed, the drill pipe can be carefully stripped through the preventer. The elastomeric sealing element can be expanded by the force exerted from the drill pipe, allowing even tool joints to pass through the preventer.

When a pipe ram is closed, the drill pipe stripping capability is much more limited because the tool joints between each length of pipe cannot pass through the ram. In order to strip the drill pipe with a pipe ram closed, another ram or annular must be closed, the pipe ram opened, the pipe stripped until the tool joint surpasses the ram in question, and the ram closed again. This procedure, called *ram-to-ram* or *ram-to-annular* stripping, must then be repeated whenever a tool joint must pass by a closed pipe ram (Schlumberger).

If the annular successfully seals, the operator will normally opt to also close one of the pipe rams, before commencing mud circulation. The purpose of closing the pipe ram is to relieve the pressure on the elastomeric sealing element of the annular preventer. Since the pipe rams are normally rated for higher working pressures, they are better suited for containing a kick over a longer time period.

If both annulars fail to close, the most natural course of action is to close one of the pipe rams. In the base case, it is principally arbitrary which of the pipe rams is closed in terms of sealing capability. The most common practice is to close the lowermost ram first, keeping the hydrocarbon influx as far as possible from the rig.

It should be noted that the type of pipe rams fitted on the stack has implications for the hang-off capabilities of the BOP, both during normal operation and in a well control situation. VBRs have much more limited hang-off capability compared to traditional, fixed pipe rams. In a well situation where the decision is made to activate the BSR, the option to hang-off the drill string on one of the pipe rams is important due to possible compressive loads in the drill string. If the drill string is carrying substantial compressive loads, the probability that the BSR can seal the well is reduced, because the shearing force required to cut through the pipe is substantially higher than during test conditions. The issue of drill string compression and its effect on BSR shearing/sealing capability is not evaluated in this report, but is further commented on in (Committee for Analysis of Causes of the Deepwater Horizon Explosion Fire and Oil Spill to Identify Measures to Prevent Similar Accidents to the Future, 2011).

A simplified reliability block diagram (RBD) illustrating the base case system redundancy is shown in Figure 2.7 below. If the BOP does fail to seal around the pipe by the means of the functions shown in Figure 2.7a, the operator has the option to activate *Function 3*, i.e. shear the

drill pipe and seal off the well. A failure of the BOP to perform this function is dependent on the shearing and sealing capability of the BSR but often also the shearing capability of the CSR. If the pressure the shear rams must close is very high, the operator may opt to use both shear rams. After shearing the pipe with the CSR, the remaining section of drill pipe still in the BOP can then be hoisted to a level above the BSR, allowing the BSR to close and seal against the mud without having to shear the drill pipe. The two alternative shearing approaches are illustrated in Figure 2.7b below. The combined use of the two shearing rams in high pressure situations is further discussed in relation to Case C below.

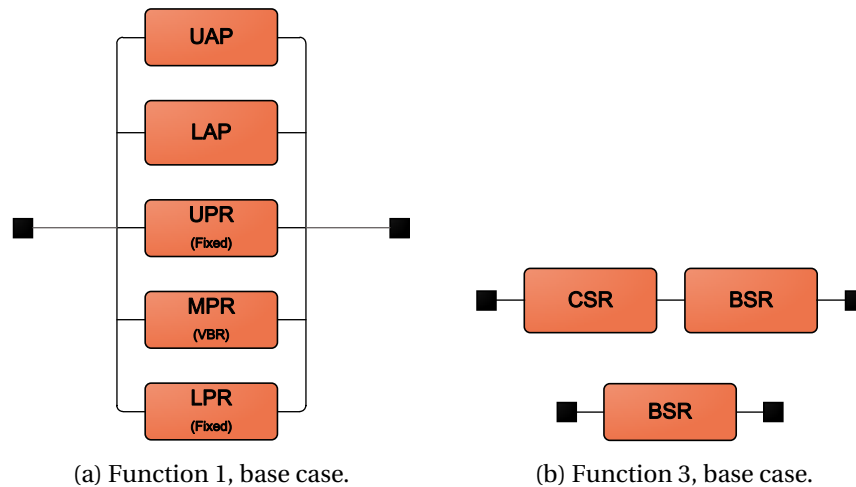


Figure 2.7: RBDs illustrating available BOP functions in the base case.

Case B: Large/small pipe diameter

At various stages of a drilling program, the drill pipe or tubular running through the BOP has properties that limit the ability of the the ram preventers to seal around it. Most commonly this involves a drill pipe or tubular with an O.D. outside the range around which the fixed pipe rams (here UPR and LPR) can close, leaving the VBR the only available pipe ram. Large or small drill pipe diameter will therefore have implications for BOP redundancy which are important to consider from a reliability perspective.

Tool joint spacing

In other cases it may be that the geometric or material properties of the drill pipe or tubular are of such character that the pipe rams and/or shear rams cannot be operated as intended. A common example of this is that a drill pipe tool joint is improperly spaced in the wellbore annulus, meaning the presence of a tool joint in the drill pipe at the depth where the desired ram is to be closed, as illustrated in Figure 2.8 below. In Figure 2.8a, the tool joints are properly spaced outside of the ram closing area. Improper spacing of tool joints is particularly critical if

a tool joint is obstructing the closing of the shearing rams, as none of these rams are designed to cut through tool joints. Incorrect spacing will also affect the closing of a fixed pipe ram (here UPR and LPR), because the O.D. of the tool joint is outside the closing range of the rams.

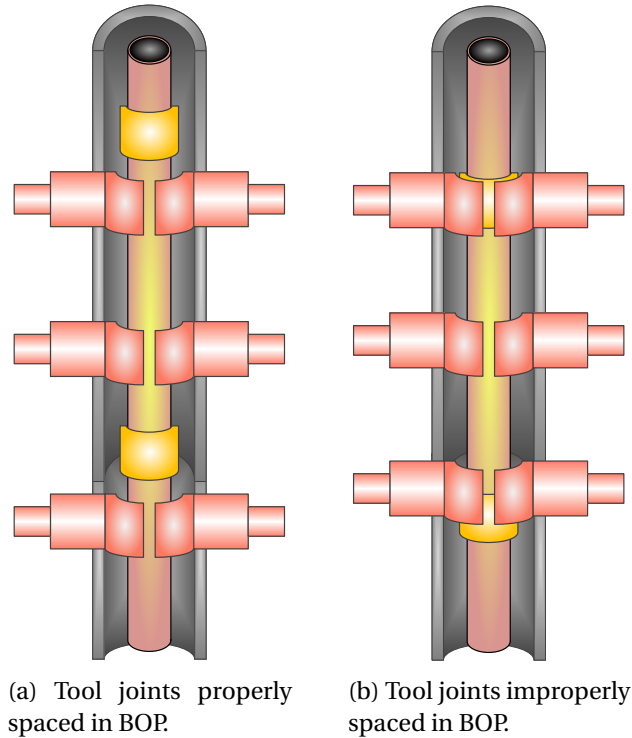


Figure 2.8: Spacing of tool joints through wellbore annulus.

For the shear rams, the increased or decreased drill pipe or tubular O.D. has no direct implication on shearing/sealing capability. However, as described above, incorrectly spaced tool joints can cause complete failure of a shearing ram. According to West Engineering Services (2004), attempting to shear at a tool joint will most likely result in an unsuccessful shear and damage or destroy shear blades. West Engineering Services (2004) further states that the development in the industry is towards longer tool joint, implying that the proportion of the drill pipe that can be cut by the shear rams decreases.

The standard length of a drill pipe joint is 9.65 meters (American Petroleum Institute, 2012), while total tool joint lengths (pin and box) range from 15 - 18 1/2 in, or 381 - 470 mm (American Petroleum Institute, 2012). The average length of a tool joint per drill pipe joint is then 0.425 m, meaning that the proportion of a drill pipe constituted by tool joints which cannot be sheared, is approximately equal to 4.2 percent ($0.425 \text{ m} / (9.65 \text{ m} + 0.425 \text{ m})$).

An important task for the driller is to always be aware of where in the BOP annulus the tool joints are located, i.e. ensure proper spacing. However, the methods applied for calculating

the location of tool joints is based on the assumption that the riser is true from the surface to the BOP. As water depths increase, this assumption becomes increasingly inaccurate due to the deformations in the riser caused by the shear environmental forces it is exposed to (buoyancy, elongation and so forth). Hence, the ability of the driller to accurately estimate the location of tool joints in the BOP becomes limited. The effect on the BOP's ability to perform *Function 3* from improper tool joint spacing is therefore an issue of great concern in terms of reliability. A very conservative assumption would be to say that the location of tool joints is close to arbitrary, which would further imply that the probability of attempting to shear a tool joint is equal to the proportion of the drill pipe constituted by tool joints, i.e. approximately 4.2 percent. A shear ram failure rate of such magnitude would be unacceptable according to OLF-070 (2004).

A simplified block diagram with available ram and annular BOPs in Case B is shown in Figure 2.9 below. For *Function 1*, the redundancy is reduced from being a 1oo5 to a 1oo3 voted system. The function of the shearing rams remains principally unchanged in comparison to the base case in terms of redundancy.

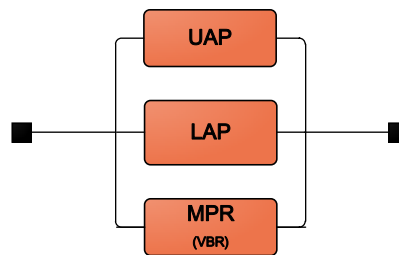


Figure 2.9: RBD of available BOP functions in Case B.

Case C: High pressure

Case C is the situation where the pressure in the wellbore is particularly high. This may be due to a well kick or simply due to the hydrostatic pressure exerted by the mud column because of the water depth. If this is the case, some of the preventers installed on the stack may be outside of their designed maximum working pressure. Annular preventers are normally rated to around 5 000 psi working pressure, which is significantly lower than the ram preventers, which are generally rated around 15 000 psi. The annulars will therefore not be able to close against the wellbore pressure in a high pressure situation. Thus only the pipe rams and the shearing rams are available in a well control situation.

For the high pressure case, it is assumed that the pressure is above the maximum pressure against which the BSR can shear and seal and/or the pressure is high in addition to the drill pipe or casing running through the BOP being of a heavy type. Based on this assumption, follows that *Function 3* can only be delivered by the BOP through the combined use of the two

shear rams. The system is then dependent on both shear rams closing in order for the well to be sealed off, and the redundancy is therefore lost for *Function 3*, as well as for *Function 1*. Figure 2.10 shows an RBD illustrating the implications on redundancy from the characteristics of Case C.

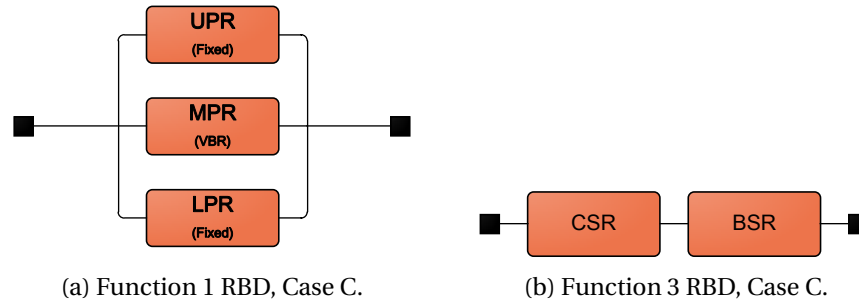


Figure 2.10: RBDs illustrating available BOP functions in the high pressure case.

Case D: Open wellbore

In *Case D* the drillstring is not running through the BOP, and the wellbore is "open". This means that the annular and ram available BOP function. Consequently, the BOP system is much more vulnerable towards well kicks in the open hole situation. Closing the BSR is principally the only available method of sealing the wellbore. In Holand and Skalle (2001), the open hole situation was present in 4.2 percent of the cases where a kick was recorded.

2.4 Recent BOP stack configurations

2.4.1 Introduction

This report is based on a typical BOP stack configuration used for deepwater drilling, equipped with two annular preventers, two fixed pipe rams and one VBR, a BSR and a CSR. All BOP stacks are principally similar, but small variations in the configuration of annular and ram BOPs on the stack can have quite large effects on the system's ability to act as a safety barrier in different well control situations. This section presents the most common variations to the "standard" deepwater BOP system, as well as some comments regarding the effect of these variations on the system reliability.

2.4.2 Stack configurations

Table 2.2 below shows three types of BOP stack configurations which are frequently used in drilling operations throughout the world. These have been denoted the "traditional", "modern", and "DWH" configurations. The "modern" configuration is the configuration considered as standard configuration in this report.

BOP Stack Configuration	Annular Preventer	Pipe Rams			Blind Shear Ram	Casing Shear Ram
		Fixed	VBR	Test		
<i>Classic</i>	2	3	-	-	1	-
<i>Modern</i>	2	1	2	-	1	1
<i>DWH</i>	2	-	2	1	1	1

Table 2.2: Three common BOP stack configurations.

The "traditional" BOP stack

The "traditional" BOP stack configuration differs from the standard configurations in two main aspects:

1. All three pipe rams are standard, fixed pipe rams
2. The stack is not equipped with a CSR

These two main configuration differences each have one important implication on the BOPs ability to act as a safety barrier. The consequence of having only fixed pipe rams is that the pipe rams may be incapable of sealing around certain tubulars running through the BOP, which reduces the system redundancy in some operational situations. The exclusion of the CSR sets limitation for the shearing ability of the BOP system. CSRs typically have better shearing capability than blind shear rams, as they are designed to shear the heaviest drill pipe and casing. The likelihood of achieving a successful shear in the most demanding well control situations is therefore higher if the stack is equipped with a CSR. The traditional BOP stack is still in use in many offshore locations throughout the world, but the industry is generally moving towards increased focus on redundant shearing capability.

Deepwater Horizon stack configuration

The Deepwater Horizon (DWH) BOP stack was installed on the wellhead of the BP licensed Macondo well while it was being drilled by Transocean's DWH drilling rig at the time of the catastrophic blowout in April 2010. The stack configuration very similar to the "modern" configuration, except for the three pipe rams. The DWH BOP pipe rams differ from the "modern" configuration in two important aspects:

1. All three pipe rams were VBRs.
2. The lowermost variable bore ram was converted to what is called a *test ram*.

The strength of this configuration is that the inclusion of three VBRs provided the DWH BOP with great flexibility and redundancy for sealing around tubular diameters. The DWH BOP VBRs were able to seal around all of the most commonly anticipated drill pipe or tubular O.Ds.

The two main weaknesses of the DWH configuration from a safety perspective is the conversion of the lower VBR into a test ram and the limited hang-off capability of the VBRs compared to fixed pipe rams.

A test ram is a pipe ram whose sealing ability has been inverted to seal against pressure from above. Test rams reduce the time required to prepare for BOP pressure testing and also reduces the time required to resume operation after the test is complete. A test ram is however no longer capable of sealing against wellbore pressure from below, hence the system "loses" one of its redundant annular sealing functions.

Chapter 3

Literature survey

3.1 Literature on BOP reliability

3.1.1 Introduction

The main objective of this master thesis is to point towards some improvements in the methods used for reliability assessment of BOP systems. For this purpose, it is necessary to conduct an investigation into previous BOP reliability studies, in order to identify possible weaknesses in the approaches used to analyse the reliability.

3.1.2 Previous BOP reliability studies

The most important and widely recognised literary sources of information on previous BOP reliability studies available to the author of this report has been the technical reports written mainly by Per Holand on behalf of SINTEF Safety and Reliability. These reports are part of an effort from SINTEF which spanned more than two decades, during which the organisation was collecting and analysing information on BOP reliability, from 1981 to 1999. Per Holand's most recent, most relevant BOP reliability study, Phase II DW, was carried out during the years from 1997 to 1998 (Holand, 1999).

The Phase II DW study was based on experienced failure data recorded in daily drilling reports from 83 wells drilled in depths ranging from 400 to 2000 meters in the US GoM OCS (Holand, 1999). These wells were drilled with 26 different rigs during 1997 and 1998. The results from the analysis of the data has been presented as a technical report; *Reliability of Subsea BOP Systems*

for Deepwater Application, Phase II DW. The report presents detailed failure statistics for BOP components, and evaluates these from both downtime and safety perspectives.

In 2001, the 1999 report was supplemented by an additional report, *Deepwater Kicks and BOP Performance*, from a follow-up study focusing on kicks and associated BOP problems and safety availability aspects (Holand and Skalle, 2001). The study applies detailed kick statistics collected from the same wells as the 1999 report to discuss parameters affecting kick occurrence and kick killing operation, and investigates occurrences of BOP failures resulting from wear and tear due to kick killing operations. Furthermore, the BOP as a safety barrier is analysed on the basis of kick experience and BOP configuration, and an alternative configuration and test practice that will improve BOP safety availability and reduce downtime is proposed.

3.1.3 Operational assumptions

In both Holand (1999) and Holand and Skalle (2001), fault tree analysis (FTA) has been used to estimate the probability of a blowout. To achieve these estimates, the author has made a number of operational assumptions regarding the BOP system, such as BOP stack design, test intervals, failure observation and so forth. In order to be able to identify possible weaknesses in Holand's approach to quantification of BOP reliability, each of these assumptions should be carefully treated. Below, the operational assumptions stated in Holand (1999) and Holand and Skalle (2001), are evaluated.

BOP stack design

The FTAs in (Holand and Skalle, 2001) and (Holand, 1999) is based on the following BOP stack configuration:

- Two annular preventers
- One blind shear ram
- Three pipe rams

Note: *Although it is not specified explicitly, it is assumed that the BOP stack presented by Holand and Skalle (2001) is equipped with two fixed pipe rams with different ram block diameters (UPR and LPR) and one VBR (MPR).*

The BOP is assumed to be equipped with a main control system only, i.e. the analysis does not include an acoustic backup system that can operate the blind shear ram, middle pipe ram

and lower pipe ram (Holand and Skalle, 2001). Furthermore, the fault tree is based on a pilot hydraulic control system from the early 1980s.

The main difference in the BOP configuration on which Holand bases the FTA versus the BOP system considered here is the control system principle. The introduction of the MUX control system has a range of implications for the reliability of the system. Most importantly, it fundamentally changes the way a demand from the operator is transformed into the actuation of a preventer. It also relieves the system of a number of hydraulic components, and replaces these with electronic ones.

A typical BOP stack used at the time when the data for Holand's studies were collected was not equipped with a CSR. The inclusion of the CSR is important, as it significantly increases the shearing capacity of the BOP. A CSR is designed to shear the heaviest drill pipe and casing, whereas the shearing capacity of a traditional BSR is limited to less heavy drill pipe types. The CSR provides the BOP with an increased level of redundancy in an escalated well control situation where attempt must be made to cut the drill pipe and seal off the well.

Tubulars running through the BOP when a demand occurs

In Holand (1999), the author assumes six different operational situations where the BOP must act as a safety barrier in the event of a kick, which have similar characteristics as the four main operational situations described in Section 2.3:

1. All preventers available.
2. LPR not available due to drill pipe diameter
3. Only the LPR and UPR available. Annulars cannot be used due to wellbore pressure, MPR and BSR unavailable due to drill pipe diameter.
4. Only MPR available. Wellbore pressure exceeds annular rating, LPR and UPR and BSR unavailable due to drill pipe diameter/material properties.
5. Only the annulars can seal around the casing in the hole (no rams available).
6. One pod is pulled for repair, all preventers available.

There are some confusing contradictions in the specification of these six situations. First, in 2., the LPR is considered unavailable because *"the ram blocks have different diameter from the pipe in the hole"* (Holand, 1999), i.e. the LPR is either larger or smaller than both the UPR and the MPR. Next, in 3., the MPR is unavailable *"due to large pipe diameter"* (Holand, 1999), whereas the UPR and LPR can still be used. This dictates that the MPR ram block diameter must be

smaller than those of the two other pipe rams. However, in 4., only the MPR can be used "*due to large pipe diameter*" (Holand, 1999), i.e. the MPR ram blocks must be larger than those of the UPR and LPR, which is contradictory to 3. Whether these inaccuracies have implications for the results from Holand's calculations is not known.

Situations such as 5., where only the annulars can seal around casing in the hole, and 6., where one pod is located topside, are not considered in this report.

Failure input data

The failure data collected during both the Phase I DW and Phase II DW studies are used as input data for the fault tree analysis in (Holand, 1999) and (Holand and Skalle, 2001). The data input is specifically the failure frequencies determined for failures that occurred in the "safety critical period" of the two studies, meaning that the failures were observed when the BOP was on the wellhead. Hence, failures that have occurred during the time when the BOP was either on the rig, being run, or undergoing the installation test have been disregarded. This is a sound approach which appropriately reflects the criticality of on-wellhead failures.

The failure frequencies used as input in Holand (1997) are an important source of data input to the quantitative analysis performed in this report. An overview of failure data used in this report can be found in Appendix B.2.

BOP testing and implications of testing on reliability

To verify that the BOP is maintained as a safety barrier, regular proof tests of its functions and its ability to withstand pressure are performed. The purpose of proof testing a safety critical system such as the BOP is to detect failures which are only revealed by a process demand, and repair them before they are allowed affect the system's ability to act as a safety barrier when a process demand occurs. It is important to emphasise that only failures considered in the analysis here are those which (Rausand and Hoyland, 2004):

1. *Have the potential to prevent activation of an essential BOP function on demand.*
2. *Are revealed only by proof testing of the BOP system.*

Such failures can be classified as *dangerous undetected (DU) failures*, according to (IEC 61508, 2010). DU failures are often also called *hidden* or *dormant* failures.

Testing of BOPs consists of two main types of tests; functional tests and pressure tests. An important difference between these tests is that a pressure test involves testing of both the function

and the ability to close in a well pressure, while a function test only checks the ability of the BOP to carry out the function, and not the ability to close in a well kick.

Functional testing

Functional tests are carried out with regular intervals, and involves testing the BOPs ability to carry out the function, e.g. closing an annular preventer. Function tests include the checking of (Holand, 1986):

- closure time of preventers and remotely controlled valves
- accumulator recharging times
- volumes pumped

Pressure testing

Pressure tests are performed in order to ensure that the BOP components have the sealing effect required for closing in a well kick. Pressure tests will often reveal failures in components and hydraulic lines, such as leakages. Pressure tests also include the checking of closure times, recharging times and pumped volumes as listed above.

Calculation of BOP unavailability and test frequencies

Generally, it can be assumed that the higher the test frequency, the higher the BOP availability (Holand, 1999). If the objective was to minimize the probability of failures without any regards to downtime, the theoretically optimal solution would be to minimize the test interval. From the operational perspective however, the purpose of proof testing the BOP is rather to maintain a certain safety level while attempting to optimize the test intervals and procedures with respect to total test time consumption, i.e. rig downtime caused by testing. In the following, some important assumptions regarding BOP testing made in Holand (1999) and Holand and Skalle (2001) will be evaluated.

The mean fractional deadtime (MFDT) of a component is the mean proportion of time the component is in a failed state, i.e. unavailable (Holand, 1991). The probability of failure on demand (PFD) is then equal to the MFDT. Considering a component with a failure rate λ which is tested at intervals τ , the equation for the MFDT, or probability of failure on demand (PFD), is:

$$PFD = MFDT = \frac{\lambda\tau}{2} \quad (3.1)$$

for $\lambda\tau \ll 1$.

In the Holand (1999) and Holand and Skalle (2001), the following assumptions have been made in order to be able to calculate the PFD of components (Holand, 1999):

1. *Tests are perfect; all inherent failures are detected by each test.*

This assumption is not conservative. As mentioned above, the shear rams cannot be fully function tested when the BOP is installed on the wellhead without shearing the drill pipe. For this reason, tests of the shearing function are generally only performed during factory acceptance tests and during re-certifications. Otherwise shear ram test are limited to a test of the closing and sealing function against an open wellbore, which will not confirm that the shearing rams are able to shear the pipe. Hence, arguably the most vulnerable function of the shearing rams, and perhaps of the most important function from a safety perspective, namely the ability to shear the drill pipe in an emergency, is not tested during weekly function tests. The shearing function may therefore fail upon demand due to a DU failure which is undetectable by the weekly tests, or a *test independent failure*. According to Hauge et al. (2010), the *probability of a test independent failure* (TIF) occurring upon a demand, P_{TIF} , should be included in the reliability calculations for such cases.

Hauge and Onshus (2010b) define the probability of a component/system TIF, P_{TIF} as:

"The probability that the component/system will fail to carry out its intended function due to a (latent) failure not detectable by functional testing(...)."

The implication of TIF on reliability calculations is discussed in section 5.1.

Alternatively, the issue of imperfect shear ram tests can be overcome by the inclusion of a *test coverage factor* C in PFD calculations where the test is known to be imperfect. It is then assumed that the fraction $(1-C)$ of DU failures that cannot be revealed by weekly functional tests, are revealed during a re-certification. The implication of this approach on reliability calculations is also discussed in 5.1.

2. *The test interval is assumed to be fixed.*

In a practical situation the test interval is likely to be unfixed. If the test interval is unfixed during a period of time, and the τ value used in the calculation of the PFD is the average test interval, the result from 5.1 will be too optimistic. It is however an assumption which is necessary to make in order to achieve PFD estimates for system components.

3. *Components are independent and have constant failure rates.*

This assumption is non-conservative. When assuming independent components, the quantification of BOP reliability disregards all potential failures caused by inherent dependencies in the system.

In relation to component dependency, it is important to clearly separate the concepts of *dependent failures* and *failure of multiple independent components due to a shared cause*,

or *common cause failures* (CCF). Dependent failures may be classified into three main groups: CCF, cascading failures and negative dependencies (Rausand and Hoyland, 2004).

Cascading failures are multiple failures initiated by the failure of one component in the system that results in a chain-reaction (Rausand and Hoyland, 2004), e.g. a building collapsing completely due to the fracture of a single load-supporting beam.

Negative dependency refers to single failures which reduce the likelihood of other components failing (Rausand and Hoyland, 2004), e.g. an electrical fuse failing reduces the likelihood that any lightbulb powered from this fuse experiences a failure, since the electric current is removed from the system.

While either of these types of dependency may exist in the BOP system, cascading failures and negative dependencies will not be discussed further in this report. In Section 4.2, an introduction to CCF is presented, along with a proposed methodology for including CCF in PFD calculations for BOP, and a discussion of the potential implication of CCF on BOP reliability.

3.2 Regulations and guidelines

3.2.1 Introduction

In most countries, governmental bodies stipulate laws and regulations for petroleum companies operating in their geographic domain. In the NSNS, all petroleum related offshore operations are under the authority of the Petroleum Safety Authority Norway (PSA). The PSA is a governmental body within the Norwegian Petroleum Directorate (NPD), and is charged with the responsibility of acting as the regulatory authority for technical and operational safety. As such, the PSA shall enforce the laws and regulations that apply to the Norwegian Sector of the North Sea. All companies operating in this area must comply to the regulations set forth by the PSA. In order to help the industry comply to these laws and regulations, *standards* are developed by organizations acting on behalf of the government and/or the industry.

3.2.2 Standards pertaining to BOP reliability

Standards are documents that specify guidelines ranging from safe design specifications for offshore structures to guidelines for waste management. The purpose of such standards is to help

the petroleum industry comply to regulations and to act according to what is considered "best practice" in the industry.

The US GoM OCS is governed by the Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE), while the standards applicable to the area are issued mostly by the American Petroleum Institute (API). In Europe, the majority of industrial standards are developed by the International Standardization Organization (ISO) and the International Electrotechnical Committee (IEC). Standards that apply to offshore operations on the NSNS are issued on behalf of the Norwegian petroleum industry and the governing authorities, PSA and NPD, by the Norwegian Oil Industry Association (OLF). In terms of safety and reliability issues, and for the purpose of this report, the most important standards that apply to the petroleum industry in Norway are:

- IEC 61508 Functional Safety of electrical/electronic/programmable electronic safety-instrumented systems
- IEC 61511 Functional Safety - Safety instrumented systems for the process industry sector
- OLF 070 Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry
- NORSOK D-010 Well integrity in drilling and well operations

IEC 61508 (2010) is a general standard which specifies functional safety guidelines that apply to all types of industrial activity. IEC 61511 (2004) is a standard which is harmonized with the general functional safety standard, but modified in order to apply more directly to the process industry. OLF-070 (2004) is a further modified standard which specifies guidelines for how to act in accordance with the two before mentioned standards while operating in the NSNS as part of the petroleum industry in Norway. D-010 (2004) is a standard which specifies requirements and guidelines for well design and planning and execution of well operations in Norway, in accordance with the previously mentioned standards. These standards specify a variety of guidelines and requirements both directly and indirectly applicable to BOP systems.

3.2.3 BOP testing regulations in the Norwegian Sector of the North Sea

The regulations pertaining to BOP testing also depend on which government has domain over the area in question. Some governments do not have any regulations for BOP testing. In these cases, internal company policies determine the requirements. In the NSNS, there are governmental regulations for BOP testing, specified by the PSA. The PSA stipulates regulations for test types and frequencies, and for tests to be performed at various stages of the drilling program. These requirements must be followed in order to be allowed operation in the NSNS. According

to (Holand, 1999), the following BOP tests are specified in these regulations:

- Installation tests
- Test after running casing
- Regular interval pressure tests (Maximum intervals of 14 days)
- Regular interval function tests(Maximum 7 days after the previous pressure test)

Table 3.1 shows an overview of the required test types and frequencies, as specified in D-010 (2004).

