NTNU – Trondheim
Norwegian University of
Science and Technology

NewModel for Reliability and Availability Assessment of Subsea BOP System

Challenges and Approaches for New
Requirements

Juntao Zhang

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: June 2015
Supervisor: Yiliu Liu, IPK
Co-supervisor: Laurent Bouillaut, IFSTTAR

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

RAMS
Reliability, Availability,
Maintainability, and Safety

New Model for Reliability and Availability Assessment of Subsea BOP System

Challenges and Approaches for New Requirements

Juntao Zhang

June 2015

PROJECT / MASTER THESIS

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

Supervisor 1: Professor Yiliu Liu (NTNU)

Supervisor 2: Professor Laurent Bouillaut (IFSTTAR)

Preface

This report documents my master thesis carried out during the spring of 2015. The thesis has been carried out as part of the RAMS Engineering MSc program at the Norwegian University of Science and Technology (NTNU), and is concerned with new method for reliability and availability assessment and investigates different configurations of blowout preventer stack in the case study. 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 Lundteigen (2014). The reader is also assumed to have knowledge of the basics concepts involved with subsea blowout preventer. 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, 2015-06-16

Juntao Zhang

Acknowledgment

This master thesis could not have been carried out without the great help of a few individuals. I would especially like to thank my primary supervisor Yiliu Liu, professor at the Department of Production and Quality Engineering at NTNU, for dedicated help and support during the work. Also I would like to thank the co-supervisor Laurent Bouillaut, who works at French institute of science and technology for transport, development and networks (IFSTTAR), for his suggestions of the suitable software for carrying out the Bayesian Network analysis and answering related questions. Finally, thanks for Anne Barros for arranging the meeting with Det Norske Veritas (DNV) employees who give useful advices for my thesis work.

Juntao Zhang

Summary and Conclusions

The blowout preventer system is acting the secondary safety barrier in a hydrocarbon well, where the drilling mud column is defined as the primary safety barrier. However, in pratical industry, there is a new demand for improved methods of assessing the reliability and availability of blowout preventer systems. The objective of this master thesis is to propose the relatively new method for reliability and availability assessment based on Bayesian Network, focusing on the comparsion between the various blowout preventers stack and the influence of the external information in the case study.

The thesis starting with introduction of safety critical system including the basic terminology for reliability and availability assessment. The relevant standards regarding oil and gas industry are also introduced.

The brief review about the blowout preventer is presented next. The basic structure of blowout preventer and the three main subsystems are identified and introduced. The classification of possible failure and desired functions of main components are reported. Finally, the brief research review about the previous reliability assessment method of subsea blowout preventer is presented, pointing out some potential weakness of the traditional methods, which indicating the Bayesian Network is the one possible solution when new requirement of reliability and availability is demanded.

Then the introduction of Bayesian Network is mainly investigated for those who are not very familiar with this method. The possible allocation of Bayesian Network in reliability assessment and the comparsion between Bayesian Network model and the traditional method are mainly discussed. Then in the end of this chapter, there are two examples to show how the traditional method used in the assessment of blowout preventer can be transferred into Bayesian Network model without losing any details, in addtion, the advanced modeling powers regarding introduction of probabilistic gates, multiple states for variables and updating information when scanerio is known are revealed in both examples.

Finally the case study about reliability and availability assessment of different blowout preventers is created. There are mainly three different type of blowout preventer stacks withing different degrees of performing the desired functions under the most demanding situations. The

Bayesian Network model is able to perform such assessment effectively and one addtional information is taken into account since the contribution of the wellbore pressure has significant implications on the blowout preventer's ability to seal around or seal off the wellbore.

Finally, the conclusion and discussion are provided. The main conclusion are summarized as three key findings. First, Bayesian Network is proven to carry out the reliability and availability assessment when there is the new requirement in pratical situations, especially for updating the information when the test data is available during the operation. Second, Bayesian Network based reliability and availability assessment is possible for applying in the large scale model since it can handle probabilistic gates and multiple states of components, where the traditional method such as Fault Tree Analysis may not be able to deal with such challenges. Third, according to the analysis results of the case study, the blowout preventer equipped with the Deepwater Horizon type of stack is considered as the most reliable one in the most demanding situation, if the correct repair strategy is applied. In addition, this kind of blowout preventer is relatively very stable under the high wellbore pressure condition even though withing lower redundancy of the pipe ram subsystem, due to inclusion of casing shear ram which improves the shearing ability significantly.