	Frequency Element	Stump	Before drilling out of casing		Before well testing	Periodic		
			Surface	Deeper casing and liners		Weekly	Each 14 days	Each 6 months
BOP	Annulars Pipe rams Shear rams Failsafe valves Well head connector Wedge locks	MWDP 1) MWDP MWDP MWDP Function	Function Function Function MSDP	MSDP 1) MSDP MSDP MSDP 3)	TSTP 1) TSTP TSTP TSTP	Function Function Function	MSDP 1) MSDP MSDP 3) MSDP	WP x 0.7 WP WP WP WP
Choke/kill line and manifold	Choke/kill lines manifold Valves Remote chokes	MWDP MWDP Function	MSDP MSDP Function	MSDP MSDP Function	TSTP TSTP Function		MSDP MSDP Function	WP WP WP
Other equipment	Kill pump Inside BOP Slabbing valves Upper kelly valve Lower kelly valve	WP 2) MWDP 2) MWDP 2) MWDP 2) MWDP 2)		MSDP MSDP MSDP MSDP MSDP	TSTP TSTP		MSDP MSDP MSDP MSDP MSDP	WP WP WP WP WP
Legend				NOTE 1 All tests shall be 1.5 MPa to 2 MPa/5 min and high pressure/10 min.				
WP	working pressure			NOTE 2 If the drilling BOP is disconnected/re-connected or moved between wells without having been disconnected from its control system, the initial leak test of the BOP components can be omitted. The wellhead connector shall be leak tested.				
MWDP	maximum well design pressure			NOTE 3 The BOP with associated valves and other pressure control equipment on the facility shall be subjected to a complete overhaul and shall be recertified every five years. The complete overhaul shall be documented.				
MSDP	maximum section design pressure							
Function	Function testing: testing shall be done from alternating panels/pods.							
TSTP	tubing string test pressure							
1)	Or maximum 70 % of WP							
2)	Or at initial installation							
3)	From above if restricted by BOP arrangement							

Table 3.1: Routine leak testing of drilling BOP and well control equipment. Source: D-010 (2004), p.157

Annulars, rams, failsafe valves, and wellhead connectors must all be function tested weekly (D-010, 2004). During these function tests it is required that testing is done from alternating panels and pods, meaning that the testing of functions is alternated between the DCP and the TCP, while also alternating which pod the commands are run through.

Annulars, pipe rams, failsafe valves and wellhead connector are also to be pressure tested to the maximum casing section design pressure minimum once per 14 days (D-010, 2004). This means that the components are to be tested to the pressure which represents the maximum design pressure of the next section of casing to be set in the wellbore. Norwegian regulations further require pipe rams, shear rams, failsafe valves and wellhead connector to be pressure tested to working pressure at least once every six months. Annulars shall be tested to 70 percent of working pressure with the same time interval.

All BOP pressure tests shall be to 1.5 MPa-2 MPa for 5 minutes, followed by high pressure for 10 minutes (D-010, 2004).

All installation tests must include a BOP test to the pressure which equals the maximum section design pressure (MSDP) of the casing string that is designed to withstand the highest pressure (D-010, 2004). Granted this test has been performed, the BOP installation test can be limited to testing of all functions (annular/ram preventers etc.) as well as the wellhead connector and the choke and kill lines (D-010, 2004).

When about to drill out of casing, it is required that the BOP is pressure tested to the MSDP of the next section of casing (D-010, 2004). Surface function testing of annulars, rams and failsafe valves, as well as surface MSDP test of the wellhead connector is also required before drilling out of casing (D-010, 2004).

Chapter 4

BOP failures

4.1 Overview of all BOP failures

4.1.1 Introduction

In order to assess the reliability of a safety critical system such as the BOP, the system familiarization and functional analysis should be followed by a process of identifying the potential failures in the system. Ideally, system failures should be identified through qualitative techniques such as failure mode, effects and criticality analysis (FMECA/FMEA), hazard identification (HAZID) and hazard and operability study (HAZOP), involving personnel from multiple disciplines with expert knowledge of the system, and/or extensive experience with the system's use. The failure modes identified in this section are partly based on failure modes from Holand (1999), Holand and Skalle (2001) and Holand (1997), expert judgments from DNV personnel, and otherwise based on the the author's best judgment. While the identification of failures may therefore contain some inadequacies, the emphasis of the further analysis is placed on the methodology rather than the detailed failure analysis of the system.

4.1.2 Safety criticality of failures

When assessing the ability of the BOP to act as a safety barrier, we are interested in failures which have the potential to prevent the BOP from performing functions required to mitigate a well control situation, or a process demand. We therefore only include in the analysis the failures which can be classified as DU failures, according to the definition presented in Section 3.1.

A safety critical system is normally not operated outside of a process demand. In this respect, the BOP is different from many other safety critical systems, because some of its functions are operated in relation to normal operation, e.g. annular preventers are closed for stripping of drill pipe and so forth. Hence, critical failures preventing these functions from being activated may be detected during normal operation, i.e. outside of a process demand. The assumption that failures are only detected during proof tests is therefore not completely accurate for the BOP system. However, the inaccuracy of the assumption will have a conservative effect on calculations, and the assumption is therefore accepted.

4.1.3 Data sources

A collection and analysis of BOP failure data has not been performed as part of this master thesis. The required data input for the quantitative analysis has been failure rates and test intervals for the relevant BOP components. The main sources of such data have been the FTAs performed in relation to the BOP reliability studies Phase I DW and Phase II DW (Holand, 1997), and the reliability data for typical subsea components (solenoid valve, SEM etc.) listed in Hauge and Onshus (2010a). Due to lack of available data, it has been necessary to use "guesstimates" for some component failure rates. A complete list of failure rates used as input the the quantitative analysis in this report can be found in Appendix B.2.

4.1.4 BOP system failure modes

Based on the system familiarization, functional analysis and analysis of operational situations, the failure modes which can potentially lead to DU failures in the BOP system have been identified. An overview of the failure modes used as input for the quantitative analysis is shown Table 4.1.

BOP failure modes					
Main control system	Annular preventers	Pipe rams	Blind shear ram	Casing shear ram	Accumulators
Severe leakage in pod selector valve.	Annular preventer internal failure; causes fail to close.	Tool joint in ram closing area; causes fail to seal.	Tool joint in ram closing area; causes fail to shear/seal.	Tool joint in ram closing area; causes fail to shear.	Severe leak through stack mounted accumulator isolation valve.
Blue/yellow surface control valve failure.	Blue/yellow pod solenoid valve fails to open.	Pipe ram internal failure; causes fail to close.	Blind shear ram internal failure; causes fail to shear/seal.	Casing shear ram internal failure; causes fail to shear.	External leakage in subsea accumulator.
Topside control panel PLC's fail to signal pods.	Shuttle valve or line to preventer leaks.	Blue/yellow pod solenoid valve fails to open.	Blue/yellow pod solenoid valve fails to open.	Blue/yellow pod solenoid valve fails to open.	Leakage in pod mounted accumulator isolation valve, blue pod.
Blue/yellow pod SEM fail to fire solenoid valve.	Shuttle valve stuck in opposite position.	Shuttle valve or line to preventer leaks.	Shuttle valve or line to preventer leaks.	Shuttle valve or line to preventer leaks.	Leakage in pod mounted accumulator isolation valve, yellow pod.
Loss of power/communications to blue/yellow pod due to MUX cable and associated equipment failure.	Hydraulic control valve failure.	Shuttle valve stuck in opposite position.	Shuttle valve stuck in opposite position.	Shuttle valve stuck in opposite position.	
Loss of hydraulic fluid due severe leakage in blue/yellow pod hydraulic supply lines.		Hydraulic control valve failure.	Hydraulic control valve failure.	Hydraulic control valve failure.	
DGP/TCP Push button failure.					

Table 4.1: Failure modes in the BOP system.

In addition to the failure modes listed in Table 4.1, the sources for potential CCFs in the system should also be identified. The following section gives a short introduction to CCF and CCF modeling, and describes the potential for CCFs in the BOP system and how these can be included in the reliability assessment of the system.

4.2 Common cause failures

4.2.1 Introduction

Safety critical systems often have a high degree of redundancy. Redundancy is introduced in the architecture of safety critical systems in order to enhance reliability (Lundteigen and Rausand, 2007). A core principle behind the design of the BOP system is redundancy of functions capable of isolating the well in the event of a well kick.

When we quantify the reliability of redundant safety critical systems it is essential to distinguish between *independent* and *dependent* failures (Hauge and Onshus, 2010b). In this respect it is also important to distinguish between *random hardware failures* and *systematic failures*. Most random hardware failures caused by natural stressors are considered as independent failures, i.e. failure of one component is not assumed to influence the failure frequency of other components in the system Hauge and Onshus (2010b). In contrast, systematic failures such as excessive stress related failures, installation failures and operational failures are by nature potentially dependent failures (Hauge and Onshus, 2010b). Systematic, dependent failures have the potential to lead to common cause failures, i.e. simultaneous failure of more than one component in the system by the same cause. Common cause failures can therefore reduce the effect

of redundancy in safety critical systems.

The system reliability of a redundant system such as the BOP can be strongly influenced by potential common cause failures. It is therefore important to identify the potential CCFs in a system and to take the necessary precautions to prevent such failures from occurring (Rausand and Hoyland, 2004). The objective of this section is to present the fundamental principles of common cause failure modeling, as well as identifying potential CCFs in the BOP system and suggesting an approach to how these should be modeled.

4.2.2 Theoretic principles behind CCF modeling

There is no widely accepted definition of CCFs. The understanding of what a CCF is will therefore depend on different personal opinions in different industry sectors. IEC 61511 (2004) defines a CCF as *"a failure which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to a system failure."* A channel is a single redundant path within a safety function, or alternatively a single safety function where more than one of the system's safety functions are required to achieve the necessary risk reduction (Lundteigen and Rausand, 2007). Whereas NASA (2002b) defines a CCF event as *"the failure (or unavailable state) of more than one component due to a shared cause during the system mission."*

A important aspect of determining how to model CCF is how the term *simultaneous* is interpreted. In the aviation industry, the term CCF describes the multiplicity of failures occurring during the same flight (Hokstad and Rausand, 2008). In the case of the BOP system, the most relevant failures from a safety perspective are those classified in IEC 61508 (2010) as DU failures. DU failures can only be detected through proof testing, hence a multiple in the BOP system failure should only be considered a CCF so long as it occurs within the *same* test interval τ .

By direct implication, the term CCF suggests the existence of a cause-effect relationship between the failure and some failure cause (Hokstad and Rausand, 2008). Such a relationship may however in many cases be difficult to identify. According to Rausand and Hoyland (2004), CCF for which the causes can be identified should be modeled explicitly in e.g. a fault tree or an RBD. In most cases, it will be difficult to find high quality input data for explicitly modeled common causes. According to Rausand and Hoyland (2004), even with low quality input data, the result of explicit modeling will still usually be more accurate compared to the outcome of including these CCF in an implicit model. In Lundteigen and Rausand (2009), it is argued that for systems with several types of common causes, such as the BOP system, the explicit approach may lead to large fault tree which are difficult to interpret, and that dependent events may then be easily

overlooked or incorrectly included in the model. Based on this argument, the implicit approach will be used for modeling of CCF in the BOP system.

Standard beta-factor model versus PDS approach

Traditionally, the most commonly used implicit model for common cause failures of safety critical systems has been the standard *beta-factor model* (Rausand and Hoyland, 2004). The model assumes that a fraction β of all the failures in a system or subsystem are common cause failures, so that the contribution to the system DU failure rate from independent and CCF failures is equal to $(1 - \beta)\lambda_{DU}$ and $\beta\lambda_{DU}$, respectively.

A problem with the beta-factor model is that it does not take into account the *voting* of the system. A M-out-of-N (MooN) voting ($M > N$) means that at least M of the N redundant components have to give a shutdown signal for a shutdown to be activated (Hauge and Onshus, 2010b). In the standard beta-factor model, any MooN voting is given the same rate of CCF, regardless of the values of M and N. With a component failure rate for dangerous, undetected failures λ_{DU} , the contribution from CCF is always equal to $\beta\lambda_{DU}$. Consequently, the resulting system failure rate due to CCF will be equal for e.g. 1oo2, 1oo3 and 2oo3 voted systems.

OLF-070 (2004) rejects the use of the beta-factor model as an appropriate method of modeling CCF, and suggests the use of the *PDS approach* instead. The PDS approach is a method that distinguishes between different types of voting by including a modification factor C_{MooN} so that the beta-factor of a MooN voted system can be expressed by (Hauge and Onshus, 2010b):

$$\beta(MooN) = \beta \cdot C_{MooN}, (M < N), \quad (4.1)$$

where β is the factor applying to a 1oo2 voted system.

Hence, for a MooN voted system of components with failure rate λ_{DU} , the contribution from CCF to the total system failure rate is equal to:

$$\lambda_{DU_{CCF}} = C_{MooN} \cdot \beta\lambda_{DU} \quad (4.2)$$

The PDS approach is quite easy to use in practice, since the effect from voting is included as the separate factor C_{MooN} which is independent of β (Hauge and Onshus, 2010b). The BOP system contains several subsystems with voting logics where N is larger than 2, and it is therefore considered that the PDS approach is the most appropriate method for modeling potential CCF in the BOP system.

4.2.3 CCF data sources

In order to determine the beta-factor and the modification factor C_{MooN} , one is dependent on relevant failure data regarding CCF. The access to relevant failure data on CCF is limited, and alternative methods to support estimation of these parameters have therefore been suggested. Hauge and Onshus (2010b) mentions the checklist in IEC 61508 (2010) as an alternative method of estimating the beta-factor. Also, OLF-070 (2004) lists beta-factor values for a selection of components which are frequently used in safety instrumented systems, such as logic controllers, valves and sensors, which will be applied in this report. It is however emphasised in OLF-070 (2004) that these values are *not* to be considered as *the* recommended values, rather examples of typical values.

For estimation of C_{MooN} , Hauge and Onshus (2010b) suggests an approach based on expert judgments, and presents a selection of C_{MooN} values for typical voting configurations based on this approach. These C_{MooN} values are used as input to the quantitative analysis in Chapter 5.

4.2.4 CCF in the BOP system

In general, common causes failures may be caused by (NASA, 2002a):

- A common *design or material deficiency*
- A common *installation error*
- A common *maintenance error*
- A common *harsh environment*

When attempting to identify potential CCF in the BOP system, we should review each of these aspects for each set of components that may be susceptible to CCF.

The BOP system contains various subsystems of identical, redundant components which can be considered susceptible to CCF, including the solenoid valves in each pod, shuttle valves, control valves, pod accumulator isolation valves, hydraulic fluid hoses, MUX cables, SEMs and PLCs. In order to identify in detail which sources of CCF each of these component types can be exposed to, CCF identification should be included as part of FMECA/FMEA or HAZID/HAZOP activities for BOP systems, utilizing expertise from across all relevant engineering disciplines.

As part of the reliability quantification method in Chapter 5, beta-factors and C_{MooN} values for the relevant components have been chosen based on values listed in OLF-070 (2004), Hauge and Onshus (2010a), or otherwise conservative guesstimates.

Chapter 5

Reliability assessment model for the BOP system

5.1 Quantification of BOP reliability

5.1.1 Introduction

So far in this report, we have described the composition of the BOP system, defined its essential functions and its functional boundaries. We have also provided a functional analysis of the BOP, and a discussion of how the BOPs ability to act as a safety barrier is affected by the operational situations and conditions to which it is exposed, and also by the configuration of the BOP stack. Previous studies of BOP reliability have been evaluated, mainly by discussing the validity of the assumptions made in order to quantify the reliability of the BOP in these studies. The most relevant BOP failure modes have been presented, along with an identification of potential sources for common cause failures in the BOP system, and discussion of the contribution from CCF may be included in BOP reliability calculations. Based on the results from the previous sections, a new approach to quantifying the reliability of the BOP system through fault tree and event tree analysis (ETA) is now suggested.

5.1.2 Background for the approach

Choice of reliability performance metric

The BOP is a system whose reliability we seek to quantify by some reliability metric based on probabilistic formulas and empirical data about the system's use. The purpose of the quantification may be to verify compliance to some regulatory requirement, e.g. a *safety integrity level* (SIL). According to the definition in (IEC 61511, 2004), a SIL is a:

"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."

In order for this definition be applied when assessing the *safety integrity* (reliability) of the BOP, the system should also be in accordance with the definition of a *safety instrumented system* (SIS), governing one or more *safety instrumented function(s)* (SIF). Placing the BOP under the SIS definition implies that the system is "*composed of any number of sensor(s), logic solver(s) and final element(s)*" (IEC 61511, 2004), which is correct. However, the term SIS is mainly intended to refer to a dedicated safety system which automatically responds to a process demand by automatically performing some SIF. Meanwhile, the BOP does not perform any such SIFs automatically in response to a process demand. Rather, it is a complex system which is entirely dependent on both the physical interaction and professional judgment of the operator(s) in order to perform its functions. Moreover, the BOPs functions are not dedicated to its role as a safety barrier, but part of normal operation as well. Hence, the SIS definition is not directly applicable to the BOP system.

Despite the inaccuracies in terms of definitions described above, BOP reliability is considered under the SIL methodology in OLF-070 (2004), where it is recommended that the required PFD/SIL levels be calculated specifically for each well and tolerable risk levels set as part of the application process for exploration and development drilling consent. As the minimum, SIL 2 requirements are recommended for both isolation of the well using the annulus function, and for *closing* of the blind shear ram (OLF-070, 2004). An important note is that a minimum SIL requirement has *not* been recommended for the actual shearing of the pipe (OLF-070, 2004).

Depending on whether the safety system is operating in a *demand mode of operation*, or a *continuous/high demand mode of operation*, compliance to SIL must be demonstrated either through verification that the average probability of failure on demand (PFD), or average probability of dangerous failure per hour (PFH), is within the range of the SIL in question. According to IEC 61508 (2010), the BOP should be considered as operating in an on demand mode of operation, and thus the reliability target for a SIF performed by the BOP system should be expressed by the average PFD of the SIF.

Selection of modeling approach

In order to determine the PFD of the BOP functions, a reliability analysis method must be chosen. (IEC 61511, 2004) and (IEC 61508, 2010) recommend the use of FTA, RBD or Markov methods for this analysis, and that the effect from CCF be taken into account using the PDS approach. Both RBD and FTA are applicable methods for analyzing the reliability of a complex SIF (Lundteigen and Rausand, 2009). We wish to select the method which is most suitable for modeling the SIF *Isolate well*, defined in Chapter 2, which is fulfilled by one or more of the three essential functions specified in OLF-070 (2004), also listed in Chapter 2.

FTA is a deductive, failure oriented method which focuses on how a function may fail. The FTA method makes it simpler to identify failures that are not directly linked to a component function, and it is an intuitive and structured approach, compared to the RBD and Markov methods.

RBD models often bear a greater resemblance to the physical structure of the system in the sense that the functional block may be set up to be similar to the sequence in which the system components are activated. A block diagram is established by focusing on how functions are achieved, rather than how they may fail. Lundteigen and Rausand (2009) point to this as a possible strength, but also a weakness, since functions that are installed, or should be installed, to protect the main system functions may easily be overlooked. Unlike the physical structure, the RBD may include the same component in different sections of the model, if the component is part of more than one function. To personnel who are unfamiliar with reliability modeling, the model may therefore become confusing (Lundteigen and Rausand, 2009).

The strength of Markov methods is the ability to model systems which are frequently switching between different operational modes, and have complex maintenance and repair processes (Rausand and Hoyland, 2004). For such applications, the FTA and RBD methods may provide too "static" an image of the system (Lundteigen and Rausand, 2009). However, when the system has a high number of components, the Markov models will become very large, and the number of fault states and operational, maintenance and repair modes may be too difficult to comprehend (Lundteigen and Rausand, 2009).

The BOP has a large variety of components, and is a complex system both in terms of design, and in terms of operation and maintenance. While it is also exposed to different operational situations, the frequency with which each of these are visited is not very high. Markov methods are therefore considered less suitable for modeling of the BOP system. RBDs can be used to model parts of the system, and has been a useful tool in terms of reviewing the effect on system redundancy when analysing the different operational situations. However, it is considered of great importance to have a strong involvement from design engineers and operators in the analysis, both in order to increase their awareness of critical failure combinations, and in order

to utilize their competence and experience with the system in the identification of potential failures and system weaknesses. Hence, we wish to select the most intuitive, structured and failure oriented approach. Based on these arguments, FTA is considered the most suitable method for the reliability assessment of the BOP system SIFs.

5.1.3 Fault tree analysis of the BOP system

Achieving conservative PFD approximations

In the previous BOP reliability studies discussed in this report, the authors have used FTA to calculate the PFD of BOP failing to close in a well kick. PFD calculations are usually based on approximations. It is therefore essential that these approximations are conservative, such that the "true" PFD is less than the calculated PFD (Lundteigen and Rausand, 2009). Previous studies have used the FTA software tool CARA Faulttree to calculate the TOP event probabilities of the fault trees. Along with most other FTA software tools, CARA FaultTree produces non-conservative, inaccurate PFD approximations.

Lundteigen and Rausand (2009) present an FTA-based approach which produces more conservative and accurate estimates of the PFD through post-processing of minimal cut sets. By following the approach by Lundteigen and Rausand (2009), the contribution from CCF can also be included in the calculations. Hence, some important weaknesses found in previous BOP reliability studies can be overcome by using this approach. In the following, it will be demonstrated how the approach presented by Lundteigen and Rausand (2009) can be applied to the BOP system in order to produce conservative PFD estimates which take into account CCF.

Consider a fault tree for a specified TOP event, with m minimal cut sets, or *minimal cuts*, MC_1, MC_2, \dots, MC_m . Let $PFD_{j,i}$ denote the (average) PFD of component i in minimal cut set j , for $j = 1, 2, \dots, m$. Minimal cut j of order m_j is a $100m_j$ voted structure, and will fail only when all m_j components in the cut set are in a failed state simultaneously. When all the components in minimal cut j are independent components, the PFD of the minimal cut is normally calculated by (Lundteigen and Rausand, 2009):

$$PFD_{MC_j} \approx \prod_{i=1}^{m_j} PFD_j \quad (5.1)$$

Along with most other FTA software tools, CARA FaultTree uses Equation 5.1 to calculate the PFD of a minimal cut, which does not give an accurate result (Dutuit et al., 2008). Due to the well known Schwartz' inequality saying that "the average of a product is not equal to the prod-

uct of averages" (Lundteigen and Rausand, 2009), Equation 5.1 produces non-conservative PFD approximations.

For a single component i in minimal cut j , with a constant DU failure rate $\lambda_{DU,j,i}$, which is periodically tested with fixed intervals τ , the average PFD $_{j,i}$ can be calculated as (Rausand and Hoyland, 2004):

$$PFD_{j,i} = \frac{1}{\tau} \int_0^{\tau} (1 - e^{-\lambda_{DU,j,i} \cdot t}) dt \approx \frac{(\lambda_{DU,j,i} \cdot \tau)}{2} \quad (5.2)$$

All BOP components are covered by the same functional test with test interval τ . The component index i is therefore omitted in the following.

According to Rausand and Hoyland (2004), Equation 5.2 is a conservative PFD approximation, which produces adequate results when:

- $\lambda_{DU,j} \cdot \tau < 10^{-2}$. For higher values, the approximation might be too conservative (Lundteigen and Rausand, 2009).
- Operation is halted upon the detection of a DU failure, and is not commenced before the failure has been repaired.
- The functional is perfect; all DU failures are revealed by the test.

For the BOP, the first two conditions are fulfilled, while the third is not fulfilled because of the imperfect functional testing conditions for the shear rams. As described in section 3.1, this issue can be overcome by two main approaches. Either by adding the TIF probability P_{TIF} to the *critical safety unavailability* (CSU), or by including a test coverage factor C to account for the fraction $(1-C)$ of DU failures which are *not* revealed by the functional test, when calculating the PFD $_{MC_j}$.

In Hauge and Onshus (2010b), the P_{TIF} is included in the reliability calculations as a contribution to the total *loss of safety*, or *critical safety unavailability*(CSU) as:

$$CSU = PFD + P_{TIF} \quad (5.3)$$

Hauge and Onshus (2010b) list TIF probabilities for various components typical to safety systems. For redundant components, the contribution from TIF to loss of safety can for a MooN voting be expressed as (Hauge and Onshus, 2010b):

$$P_{TIF} \approx C_{MooN} \cdot \beta \cdot P_{TIF} \quad (5.4)$$

where the numerical values of C_{MoON} are assumed to be identical to the values used in the PFD calculations. In Hauge and Onshus (2010b) TIF probabilities are listed for various components typical to safety systems.

Alternatively, the issue of imperfect tests can be introduced by the test coverage factor C . Hauge et al. (2010) gives an example of how the test coverage factor is included in the reliability calculations for a workover control system. In this example, the test coverage factor is set to 75%, and the test interval τ with which the unrevealed fraction of DU failures $(1-C)$ can be detected is set equal to the re-certification interval τ_{CT} . The BOP is re-certified with 5 year intervals (Holand, 1986). Assuming that DU failures undetected by weekly functional BOP tests cannot be detected outside of these re-certification intervals, we find that the PFD for a single component failure mode, e.g. "BSR fail to shear drill pipe", with assumed failure rate $\lambda_{BSR} = 1 \cdot 10^{-6}$, when including the test coverage factor C becomes:

$$PFD_{BSR} \approx C \cdot \lambda_{BSR} \frac{\tau}{2} + (1 - C) \lambda_{BSR} \frac{\tau_{CT}}{2} \quad (5.5)$$

$$PFD_{BSR} \approx 0,75 \cdot 1 \cdot 10^{-6} \cdot \frac{168}{2} + 0,25 \cdot 1 \cdot 10^{-6} \cdot \frac{5 \cdot 8760}{2} = 6,3 \cdot 10^{-5} + 5,475 \cdot 10^{-3} = 5,538 \cdot 10^{-3} \quad (5.6)$$

Hence, in this example, the fraction of the total PFD_{Shear} contributed from DU failures unrevealed by tests is $0,05475/0,05538 = 0,98862$, i.e 98,9%. This example is perhaps too conservative either in terms of the assumed value of the test coverage factor, or in terms of the assumed interval $\tau_{Certification}$ with which these failure can be detected. However, the example certainly indicates that the contribution from DU failures unrevealed by shear ram tests may be significant, and that the test coverage factor C should therefore be included when calculating the PFD for the BOP components/systems which are exposed to such failures.

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

$$PFD_{j,i} = \frac{1}{\tau} \int_0^{\tau} \prod_{i=1}^{m_j} (1 - e^{-\lambda_{DU,j} \cdot t}) dt \leq \frac{1}{\tau} \int_0^{\tau} \prod_{i=1}^{m_j} (\lambda_{DU,j} \cdot t) dt = \frac{(\prod_{i=1}^{m_j} \lambda_{DU,j}) \cdot \tau^{m_j}}{m_j + 1} = \frac{(\bar{\lambda}_{DU,j} \cdot \tau)^{m_j}}{m_j + 1} \quad (5.7)$$

where

$$\bar{\lambda}_{DU,j} = \left(\prod_{i=1}^{m_j} \lambda_{DU,j} \right)^{\frac{1}{m_j}} \quad (5.8)$$

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

To illustrate the difference between the conservative and non-conservative approximations, consider a minimal cut j consisting of two independent components with failure rate $\lambda_{DU,j}$. By combining 5.1 and 5.2, we get $\text{PFD}_{MC_j} = (\lambda_{DU,j} \cdot \tau)^2/4$, while from 5.3 we get $\text{PFD}_{MC_j} = (\lambda_{DU,j} \tau)^2/3$, i.e. the non-conservative approximation is 25 percent lower than the conservative value. This percentage increases with the order m_j of the minimal cut. Thus, the accuracy of PFD approximations achieved through FTA software tools can be greatly improved by post-processing the minimal cut sets using the approach presented by Lundteigen and Rausand (2009).

TOP event definition

Earlier in this report, four main BOP operational situations A,B,C and D have been presented. The purpose of the current FTA is to assess the BOP system's ability to perform the overall system SIF *Isolate well* for each of these operational situations. For each operational situation, a separate TOP event representing the non-fulfillment of the SIF has been defined:

- *TOP event A: Failure of the BOP to isolate well when 5" drill pipe is running through BOP*
- *TOP event B: Failure of the BOP to isolate well during large/small pipe diameter*
- *TOP event C: Failure of the BOP to isolate well during high wellbore pressure*
- *TOP event D: Failure of the BOP to isolate well during open hole*

Fault tree construction

In the ideal situation, the fault tree should be constructed in close cooperation with BOP design engineers and operators such as drillers, toolpushers, subsea engineers and so forth. The author of this report has not had access to such expertise directly, but has received consultation from DNV personnel, both with competence within well control and BOP reliability, and with competence regarding operation of the BOP system. It should be emphasised that due to the author's lack of experience with the system's use, and due to the limited access to expert knowledge and experience, some critical failures may have been overlooked or incorrectly included in the fault tree.