Contents

Chapter 1

Introduction

1.1 Background

The Macondo accident is the most severe blowout accident with the extreme consequence in oil and gas industry, recently. 11 crews were killed and the Gulf of Mexico was irretrievably polluted during this disaster. A considerable amount of literatures has investigated the main causes of the accident. Accordingly, most of them argued that the improvement of reliability assessment of safety critical system is crucial to prevent from happening again in the future. In the final report on the investigation of Macondo well blowout (Deepwater-Horizon-Study-Group, 2008), they concluded that the uncontrolled blowout is caused by three categories: unrecognized risk in production casing design and construction, procedure of temporary abandonment of the well and the failure in attempting to shut-in the well such as disconnecting the drill rig from the well and activating the blowout preventer (BOP). The report also indicates that failure of the BOP as one of final barrier when dealing with well control problems is one of main causes of the accident. In the weak of the occurrence of Macondo accident, the improved reliability assessment of BOP is becoming recognized.

After reviewing standards and guidelines concerning oil and gas industries: the basic idea behind the safety critical system and relevant reliability assessment methods are discussed in this report. However, some weaknesses in the previous reliability study of BOP system are revealed after reviewing the BOP system, where the traditional methods is no longer adequate enough to perform the suitable analysis under the specific requirement. Since the BOP system is not only acting as the safety barrier but also perform the operational functions, some external causes should be taken into account such as the wellbore conditions; Due to the data collection and estimation of unknown parameters of modelling, some issues such as common cause failure (CCF) have not been fully covered in the previous assessment (Hokstad and Rausand, 2008); In addition, one may expect that there is a reassessment method for updating reliability information once the testing data of BOP system is available, which means making the diagnostic analysis possible in reliability assessment of BOP system. In order to carry out the more accurate reliability assessment of BOP system, one appropriate probabilistic assessment model so called Bayesian Network (BN) should be introduced to face challenges upon the special features and requirement of BOP system.

This Master thesis is starting with the review of basic concepts of the reliability assessment of safety critical system. Then, the problem existing in the previous BOP reliability assessment is presented. The detailed introduction of Bayesian Network is given by descriptive examples afterwards. Firstly, two examples are created for demonstrating how the traditional method is converted into Bayesian Network and the relevant comparison between them is revealed to indicating the advantage of Bayesian Network . Then the case study is carried out by using Bayesian Network model regarding overcoming existing challenges.

1.2 Objectives

The main objective of this master thesis is to indicate the new requirement of reliability assessment in the existing subsea BOP system and propose the new method to fulfill those kinds of requirement. To be more specific, the objectives are:

1. Give the overall review about main concepts and approaches for reliability assessment related to safety-critical systems:

    - To describe the conceptions and relevant terminology and of safety critical system, in order to help understanding the following part
    - To investigate the reliability measures with different calculation methods in order to understand the difference between two major reliability measures

- To identify the safety integrity level and its requirement and allocation method

2. Present a basic understanding of BOP system, its basic structure, functions, failure modes and relevant information

    - To describe the main elements of BOP and what they are mainly used for, and present and compare the different configuration of BOP stack
    - To classify essential functions and failure modes of the whole BOP system
    - To identify the possible weakness or existing research gaps by reviewing the previous work

3. Introduce the suitable method for new reliability assessment in case of BOP system

    - To give brief introduction to the basic conceptions of Bayesian Network
    - To discuss the possible solution of applying Bayesian Network in reliability assessment, by illustrating simple examples concerning transferring Fault Tree Analysis to Bayesian Network

4. Carry out the case study about the Bayesian Network based assessment of BOP system

    - To describe the current problem existing in the BOP system reliability assessment
    - To solve the existing problems by Bayesian Network Model
    - To discuss the key findings based on the results of the analysis

1.3 Delimitations

Since viewers are supposed to have the basic knowledge in reliability assessment or relevant backgrounds, some aspects related to safety critical system and some specific calculations and formulas are only briefly investigated but not specifically described due to the limited space in this report.

In the calculation of proposed assessment method, some simplification of modeling of BOP system is made so that the loss of details is unavoidable and the operation of some components of BOP system is not included. And some parameters are estimated by expert judgment and personal opinion of author.

1.4 Approach

- Interviews: The formulated problem is identified based on the literature review from the semester project, professional supervisions and some opinions and suggestions from the industrial companies, DNV and Rio. After discussing with experts from industry with operation and modelling experiences, the suitable method and the scope of the thesis is finally chosen for solutions.
- Literature research: Some contexts in this thesis are abstracted from the semester project report written by the author to avoid some unnecessary efforts, such as the summary of safety critical system, the investigation about the BOP system and the potential problems in its previous reliability assessment of BOP system.
- Case study:As suggested by supervisors, the main approach for creating Bayesian Network model in this master thesis is to use Matlab, which has the professional computational power and the specific toolbox for Bayesian Network. The instruction manual and the relevant programming can be find in the website of Bayesian Network Toolbox of Matlab (Matlab, 2015).

1.5 Structure of the Report

Chapter 2 gives the overview of safety critical system conception in addition with the terminology of safety instrumented system before explanation and discussion of reliability measure and performance evaluation of related system.
Chapter 3 starts with the system familiarization of the BOP system with respect to its physical structure, and then classifies the functions and possible failure of the BOP system from the previous research in reliability evaluation of the BOP system to identify the possible challenges in its traditional reliability assessment.