Using CARA FaultTree (Exprosoft AS, 2008), a separate fault tree has been constructed for each of the TOP events A, B, C and D listed above. The fault trees can be found in Appendix B.1.

The basic events included in each fault tree are listed in Appendix B.2.

Identification and verification of minimal cut sets

The minimal cut sets for each fault tree were easily identified using the built-in function in CARA FaultTree. The minimal cuts have then been verified, and then post-processed using Excel. An important finding is that most of the minimal cuts containing "preventer-specific" basic events, e.g. BRSOLVBP, BRSRSHV, LPRIF and so forth, produce negligible PFD values ($PFD_{MC_j} < 10^{-5}$ i.e. below the SIL 4 requirement). Some of the negligible minimal cuts have been included in the further calculations nonetheless, for the purpose of demonstrating the methodology for including CCF contributions. An overview of all cut sets up to order 4 for each TOP event can be found in Appendix B.3.

TOP event A minimal cuts

The minimal cuts for TOP event A included in PFD calculations is shown in Table 5.1 below.

ID (j)	Minimal cut sets j of order up to 4
A1	{SELECT}
A2	{PWR}
A3	{HYSLBLU, HYSLYEL}
A4	{SCVYP, SCVBP}
A5	{PLCA, PLCB}
A6	{MUXBP, MUXYP}
A7	{SEMAYP, SEMBYP, SCVBP}
A8	{SCVYP, SEMABP, SEMBBP}
A9	{ACCVL, EXLACC, ACCIVBP, ACCIVYP}
A10	{[SEMAYP, SEMBYP], [SEMABP, SEMBBP]}

Table 5.1: TOP event A minimal cuts.

TOP event B minimal cuts

The minimal cuts for TOP event B included in PFD calculations is shown in Table 5.2 below.

ID (j)	Minimal cut sets j of order up to 4
B1	{SELECT}
B2	{PWR}
B3	{SCVYP,SCVBP}
B4	{HYSLBLU,HYSLYEL}
B5	{PLCA,PLCB}
B6	{MUXBP, MUXYP}
B7	{SCVYP,SEMABP,SEMBBP}
B8	{SEMAYP,SEMBYP,SCVBP}
B9	{BSRTJOC,UAPIF,LAPIF,MPRIF}
B10	{BSRIF,UAPIF,LAPIF,MPRIF}
B11	{ACCVL,EXLACC,ACCIVBP,ACCIVYP}
B12	{[SEMAYP,SEMBYP],[SEMABP,SEMBBP]}

Table 5.2: TOP event B minimal cuts.

TOP event C minimal cuts

The minimal cuts for TOP event C included in PFD calculations is shown in Table 5.3 below.

ID (j)	Minimal cut sets j of order up to 4
C1	{SELECT}
C2	{PWR}
C3	{HYSLBLU,HYSLYEL}
C4	{SCVYP,SCVBP}
C5	{PLCA,PLCB}
C6	{SEMAYP,SEMBYP,SCVBP}
C7	{SCVYP,SEMABP,SEMBBP}
C8	{MUXBP, MUXYP}
C9	{ACCVL,EXLACC,ACCIVBP,ACCIVYP}
C10	{[SEMAYP,SEMBYP],[SEMABP,SEMBBP]}
C11	{BSRTJOC,LPRIF,MPRIF,UPRIF}
C12	{BSRIF,LPRIF,MPRIF,UPRIF}
C13	{CSRTJOC,LPRIF,MPRIF,UPRIF}
C14	{CSRIF,LPRIF,MPRIF,UPRIF}

Table 5.3: TOP event C minimal cuts.

TOP event D minimal cuts

The minimal cuts for TOP event D included in PFD calculations is shown in Table 5.4 below.

ID (j)	Minimal cut sets j of order up to 4
D1	{SELECT}
D2	{BSRIF}
D3	{PWR}
D4	{BSRHCV}
D5	{BSRSHV}
D6	{PLCA,PLCB}
D7	{HYSLBLU,HYSLVEL}
D8	{SCVYP,SCVBP}
D9	{MUXBP, MUXYP}
D10	{BSRPBDCP, BSRPBTCP}
D11	{SCVYP,BSRSOLVBP}
D12	{SCVYP,BSRSHVBP}
D13	{BSRSOLVYP,SCVBP}
D14	{BSRSOLVYP,BSRSOLVBP}
D15	{BSRSOLVYP,BSRSHVBP}
D16	{BSRSHVYP,SCVBP}
D17	{BSRSHVYP,BSRSOLVBP}
D18	{BSRSHVYP,BSRSHVBP}
D19	{SEMAYP,SEMBYP,SCVBP}
D20	{SEMAYP,SEMBYP,BSRSOLVBP}
D21	{SEMAYP,SEMBYP,BSRSHVBP}
D22	{SCVYP,SEMABP,SEMBBP}
D23	{BSRSOLVYP,SEMABP,SEMBBP}
D24	{BSRSHVYP,SEMABP,SEMBBP}
D25	{ACCVL,EXLACC,ACCIVBP,ACCIVYP}
D26	{[SEMAYP,SEMBYP].[SEMABP,SEMBBP]}

Table 5.4: TOP event D minimal cuts.

Identification of common cause component groups

For each minimal cut MC_j , it must be determined whether the components in the cut are independent or dependent. Each minimal cut must be reviewed looking for root causes and coupling factors. BOP components that are dependent and share the *same* common failure cause, are included in the *same* common cause component group $CG_{j,\nu}$, for $j = 1, 2, \dots, m$, and $\nu = 1, 2, \dots, r_j$, where r_j is the number of different common cause component groups in minimal cut MC_j (Lundteigen and Rausand, 2009). In many cases, one minimal cut will only contain a single common cause component group. The index ν is then omitted from the notation. Each $CG_{j,\nu}$ is then assigned a beta factor $\beta_{j,\nu}(Moon)$ according to the PDS approach.

The identified common cause component groups $CG_{j,\nu}$ for each of the TOP events A, B, C and D are shown in bold in Figures 5.1, 5.2, 5.3 and 5.4 above. Among the minimal cuts included in the current calculation, $CG_1, CG_2, CG_3, CG_4, CG_5, CG_7, CG_8$ are common cause components groups

containing only identical components which are thought to be dependent and susceptible to the same common failure cause such as similar design and materials, and/or exposure to the same excess stressors (temperature, vibration, pressure and so forth). $CG_{6,1}$ and $CG_{6,2}$ are two common cause component groups belonging to the same minimal cut.

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

All of the identified $CG_{j,v}$ have voting logic 1oo2, meaning that the C_{Moon} factor is equal to 1. Hence, the use of the PDS approach as opposed to the standard beta-factor model does not have any consequences for the assignment of β factors in the current analysis.

The assigned beta-factors are shown in Table 5.5 below. The β -values for PLCs and SEMs have been in Table 5.5 have been obtained from OLF-070 (2004). Otherwise, conservative estimates have been used. Alternatively, the beta-factors can be determined through thorough analysis of each sets of components using the checklist in IEC 61508 (2010).

CCF component groups (CG)	Components	Beta
CG A5	PLCA,PLCB	0,01
CG A3	HYSLBLU, HYSLYEL	0,10
CG A6	MUXBP, MUXYP	0,10
CG A9	ACCIVBP, ACCIVYP	0,10
CG A4	SCVBP, SCVYP	0,10
CG A10,1	SEMABP, SEMBBP	0,01
CG A10,2	SEMYP, SEMBYP	0,01

Table 5.5: β -factors.

Methodology used for PFD calculations

Based on the minimal cuts and common cause component groups identified, the PFD of each minimal cut has been calculated. The calculation method presented in the following is mostly reproduced from (Lundteigen and Rausand, 2009), and applied to the BOP system.

The calculation of the PFD_{MC_j} is influenced by (Lundteigen and Rausand, 2009):

1. The order m_j of the minimal cut
2. Whether or not the components of the minimal cut are dependent
3. Whether or not the components of the minimal cut are identical
4. Whether or not the components of the minimal cut are tested simultaneously

As mentioned above, only minimal cuts of order up to 4 have been included in the calculations. Also, we know that all components are tested simultaneously.

For the minimal cuts consisting only of independent BOP components, e.g. minimal cut D11, the $PFD_{MC_{D11}}$ has been calculated directly from 5.3.

For minimal cut sets where the components are identical, but dependent, e.g. minimal cut A4, the PFD_{MC_j} is calculated from (Lundteigen and Rausand, 2009):

$$PFD_{MC_j} \approx \frac{((1 - \beta)\lambda_{DU,j}\tau)^{m_j}}{m_j + 1} + \frac{\beta\lambda_{DU,j}\tau}{2} \quad (5.9)$$

Minimal cuts consisting of non-identical components may still be susceptible to the same CCF, such as a temperature or pressure increase. According to Hauge and Onshus (2010b), the beta-factor should then be smaller than for identical components, since "diverse redundancy" gives a lower degree of dependency or coupling. Lundteigen and Rausand (2009) states that some care must be taken when using the beta-factor model to calculate the contribution from CCF when the failure rates of the components in the minimal cut are different, and suggest that this problem may be overcome by defining the beta-factor to be a fraction of the *lowest* component failure rate, as this rate will often limit the frequency with which the parallel structure may fail simultaneously.

Using this approach, the PFD_{MC_j} of a minimal cut with non-identical, dependent components which belong to the *same* common cause component group becomes (Lundteigen and Rausand, 2009):

$$PFD_{MC_j} \approx \frac{[(1 - \beta)\bar{\lambda}_{DU,j}\tau]^{m_j}}{m_j + 1} + \frac{\beta \cdot \lambda_{DU,j}^{min} \cdot \tau}{2} \quad (5.10)$$

where

$$\lambda_{DU,j}^{min} = \min\{\lambda_{DU,j,i}\} \quad (5.11)$$

is the lowest DU failure rate in minimal cut MC_j .

When a minimal cut consists of more than one common cause component group, or includes both independent and dependent components, the calculation of the PFD_{MC_j} becomes more complex. Lundteigen and Rausand (2009) suggest an approach which can be applied in such cases. Consider minimal cut A10, illustrated as an RBD in Figure 5.1, which in the following will be used as an example to illustrate the approach. The minimal cut has two common cause

component groups, $CG_{A10,1}$ and $CG_{A10,2}$, each with two components. The CCF are included as virtual components in series with each parallel structure.

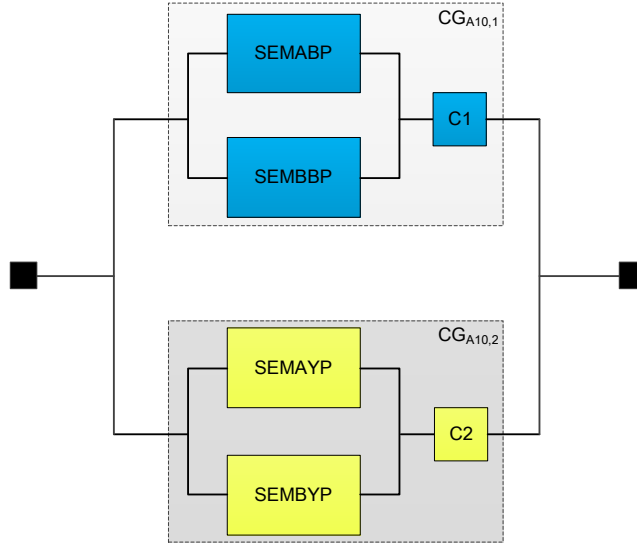


Figure 5.1: Minimal cut A10, with two common cause component groups.

The remaining components, H_j , are the number of independent components in MC_j (Lundteigen and Rausand, 2009). The order of H_j is denoted by $k_j^{(I)}$, and the order of $CG_{j,v}$ is denoted by $k_{j,v}^{(C)}$ (Lundteigen and Rausand, 2009). Components in H_j have failure rates $\lambda_{DU,j,i}^{(I)}$ for $i = 1, 2, \dots, k_j^{(I)}$ and the components in $CG_{j,v}$ have failure rates $\lambda_{DU,j,v,l}$ for $v = 1, 2, \dots, r_j$ and $l = 1, 2, \dots, k_{j,v}^{(C)}$ (Lundteigen and Rausand, 2009). For the minimal cut in Figure 5.5, $k^{(I)} = 0$, $r = 2$, $k_1^{(C)} = 2$, and $k_2^{(C)} = 2$.

According to the approach by Lundteigen and Rausand (2009), the PFD of the virtual cut set of lowest order in a minimal cut containing more than one common cause component group and/or both dependent and independent components is:

$$PFD_{MC_j}^{(I)} \approx \frac{\left(\prod_{i=1}^{k_j^{(I)}} \lambda_{DU,j,i}^{(I)} \cdot \prod_{v=1}^{r_j} \beta_{j,v} \cdot \lambda_{DU,j}^{min,v} \right) \cdot \tau_j^{k_j^{(I)}} + r_j}{k^{(I)} + r_j + 1} \quad (5.12)$$

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

Minimal cut A10 shown in Figure 5.6 has virtual cut sets $\{C1, C2\}$, $\{C1, SEMAYP, SEMBYP\}$, $\{C2, SEMABP, SEMBBP\}$ and $\{SEMABP, SEMBBP, SEMAYP, SEMBYP\}$. All of the components in MC_{A10} have the same failure rate, and the same β -factor. $\{C1, C2\}$ is the virtual cut of the lowest order. DU failure rates are identical. Using 5.12, with $k_{A10}^{(I)} = 0$, $k_{A10,1}^{(C)} = 2$, $k_{A10,2}^{(C)} = 2$, $r_{A10} = 2$, the PFD of $\{C1, C2\}$ is then:

$$PFD_{MC_{A10}}^{(1)} \approx \frac{\beta_{A10}^2 \lambda_{DU,A10}^2 \cdot \tau^2}{3} \quad (5.13)$$

The PFD of the remaining virtual cuts in MC_{A10} is determined in a similar way using the method presented in (Lundteigen and Rausand, 2009):

$$PFD_{MC_{A10}}^{(2)} = PFD_{MC_{A10}}^{(3)} \approx \frac{(1 - \beta_{A10})^2 \lambda_{DU,A10}^2 \beta_{A10} \lambda_{DU,A10} \cdot \tau^3}{4} \quad (5.14)$$

$$PFD_{MC_{A10}}^{(4)} \approx \frac{(1 - \beta_{A10})^2 \lambda_{DU,A10}^2 (1 - \beta_{A10})^2 \lambda_{DU,A10}^2 \cdot \tau^4}{5} \quad (5.15)$$

Similar equations have been derived for all minimal cuts included in the current FTA which have more than one common cause component group or include both dependent and independent BOP components.

The PFD_{MC_j} of a minimal cut j can then be calculated by using the "upper bound approximation" (Lundteigen and Rausand, 2009):

$$PFD_{MC_j} \approx 1 - \prod_{i=1}^n (1 - PFD_{MC_j}^{(k)}) \quad (5.16)$$

where n is the number of virtual cuts in MC_j .

Calculate the system PFD_{SIF}

Finally, we can evaluate the SIF *Isolate well* for each of the TOP events A, B, C and D by calculating the system PFD_{SIF} in each case. This is done by once again using the "upper bound approximation", this time on the minimal cuts MC_1, MC_2, \dots, MC_m :

$$PFD_{SIF} \approx 1 - \prod_{j=1}^m (1 - PFD_{MC_j}) \quad (5.17)$$

The results from the calculations are presented in the following section.

PFD calculation results

In this section, the resulting PFD_{SIF} for each of the TOP events, i.e. the probability that the BOP is unable to perform the SIF *Isolate well*, are presented and discussed. The PFDs of each minimal cut from each separate fault tree have been calculated in Excel using the methodology described above. The results are shown in Tables 5.6, 5.7, 5.8 and 5.9.

TOP Event A: Failure of the BOP to isolate well when 5" drill pipe is running through BOP

ID (j)	Minimal cut sets j of order up to 4	Geometric mean	Non-Cons. PFD w/out CCF	Cons. PFD w/out CCF	Cons. PFD w/ CCF	1-PFD
A1	{SELECT}	-	-	1,75E-05	-	0,99998250000
A2	{PWR}	-	-	8,40E-06	-	0,99999160000
A3	{HYSLBLU,HYSLYEL}	-	6,00E-06	8,00E-06	2,51E-04	0,99974851730
A4	{SCVYP,SCVBP}	-	3,06E-10	4,08E-10	1,75E-06	0,99999824967
A5	{PLCA,PLCB}	-	3,46E-09	4,08E-10	5,93E-07	0,99999940748
A6	{MUXBP, MUXYP}	-	3,46E-09	4,08E-10	3,36E-07	0,99999966399
A7	{SEMAYP,SEMBYP,SCVBP}	6,69E-07	1,78E-13	3,56E-13	2,96E-09	0,9999999704
A8	{SCVYP,SEMABP,SEMBBP}	6,69E-07	1,78E-13	3,56E-13	2,96E-09	0,9999999704
A9	{ACCVL,EXLACC,ACCIVBP,ACCIVYP}	1,97E-06	7,50E-16	2,40E-15	1,15E-10	0,99999999888
A10	{[SEMAYP,SEMBYP],[SEMABP,SEMBBP]}	-	1,03E-16	3,30E-16	1,40E-12	0,99999999999
					PFDsif	2,80060E-04

Table 5.6: PFD calculation results for TOP Event A.

TOP event B: Failure of the BOP to isolate well during larges/small pipe diameter

ID (j)	Minimal cut sets j of order up to 4	Geometric mean	Non-Cons. PFD w/out CCF	Cons. PFD w/out CCF	Cons. PFD w/ CCF	1-PFD
B1	{SELECT}	-	-	1,75E-05	-	0,99998250000
B2	{PWR}	-	-	8,40E-06	-	0,99999160000
B3	{SCVYP,SCVBP}	-	3,06E-10	4,08E-10	1,75E-06	0,999998249669
B4	{HYSLBLU,HYSLYEL}	-	6,00E-06	8,00E-06	2,51E-04	0,999748517300
B5	{PLCA,PLCB}	-	3,46E-09	4,61E-09	5,93E-07	0,999999407482
B6	{MUXBP, MUXYP}	-	1,13E-11	1,51E-11	3,36E-07	0,999999663988
B7	{SCVYP,SEMABP,SEMBBP}	-	5,36E-15	1,07E-14	2,96E-09	0,99999997036
B8	{SEMAYP,SEMBYP,SCVBP}	-	5,36E-15	1,07E-14	2,96E-09	0,99999997036
B9	{BSRTJOC,UAPIF,LAPIF,MPRIF}	6,40E-05	8,36E-10	2,68E-09	-	0,9999999973
B10	{BSRIF,UAPIF,LAPIF,MPRIF}	9,72E-06	4,44E-13	1,42E-12	-	0,99999999999
B11	{ACCVL,EXLACC,ACCIVBP,ACCIVYP}	1,97E-06	7,50E-16	2,40E-15	1,15E-10	0,99999999885
B12	{[SEMAYP,SEMBYP],[SEMABP,SEMBBP]}	-	1,03E-16	3,30E-16	1,40E-12	0,99999999999
					PFDsif	2,80063E-04

Table 5.7: PFD calculation results for TOP Event B.

TOP event C: Failure of the BOP to isolate well during high wellbore pressure

ID (j)	Minimal cut sets j of order up to 4	Geometric mean	Non-Cons. PFD w/out CCF	Cons. PFD w/out CCF	Cons. PFD w/ CCF	1-PFD
C1	{SELECT}	-	-	1,75E-05	-	0,99998250000
C2	{PWR}	-	-	8,40E-06	-	0,99999160000
C3	{HYSLBLU,HYSLYEL }	-	6,00E-06	8,00E-06	2,51E-04	0,99974851730
C4	{SCVYP,SCVBP }	-	3,06E-10	4,08E-10	1,75E-06	0,99999824967
C5	{PLCA,PLCB }	-	3,46E-09	4,08E-10	5,93E-07	0,99999940748
C6	{SEMAYP,SEMBYP,SCVBP}	-	3,79E-17	7,59E-17	2,96E-09	0,99999999704
C7	{SCVYP,SEMABP,SEMBBP }	-	3,79E-17	7,59E-17	2,96E-09	0,99999999704
C9	{MUXBP, MUXYP }	-	1,13E-11	1,51E-11	3,36E-07	0,999999663988
C10	{ACCVL,EXLACC,ACCIVBP,ACCIVYP }	1,97E-06	7,50E-16	2,40E-15	1,15E-10	0,999999999885
C11	{[SEMAYP,SEMBYP],[SEMABP,SEMBBP]}	4,00E-08	1,03E-16	3,30E-16	1,40E-12	0,999999999999
C12	{BSRTJOC,LPRIF,MPRIF,UPRIF}	3,70E-05	9,29E-11	2,97E-10	-	0,999999999703
C13	{BSRIF,LPRIF,MPRIF,UPRIF}	5,61E-06	4,93E-14	1,58E-13	-	0,9999999999998
C14	{CSRTJOC,LPRIF,MPRIF,UPRIF}	3,70E-05	9,29E-11	2,97E-10	-	0,9999999997027
C15	{CSRIF,LPRIF,MPRIF,UPRIF}	5,61E-06	4,93E-14	1,58E-13	-	0,9999999999998
					PFDsif	2,80061E-04

Table 5.8: PFD calculation results for TOP Event C.

TOP event D: Failure of the BOP to isolate well during open wellbore

ID (j)	Minimal cut sets j of order up to 4	Geometric mean	Non-Cons. PFD w/out CCF	Cons. PFD w/out CCF	Cons. PFD w/ CCF	1-PFD
D1	{SELECT}	-	-	1,75E-05	-	0,99998250000
D2	{BSRIF}	-	-	1,87E-03	-	0,99812750000
D3	{PWR}	-	-	8,40E-06	-	0,99999160000
D4	{BSRHCV}	-	-	8,40E-06	-	0,99999160000
D5	{BSRSHV}	-	-	2,10E-05	-	0,99997900000
D6	{PLCA,PLCB}	-	3,46E-09	4,61E-09	5,93E-07	0,99999940748
D7	{HYSLBLU,HYSLYEL}	-	6,00E-06	8,00E-06	2,51E-04	0,99974851730
D8	{SCVYP,SCVBP}	-	3,06E-10	4,08E-10	1,75E-06	0,99999824967
D9	{MUXBP, MUXYP}	-	1,13E-11	1,51E-11	3,36E-07	0,99999966399
D10	{BSRPBDCP, BSRPBTCP}	-	1,13E-09	1,51E-09	3,37E-07	0,99999966252
D11	{SCVYP,BSRSOLVBP}	1,83E-07	2,35E-10	3,14E-10	-	0,99999999969
D12	{SCVYP,BSRSHVBP}	1,86E-07	2,45E-10	3,27E-10	-	0,99999999967
D13	{BSRSOLVYP,SCVBP}	1,83E-07	2,35E-10	3,14E-10	-	0,99999999969
D14	{BSRSOLVYP,BSRSOLVBP}	-	1,81E-10	2,41E-10	1,34E-06	0,99999865580
D15	{BSRSOLVYP,BSRSHVBP}	1,63E-07	1,88E-10	2,51E-10	-	0,99999999975
D16	{BSRSHVYP,SCVBP}	1,83E-07	2,35E-10	3,14E-10	-	0,99999999969
D17	{BSRSHVYP,BSRSOLVBP}	1,63E-07	1,88E-10	2,51E-10	-	0,99999999975
D18	{BSRSHVYP,BSRSHVBP}	-	1,96E-10	2,61E-10	-	0,99999999974
D19	{SEMAYP,SEMBYP, SCVBP}	2,08E-07	5,36E-15	1,07E-14	2,96E-09	0,99999999704
D20	{SEMAYP,SEMBYP,BSRSOLVBP}	6,13E-07	1,37E-13	2,73E-13	2,37E-09	0,99999999763
D21	{SEMAYP,SEMBYP,BSRSHVBP}	6,21E-07	1,42E-13	2,84E-13	2,96E-09	0,99999999704
D22	{SCVYP,SEMABP,SEMBBP}	2,08E-07	5,36E-15	1,07E-14	2,96E-09	0,99999999704
D23	{BSRSOLVYP,SEMABP,SEMBBP}	6,13E-07	1,37E-13	2,73E-13	2,28E-09	0,99999999772
D24	{BSRSHVYP,SEMABP,SEMBBP}	6,21E-07	1,42E-13	2,84E-13	2,37E-09	0,99999999763
D25	{ACCVL,EXLACC,ACCIVBP,ACCIVYP}	1,97E-06	7,50E-16	2,40E-15	1,15E-10	0,99999999988
D26	{SEMAYP,SEMBYP,SEMABP,SEMBBP}	-	1,03E-16	3,30E-16	1,40E-12	0,99999999999
					PFDsif	2,18306E-03

Table 5.9: PFD calculation results for TOP Event D.

Discussion

The calculated PFD_{SIF} for the base case TOP event is approximately $2,80 \cdot 10^{-4}$, i.e. within the SIL 3 requirement specified by IEC 61508 (2010). The PFD_{SIF} for TOP events B and C have also been estimated to $2,80 \cdot 10^{-4}$, while in the open hole situation the PFD_{SIF} is approximately $2,18 \cdot 10^{-3}$, i.e. within the SIL 2 requirement (OLF-070, 2004). Hence, a key finding is that the PFD_{SIF} is largely unaffected by the impact of the different operational situations, except for in the open hole situation, where the PFD becomes significantly higher due to the severely reduced system redundancy from unavailability of the annular BOP functions. In Holand and Skalle (2001), it is stated that the open hole situation was present only in 4.2% of the cases where a kick was detected, while in 85.4% of the cases, all preventers were available. This distribution

of operational situations in which kicks are recorded should be taken into consideration when interpreting the calculation results.

The results indicate the criticality of the components in the control system, such as the hydraulic supply lines, rather than of those specific to each preventer, e.g. solenoid valves, shuttle valves and so forth. Preventer-specific components produce only negligible contributions to the total PFD_{SIF} , and are therefore seemingly insignificant in terms of the system reliability in cases A, B and C. This is also to a certain extent consistent with the results from FTAs performed as part of previous BOP reliability studies (Holand, 1997), (Holand, 1999), (Holand and Skalle, 2001). This is an interesting finding, given that there is currently a tendency in the industry towards wanting to increase the number of rams in the BOP stack as a measure towards increasing the reliability. It could be argued that, based on the findings in the current FTA, and in previous BOP reliability studies, the focus should rather be placed on increasing the redundancy of the control system. The redundancy of functions that are capable of sealing around the drill pipe does not increase the reliability of the system so long as the redundancy in the control system remains so limited.

The results from the calculations clearly illustrate the importance of using conservative PFD approximations, and how these can be achieved by applying the approach by Lundteigen and Rausand (2009). By post-processing the minimal cut sets as opposed to producing the PFD approximations directly from the fault tree software tool, the PFD_{MC_j} of the cut sets consisting of two or more components are significantly increased. It can also be observed that the contribution from CCF gives a substantial increase in the PFD_{MC_j} of the minimal cuts containing one or more common cause components group. It should be noted that this effect may however have been overstated by the use of too conservative beta-factors.

5.1.4 Event tree analysis

Introduction

A fault tree model represents a "static" image of a system in a given condition at a given time, and illustrates the various paths along which the system may reach a failed state through a series of events. A weakness of the fault tree is that it does not take into account the sequence with which these events occur. As such, an event tree can be described as a more "dynamic" method of modeling a system. According to Rausand and Hoyland (2004) ETA is the most commonly used method for analysis of accident progression. It starts with an initiating event, e.g. a subsea well kick, and provides a systematic coverage of the time sequence of event propagation to its potential outcome, e.g. a blowout (Rausand and Hoyland, 2004). In this section, some suggestions are made regarding how ETA can be used to support the reliability analysis of BOP systems.

Event tree analysis of well barrier systems

In order to gain a wider perspective of how the risk picture may develop during the escalation of a well control situation, and the risks associated with different BOP operational situations, ETA can be a useful method. However, in order to establish a model which describes how the sequence of events leading to a loss of well control may take place, it is necessary to take into account systems that are outside of the scope of this master thesis, such as the mud column, the IBOP, and the choke and kill lines, since these are essential to the process of mitigating a well control situation. Since no reliability assessment has been performed for these systems, only a qualitative event tree model for selected operational situations which incorporates these barriers has been developed in order to illustrate how event trees may be used as a possible improvement to reliability assessments of BOP systems and well barrier systems as a whole. Event trees which illustrate the potential escalation of a well control situation into loss of well control for the two operational situations Case B and Case C, in the event that the kick is detected before the hydrocarbons reach the BOP annulus, can be found in Appendix C. The event trees, modified from Lundteigen and Rausand (2011), illustrate the number of paths along which a well control situation may escalate, and also provides an image of the residual risk. The PFD estimates produced from a fault tree analysis may be used as input for quantification of the event tree. However, a wider reliability analysis which also incorporates the other well barrier systems must be performed in order to be able to quantify the event tree in its entirety.

Chapter 6

Summary and Recommendations for Further Work

6.1 Introduction

So far in this report, a typical deepwater drilling BOP system has been described, and analysed both qualitatively and quantitatively using proven methods from the reliability engineering discipline, with the objective of assessing the system's ability to act as a safety barrier in different operational situations. In this final section of the report, a short summary of the previous sections is given, before the conclusions that can be drawn from the thesis work are presented. Finally, a few recommendations are given based on the key findings of the master thesis, along with some suggestions for further work within the area of BOP reliability.