Chapter 4 introduces the basic ideas and rules behind Bayesian Network and its relevant calculations. And the detailed introduction about building Bayesian Network model is given by a simple example. Then the discussion about how Bayesian Network applying in the reliability assessment and the comparison from traditional method are given afterwards.

Chapter 5 carrys out the case study of the BOP system regarding the different configuration stack: Classical, Modern and Deepwater Horizon, which equipped with different subsystem within various redundancy. In addition, the effect of the wellbore pressure is also investigated by using the forward analysis and backward analysis.

Chapter 6 discusses the generated results from the previous chapters, especially for case study. The research respective is also proposed for future development in this area.

Chapter 2

Reliability Assessment of Safety Critical Systems

In this chapter, some basic terminology and conceptions about safety critical system are introduced briefly from subchapter 2.1 to 2.5. And subchapter 2.6 gives the introduction about reliability measures of safety critical system and how the terms are used in the calculation. In addition, subchapter 2.7 presents how to evaluate the performance of safety critical system by allocating the reliability measures.

2.1 Basic Conceptions of Safety-Critical Systems

A safety-critical system is a system whose failure may lead to harm to people, economic loss, and/or environmental damage.

—(Rausand and Lundteigen, 2014)

When the failure of the system would lead to the unacceptable consequence, this kind of system is called as safety-critical system. The safety-critical system is designed to perform the safety functions that can prevent equipment under control (EUC) from undesirable consequence. Note that EUC could be people in case that system is designed to protect person from harms. EUC can be protected more than one safety barrier, but all the safety barriers with respect to EUC are not necessarily safety critical system.

2.2 Relevant Technologies and Applicable Standards

Electrical,electronic,or programmable electronic (E/E/PE) technology is mostly applied in safety-critical systems (Rausand and Lundteigen, 2014), often together with mechanical or other technology items. The system-critical system should include at least one of E/E/PE technology. If the system excludes the E/E/PE technology, the system can use the term as *Safety-related system*, but it may be difficult to distinguish these two.

There are many sector-specific standards for process industry, machinery system, nuclear power plants and automotive industry. The sector-specific standards can restrict its application to the most typical and desired way of designing and operating a safety-critical system. In this master thesis, the case study is about subsea blowout preventer system, and then the standards of application of safety instrumented system in the process industry including oil and gas industry are mainly mentioned and discussed in this report. Especially the standard *Functional safety of electrical/electronic/programmable electronic safety related systems* (IEC-61508, 2010) and the standard *Functional safety – safety instrumented systems for the process industry sector* (IEC-61511, 2003) are very important standards for introducing safety related systems that involve E/E/PE technology. In addition, *Norwegian oil and gas application of IEC 61508 and IEC 61511 in the Norwegian Petroleum industry* (NOG-070, 2004) gives the summary of these standards and related applications in oil and gas industry.

2.3 Safety Instrumented Systems

As indicated in subchapter 2.2, the system-critical system should include at least one of E/E/PE technology. This kind of system may also be referred as the term safety instrumented system (SIS) in the process industry, which is used as a protection layer between the hazards of the process and the public (Rausand and Lundteigen, 2014). For the rest of report, SIS is used in line with the term in process industry instead of safety critical system. A typical SIS shown in Figure 2.1 consists of at least three subsystems:sensor subsystem, logic solver subsystem and final element subsystem.

- *Sensor subsystem* also called as $input\ elements$. The function is to monitor the state of

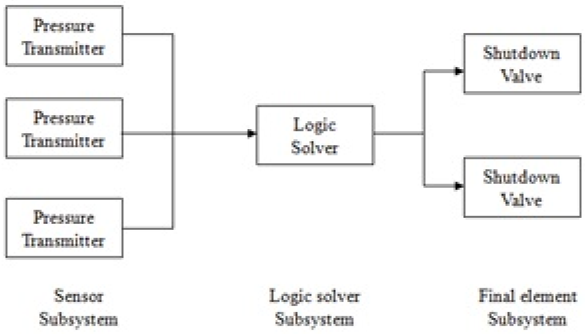


Figure 2.1: A typical SIS system

EUC and detect the undesired event and send the electrical signal to the logic solver. For example, fire and gas detectors in the process industry.

- *Logic solver subsystem* received the electrical signal from at least one sensor and determine of required actions based on the interpretation of signals. The logic solver is also considered "brain" of the SIS. The programmable logic controller (PLC) is the typical logic solver automation and safety of electromechanical processes, control system, shutdown system and so forth. When the SIS has n logic solvers, it may require k out of n logic solvers to agree on the following actions.