6.2 Summary and conclusions

The failure of the DWH drilling rig's BOP has been pointed to as one of the main causes of the Macondo accident on April 10th 2010. The BOP system is one of the most important safety barriers in a hydrocarbon well. The Macondo accident has created a demand for improved methods of assessing the reliability of BOP systems. The objective of this master thesis has been to propose improvements to current reliability assessment methods for complex safety critical systems such as the BOP.

In Chapter 2 of this report, a typical subsea drilling BOP system designed for deepwater application has been presented, with a description of its main components and functions. The BOP

has been classified as a safety barrier in light of the terminology in D-010 (2004). Furthermore, a functional analysis of the BOP system has been performed, where an overall system SIF and three essential BOP sealing functions have been specified. Methods for classifying BOP functions, and assigning them with performance criteria have also been proposed. Chapter 2 has also discussed different operational situations that the BOP system is exposed to during the course of a typical exploration drilling program, whose characteristics have implications for the system's ability to act as a safety barrier. The pros and cons of different widely used BOP system configurations have also been discussed. Three main types of configurations have been considered in this report; the "modern" configuration, the "traditional" configuration and the DWH BOP system configuration.

Chapter 3 has documented a literature survey on previous BOP reliability studies performed by Per Holand on behalf of SINTEF. An evaluation of the validity of the operational assumptions which have been made in these previous studies have been provided, such as assumptions regarding operational situations, failure input data, and several important assumptions regarding testing of BOP systems. Regulations and guidelines which are relevant to BOP reliability have also been described in Chapter 3.

In Chapter 4, the report has discussed how the BOP may fail, and which types of failure modes are considered critical from a safety perspective. Some theoretic principles behind common cause failures have been presented, along with a description of how common cause failures should be included in reliability assessments of safety critical systems through an approach called the *PDS approach*. In the final section of Chapter 3, possible sources for common cause failures in the BOP system have been commented on.

As a suggestion towards how reliability assessments of BOPs can be improved, and some of the identified challenges solved, a reliability quantification method has been presented in Chapter 5. The method is based on post-processing of minimal cut sets from an FTA of the BOP system, and produces more conservative and accurate approximations of the reliability than those produced through conventional methods. The method is also capable of taking into account common cause failures. The results from the calculations have been presented and discussed.

Event trees which illustrate the escalation of a well kick in two different operational situations have also been presented in Chapter 5, along with a discussion of how event tree analysis may be used to improve the quality of BOP reliability assessments and well barrier reliability in general.

The main conclusions from this master thesis can be summarized by three key findings. One is that the approach based on fault trees and post-processing of minimal cut sets which has been applied to the BOP system, improves the quality of BOP reliability estimates, and also provides a

sound platform for including common cause failures in the analysis. Another key finding is that the failure modes in control system components contribute by far the majority of unreliability in the BOP system, since it has been shown that the unavailability of certain BOP functions due to operational conditions has little or no implication on the reliability estimates produced. The third key finding is that a test coverage factor should be introduced when calculating the PFD of the shearing BOP functions to account for the proportion of failures that cannot be revealed by shear ram function tests.

6.3 Recommendations and ideas for further work

It is recommended that a test coverage factor be included when calculating the reliability of shearing rams, since these cannot be fully function tested through conventional, non-destructive BOP function tests. It is also recommended that the industry investigate the accuracy with which the location of tool joints in the wellbore annulus can be determined through current methods.

To further improve the reliability of well barrier systems, it is also suggested that the industry investigate possible gains from modeling well control situations through event trees that are not limited to the BOP system, but which incorporate all of the well barrier systems involved in the mitigation of well control situations. The author would also be very interested in helping with the development of future master thesis assignments within the area of BOP reliability.

References

American Petroleum Institute (2012). *API Drill Pipe and Tool Joint Combinations*.

BP (2010). *Deepwater Horizon Investigation Report - Appendix H - Description of the BOP Stack and Control System*.

Committee for Analysis of Causes of the Deepwater Horizon Explosion Fire and Oil Spill to Identify Measures to Prevent Similar Accidents to the Future (2011). *Macondo Well-Deepwater Horizon Blowout: Lessons for Offshore Drilling Safety*.

D-010, N. S. (2004). *Well integrity in drilling and well operations*.

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.

Exprosoft AS (2008). CARA FaultTree Version 4.2.

Hauge, S., Haabrekke, S., and Lundteigen, M. A. (2010). *Reliability Prediction Method for Safety Instrumented Safety Instrumented Systems - PDS Example Collection, 2010 Edition*.

Hauge, S. and Onshus, T. (2010a). *Reliability Data for Safety Instrumented Systems - PDS Data Handbook - 2010 Edition*.

Hauge, S. and Onshus, T. (2010b). *Reliability Prediction Method for Safety Instrumented Systems. PDS Method Handbook, 2010 Edition*.

Hokstad, P. and Rausand, M. (2008). Common Cause Failure Modeling: Status and Trends.

Holand, P. (1985). Reliability of Subsea BOP Systems - Phase II - Main Report. Technical report, SINTEF: Division of Safety and Reliability.

Holand, P. (1986). Reliability of Subsea BOP Systems - Phase III - Testing and Maintenance - Main Report. Technical report, SINTEF: Division of Safety and Reliability.

Holand, P. (1991). Subsea Blowout Preventer Systems - Reliability and Testing. Technical report, SINTEF: Division of Safety and Reliability.

- Holand, P. (1997). Reliability of Subsea BOP System for Deepwater Application. Technical report, SINTEF: Division of Safety and Reliability.
- Holand, P. (1999). Reliability of Subsea BOP Systems for Deepwater Application - Phase II DW. Technical report, SINTEF: Division of Safety and Reliability.
- Holand, P. and Skalle, P. (2001). Deepwater Kicks and BOP Performance. Technical report, SINTEF: Division of Safety and Reliability.
- IEC 61508 (2010). *Functional safety*. International Electrotechnical Commission.
- IEC 61511 (2004). *Functional safety - Safety instrumented systems for the process industry sector*. International Electrotechnical Commission.
- Lundteigen, M. A. (2009). *Safety instrumented systems in the oil and gas industry*. PhD thesis, NTNU.
- 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.
- 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.
- Lundteigen, M. A. and Rausand, M. (2011). *Reliability of BOP*.
- NASA (2002a). *Fault Tree Handbook with Aerospace Applications*.
- NASA (2002b). *Probabilistic risk assessment procedures guide for NASA managers and practitioners*.
- OLF-070 (2004). *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry*.
- Rausand, M. and Hoyland, A. (2004). *System Reliability Theory - Models, Statistical Methods, and Applications - Second Edition*. Wiley.
- Schlumberger. Schlumberger Oilfield Glossary.
- Sklet, S. (2006). Safety Barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*.
- Transocean (2011). *Macondo Well Incident Report - Transocean Investigation Report - Volume I*.
- West Engineering Services (2004). *Shear Ram Capabilities Study*.

Appendices

Appendix A

Acronyms

BOEMRE Bureau of Ocean Energy Management Regulation and Enforcement

BOP Blowout preventer

BSR Blind shear ram

CCF Common cause failures

CCU Central control unit

CG Common cause component group

CSR Casing shear ram

CSU Critical safety unavailability

DCP Driller's control panel

DU Dangerous undetected

DWH Deepwater Horizon

DNV Det Norske Veritas

ETA Event tree analysis

FMEA Failure modes and effects analysis

FMECA Failure modes, effects and criticality analysis

FTA Fault tree analysis

HAZID Hazard identification

HAZOP Hazard and operability study

HPU Hydraulic power unit

IEC International Electrotechnical Committee

LAP Lower annular preventer

LPR Lower pipe ram

LMRP Lower marine riser package

MC Minimal cut set (minimal cut)

MFDT Mean fractional dead time

MooN M-out-of-N

MPR Middle pipe ram

MUX Multiplexed

NPD Norwegian Petroleum Directorate

NSNS Norwegian Sector of the North Sea

OLF Oljeindustriens Landsforening (Norwegian Oil Industry Association)

O.D. Outer diameter

PDF Probability of failure on demand

PFH Probability of dangerous failure per hour

PLC Programmable logic solver

PSA Petroleum Safety Authority

RAMS Reliability, availability, maintainability, and safety

RBD Reliability block diagram

SCV Surface control valve

SEM Subsea electronic module

SIF Safety instrumented function

SIL Safety integrity level

SIS Safety instrumented system

TCP Toolpusher's control panel

TIF Test independent failure

UAP Upper annular preventer

UPR Upper pipe ram

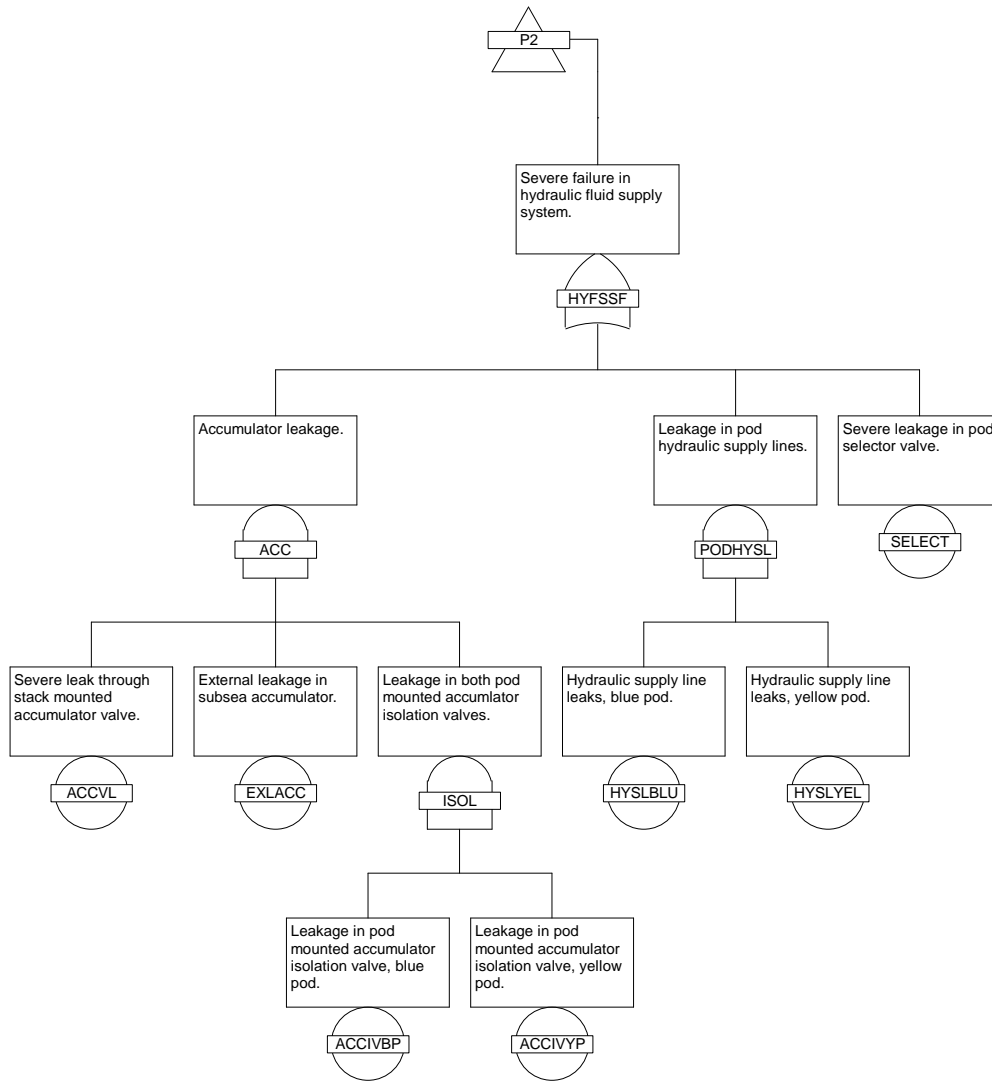
US GoM OCS United States Gulf of Mexico Outer Continental Shelf