- *Final element subsystem* also called as *actuating devices*. The function is to perform the safety function to prevent harm. The final elements could be more than one to perform the same function. A group with n identical final elements can function when at least k of n channels are functioning, then it is said to be a $koon$ *voting*. As show in Figure 2.2, when three valves located on the same pipeline, each can stop the pipeline therefore it is a 2oo3 voting.

2.3.1 Safety-instrumented Functions

Safety-instrumented Function (SIF) is a function that has been intentionally designed to protect the EUC against a specific demand. However, a safety function is not necessarily to be a SIF and a SIS can perform more than one SIF. Then it is imprecise to say the reliability of a SIF is the same as the reliability of the SIS or the safety loop which is performing the SIF. A SIS that implements a

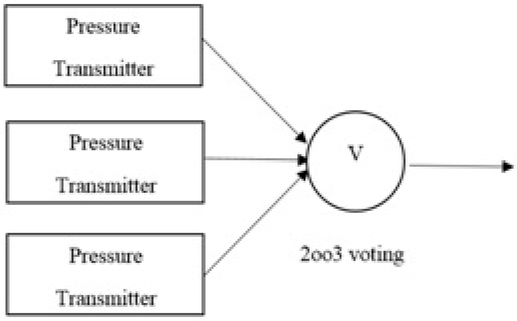


Figure 2.2: 2oo3 voting system

SIF is not only designed to perform the SIF on demand, but also to keep SIF in deactivates state without the presence of demand.

2.3.2 Modes of Operations

According to the IEC 61508 (IEC-61508, 2010), *demand* is the condition that activates the SIF, and it is normally categorized based on how often the SIF are demanded. Normally, once per year is considered as the borderline but the rationale behind has not been clearly argued in related standards.

- *Low-demand mode*: is operated seldom and demanded less than once every year
- *High-demand mode*: is operated frequently and demanded more than once every year
- *Continuous mode*: is operated continuously. The safety function is always at demand, and is also a special case of high demand mode.

It is important to distinguish the difference between the low-demanded mode and high/continuous mode. A SIF in EUC with low-demanded mode is usually kept passive and only activate when there is the response. A SIF that operates in high/continuous mode plays an active role in control of the EUC. The importance of classification is revealed in the calculations of reliability assessment which would be introduced in subchapter 2.6, since the input parameter and calculated formula are different based on the demand mode.

2.4 Failures and Failure Modes

A *failure* is the event that terminates the ability of required function where a *failure mode* is to tell how the item or system fails to perform the required function (Rausand and Lundteigen, 2014). The *failure rate* is described as frequency of occurrence of failure in the certain time period.

The(IEC-61508, 2010) also indicates two types of failures:

- The random hardware failure. It can be caused by aging, inadequate maintenance, excessive stress and human errors, but some analysts may not agree on that human errors and excessive stress should be classified as random hardware failure.

- The systematic faults. It is related to the deterministic cause in design phase, operational phase, documentation and other relevant factors resulting from systematic failures, which means that the appropriate modification of the design, manufacturing process and operational procedures will availably eliminate such faults.

  The category of hardware failures/faults based on consequence and detect ability is of vital importance in calculation of reliability of SIFs, which can be distinguished as:

- Dangerous undetected (DU) faults: This kind of failure will bring the component into fail state and can be only revealed by proof-test or occurrence of demand. The DU faults mainly contribute to SIF unavailability.

- Dangerous detected (DD) faults: This kind of failure will terminate the item to perform the required function and can be detected in the short time or immediately.

- Safe undetected (SU) failure: The failure will not cause the item to perform safety functions.

- Safe detected (SD) failure: The failure is not dangerous and can be detected by automatic self-testing.

2.5 Testing Interval of SIS

Test is one of the important ways to detect the potential failure, which has the significant influence on the system reliability. There are two parameters *interval* and *coverage* can be use to describe two types of test:

- *Proof test*: It is used to reveal DU failures before a demand occurs. The time region between initiations of proof tests is called proof test interval. The proof test coverage is expressed as the percentage of DU failures that are detected during a proof test, which means that the higher value of coverage, then the better proof test. In general, the proof test is important to prevent DU failures in low demand system. However, it is not so evident in high demand system since the demand rate is so high so that there is not enough time for high demand system to response for restoration. Then contribution of DD failure to PFH is considered as negligible.
- *Diagnostic test*: It is used to automatically detect the specific failure to avoid fully shutdown, usually in shorter time interval than proof test. The Diagnostic test coverage can be expressed as the ratio between the dangerous failures detected during diagnostic tests and the all dangerous failures.

2.6 Reliability Measures

Probability of failure on demand (PFD) is most widely used reliability measure in low-demand system. It can be expressed as the probability that SIF operated in low-demand mode cannot be performed at time t when there is a dangerous failure.

$$\text{PFD}(t) = \Pr(\text{The SIF cannot be performed at time } t) \tag{2.1}$$

In the practical cases, the average value of PFD is used rather than a function of time. As assumptions in (Rausand and Lundteigen, 2014) , a SIF is proof-tested after regular intervals of length t and the system is considered to be as good as new after proof test. Then long term average probability of failure on demand can be expressed as follows, where the two key parameters are 1) estimated failure rates from large data collection and 2) the typical test interval.

$$\mathrm{PFD}_{avg} = \frac{1}{\tau}\int_{\tau}^{0} \mathrm{PFD}(t)dt. \tag{2.2}$$

PFDavg can be interpreted in two ways according to formula:

- It can be the probability that SIF cannot be performed in response to the demand or
- It is able to be expressed as mean proportion of downtime that item cannot perform required function.

For the typical SIS, the simplified equation could be easily used in calculations of PFDavg, the PFD of SIS can be the sum of the PFDs of three individual elements. This simplified equation is originally driven from Markov models, unlike Markov model, however, the time dependent failures or sequence dependent failures are not involved in the simplified equation, which means that the simplified equation cannot be used for analysis of programmable logic solvers.

$$\mathrm{PFD}_{SIS} = \sum \mathrm{PFD}_{IE} + \sum \mathrm{PFD}_{LS} + \sum \mathrm{PFD}_{FE} \tag{2.3}$$

Frequency of dangerous failure per hour (PFH) is defined as the time-dependent frequency given as number of dangerous failures per hour for SIF operated in high or continuous demand. High-demand means that the SIS is seldom proof-tested since the higher demand rate results in no time for response. The time interval (0, τ) can be the proof test interval if the SIS is proof-tested or be chosen as estimated lifetime of the SIS if the SIS is not proof-tested. The average PFH in time interval (t_1, t_2) is

$$\mathrm{PFD}(t_1, t_2) = \frac{E(N_D(t_2)) - E(N_D(t_1))}{t_2 - t_1} \tag{2.4}$$

Where $N_D(t_i)$ denotes the mean number of dangerous failure in interval (t_1, t_2).

In the part 6 of (IEC-61508, 2010), the approximation formula is calculated for a group of channels or single channel and assumed the channels are independent and any parallel structure of channels constitutes identical components. The IEC formula is calculated as follows,where two parameters are used : 1) group failure frequency $\lambda_{D,G}$; and 2) group-equivalent mean downtime $t_{G,E}$ and the approximation is adequate when $\lambda_{D,G}\ t_{G,E}$ is small. :

$$\text{PFD}_{avg} = \lambda_{D,G} t_{G,E} \tag{2.5}$$

In addition, there are two other parameters to derive the formulas: 1) Channel dangerous failure rate λ_D and 2) Channel equivalent mean downtime $t_{C,E}$ where ith failure t_{G,E_i} for multiple channel failures in $koon$ voted group does not result in group failure.

$$t_{C,E} = \frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{2} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{2.6}$$

$$t_{G,E_i} = \frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{n-k+2} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{2.7}$$

Where MRT is the mean repair time after detected failure and $MTTR$ is the mean time to restoration.

Consider a $1oo2$ system as the example, then the first dangerous failure occurs with $2\lambda_D$ and means downtime of a single channel is $t_{C,E}$; the dangerous group failure occurs if the second channel fails when there is one failed channel. The probability is then $1 - e^{-\lambda_D t_{C,E}}$is approximated as $\lambda_D t_{C,E}$ if it is less than 0.1. Then $\lambda_{D,G}$ is approximated as $\lambda_D^2 t_{C,E}$.Then group-equivalent mean down time $t_{G,E}$ is equal to $\frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{3} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR$. The similar reduced equations are achieved for $1oo1$, $1oo2$, $1oo3$, $2oo3$, $1oo4$, $2oo4$.

If the CCFs is considered to contribute in IEC formulas, then the standard beta factor model is suggested to use. For $1oo2$ system, the PFD_{avg} includes CCF can be expressed as:

$$\text{PFD}_{avg} = 2[(1-\beta_D)\lambda_{DD} + (1-\beta_D)\lambda_{DU}]^2 t_{C,E} t_{G,E} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}(\frac{\tau}{2} + MRT) \tag{2.8}$$

Where β is the factor of common cause failure and β_D indicates the fraction of detected dangerous failures in the common cause failure factor and is usually assumed to be 0.5.