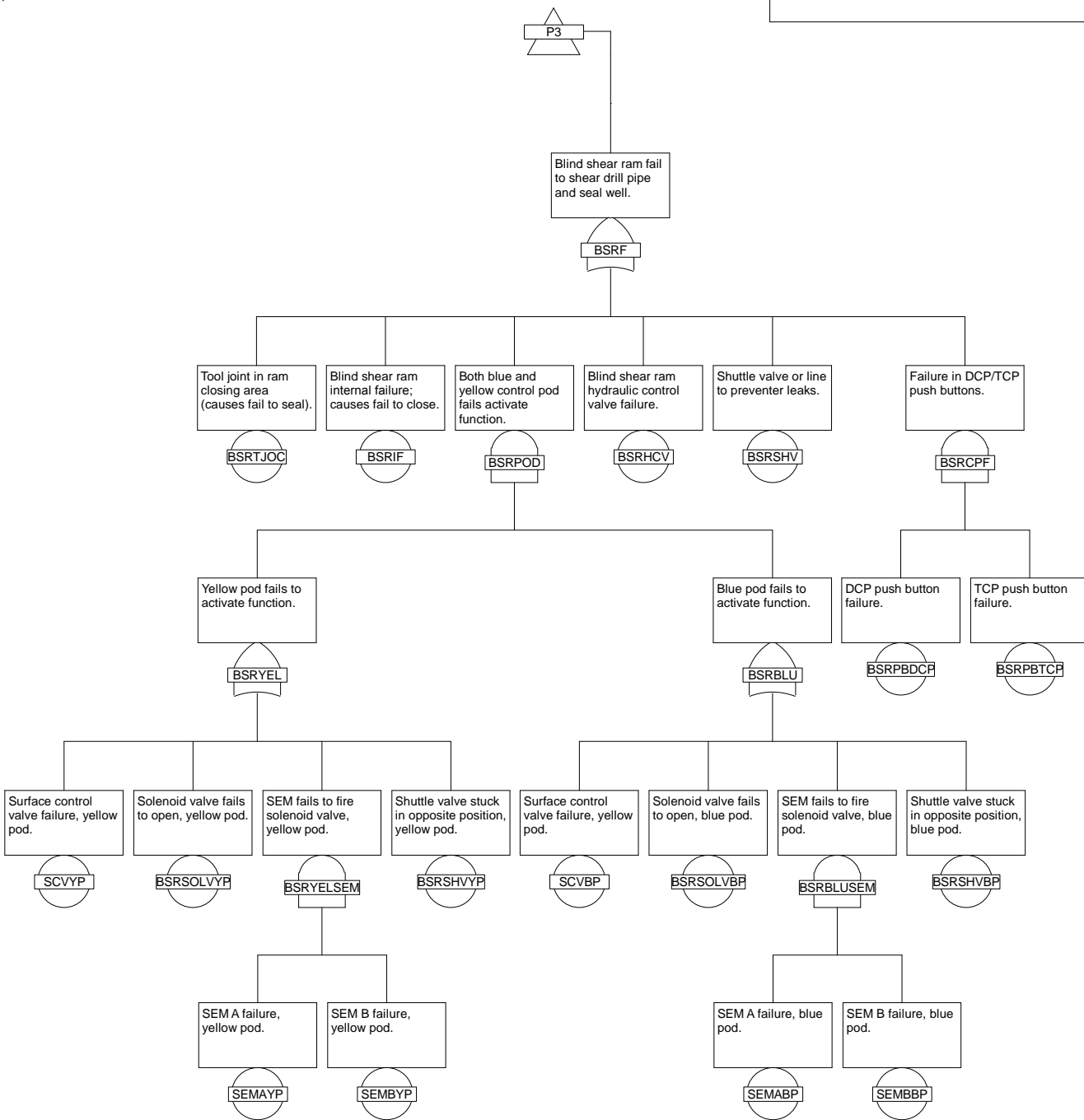
VBR Variable bore ram

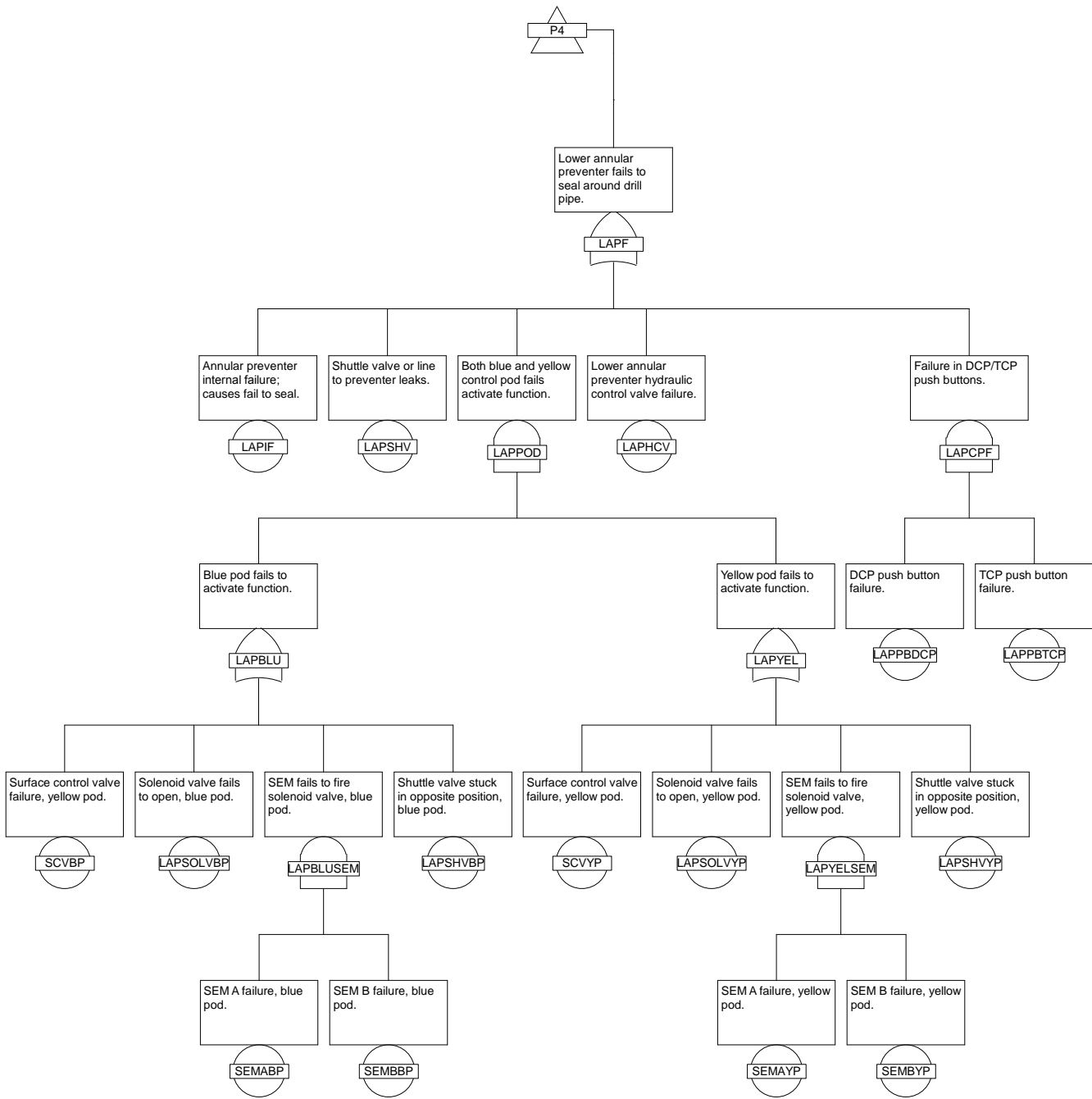
Appendix B

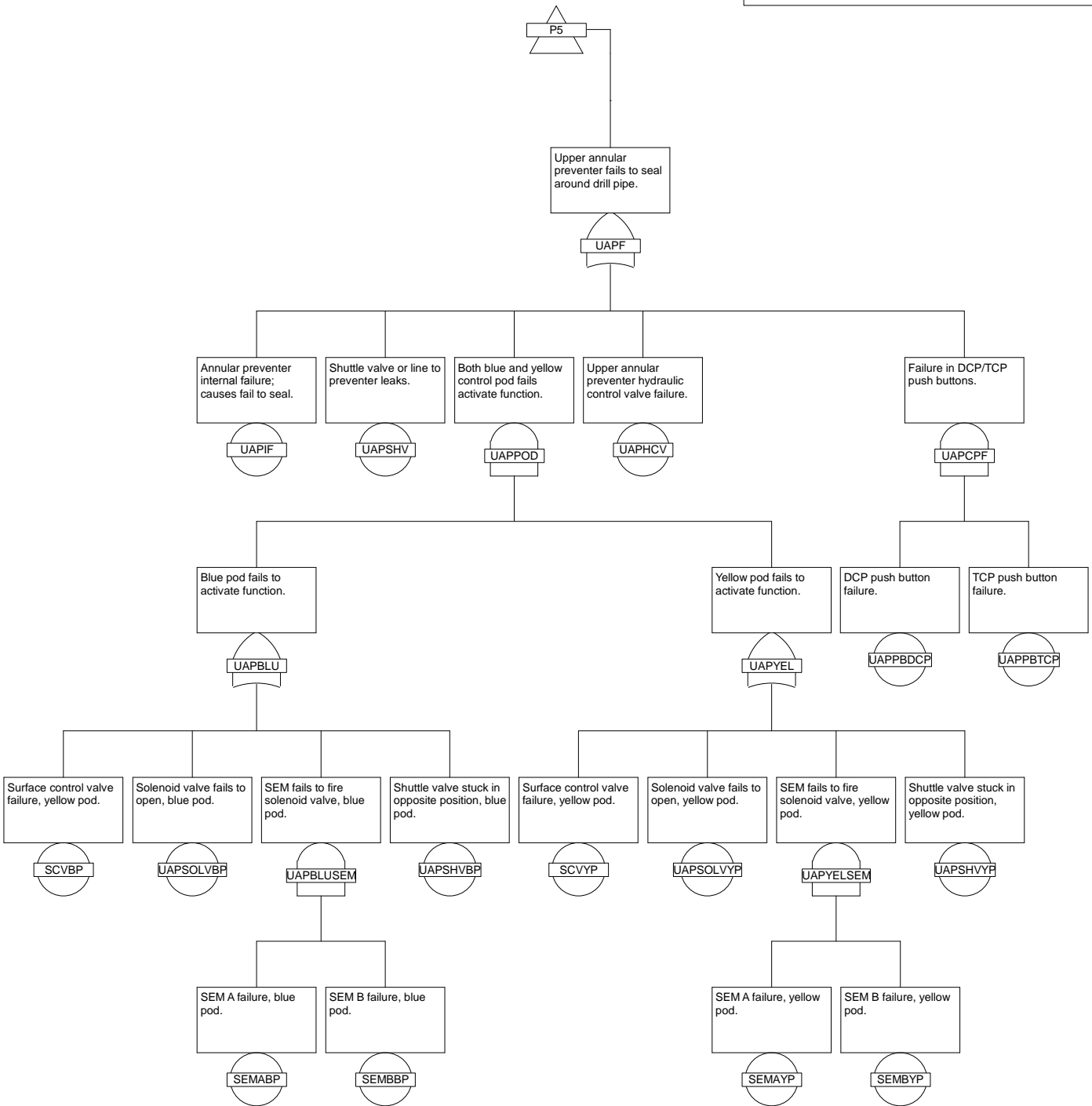
Fault Tree Analysis

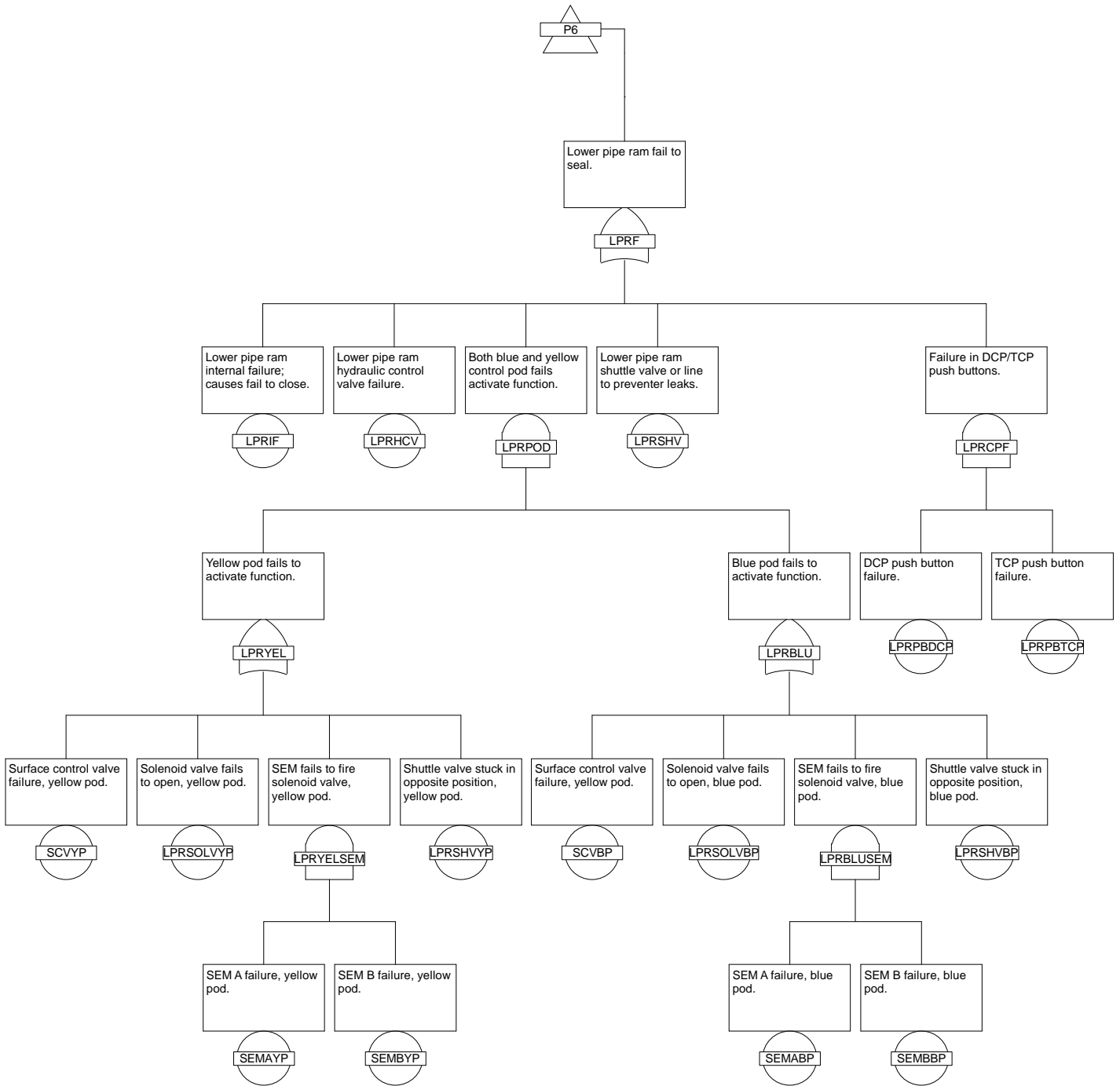
B.1 Fault trees

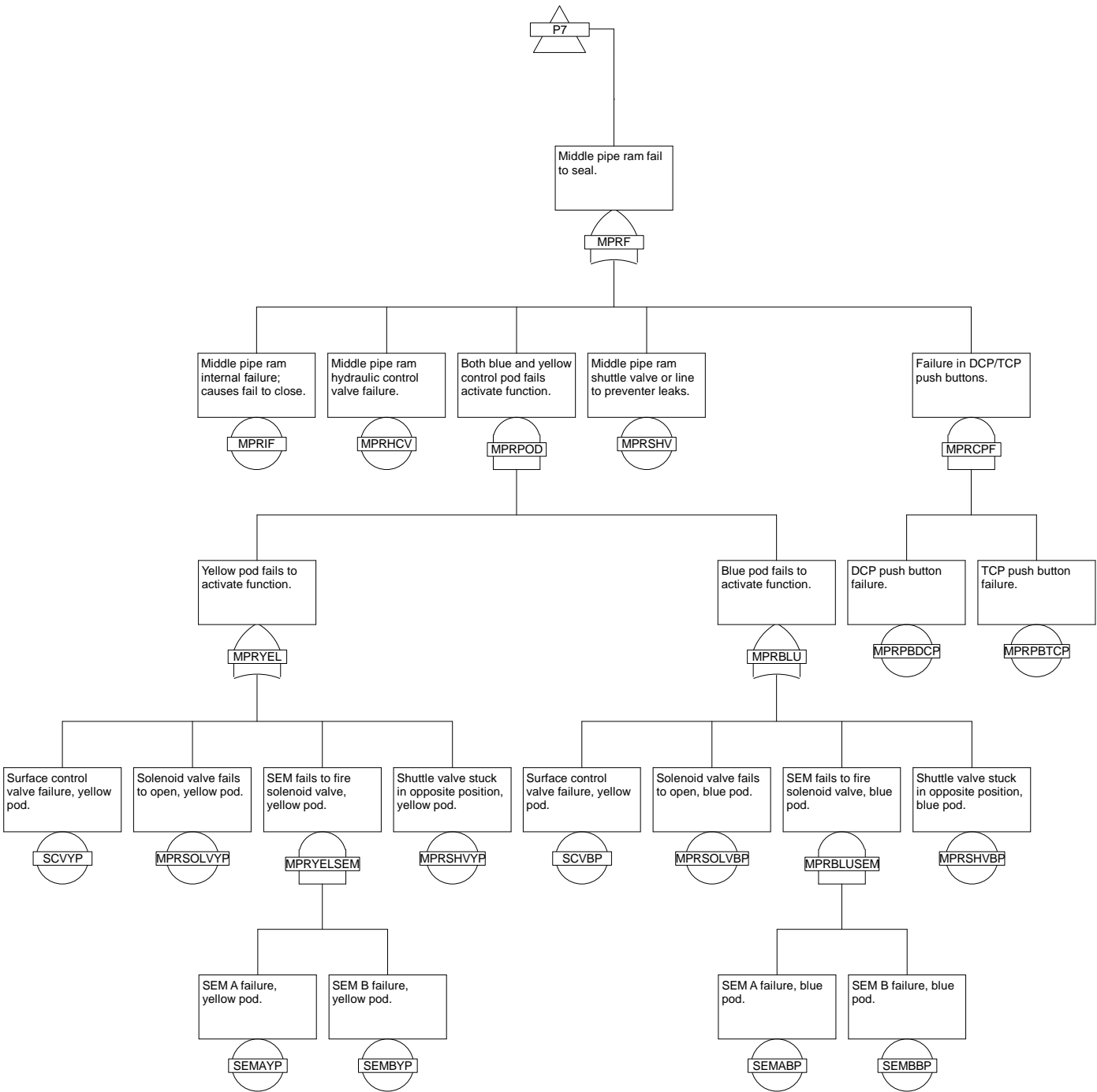


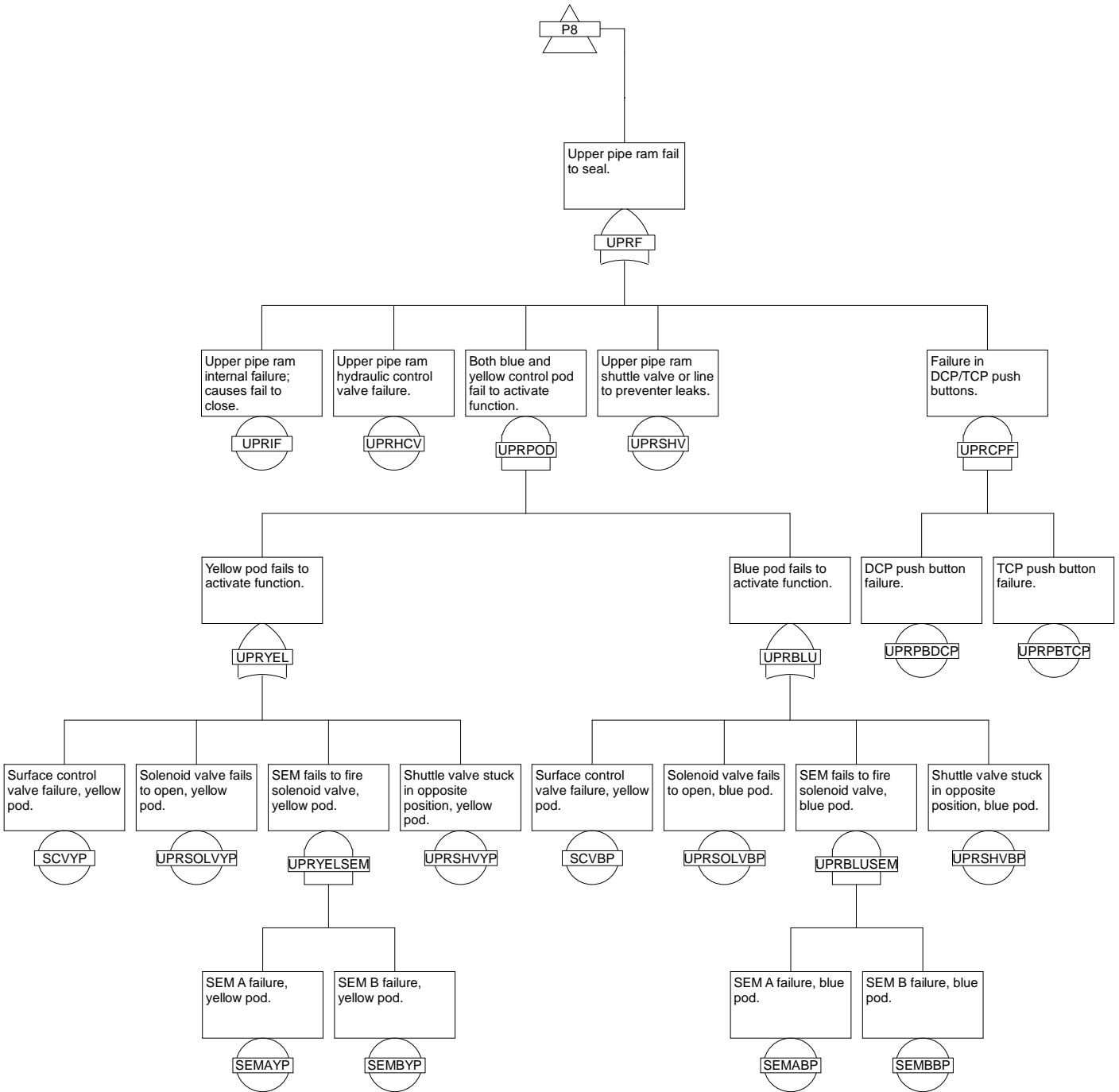


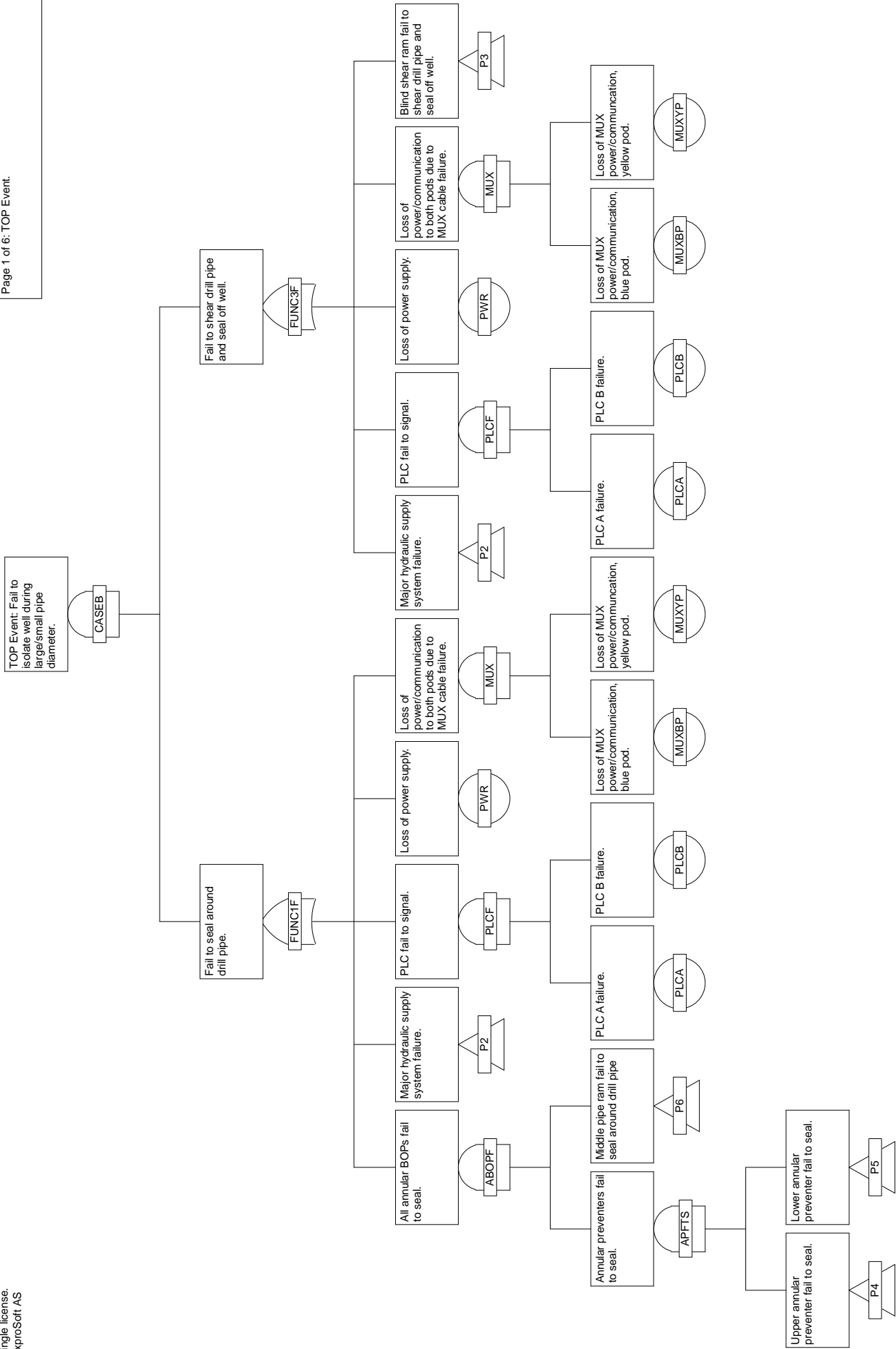


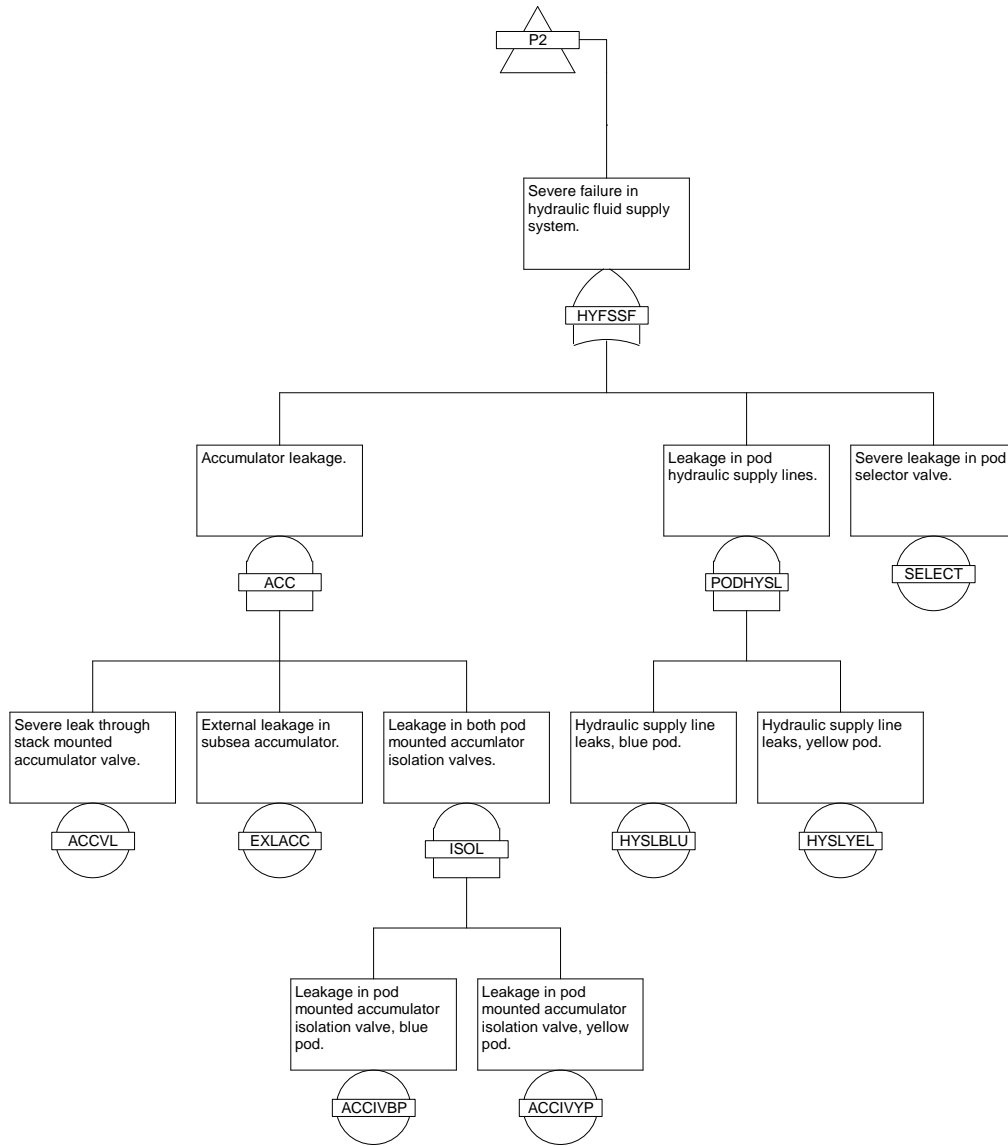


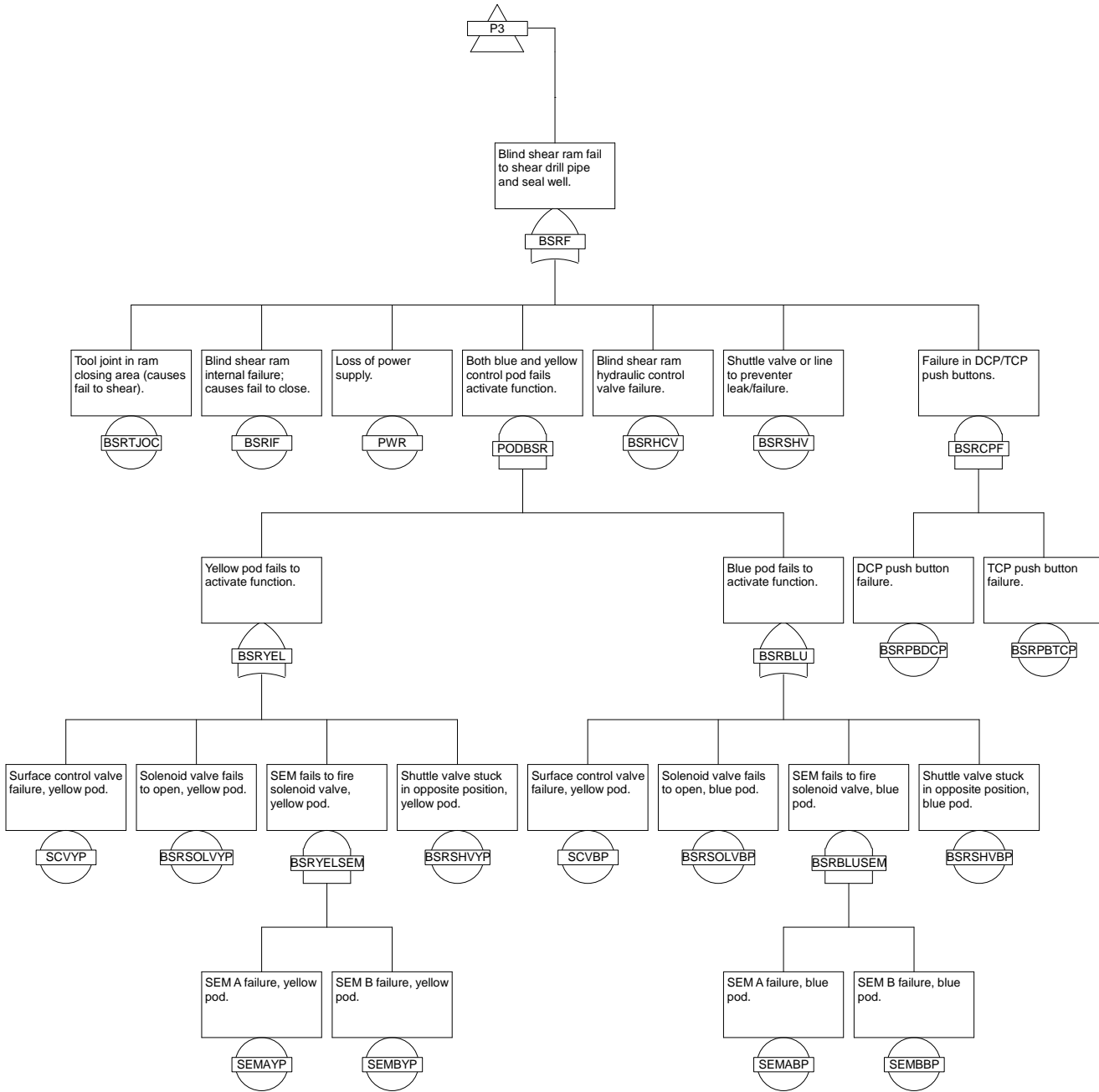


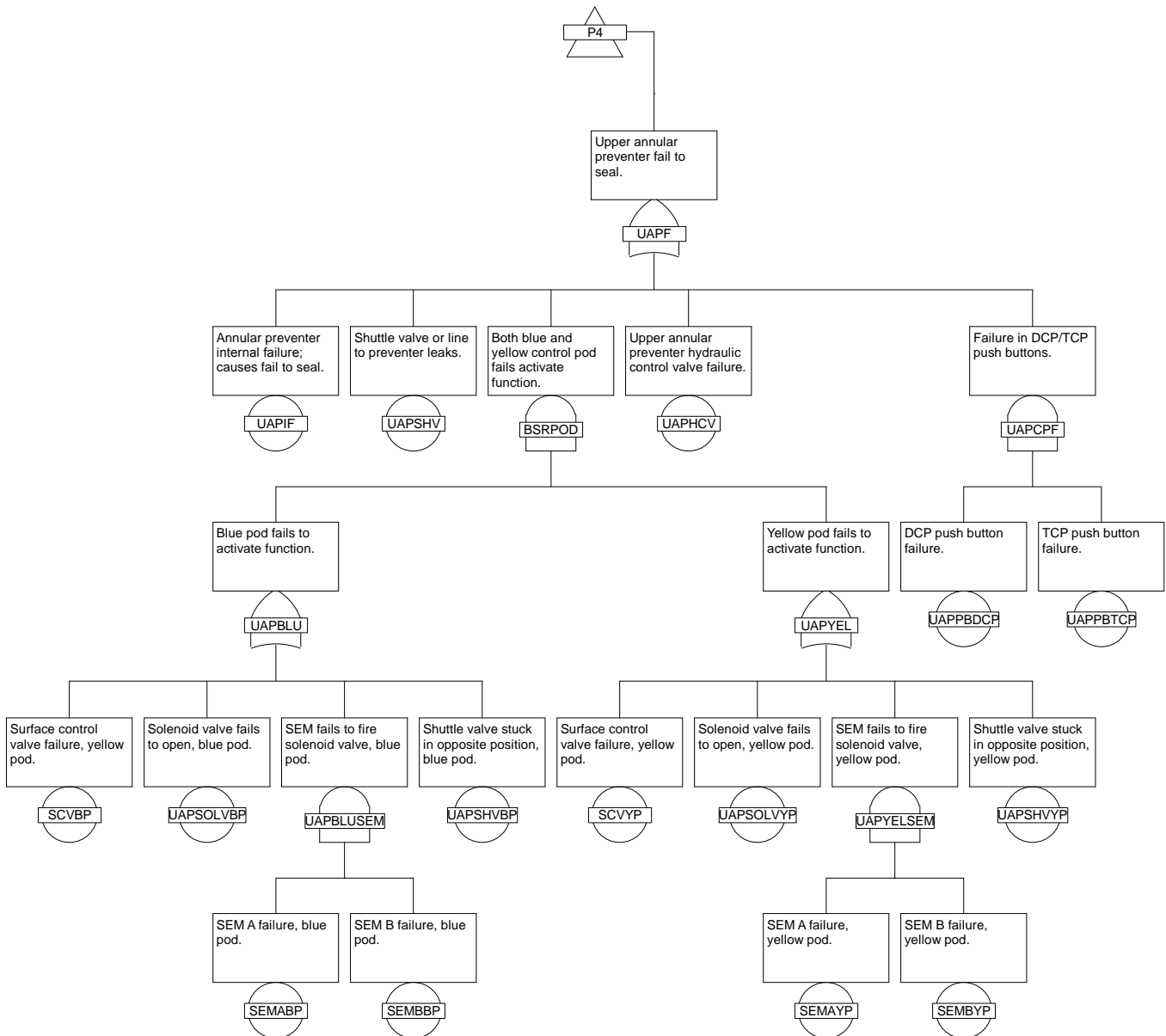


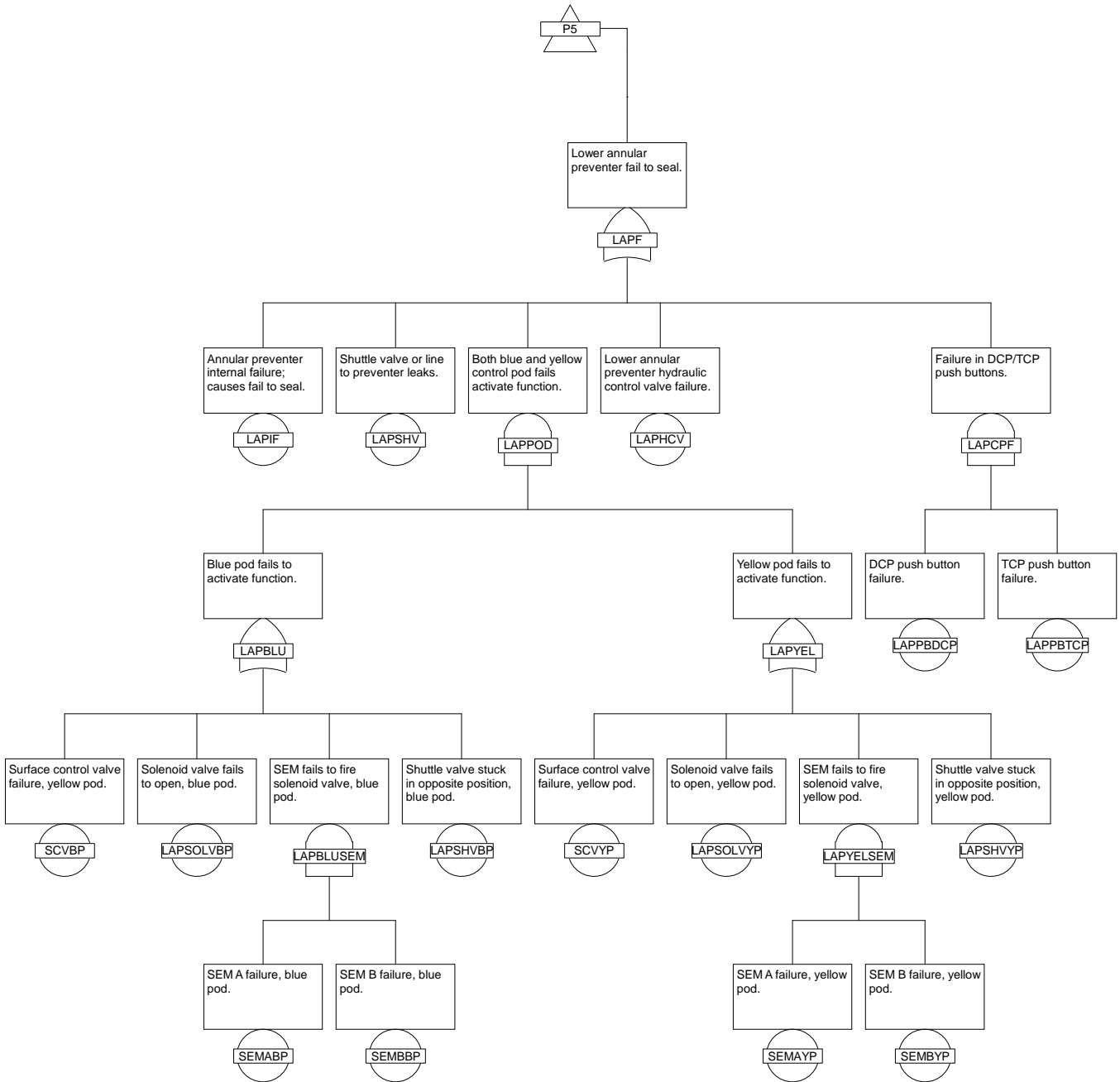


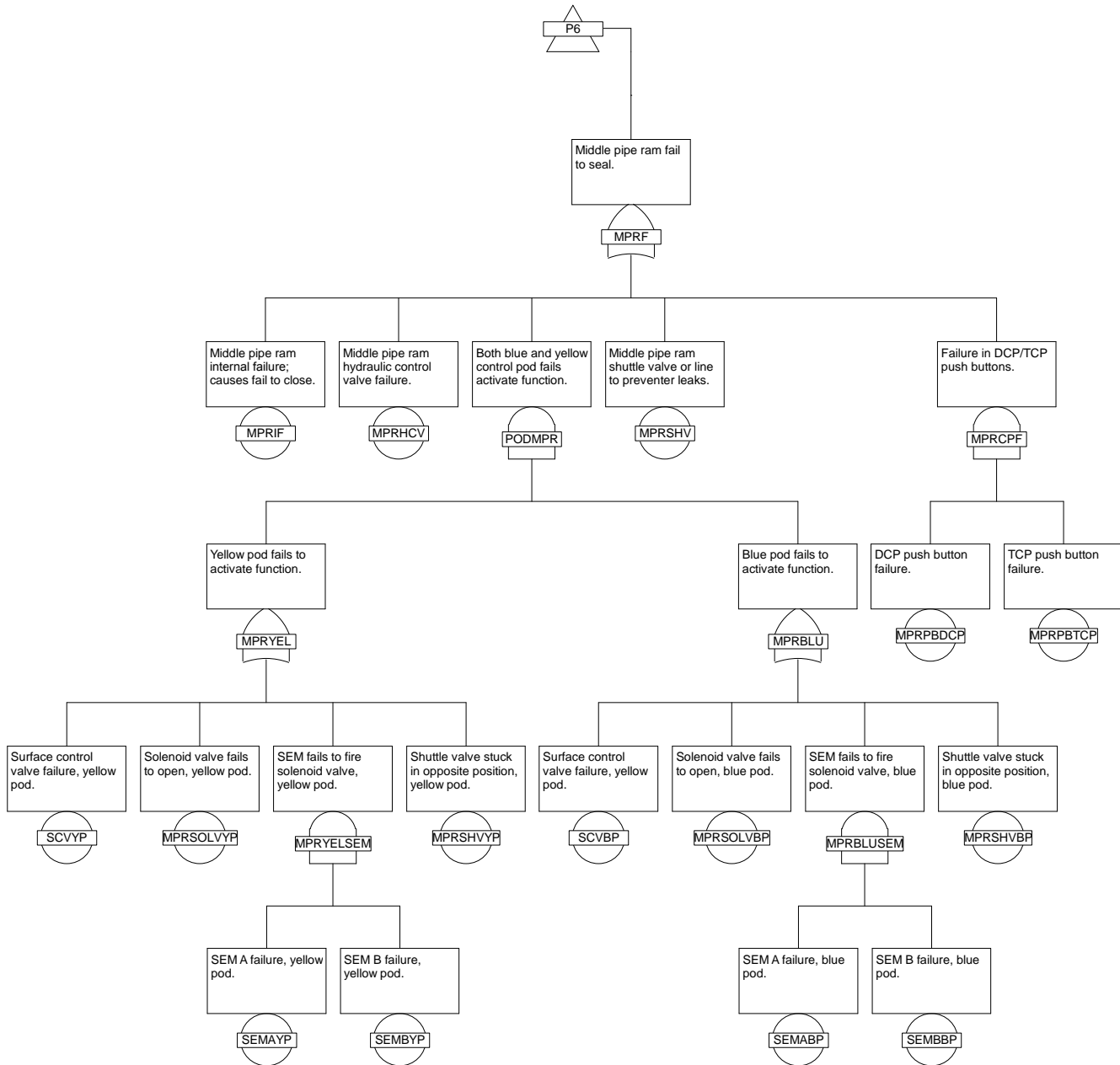


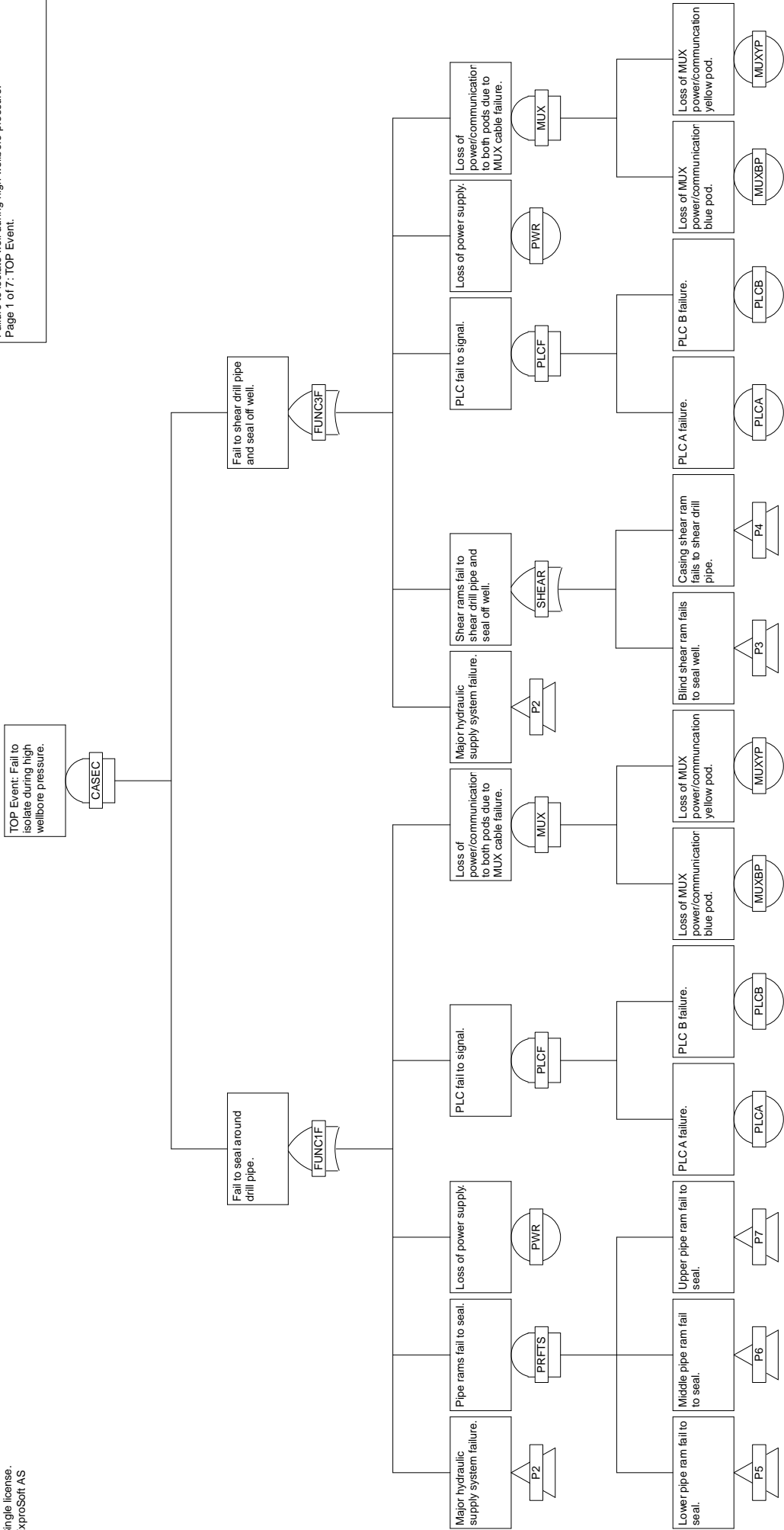


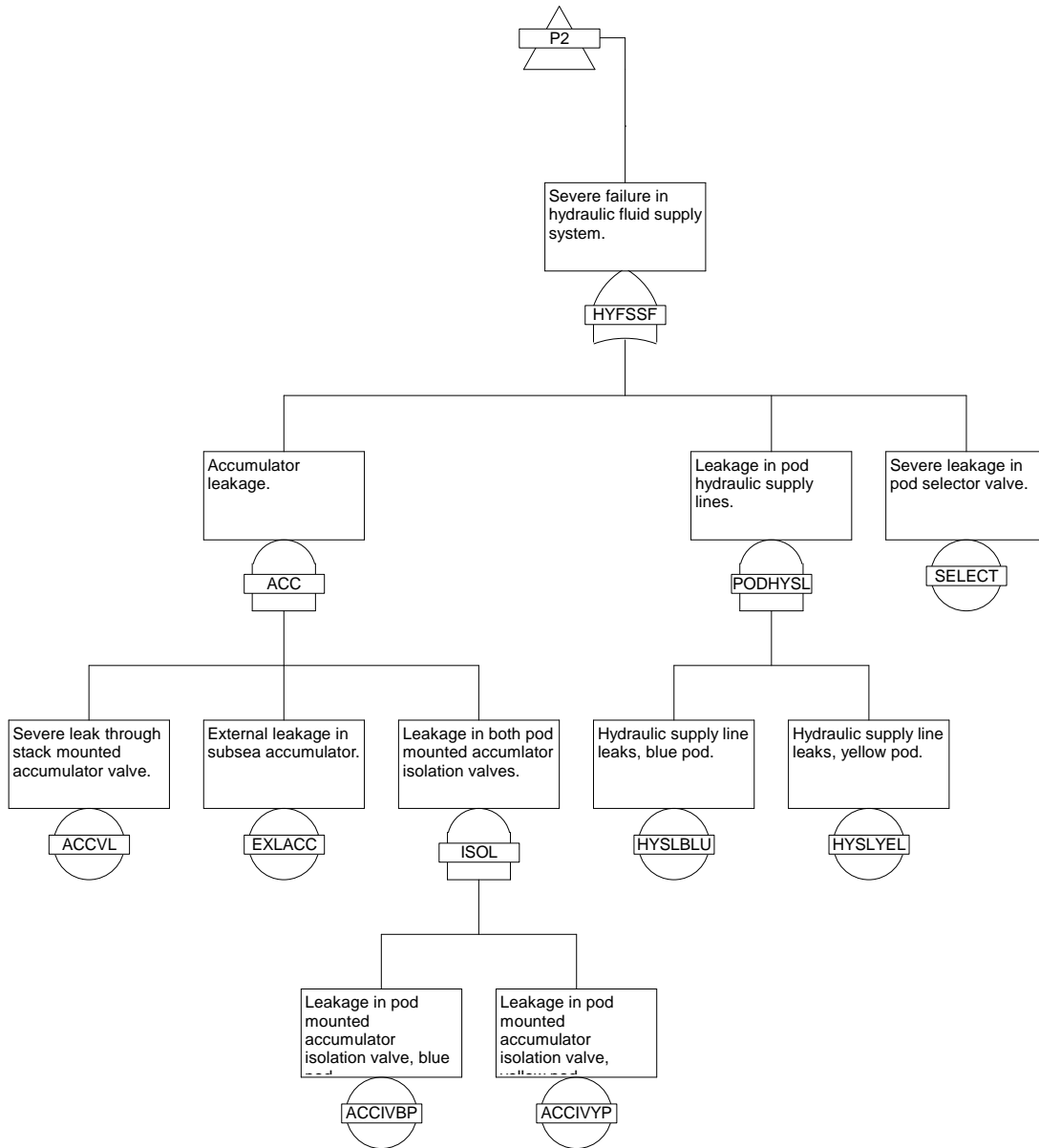


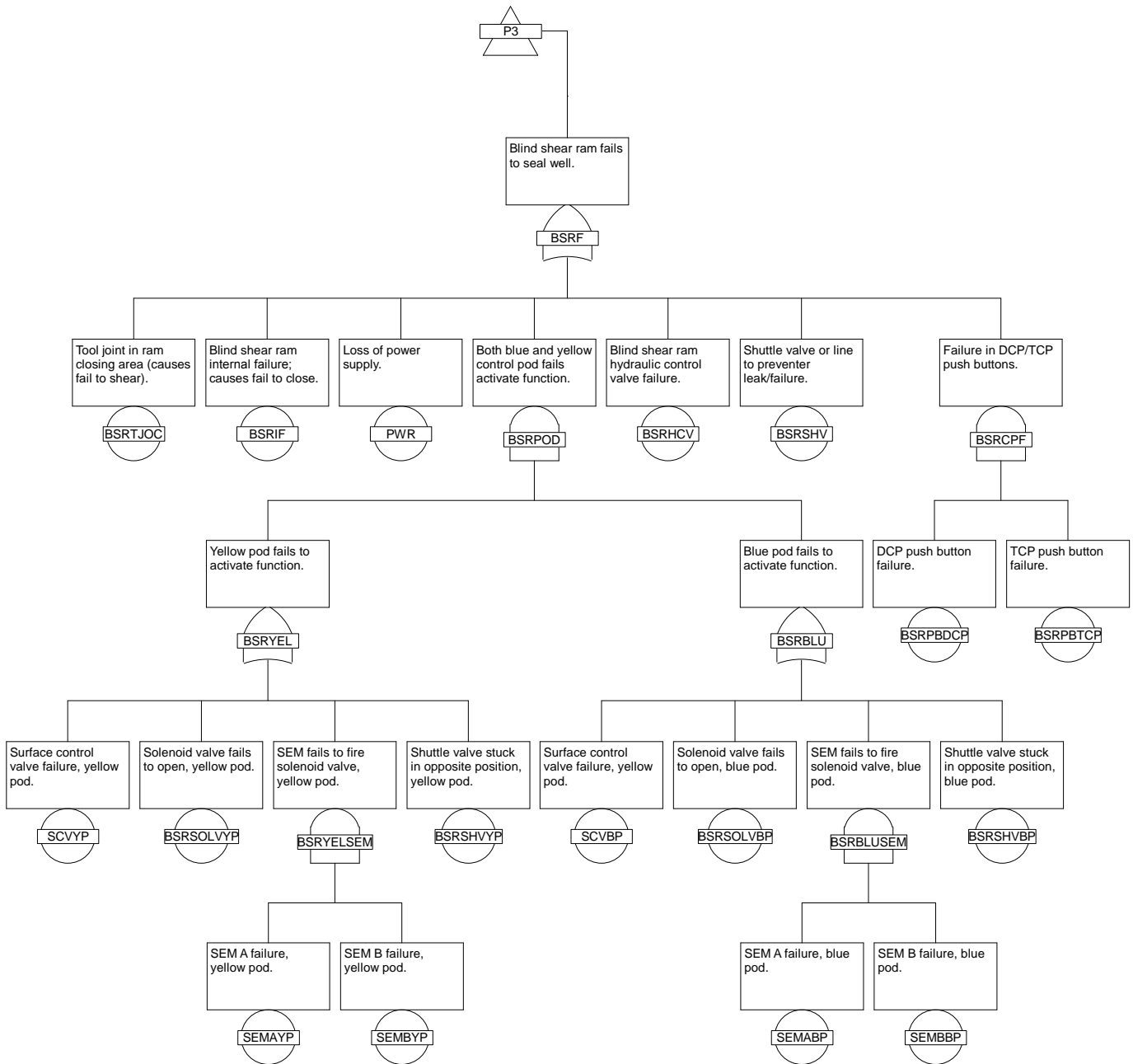


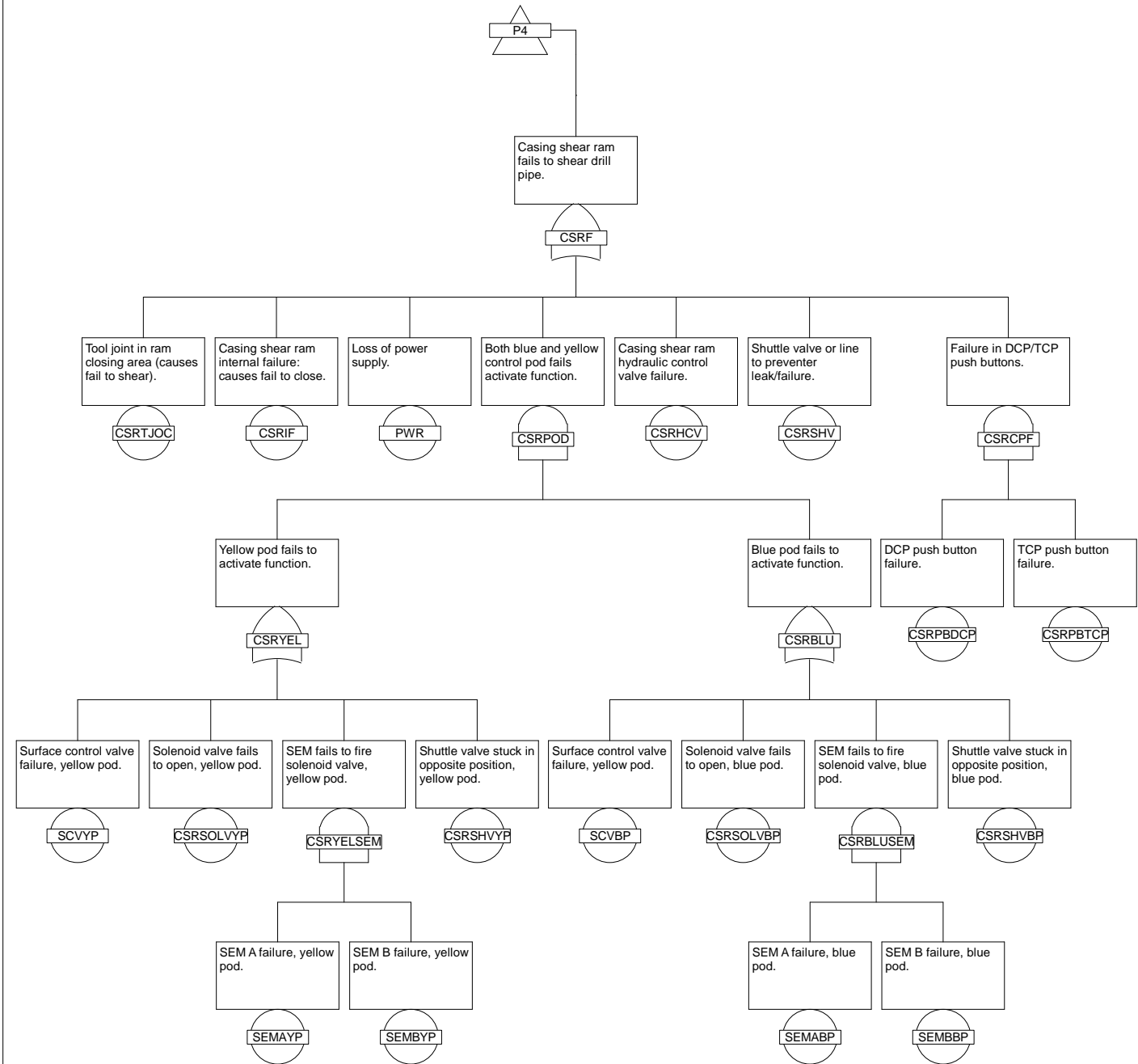


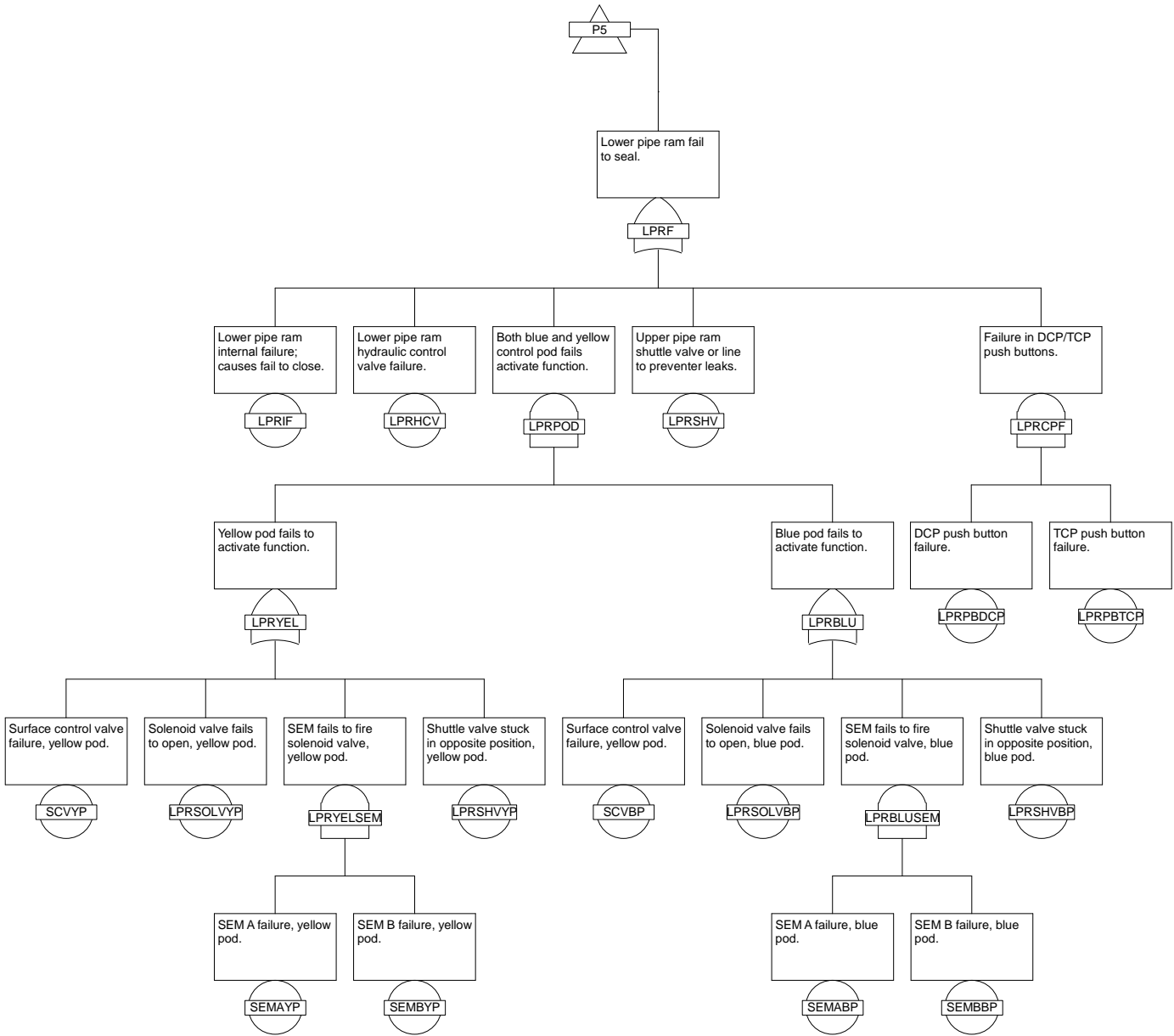


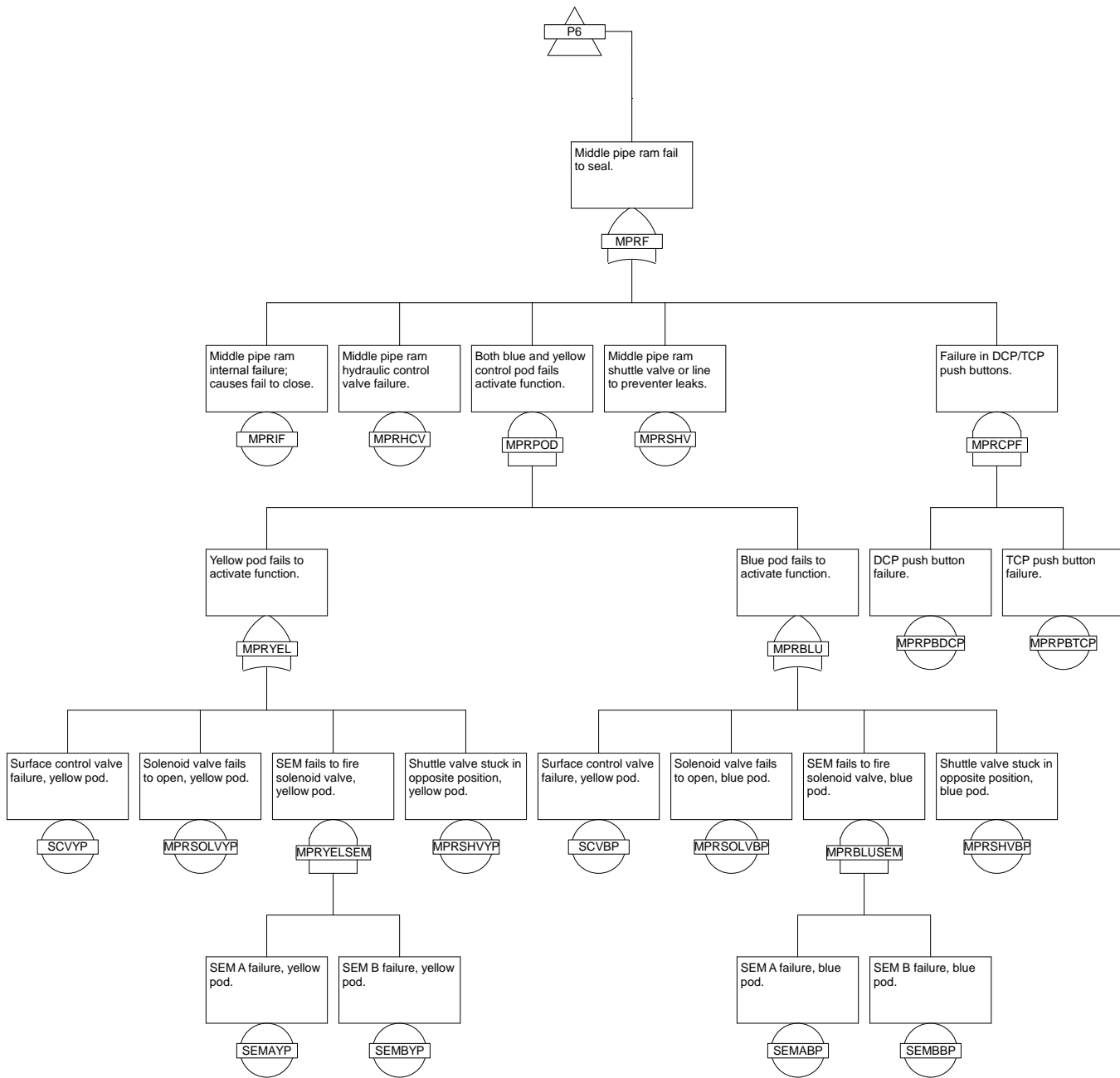


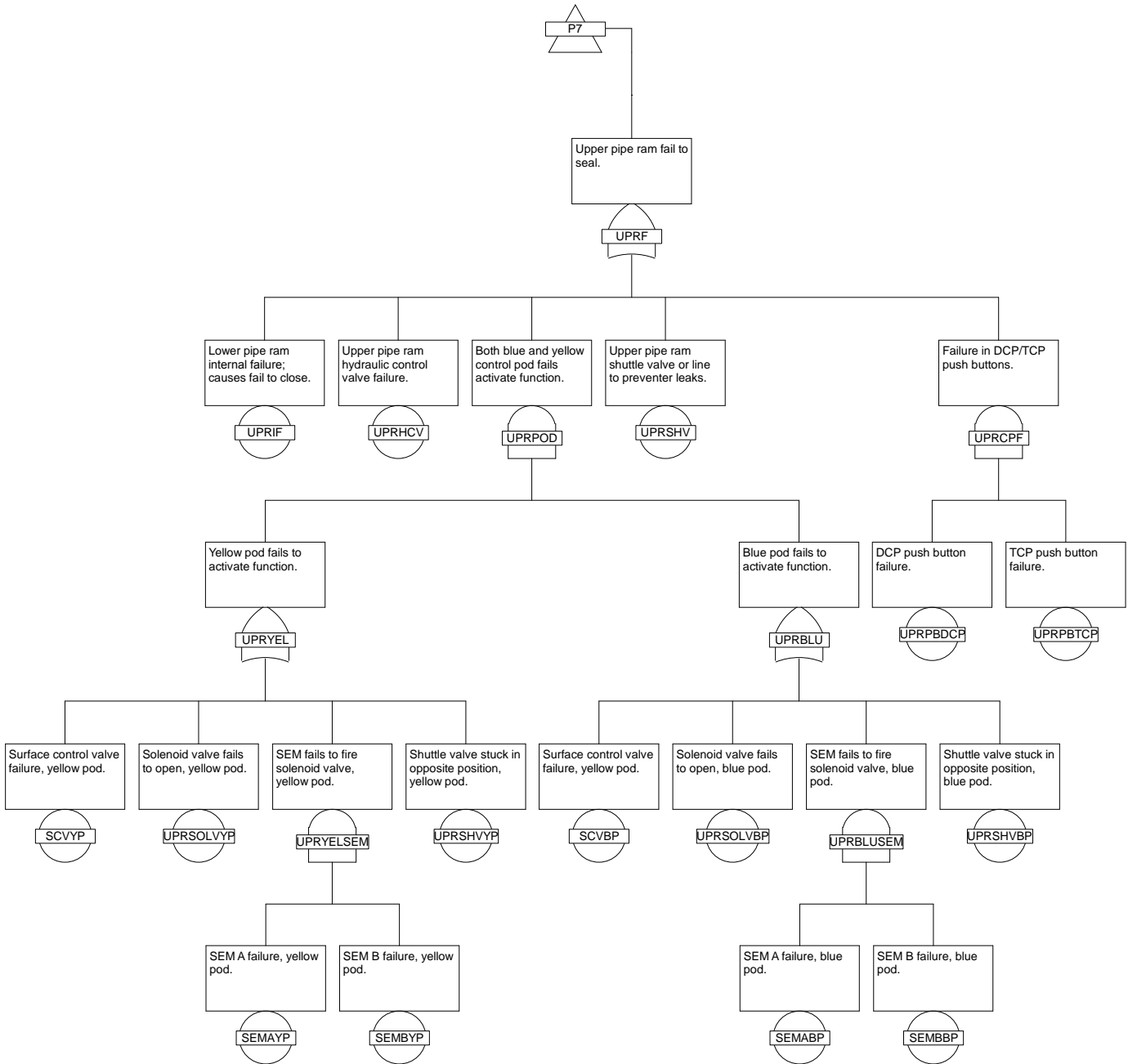


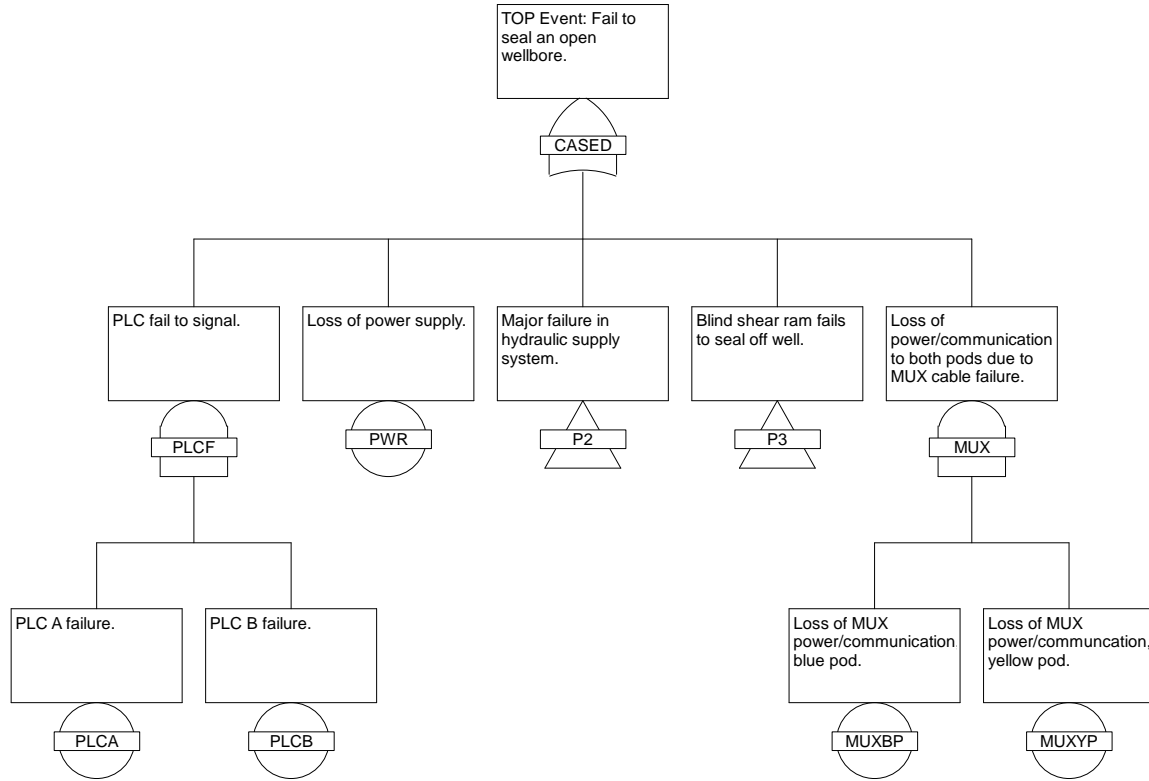


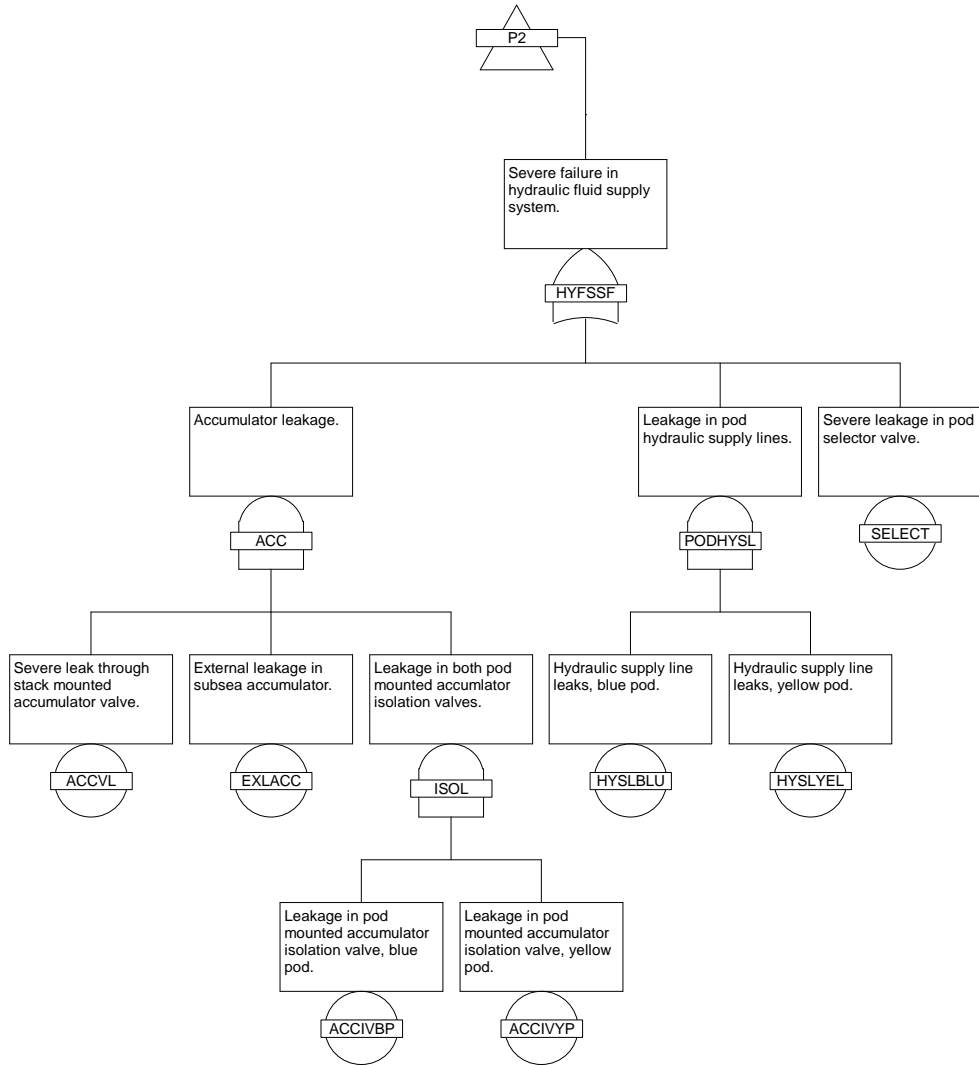


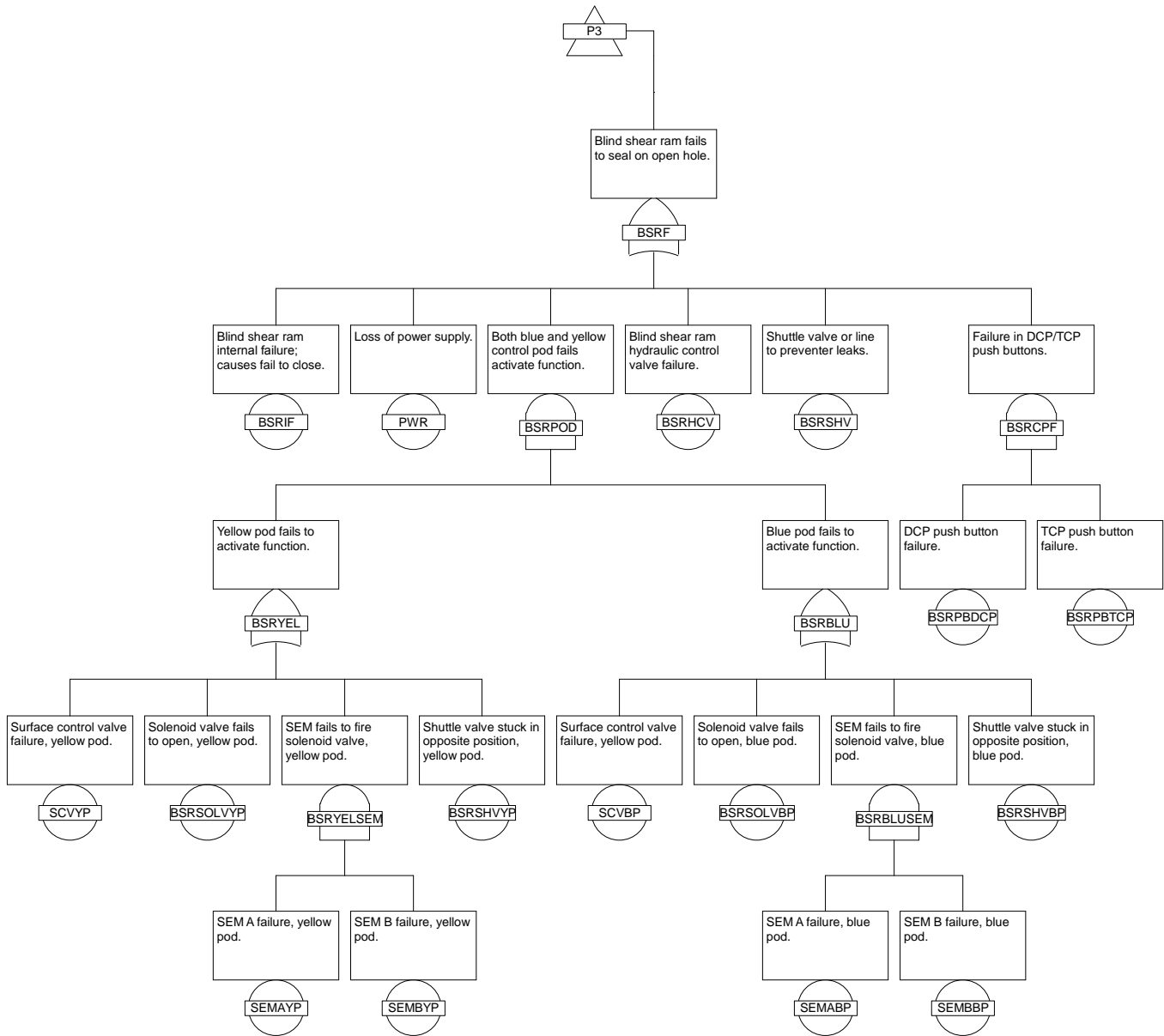












B.2 Fault tree basic events

The basic events of each fault tree are listed on the following pages. The failure rates marked with purple color have been derived from Holand (1997). Those failure rates marked with blue color have been derived from Hauge and Onshus (2010a), while those marked with yellow color are guesstimates. Finally, the failure rate of shear rams due to tool joint obstruction is marked with green.

TOP EVENT A

Basic events	Failure mode description	Related component(s)/subsystem(s)	Failure rate per 10 ⁶ h
SELECT	Severe leakage in pod selector valve.	Pod selector valve	2,083E-07
PWR	Loss of power supply	Central Control Unit (CCU)	1,000E-07
SCVFBP	Surface control valve failure, blue pod.	Surface control valve, blue pod.	2,083E-07
SCVFYP	Surface control valve failure, yellow pod.	Surface control valve, yellow pod.	2,083E-07
HYSLBLU	Hydraulic supply line leaks, blue pod.	Hydraulic fluid supply line, blue pod.	2,917E-05
HYSLYEL	Hydraulic supply line leaks, yellow pod.	Hydraulic fluid supply line, yellow pod.	2,917E-05
PLC A	PLC A failure.	PLC A	7,000E-07
PLC B	PLC B failure.	PLC B	7,000E-07
MUXBP	Loss of MUX power/communication, blue pod.	MUX cables/reels, blue pod.	4,000E-08
MUXYP	Loss of MUX power/communication, yellow pod.	MUX cables/reels, yellow pod.	4,000E-08
SEMABP	SEM A failure, blue pod.	SEM A, blue pod.	1,200E-06
SEMBBP	SEM B failure, blue pod.	SEM B, blue pod.	1,200E-06
SEMAYP	SEM A failure, yellow pod.	SEM A, yellow pod.	1,200E-06
SEMBYP	SEM B failure, yellow pod.	SEM B, yellow pod.	1,200E-06
BSRTJOC	Tool joint in ram closing area; causes fail to shear.	Blind shear ram.	4,200E-02
ACCVL	Severe leak through stack mounted acc. isol. valve.	Stack mounted acc. isol. valve.	2,083E-07
EXLACC	External leakage in subsea accumulator.	Subsea accumulator bottles.	1,667E-05
ACCIVBP	Leakage in pod mounted acc. isol. valve, blue pod.	Pod mounted acc. isol. valve, blue pod.	2,083E-06
ACCIVYP	Leakage in pod mounted acc. isol. valve, yellow pod.	Pod mounted acc. isol. valve, yellow pod.	2,083E-06
BSRPBDCP	BSR push button fails, DCP.	BSR push button, DCP	4,000E-07
BSRPBTCP	BSR push button fails, TCP.	BSR push button, TCP.	4,000E-07
UAPPBDCP	UAP push button fails, DCP.	UAP push button, DCP.	4,000E-07
UAPPBTCP	UAP push button fails, TCP.	UAP push button, TCP.	4,000E-07
LAPPBDCP	LAP push button fails, DCP.	LAP push button, DCP.	4,000E-07
LAPPBTCP	LAP push button fails, TCP.	LAP push button, TCP.	4,000E-07
LPRPBDCP	LPR push button fails, DCP.	LPR push button, DCP.	4,000E-07
LPRPBTCP	LPR push button fails, TCP.	LPR push button, TCP.	4,000E-07
MPRPBDCP	MPR push button fails, DCP.	MPR push button, DCP.	4,000E-07
MPRPBTCP	MPR push button fails, TCP.	MPR push button, TCP.	4,000E-07
UPRPBDCP	UPR push button fails, DCP.	UPR push button, DCP.	4,000E-07
UPRPBTCP	UPR push button fails, TCP.	UPR push button, TCP.	4,000E-07
BSRIF	BSR internal failure; causes fail to close.	BSR.	2,229E-05
LAPIF	LAP internal failure; causes fail to close.	LAP	1,063E-05
UAPIF	UAP internal failure; causes fail to close	UAP.	1,063E-05
LPRIF	LPR internal failure; causes fail to close.	LPR (fixed).	3,542E-06
MPRIF	MPR internal failure; causes fail to close.	MPR (VBR)	3,542E-06
UPRIF	UPR internal failure; causes fail to close.	UPR (fixed).	3,542E-06
BSRSOLVBP	BSR solenoid valve fails to open, blue pod.	BSR solenoid valve, blue pod.	1,600E-07
BSRSOLVYP	BSR solenoid valve fails to open, yellow pod.	BSR solenoid valve, yellow pod.	1,600E-07
LAPSOLVBP	LAP solenoid valve fails to open, blue pod.	LAP solenoid valve, blue pod.	1,600E-07
LAPSOLVYP	LAP solenoid valve fails to open, yellow pod.	LAP solenoid valve, yellow pod.	1,600E-07
UAPSOLVBP	UAP solenoid valve fails to open, blue pod.	UAP solenoid valve, blue pod.	1,600E-07
UAPSOLVYP	UAP solenoid valve fails to open, yellow pod.	UAP solenoid valve, yellow pod.	1,600E-07
LPRSOLVBP	LPR solenoid valve fails to open, blue pod.	LAP solenoid valve, blue pod.	1,600E-07
LPRSOLVYP	LPR solenoid valve fails to open, yellow pod.	LAP solenoid valve, yellow pod.	1,600E-07
MPRSOLVBP	MPR solenoid valve fails to open, blue pod.	MPR solenoid valve, blue pod.	1,600E-07
MPRSOLVYP	MPR solenoid valve fails to open, yellow pod.	MPR solenoid valve, yellow pod.	1,600E-07
UPRSOLVBP	UPR solenoid valve fails to open, blue pod.	UPR solenoid valve, blue pod.	1,600E-07
UPRSOLVYP	UPR solenoid valve fails to open, yellow pod.	UPR solenoid valve, yellow pod.	1,600E-07
LAPSHV	LAP shuttle valve or line to preventer leaks.	LAP shuttle valve and fluid line.	2,500E-07
UAPSHV	UAP shuttle valve or line to preventer leaks.	UAP shuttle valve and fluid line.	2,500E-07
BSRSHV	BSR shuttle valve or line to preventer leaks.	BSR shuttle valve and fluid line.	2,500E-07
LPRSHV	LPR shuttle valve or line to preventer leaks.	LPR shuttle valve and fluid line.	2,500E-07
MPRSHV	MPR shuttle valve or line to preventer leaks.	MPR shuttle valve and fluid line.	2,500E-07
UPRSHV	UPR shuttle valve or line to preventer leaks..	UPR shuttle valve and fluid line.	2,500E-07
LAPSHVBP	LAP shuttle valve stuck in opposite position, blue pod	LAP shuttle valve.	1,667E-07
LAPSHVYP	LAP shuttle valve stuck in opposite position, yellow pod.	LAP shuttle valve.	1,667E-07
UAPSHVBP	UAP shuttle valve stuck in opposite position, blue pod.	UAP shuttle valve.	1,667E-07
UAPSHVYP	UAP shuttle valve stuck in opposite position, yellow pod.	UAP shuttle valve.	1,667E-07
LPRSHVBP	LPR shuttle valve stuck in opposite position, blue pod.	LPR shuttle valve.	1,667E-07
LPRSHVYP	LPR shuttle valve stuck in opposite position, yellow pod.	LPR shuttle valve.	1,667E-07
MPRSHVBP	MPR shuttle valve stuck in opposite position, blue pod.	MPR shuttle valve.	1,667E-07
MPRSHVYP	MPR shuttle valve stuck in opposite position, yellow pod.	MPR shuttle valve.	1,667E-07
UPRSHVBP	UPR shuttle valve stuck in opposite position, blue pod.	UPR shuttle valve.	1,667E-07
UPRSHVYP	UPR shuttle valve stuck in opposite position, yellow pod.	UPR shuttle valve.	1,667E-07
BSRSHVBP	BSR shuttle valve stuck in opposite position, blue pod.	BSR shuttle valve.	1,667E-07
BSRSHVYP	BSR shuttle valve stuck in opposite position, yellow pod.	BSR shuttle valve.	1,667E-07
BSRHCV	BSR hydraulic control valve failure.	BSR hydraulic control valve.	1,000E-07
LAPHCV	LAP hydraulic control valve failure..	LAP hydraulic control valve.	1,000E-07
UAPHCV	UAP hydraulic control valve failure.	UAP hydraulic control valve.	1,000E-07
LPRHCV	LPR hydraulic control valve failure.	LPR hydraulic control valve.	1,000E-07
MPRHCV	MPR hydraulic control valve failure.	MPR hydraulic control valve.	1,000E-07
UPRHCV	UPR hydraulic control valve failure.	UPR hydraulic control valve.	1,000E-07

TOP EVENT B

Basic events	Failure mode description	Related component(s)/subsystem(s)	Failure rate (per 10 ⁶ h)
SELECT	Severe leakage in pod selector valve.	Pod selector valve	2,083E-07
PWR	Loss of power supply	Central Control Unit (CCU)	1,000E-07
SCVFBP	Surface control valve failure, blue pod.	Surface control valve, blue pod.	2,083E-07
SCVFYP	Surface control valve failure, yellow pod.	Surface control valve, yellow pod.	2,083E-07
HYSLBLU	Hydraulic supply line leaks, blue pod.	Hydraulic fluid supply line, blue pod.	2,917E-05
HYSLYEL	Hydraulic supply line leaks, yellow pod.	Hydraulic fluid supply line, yellow pod.	2,917E-05
PLC A	PLC A failure.	PLC A	7,000E-07
PLC B	PLC B failure.	PLC B	7,000E-07
MUXBP	Loss of MUX power/communication , blue pod.	MUX cables/reels, blue pod.	4,000E-08
MUXYP	Loss of MUX power/commouication, yellow pod.	MUX cables/reels, yellow pod.	4,000E-08
SEMABP	SEM A failure, blue pod.	SEM A, blue pod.	1,200E-06
SEMBBP	SEM B failure, blue pod.	SEM B, blue pod.	1,200E-06
SEMAYP	SEM A failure, yellow pod.	SEM A, yellow pod.	1,200E-06
SEMBYP	SEM B failure, yellow pod.	SEM B, yellow pod.	1,200E-06
BSRTJOC	Tool joint in ram closing area; causes fail to shear.	BSR.	4,200E-02
ACCVL	Severe leak through stack mounted acc. isol. valve.	Stack mounted acc. isol. valve .	2,083E-07
EXLACC	External leakage in subsea accumulator.	Subsea accumulator bottles.	1,667E-05
ACCIVBP	Leakage in pod mounted acc. isol. valve, blue pod.	Pod mounted acc. isol. valve, blue pod.	2,083E-06
ACCIVYP	Leakage in pod mounted acc. isol. valve, yellow pod.	Pod mounted acc. isol. valve, yellow pod.	2,083E-06
BSRPBDCP	BSR push button fails, DCP.	BSR push button, DCP	4,000E-07
BSRPBTCP	BSR push button fails, TCP.	BSR push button, TCP.	4,000E-07
UAPPBDCP	UAP push button fails, DCP.	UAP push button, DCP.	4,000E-07
UAPPBTCP	UAP push button fails, TCP.	UAP push button, TCP.	4,000E-07
LAPPBDCP	LAP push button fails, DCP.	LAP push button, DCP.	4,000E-07
LAPPBTCP	LAP push button fails, TCP.	LAP push button, TCP.	4,000E-07
MPRPBDCP	MPR push button fails, DCP.	MPR push button, TCP.	4,000E-07
MPRPBTCP	MPR push button fails, TCP.	MPR push button, DCP.	4,000E-07
BSRIF	BSR internal failure; causes fail to close.	BSR.	2,229E-05
LAPIF	LAP internal failure: causes fail to close.	LAP.	1,063E-05
UAPIF	UAP internal failure: causes fail to close	UAP.	1,063E-05
MPRIF	MPR internal failure; causes fail to close.	MPR (VBR)	3,542E-06
BSRSOLVBP	BSR solenoid valve fails to open, blue pod.	BSR solenoid valve, blue pod.	1,600E-07
BSRSOLVYP	BSR solenoid valve fails to open, yellow pod.	BSR solenoid valve, yellow pod.	1,600E-07
LAPSOLVBP	LAP solenoid valve fails to open, blue pod.	LAP solenoid valve, blue pod.	1,600E-07
LAPSOLVYP	LAP solenoid valve failst to open, yellow pod.	LAP solenoid valve, yellow pod.	1,600E-07
UAPSOLVBP	UAP solenoid valve fails to open, blue pod.	UAP solenoid valve, blue pod.	1,600E-07
UAPSOLVYP	UAP solenoid valve fails to open, yellow pod.	UAP solenoid valve, yellow pod.	1,600E-07
MPRSOLVBP	MPR solenoid valve fails to open, blue pod.	MPR solenoid valve, blue pod.	1,600E-07
MPRSOLVYP	MPR solenoid valve fails to open, yellow pod.	MPR solenoid valve, yellow pod.	1,600E-07
LAPSHV	LAP shuttle valve or line to preventer leaks.	LAP shuttle valve and fluid line.	2,500E-07
UAPSHV	UAP shuttle valve or line to preventer leaks.	UAP shuttle valve and fluid line.	2,500E-07
BSRSHV	BSR shuttle valve or line to preventer leaks.	BSR shuttle valve and fluid line.	2,500E-07
MPRSHV	MPR shuttle valve or line to preventer leaks .	MPR shuttle valve and fluid line.	2,500E-07
LAPSHVBP	LAP shuttle valve stuck in opposite position, blue pod	LAP shuttle valve.	1,667E-07
LAPSHVYP	LAP shuttle valve stuck in opposite position, yellow pod.	LAP shuttle valve.	1,667E-07
UAPSHVBP	UAP shuttle valve stuck in opposite position, blue pod.	UAP shuttle valve.	1,667E-07
UAPSHVYP	UPR shuttle valve stuck in opposite position, yellow pod.	UAP shuttle valve.	1,667E-07
MPRSHVBP	MPR valve stuck in opposite position, blue pod.	MPR shuttle valve.	1,667E-07
MPRSHVYP	MPR shuttle valve stuck in opposite position, yellow pod.	MPR shuttle valve.	1,667E-07
BSRSHVBP	BSR shuttle valve stuck in opposite position, blue pod.	BSR shuttle valve.	1,667E-07
BSRSHVYP	BSR shuttle valve stuck in opposite position, yellow pod.	BSR shuttle valve.	1,667E-07
BSRHCV	BSR hydraulic control valve failure.	BSR hydraulic control valve.	1,000E-07
LAPHCV	LAP hydraulic control valve failure..	LAP hydraulic control valve.	1,000E-07
UAPHCV	UAP hydraulic control valve failure.	UAP hydraulic control valve.	1,000E-07
MPRHCV	MPR hydraulic control valve failure.	MPR hydraulic control valve.	1,000E-07

TOP EVENT C

Basic events	Failure mode description	Related component(s)/subsystem(s)	Failure rate (per 10 ⁶ h)
SELECT	Severe leakage in pod selector valve.	Pod selector valve	2,083E-07
PWR	Loss of power supply	Central Control Unit (CCU)	1,000E-07
SCVFBP	Surface control valve failure, blue pod.	Surface control valve, blue pod.	2,083E-07
SCVFYP	Surface control valve failure, yellow pod.	Surface control valve, yellow pod.	2,083E-07
HYSLBLU	Hydraulic supply line leaks, blue pod.	Hydraulic fluid supply line, blue pod.	2,917E-05
HYSLYEL	Hydraulic supply line leaks, yellow pod.	Hydraulic fluid supply line, yellow pod.	2,917E-05
PLC A	PLC A failure.	PLC A	7,000E-07
PLC B	PLC B failure.	PLC B	7,000E-07
MUXBP	Loss of MUX power/communication , blue pod.	MUX cables/reels, blue pod.	4,000E-08
MUXYP	Loss of MUX power/commounication, yellow pod.	MUX cables/reels, yellow pod.	4,000E-08
SEMABP	SEM A failure, blue pod.	SEM A, blue pod.	1,200E-06
SEMBBP	SEM B failure, blue pod.	SEM B, blue pod.	1,200E-06
SEMAYP	SEM A failure, yellow pod.	SEM A, yellow pod.	1,200E-06
SEMBYP	SEM B failure, yellow pod.	SEM B, yellow pod.	1,200E-06
BSRTJOC	Tool joint in ram closing area; causes fail to shear.	BSR.	4,200E-02