The part 6 of (IEC-61508, 2010) also provides the similar approximation formulas for PFH. Then $PFH_{G,i}$ for a $koon$ voted group is determined as follows, where for a $1oo1$ system the PFH is equal to the frequency of DU:

$$\text{PFH} = \lambda_{DU} \tag{2.9}$$

$$\mathrm{PFH}_{G,i}^{koon} = n \begin{pmatrix} n-1 \\ n-k \end{pmatrix} (\lambda_D^{(i)})^{n-k+1} (\lambda_{CE}^{(i)})^{n-k} \tag{2.10}$$

For a $1oo2$ system the formula of PFH is shown as:

$$\mathrm{PFH}_{1oo2} = 2[(1-\beta_D)\lambda_{DD} + (1-\beta_D)\lambda_{DU}]^2 t_{C,E} + \beta_D \lambda_{DD} + \beta \lambda_{DU} \tag{2.11}$$

For most of the SIS low demand mode has been assumed, and a considerable amount of literature has been focused on this kind of system. In recent years, however, the research emphasis has been shifted in the discussion of high demand mode. The main differences between PFD and PFH can be driven from three aspects:

- PFD is the probability that fails to function when demand, where PFH is the frequency given as the number of dangerous failures per hour
- PFD is applied in calculation of the low demand mode where has enough time for proof-test. PFH is applied in calculation of the high demand mode or continuous mode where there is no time for response of proof test due to the higher demand rate.
- DD failure contribute less significantly to the calculation of PFH, since the demand rate is so high that there is no enough time to repair or restore the system.

When the demand rate close to once per year, the choice of these two reliability measures may lead to the different conclusion. However, conclusion has not been drawn in the Rausand's book (Rausand and Lundteigen, 2014) yet. For the further treatment of this issue, see (Jin et al., 2011) and (Liu and Rausand, 2011) . In addition, Hauge (2013) provides the further discussion about choice between PFD and PFH.

2.7 Safety Integrity Level

Safety integrity is defined as the performance measure for a SIF in the IEC-61508 (2010) . The Safety integrity level (SIL), measures for safety performance of the system in order to reduce the risk and increase the safety for system. SIL is divided into four, SIL1, SIL 2, SIL 3 and SIL 4, with SIL 4 being the most reliable and SIL 1 being the least.

The (IEC-61508, 2010) distinguishes between hardware safety integrity, software safety integrity and systematic safety integrity. In Rausand's book (Rausand and Lundteigen, 2014), hardware safety integrity is mainly introduced and is covered partly in random hardware safety integrity. If a SIF is said to meet the SIL requirement, then each of these three integrities must be fulfilled. There is a close relationship between reliability measures and safety integrity. Safety integrity is particular application rather than generic statement since it is related to reliability measures with some specific conditions, such as stated period of time. Average PFD and PFH are mainly used for safety integrity, which has already been introduced in the previous sub-chapter 2.6. In Rausand's book (Rausand and Lundteigen, 2014), there are several important terminology issues should be noticed:

- A SIL is always related to a specific SIF instead of a SIS
- A SIL is to evaluate the whole safety loop (including sensors, logic solver, and final elements) instead of any subsystem or components

2.7.1 SIL Requirement

To achieve a given SIL, there are three main types of requirements that must be fulfilled in (NOG-070, 2004):

- *Quantitative requirement,* expressed as PFD or PFH. A quantitative analysis should include random hardware failure, common cause failure and relevant failures. Separate function can be certified, but required failure probability should be verified for complete function so that the SIL requirement applies to a complete function instead of individual component that perform the function. Since PFD is used as the demand rate per year, where PFH is defined as frequency per hour and one year is approximately 10^4 hours, then there is 10^4 difference in values between two different modes on the same SIL as observed in Table 2.1.
- *Qualitative requirement,* expressed as architectural constraints besides PFD and PFH requirement which can be given in terms of three parameters:

Table 2.1: SIL for safety functions on different modes (modified from (NOG-070, 2004), Table8.1)

Safety Intergrity Level	**Demand Mode of Operation (PFD)**	**Continuous/ High Demand of Operation(PFH)**
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Table 2.2: Architectural constraint on type A subsystem (modified from (NOG-070, 2004) , Table 8.2)

Safety Failure fraction	**Hardware fault tolerance**		
	0	1	2
$< 60\%$	SIL1	SIL2	SIL3
$60\% - 90\%$	SIL2	SIL3	SIL4
$90\% - 99\%$	SIL3	SIL4	SIL4
$> 99\%$	SIL3	SIL4	SIL4

1. Hardware fault tolerance (HFT): in the IEC 61508 , it is defined as the digit to show the ability of a hardware subsystem to continue to perform a required function when there are faults or errors. If there is a channel that still is able to perform the required function as normal under the condition that other channels fails, then the HFT of the system is 1. For example, $2oo3$ voted group is HFT=1.

2. Safe failure fraction (SFF): it is defined as in IEC 61508, the ratio of the failure rate besides DU failure to the total failure rate, where the total failure contains the safe failure SD, SU and dangerous failure DU, DD.

3. *Types of subsystem*: all possible failure modes can be determined for all constituent components for type A system but the behavior of type B subsystems cannot be completely determined for at least one component. The relevant information is given in Table 2.2 and 2.3.