CSRTJOC	Tool joint in ram closing area; causes fail to shear.	CSR.	4,200E-02
ACCVL	Severe leak through stack mounted acc. isol. valve.	Stack mounted acc. isol. valve .	2,083E-07
EXLACC	External leakage in subsea accumulator.	Subsea accumulator bottles.	1,667E-05
ACCIVBP	Leakage in pod mounted acc. isol. valve, blue pod.	Pod mounted acc. isol. valve, blue pod.	2,083E-06
ACCIVYP	Leakage in pod mounted acc. isol. valve, yellow pod.	Pod mounted acc. isol. valve, yellow pod.	2,083E-06
BSRPBDCP	BSR push button fails, DCP.	BSR push button, DCP	4,000E-07
BSRPBTCP	BSR push button fails, TCP.	BSR push button, TCP.	4,000E-07
CSRPBDCP	CSR push button fails, DCP.	CSR push button, DCP.	4,000E-07
CSRPBTCP	CSR push button fails, TCP.	CSR push button, TCP.	4,000E-07
LPRPBDCP	LPR push button fails, DCP.	LPR push button, DCP.	4,000E-07
LPRPBTCP	LPR push button fails, TCP.	LPR push button, TCP.	4,000E-07
MPRPBDCP	MPR push button fails, DCP.	MPR push button, DCP.	4,000E-07
MPRPBTCP	MPR push button fails, TCP.	MPR push button, TCP.	4,000E-07
UPRPBDCP	UPR push button fails, DCP.	UPR push button, DCP.	4,000E-07
UPRPBTCP	UPR push button fails, TCP.	UPR push button, TCP.	4,000E-07
BSRIF	Blind shear ram internal failure; causes fail to close.	BSR.	2,229E-05
CSRIF	Casing shear ram internal failure; causes fail to close.	CSR.	2,229E-05
LPRIF	LPR internal failure; causes fail to close.	LPR (fixed).	3,542E-06
MPRIF	MPR internal failure; causes fail to close.	MPR (VBR)	3,542E-06
UPRIF	UPR internal failure; causes fail to close.	UPR (fixed).	3,542E-06
BSRSOLVBP	BSR solenoid valve fails to open, blue pod.	BSR solenoid valve, blue pod.	1,600E-07
BSRSOLVYP	BSR solenoid valve fails to open, yellow pod.	BSR solenoid valve, yellow pod.	1,600E-07
CSRSOLVBP	CSR solenoid valve fails to open, blue pod.	CSR solenoid valve, blue pod.	1,600E-07
CSRSOLVYP	CSR solenoid valve fails to open, yellow pod.	CSR solenoid valve, yellow pod.	1,600E-07
LPRSOLVBP	LPR solenoid valve fails to open, blue pod.	LAP solenoid valve, blue pod.	1,600E-07
LPRSOLVYP	LPR solenoid valve fails to open, yellow pod.	LAP solenoid valve, yellow pod.	1,600E-07
MPRSOLVBP	MPR solenoid valve fails to open, blue pod.	MPR solenoid valve, blue pod.	1,600E-07
MPRSOLVYP	MPR solenoid valve fails to open, yellow pod.	MPR solenoid valve, yellow pod.	1,600E-07
UPRSOLVBP	UPR solenoid valve fails to open, blue pod.	UPR solenoid valve, blue pod.	1,600E-07
UPRSOLVYP	UPR solenoid valve fails to open, yellow pod.	UPR solenoid valve, yellow pod.	1,600E-07
BSRSHV	BSR shuttle valve or line to preventer leaks.	BSR shuttle valve and fluid line.	2,500E-07
CSRSHV	CSR shuttle valve or line to preventer leaks.	CSR shuttle valve and fluid line.	2,500E-07
LPRSHV	LPR shuttle valve or line to preventer leaks.	LPR shuttle valve and fluid line.	2,500E-07
MPRSHV	MPR shuttle valve or line to preventer leaks .	MPR shuttle valve and fluid line.	2,500E-07
UPRSHV	UPR shuttle valve or line to preventer leaks.,.	UPR shuttle valve and fluid line.	2,500E-07
LPRSHVBP	LPR shuttle valve stuck in opposite position, blue pod.	LPR shuttle valve.	1,667E-07
LPRSHVYP	LPR shuttle valve stuck in opposite position, yellow pod.	LPR shuttle valve.	1,667E-07
MPRSHVBP	MPR shuttle valve stuck in opposite position, blue pod.	MPR shuttle valve.	1,667E-07
MPRSHVYP	MPR shuttle valve stuck in opposite position, yellow pod.	MPR shuttle valve.	1,667E-07
UPRSHVBP	UPR shuttle valve stuck in opposite position, blue pod.	UPR shuttle valve.	1,667E-07
UPRSHVYP	UPR shuttle valve stuck in opposite position, yellow pod.	UPR shuttle valve.	1,667E-07
BSRSHVBP	BSR shuttle valve stuck in opposite position, blue pod.	BSR shuttle valve.	1,667E-07
BSRSHVYP	BSR shuttle valve stuck in opposite position, yellow pod.	CSR shuttle valve.	1,667E-07
CSRSHVBP	CSR shuttle valve stuck in opposite position, blue pod.	CSR shuttle valve.	1,667E-07
CSRSHVYP	CSR shuttle valve stuck in opposite position, yellow pod.	BSR shuttle valve.	1,667E-07
BSRHCV	BSR hydraulic control valve failure.	BSR hydraulic control valve.	1,000E-07
CSRHCV	CSR hydraulic control valve failure.	CSR hydraulic control valve.	1,000E-07
LPRHCV	LPR hydraulic control valve failure.	LPR hydraulic control valve.	1,000E-07
MPRHCV	MPR hydraulic control valve failure.	MPR hydraulic control valve.	1,000E-07
UPRHCV	UPR hydraulic control valve failure.	UPR hydraulic control valve.	1,000E-07

TOP EVENT D

Basic events	Failure mode description	Related component(s)/subsystem(s)	(per 10 ⁶ h)
SELECT	Severe leakage in pod selector valve.	Pod selector valve	2,083E-07
PWR	Loss of power supply	Central Control Unit (CCU)	1,000E-07
SCVFBP	Surface control valve failure, blue pod.	Surface control valve, blue pod.	2,083E-07
SCVFYP	Surface control valve failure, yellow pod.	Surface control valve, yellow pod.	2,083E-07
HYSLBLU	Hydraulic supply line leaks, blue pod.	Hydraulic fluid supply line, blue pod.	2,917E-05
HYSLYEL	Hydraulic supply line leaks, yellow pod.	Hydraulic fluid supply line, yellow pod.	2,917E-05
PLC A	PLC A failure.	PLC A	7,000E-07
PLC B	PLC B failure.	PLC B	7,000E-07
MUXBP	Loss of MUX power/communication , blue pod.	MUX cables/reels, blue pod.	4,000E-08
MUXYP	Loss of MUX power/communciation, yellow pod.	MUX cables/reels, yellow pod.	4,000E-08
SEMABP	SEM A failure, blue pod.	SEM A, blue pod.	1,200E-06
SEMBBP	SEM B failure, blue pod.	SEM B, blue pod.	1,200E-06
SEMAYP	SEM A failure, yellow pod.	SEM A, yellow pod.	1,200E-06
SEMBYP	SEM B failure, yellow pod.	SEM B, yellow pod.	1,200E-06
ACCVL	Severe leak through stack mounted acc. isol. valve.	Stack mounted acc. isol. valve .	2,083E-07
EXLACC	External leakage in subsea accumulator.	Subsea accumulator bottles.	1,667E-05
ACCIVBP	Leakage in pod mounted acc. isol. valve, blue pod.	Pod mounted acc. isol. valve, blue pod.	2,083E-06
ACCIVYP	Leakage in pod mounted acc. isol. valve, yellow pod.	Pod mounted acc. isol. valve, yellow pod.	2,083E-06
BSRPBDCP	BSR push button fails, DCP.	BSR push button, DCP	4,000E-07
BSRPBTCP	BSR push button fails, TCP.	BSR push button, TCP.	4,000E-07
BSRIF	BSR internal failure; causes fail to close.	BSR.	2,229E-05
BSRSOLVBP	BSR solenoid valve fails to open, blue pod.	BSR solenoid valve, blue pod.	1,600E-07
BSRSOLVYP	BSR solenoid valve fails to open, yellow pod.	BSR solenoid valve, yellow pod.	1,600E-07
BSRSHV	BSR shuttle valve or line to preventer leaks.	BSR shuttle valve and fluid hose.	2,500E-07
BSRSHVBP	BSR shuttle valve stuck in opposite position, blue pod.	BSR shuttle valve.	1,667E-07
BSRSHVYP	BSR shuttle valve stuck in opposite position, yellow pod.	BSR shuttle valve.	1,667E-07
BSRHCV	BSR hydraulic control valve failure.	BSR hydraulic control valve.	1,000E-07

B.3 Minimal cut sets

CARA Fault Tree version 4.2 (c) ExproSoft AS 2000

Single license.

Supplied by ExproSoft AS

Date: 31.05.2012 Time: 10:32:45

File: CASEA.CFT

New fault tree

Maximum cut size: 4 Mod. level: 0 Top event: CASEA

Cut set(s) with 1 component (Total: 2)

{SELECT}

{PWR}

Cut set(s) with 2 components (Total: 4)

{PLCA,PLCB}

{HYSLBLU,HYSLYEL}

{SCVYP,SCVBP}

{MUXBP,MUXYP}

Cut set(s) with 3 components (Total: 2)

{SEMAYP,SEMBYP,SCVBP}

{SCVYP,SEMABP,SEMBBP}

Cut set(s) with 4 components (Total: 2)

{ACCVL,EXLACC,ACCIVBP,ACCIVYP}

{SEMAYP,SEMBYP,SEMABP,SEMBBP}

Total number of cut sets up to order 4: 10

CARA Fault Tree version 4.2 (c) ExproSoft AS 2000

Single license.

Supplied by ExproSoft AS

Date: 31.05.2012 Time: 10:35:35

File: CASEB.CFT

New fault tree

Maximum cut size: 4 Mod. level: 0 Top event: CASEB

Cut set(s) with 1 component (Total: 2)

{SELECT}

{PWR}

Cut set(s) with 2 components (Total: 4)

{SCVYP,SCVBP}

{HYSLBLU,HYSLYEL}

{PLCA,PLCB}

{MUXBP,MUXYP}

Cut set(s) with 3 components (Total: 2)

{SCVYP,SEMABP,SEMBBP}

{SEMAYP,SEMBYP,SCVBP}

Cut set(s) with 4 components (Total: 110)

{SEMAYP,SEMBYP,SEMABP,SEMBBP}

{BSRTJOC,UAPIF,LAPIF,MPRIF}

{BSRIF,UAPIF,LAPIF,MPRIF}

{BSRHCV,UAPIF,LAPIF,MPRIF}

{BSRSHV,UAPIF,LAPIF,MPRIF}

{BSRTJOC,UAPIF,LAPIF,MPRHCV}

{BSRIF,UAPIF,LAPIF,MPRHCV}

{BSRHCV,UAPIF,LAPIF,MPRHCV}

{BSRSHV,UAPIF,LAPIF,MPRHCV}

{BSRTJOC,UAPIF,LAPIF,MPRSHV}

{BSRIF,UAPIF,LAPIF,MPRSHV}

{BSRHCV,UAPIF,LAPIF,MPRSHV}

{BSRSHV,UAPIF,LAPIF,MPRSHV}

{BSRTJOC,UAPIF,LAPSHV,MPRIF}

{BSRIF,UAPIF,LAPSHV,MPRIF}

{BSRHCV,UAPIF,LAPSHV,MPRIF}

{BSRSHV,UAPIF,LAPSHV,MPRIF}

{BSRTJOC,UAPIF,LAPSHV,MPRHCV}

{BSRIF,UAPIF,LAPSHV,MPRHCV}

{BSRHCV,UAPIF,LAPSHV,MPRHCV}

{BSRSHV,UAPIF,LAPSHV,MPRHCV}

{BSRTJOC,UAPIF,LAPSHV,MPRSHV}

{BSRIF,UAPIF,LAPSHV,MPRSHV}

{BSRHCV,UAPIF,LAPSHV,MPRSHV}

{BSRSHV,UAPIF,LAPSHV,MPRSHV}

{BSRTJOC,UAPIF,LAPHCV,MPRIF}

{BSRIF,UAPIF,LAPHCV,MPRIF}

{BSRHCV,UAPIF,LAPHCV,MPRIF}

{BSRSHV,UAPIF,LAPHCV,MPRIF}

{BSRTJOC,UAPIF,LAPHCV,MPRHCV}

{BSRIF,UAPIF,LAPHCV,MPRHCV}
{BSRHCV,UAPIF,LAPHCV,MPRHCV}
{BSRSHV,UAPIF,LAPHCV,MPRHCV}
{BSRTJOC,UAPIF,LAPHCV,MPRSHV}
{BSRIF,UAPIF,LAPHCV,MPRSHV}
{BSRHCV,UAPIF,LAPHCV,MPRSHV}
{BSRSHV,UAPIF,LAPHCV,MPRSHV}
{BSRTJOC,UAPSHV,LAPIF,MPRIF}
{BSRIF,UAPSHV,LAPIF,MPRIF}
{BSRHCV,UAPSHV,LAPIF,MPRIF}
{BSRSHV,UAPSHV,LAPIF,MPRIF}
{BSRTJOC,UAPSHV,LAPIF,MPRHCV}
{BSRIF,UAPSHV,LAPIF,MPRHCV}
{BSRHCV,UAPSHV,LAPIF,MPRHCV}
{BSRSHV,UAPSHV,LAPIF,MPRHCV}
{BSRTJOC,UAPSHV,LAPIF,MPRSHV}
{BSRIF,UAPSHV,LAPIF,MPRSHV}
{BSRHCV,UAPSHV,LAPIF,MPRSHV}
{BSRSHV,UAPSHV,LAPIF,MPRSHV}
{BSRTJOC,UAPSHV,LAPSHV,MPRIF}
{BSRIF,UAPSHV,LAPSHV,MPRIF}
{BSRHCV,UAPSHV,LAPSHV,MPRIF}
{BSRSHV,UAPSHV,LAPSHV,MPRIF}
{BSRTJOC,UAPSHV,LAPSHV,MPRHCV}
{BSRIF,UAPSHV,LAPSHV,MPRHCV}
{BSRHCV,UAPSHV,LAPSHV,MPRHCV}
{BSRSHV,UAPSHV,LAPSHV,MPRHCV}
{BSRTJOC,UAPSHV,LAPSHV,MPRSHV}
{BSRIF,UAPSHV,LAPSHV,MPRSHV}
{BSRHCV,UAPSHV,LAPSHV,MPRSHV}
{BSRSHV,UAPSHV,LAPSHV,MPRSHV}
{BSRTJOC,UAPSHV,LAPHCV,MPRIF}
{BSRIF,UAPSHV,LAPHCV,MPRIF}
{BSRHCV,UAPSHV,LAPHCV,MPRIF}
{BSRSHV,UAPSHV,LAPHCV,MPRIF}
{BSRTJOC,UAPSHV,LAPHCV,MPRHCV}
{BSRIF,UAPSHV,LAPHCV,MPRHCV}
{BSRHCV,UAPSHV,LAPHCV,MPRHCV}
{BSRSHV,UAPSHV,LAPHCV,MPRHCV}
{BSRTJOC,UAPSHV,LAPHCV,MPRSHV}
{BSRIF,UAPSHV,LAPHCV,MPRSHV}
{BSRHCV,UAPSHV,LAPHCV,MPRSHV}
{BSRSHV,UAPSHV,LAPHCV,MPRSHV}
{BSRTJOC,UAPHCV,LAPIF,MPRIF}
{BSRIF,UAPHCV,LAPIF,MPRIF}
{BSRHCV,UAPHCV,LAPIF,MPRIF}
{BSRSHV,UAPHCV,LAPIF,MPRIF}
{BSRTJOC,UAPHCV,LAPIF,MPRHCV}
{BSRIF,UAPHCV,LAPIF,MPRHCV}
{BSRHCV,UAPHCV,LAPIF,MPRHCV}
{BSRSHV,UAPHCV,LAPIF,MPRHCV}
{BSRTJOC,UAPHCV,LAPIF,MPRSHV}
{BSRIF,UAPHCV,LAPIF,MPRSHV}
{BSRHCV,UAPHCV,LAPIF,MPRSHV}
{BSRSHV,UAPHCV,LAPIF,MPRSHV}
{BSRTJOC,UAPHCV,LAPSHV,MPRIF}

{BSRIF,UAPHCV,LAPSHV,MPRIF}
{BSRHCV,UAPHCV,LAPSHV,MPRIF}
{BSRSHV,UAPHCV,LAPSHV,MPRIF}
{BSRTJOC,UAPHCV,LAPSHV,MPRHCV}
{BSRIF,UAPHCV,LAPSHV,MPRHCV}
{BSRHCV,UAPHCV,LAPSHV,MPRHCV}
{BSRSHV,UAPHCV,LAPSHV,MPRHCV}
{BSRTJOC,UAPHCV,LAPSHV,MPRSHV}
{BSRIF,UAPHCV,LAPSHV,MPRSHV}
{BSRHCV,UAPHCV,LAPSHV,MPRSHV}
{BSRSHV,UAPHCV,LAPSHV,MPRSHV}
{BSRTJOC,UAPHCV,LAPHCV,MPRIF}
{BSRIF,UAPHCV,LAPHCV,MPRIF}
{BSRHCV,UAPHCV,LAPHCV,MPRIF}
{BSRSHV,UAPHCV,LAPHCV,MPRIF}
{BSRTJOC,UAPHCV,LAPHCV,MPRHCV}
{BSRIF,UAPHCV,LAPHCV,MPRHCV}
{BSRHCV,UAPHCV,LAPHCV,MPRHCV}
{BSRSHV,UAPHCV,LAPHCV,MPRHCV}
{BSRTJOC,UAPHCV,LAPHCV,MPRSHV}
{BSRIF,UAPHCV,LAPHCV,MPRSHV}
{BSRHCV,UAPHCV,LAPHCV,MPRSHV}
{BSRSHV,UAPHCV,LAPHCV,MPRSHV}
{ACCVL,EXLACC,ACCIVBP,ACCIVYP}

Total number of cut sets up to order 4: 118

CARA Fault Tree version 4.2 (c) ExproSoft AS 2000

Single license.

Supplied by ExproSoft AS

Date: 31.05.2012 Time: 10:36:01

File: CASEC.CFT

New fault tree

Maximum cut size: 4 Mod. level: 0 Top event: CASEC

Cut set(s) with 1 component (Total: 2)

{SELECT}

{PWR}

Cut set(s) with 2 components (Total: 4)

{HYSLBLU,HYSLYEL}

{SCVYP,SCVBP}

{PLCA,PLCB}

{MUXBP,MUXYP}

Cut set(s) with 3 components (Total: 2)

{SEMAYP,SEMBYP,SCVBP}

{SCVYP,SEMABP,SEMBBP}

Cut set(s) with 4 components (Total: 218)

{ACCVL,EXLACC,ACCIVBP,ACCIVYP}

{SEMAYP,SEMBYP,SEMABP,SEMBBP}

{BSRTJOC,LPRIF,MPRIF,UPRIF}

{BSRIF,LPRIF,MPRIF,UPRIF}

{BSRHCV,LPRIF,MPRIF,UPRIF}

{BSRSHV,LPRIF,MPRIF,UPRIF}

{CSRTJOC,LPRIF,MPRIF,UPRIF}

{CSRIF,LPRIF,MPRIF,UPRIF}

{CSRHCV,LPRIF,MPRIF,UPRIF}

{CSRSHV,LPRIF,MPRIF,UPRIF}

{BSRTJOC,LPRIF,MPRIF,UPRHCV}

{BSRIF,LPRIF,MPRIF,UPRHCV}

{BSRHCV,LPRIF,MPRIF,UPRHCV}

{BSRSHV,LPRIF,MPRIF,UPRHCV}

{CSRTJOC,LPRIF,MPRIF,UPRHCV}

{CSRIF,LPRIF,MPRIF,UPRHCV}

{CSRHCV,LPRIF,MPRIF,UPRHCV}

{CSRSHV,LPRIF,MPRIF,UPRHCV}

{BSRTJOC,LPRIF,MPRIF,UPRSHV}

{BSRIF,LPRIF,MPRIF,UPRSHV}

{BSRHCV,LPRIF,MPRIF,UPRSHV}

{BSRSHV,LPRIF,MPRIF,UPRSHV}

{CSRTJOC,LPRIF,MPRIF,UPRSHV}

{CSRIF,LPRIF,MPRIF,UPRSHV}

{CSRHCV,LPRIF,MPRIF,UPRSHV}

{CSRSHV,LPRIF,MPRIF,UPRSHV}

{BSRTJOC,LPRIF,MPRHCV,UPRIF}

{BSRIF,LPRIF,MPRHCV,UPRIF}

{BSRHCV,LPRIF,MPRHCV,UPRIF}

{BSRSHV,LPRIF,MPRHCV,UPRIF}

{CSRTJOC,LPRIF,MPRHCV,UPRIF}
{CSRIF,LPRIF,MPRHCV,UPRIF}
{CSRHCV,LPRIF,MPRHCV,UPRIF}
{CSRSHV,LPRIF,MPRHCV,UPRIF}
{BSRTJOC,LPRIF,MPRHCV,UPRHCV}
{BSRIF,LPRIF,MPRHCV,UPRHCV}
{BSRHCV,LPRIF,MPRHCV,UPRHCV}
{BSRSHV,LPRIF,MPRHCV,UPRHCV}
{CSRTJOC,LPRIF,MPRHCV,UPRHCV}
{CSRIF,LPRIF,MPRHCV,UPRHCV}
{CSRHCV,LPRIF,MPRHCV,UPRHCV}
{CSRSHV,LPRIF,MPRHCV,UPRHCV}
{BSRTJOC,LPRIF,MPRHCV,UPRSHV}
{BSRIF,LPRIF,MPRHCV,UPRSHV}
{BSRHCV,LPRIF,MPRHCV,UPRSHV}
{BSRSHV,LPRIF,MPRHCV,UPRSHV}
{CSRTJOC,LPRIF,MPRHCV,UPRSHV}
{CSRIF,LPRIF,MPRHCV,UPRSHV}
{CSRHCV,LPRIF,MPRHCV,UPRSHV}
{CSRSHV,LPRIF,MPRHCV,UPRSHV}
{BSRTJOC,LPRIF,MPRSHV,UPRIF}
{BSRIF,LPRIF,MPRSHV,UPRIF}
{BSRHCV,LPRIF,MPRSHV,UPRIF}
{BSRSHV,LPRIF,MPRSHV,UPRIF}
{CSRTJOC,LPRIF,MPRSHV,UPRIF}
{CSRIF,LPRIF,MPRSHV,UPRIF}
{CSRHCV,LPRIF,MPRSHV,UPRIF}
{CSRSHV,LPRIF,MPRSHV,UPRIF}
{BSRTJOC,LPRIF,MPRSHV,UPRHCV}
{BSRIF,LPRIF,MPRSHV,UPRHCV}
{BSRHCV,LPRIF,MPRSHV,UPRHCV}
{BSRSHV,LPRIF,MPRSHV,UPRHCV}
{CSRTJOC,LPRIF,MPRSHV,UPRHCV}
{CSRIF,LPRIF,MPRSHV,UPRHCV}
{CSRHCV,LPRIF,MPRSHV,UPRHCV}
{CSRSHV,LPRIF,MPRSHV,UPRHCV}
{BSRTJOC,LPRIF,MPRSHV,UPRSHV}
{BSRIF,LPRIF,MPRSHV,UPRSHV}
{BSRHCV,LPRIF,MPRSHV,UPRSHV}
{BSRSHV,LPRIF,MPRSHV,UPRSHV}
{CSRTJOC,LPRIF,MPRSHV,UPRSHV}
{CSRIF,LPRIF,MPRSHV,UPRSHV}
{CSRHCV,LPRIF,MPRSHV,UPRSHV}
{CSRSHV,LPRIF,MPRSHV,UPRSHV}
{BSRTJOC,LPRHCV,MPRIF,UPRIF}
{BSRIF,LPRHCV,MPRIF,UPRIF}
{BSRHCV,LPRHCV,MPRIF,UPRIF}
{BSRSHV,LPRHCV,MPRIF,UPRIF}
{CSRTJOC,LPRHCV,MPRIF,UPRIF}
{CSRIF,LPRHCV,MPRIF,UPRIF}
{CSRHCV,LPRHCV,MPRIF,UPRIF}
{CSRSHV,LPRHCV,MPRIF,UPRIF}
{BSRTJOC,LPRHCV,MPRIF,UPRHCV}
{BSRIF,LPRHCV,MPRIF,UPRHCV}
{BSRHCV,LPRHCV,MPRIF,UPRHCV}
{BSRSHV,LPRHCV,MPRIF,UPRHCV}

{CSRTJOC,LPRHCV,MPRIF,UPRHCV}
{CSRIF,LPRHCV,MPRIF,UPRHCV}
{CSRHCV,LPRHCV,MPRIF,UPRHCV}
{CSRSHV,LPRHCV,MPRIF,UPRHCV}
{BSRTJOC,LPRHCV,MPRIF,UPRSHV}
{BSRIF,LPRHCV,MPRIF,UPRSHV}
{BSRHCV,LPRHCV,MPRIF,UPRSHV}
{BSRSHV,LPRHCV,MPRIF,UPRSHV}
{CSRTJOC,LPRHCV,MPRIF,UPRSHV}
{CSRIF,LPRHCV,MPRIF,UPRSHV}
{CSRHCV,LPRHCV,MPRIF,UPRSHV}
{CSRSHV,LPRHCV,MPRIF,UPRSHV}
{BSRTJOC,LPRHCV,MPRHCV,UPRIF}
{BSRIF,LPRHCV,MPRHCV,UPRIF}
{BSRHCV,LPRHCV,MPRHCV,UPRIF}
{BSRSHV,LPRHCV,MPRHCV,UPRIF}
{CSRTJOC,LPRHCV,MPRHCV,UPRIF}
{CSRIF,LPRHCV,MPRHCV,UPRIF}
{CSRHCV,LPRHCV,MPRHCV,UPRIF}
{CSRSHV,LPRHCV,MPRHCV,UPRIF}
{BSRTJOC,LPRHCV,MPRHCV,UPRHCV}
{BSRIF,LPRHCV,MPRHCV,UPRHCV}
{BSRHCV,LPRHCV,MPRHCV,UPRHCV}
{BSRSHV,LPRHCV,MPRHCV,UPRHCV}
{CSRTJOC,LPRHCV,MPRHCV,UPRHCV}
{CSRIF,LPRHCV,MPRHCV,UPRHCV}
{CSRHCV,LPRHCV,MPRHCV,UPRHCV}
{CSRSHV,LPRHCV,MPRHCV,UPRHCV}
{BSRTJOC,LPRHCV,MPRHCV,UPRSHV}
{BSRIF,LPRHCV,MPRHCV,UPRSHV}
{BSRHCV,LPRHCV,MPRHCV,UPRSHV}
{BSRSHV,LPRHCV,MPRHCV,UPRSHV}
{CSRTJOC,LPRHCV,MPRHCV,UPRSHV}
{CSRIF,LPRHCV,MPRHCV,UPRSHV}
{CSRHCV,LPRHCV,MPRHCV,UPRSHV}
{CSRSHV,LPRHCV,MPRHCV,UPRSHV}
{BSRTJOC,LPRHCV,MPRSHV,UPRIF}
{BSRIF,LPRHCV,MPRSHV,UPRIF}
{BSRHCV,LPRHCV,MPRSHV,UPRIF}
{BSRSHV,LPRHCV,MPRSHV,UPRIF}
{CSRTJOC,LPRHCV,MPRSHV,UPRIF}
{CSRIF,LPRHCV,MPRSHV,UPRIF}
{CSRHCV,LPRHCV,MPRSHV,UPRIF}
{CSRSHV,LPRHCV,MPRSHV,UPRIF}
{BSRTJOC,LPRHCV,MPRSHV,UPRHCV}
{BSRIF,LPRHCV,MPRSHV,UPRHCV}
{BSRHCV,LPRHCV,MPRSHV,UPRHCV}
{BSRSHV,LPRHCV,MPRSHV,UPRHCV}
{CSRTJOC,LPRHCV,MPRSHV,UPRHCV}
{CSRIF,LPRHCV,MPRSHV,UPRHCV}
{CSRHCV,LPRHCV,MPRSHV,UPRHCV}
{CSRSHV,LPRHCV,MPRSHV,UPRHCV}
{BSRTJOC,LPRHCV,MPRSHV,UPRSHV}
{BSRIF,LPRHCV,MPRSHV,UPRSHV}
{BSRHCV,LPRHCV,MPRSHV,UPRSHV}
{BSRSHV,LPRHCV,MPRSHV,UPRSHV}

{CSRTJOC,LPRHCV,MPRSHV,UPRSHV}
{CSRIF,LPRHCV,MPRSHV,UPRSHV}
{CSRHCV,LPRHCV,MPRSHV,UPRSHV}
{CSRSHV,LPRHCV,MPRSHV,UPRSHV}
{BSRTJOC,LPRSHV,MPRIF,UPRIF}
{BSRIF,LPRSHV,MPRIF,UPRIF}
{BSRHCV,LPRSHV,MPRIF,UPRIF}
{BSRSHV,LPRSHV,MPRIF,UPRIF}
{CSRTJOC,LPRSHV,MPRIF,UPRIF}
{CSRIF,LPRSHV,MPRIF,UPRIF}
{CSRHCV,LPRSHV,MPRIF,UPRIF}
{CSRSHV,LPRSHV,MPRIF,UPRIF}
{BSRTJOC,LPRSHV,MPRIF,UPRHCV}
{BSRIF,LPRSHV,MPRIF,UPRHCV}
{BSRHCV,LPRSHV,MPRIF,UPRHCV}
{BSRSHV,LPRSHV,MPRIF,UPRHCV}
{CSRTJOC,LPRSHV,MPRIF,UPRHCV}
{CSRIF,LPRSHV,MPRIF,UPRHCV}
{CSRHCV,LPRSHV,MPRIF,UPRHCV}
{CSRSHV,LPRSHV,MPRIF,UPRHCV}
{BSRTJOC,LPRSHV,MPRIF,UPRSHV}
{BSRIF,LPRSHV,MPRIF,UPRSHV}
{BSRHCV,LPRSHV,MPRIF,UPRSHV}
{BSRSHV,LPRSHV,MPRIF,UPRSHV}
{CSRTJOC,LPRSHV,MPRIF,UPRSHV}
{CSRIF,LPRSHV,MPRIF,UPRSHV}
{CSRHCV,LPRSHV,MPRIF,UPRSHV}
{CSRSHV,LPRSHV,MPRIF,UPRSHV}
{BSRTJOC,LPRSHV,MPRHCV,UPRIF}
{BSRIF,LPRSHV,MPRHCV,UPRIF}
{BSRHCV,LPRSHV,MPRHCV,UPRIF}
{BSRSHV,LPRSHV,MPRHCV,UPRIF}
{CSRTJOC,LPRSHV,MPRHCV,UPRIF}
{CSRIF,LPRSHV,MPRHCV,UPRIF}
{CSRHCV,LPRSHV,MPRHCV,UPRIF}
{CSRSHV,LPRSHV,MPRHCV,UPRIF}
{BSRTJOC,LPRSHV,MPRHCV,UPRHCV}
{BSRIF,LPRSHV,MPRHCV,UPRHCV}
{BSRHCV,LPRSHV,MPRHCV,UPRHCV}
{BSRSHV,LPRSHV,MPRHCV,UPRHCV}
{CSRTJOC,LPRSHV,MPRHCV,UPRHCV}
{CSRIF,LPRSHV,MPRHCV,UPRHCV}
{CSRHCV,LPRSHV,MPRHCV,UPRHCV}
{CSRSHV,LPRSHV,MPRHCV,UPRHCV}
{BSRTJOC,LPRSHV,MPRHCV,UPRSHV}
{BSRIF,LPRSHV,MPRHCV,UPRSHV}
{BSRHCV,LPRSHV,MPRHCV,UPRSHV}
{BSRSHV,LPRSHV,MPRHCV,UPRSHV}
{CSRTJOC,LPRSHV,MPRHCV,UPRSHV}
{CSRIF,LPRSHV,MPRHCV,UPRSHV}
{CSRHCV,LPRSHV,MPRHCV,UPRSHV}
{CSRSHV,LPRSHV,MPRHCV,UPRSHV}
{BSRTJOC,LPRSHV,MPRSHV,UPRIF}
{BSRIF,LPRSHV,MPRSHV,UPRIF}
{BSRHCV,LPRSHV,MPRSHV,UPRIF}
{BSRSHV,LPRSHV,MPRSHV,UPRIF}

{CSRTJOC,LPRSHV,MPRSHV,UPRIF}
{CSRIF,LPRSHV,MPRSHV,UPRIF}
{CSRHCV,LPRSHV,MPRSHV,UPRIF}
{CSRSHV,LPRSHV,MPRSHV,UPRIF}
{BSRTJOC,LPRSHV,MPRSHV,UPRHCV}
{BSRIF,LPRSHV,MPRSHV,UPRHCV}
{BSRHCV,LPRSHV,MPRSHV,UPRHCV}
{BSRSHV,LPRSHV,MPRSHV,UPRHCV}
{CSRTJOC,LPRSHV,MPRSHV,UPRHCV}
{CSRIF,LPRSHV,MPRSHV,UPRHCV}
{CSRHCV,LPRSHV,MPRSHV,UPRHCV}
{CSRSHV,LPRSHV,MPRSHV,UPRHCV}
{BSRTJOC,LPRSHV,MPRSHV,UPRSHV}
{BSRIF,LPRSHV,MPRSHV,UPRSHV}
{BSRHCV,LPRSHV,MPRSHV,UPRSHV}
{BSRSHV,LPRSHV,MPRSHV,UPRSHV}
{CSRTJOC,LPRSHV,MPRSHV,UPRSHV}
{CSRIF,LPRSHV,MPRSHV,UPRSHV}
{CSRHCV,LPRSHV,MPRSHV,UPRSHV}
{CSRSHV,LPRSHV,MPRSHV,UPRSHV}

Total number of cut sets up to order 4: 226

CARA Fault Tree version 4.2 (c) ExproSoft AS 2000

Single license.

Supplied by ExproSoft AS

Date: 31.05.2012 Time: 10:37:06

File: CASED.CFT

New fault tree

Maximum cut size: 4 Mod. level: 0 Top event: CASED

Cut set(s) with 1 component (Total: 5)

- {SELECT}
- {BSRIF}
- {PWR}
- {BSRHCV}
- {BSRSHV}

Cut set(s) with 2 components (Total: 13)

- {PLCA,PLCB}
- {HYSLBLU,HYSLYEL}
- {SCVYP,SCVBP}
- {SCVYP,BSRSOLVBP}
- {SCVYP,BSRSHVBP}
- {BSRSOLVYP,SCVBP}
- {BSRSOLVYP,BSRSOLVBP}
- {BSRSOLVYP,BSRSHVBP}
- {BSRSHVYP,SCVBP}
- {BSRSHVYP,BSRSOLVBP}
- {BSRSHVYP,BSRSHVBP}
- {BSRPBDCP,BSRPBTC}
- {MUXBP,MUXYP}

Cut set(s) with 3 components (Total: 6)

- {SEMAYP,SEMBYP,SCVBP}
- {SEMAYP,SEMBYP,BSRSOLVBP}
- {SEMAYP,SEMBYP,BSRSHVBP}
- {SCVYP,SEMABP,SEMBBP}
- {BSRSOLVYP,SEMABP,SEMBBP}
- {BSRSHVYP,SEMABP,SEMBBP}

Cut set(s) with 4 components (Total: 2)

- {ACCVL,EXLACC,ACCIVBP,ACCIVYP}
- {SEMAYP,SEMBYP,SEMABP,SEMBBP}

Total number of cut sets up to order 4: 26

Appendix C

Event trees

C.1 Event trees for Case B and C