- *Avoid and control systematic faults.* The systematic faults are the faults in hardware and software corresponding to design, operation and maintenance or testing. This kind of fault is not quantified in (IEC-61508, 2010) and (IEC-61511, 2003). But there are some certain measures are recommended in order to avoid and control systematic faults during

Table 2.3: Architectural constraint on type B subsystem (modified from (NOG-070, 2004) , Table 8.3)

Safety Failure fraction	**Hardware fault tolerance**		
	0	1	2
$< 60\%$	Not allowed	SIL1	SIL2
$60\% - 90\%$	SIL1	SIL2	SIL3
$90\% - 99\%$	SIL2	SIL3	SIL4
$> 99\%$	SIL3	SIL4	SIL4

the design phase.

2.7.2 SIL Allocation

SIL allocation is the process in order to optimize the design to meet the SIL requirement for a SIF. The methods of SIL allocation can be categorized as:

- Qualitative methods, which determine the SIL from knowledge of risks associated to system. The typical method is Risk Graph.

- Quantitative methods, which are required to compute the reliability of SIS based on the failure rate and repair rate of components. Fault Tree Analysis (FTA), Markov approach and Petri-Nets are the well-known methods to fulfill the requirement.

- Semi-quantitative methods, which assign the value but not necessarily based on exact measurements. The most widespread method is *Risk Matrix*, which defines SIL according to the extent of risk and the frequency of occurrence. The other methods like Layer of Protection Analysis (LOPA) and Event Tree Analysis (ETA) are also recommended. *Minimum SIL requirement* is usually used in Norwegian oil and gas industry for commonly used SIFs, which is not described in the (IEC-61508, 2010) but is suggested in (NOG-070, 2004).

Chapter 3

Blowout Preventer System

3.1 System Introduction of Blowout Preventer

The BOP system is one of the safety critical parts of the subsea drilling system since it acts as the final barrier to prevent loss of well control. In addition, the BOP system is used for a range of routine operational tasks, such as casing pressure and formation strength tests (British-Petroleum, 2010).

There are three important components of the BOP system: lower marine riser package(LMRP), BOP stack and control system. The BOP system includes two types of preventers: ram preventer and annular preventer. In addition, the valves and piping (choke lines and kill lines) are used to maintain pressure control in the well. A typical subsea BOP system is shown in Figure 3.1.

A typical subsea BOP system is equipped with five to six ram preventers and one or two annular preventers. Annular preventers are located above ram preventers since their working pressures are different from ram preventers. The typical configuration has two shear rams in order to establish a redundant system to increase the reliability. The BOP stack is attached to the wellhead with a hydraulically operated, high-pressure wellhead connector attached the LMRP to the marine drilling riser. The detailed discussion for each main element is presented as follows (British-Petroleum, 2010).

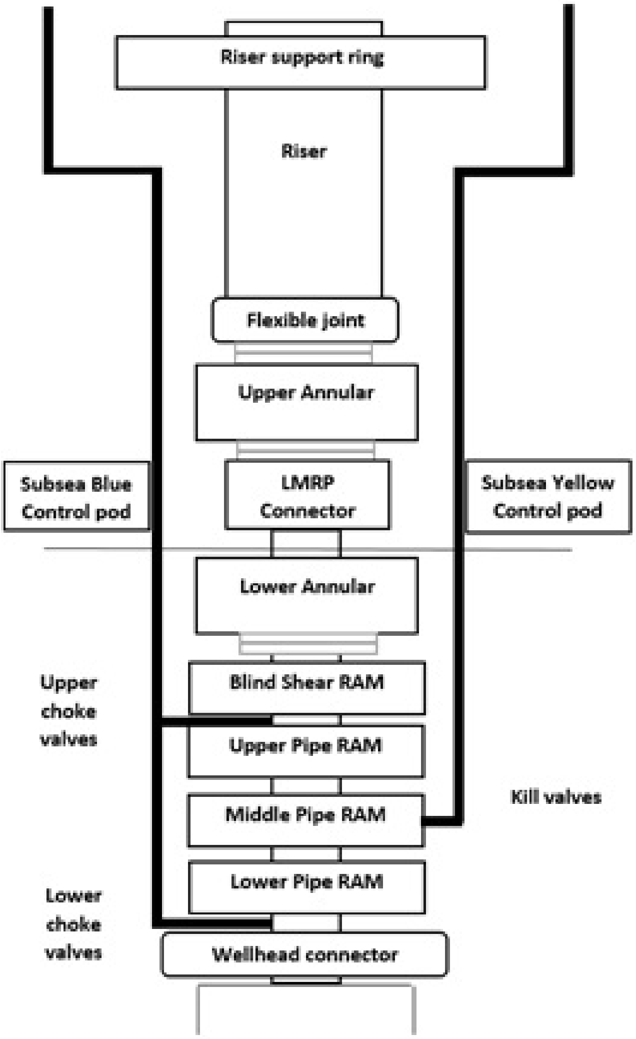


Figure 3.1: A typical BOP structure, modified from (NOG-070, 2004), Figure A.22

3.1.1 Main Elements of LMRP

The LMRP mainly consists of flexible joint, annular preventer, control pods, LMRP connector and choke and kill line connector:

- Flexible joint: this component is located at the top of the LMRP. It is designed to handle up to angular deflection from vertical axis of BOP (no more than 10 degree).

- Annular preventer: the function of upper annular preventer is to seal the wellbore annulus while drill pipe is running through LMRP and BOP stack. The lower annular preventer is acting as the first barrier of BOP to close around the drill pipe when there is an accident. It is installed above the ram preventers, since the working pressure of annular preventer is 10000 psi when close around the pipe and 5000 psi when close on the open hole, which is lower than the working pressure of ram preventers (Transocean, 2011).

- Control pods: It provides the communication between the LMRP and BOP stack components and the surface control system. The two pods are usually called as “blue pod” and “yellow pod”, which are identical and redundant modules. There is generally a spare pod located on the rig besides the blue pod and the yellow pod. The control pods can activate all the BOP functions, which makes safety and reliability of control pods is of importance.

- LMRP connector: It provides the connection between bottom of LMRP and the top of BOP stack. It allows the disconnection of the LMRP when there is the requirement of repairing control pods, and in event of an emergency or loss of rig dynamic-position station keeping.

- Choke and kill line connector: It connect between choke and kill lines on the LMRP and BOP stack with hydraulically operation.

3.1.2 Main Elements of Blowout Preventer Stack

BOP stack mainly consists of blind shear ram, casing shear ram, pipe ram, wellhead connector, choke and kill line valves and BOP stack hydraulic accumulators.

- Blind shear ram (BSR): it is used to cut the drill pipe and seal the wellbore and can be actuated in two modes: under 3000 psi closing pressure, or 4000 psi closing pressure. The activation of BSR is the last-option in case of emergency since it can completely seal off the wellbore, which leads to the serve damage of the equipment and rig downtime.

- Casing shear ram (CSR): it is similar to the BSR when drill pipe, casing and tool joints. The cutting ability of CSR is designed to be higher than BSR but it cannot seal the wellbore. The CSR is critical if cutting the heaviest drill pipe or casing is beyond the ability of BSR.

- Pipes ram: there are three type of pipe ram based on the positions: upper, middle and lower. They are designed to close and seal on tubular with specific range of outer diameter (OD). For lower pipe ram, it is usually referred as the "test ram". Based on the design principle, there are two types: 1) standard pipe rams can seal with specific OD tolerance and 2) variable bore rams (VBR) can seal must of tubular dimension.

- Wellhead connector: this hydraulically-actuated connector can be used to connect the BOP stack to subsea wellhead housing.

- Choke and kill line valves: they are operated in fail-safe 'close' and can be used to isolate the choke and kill line piping connections to the BOP ram.

- BOP stack hydraulic accumulators: .The accumulator store pressurized hydraulic fluid at 5000 psi CSRs supplied from topside hydraulic power unit (HPU). It will be reduced to 4000 psi by manually-set hydraulic regulators when the accumulator bottles are used for normal closing operation of the high-pressure BSRs and high-pressure operation. The leak of accumulators will affect both pods.

There are various types of stack configurations even all BOP stacks are principally similar. For traditional BOP stack, which is still in use in many offshore locations, all the pipe rams are standard and there is not any CSR installed in BOP system. The disadvantages are revealed distinctly, since the pipe ram can only seal with certain OD tolerance, which is not in favor of the redundancy of BOP system. Moreover, the exclusion of CSR would lead to the insufficient ability for shearing the heavy pipe.

For modern BOP stack, there is only one standard pipe ram instead of three in traditional stack for improvement in redundancy. And the modern BOP stack is equipped with the CSR for increasing the ability for shearing in the most demanding well control situations. This type of BOP stack is usually referred as standard stack configuration.

Deepwater Horizon (DWH) BOP stack was the one that used in Macondo well. The only difference between the standard BOP stack and DWH BOP stack is the pipe rams, where pipe rams in DWH BOP stack are all VBRs and lower pipe ram is the test ram. Compared to the standard BOP stack, three VBRs increase the flexibility and redundancy to shear tubular OD to the new higher level, and the test ram reduce the prepared time before the test starts and resumed time after the test completes. However, the converting of normal pipe ram to test ram results in the loss of redundant annual sealing function since the test ram can only seal the wellbore pressure from above but not from below.

3.1.3 Main Elements of Control System

Unlike most of BOP components actuated hydraulically, the multiplexed (MUX) control system involved in performing most of the BOP desired functions is supported by both electrical/electronic and hydraulic components. The control systems are mounted both at topside and subsea BOP.

On the topside, the main component is the central control unit (CCU), which generally consists of two control panels: the driller's control panel (DCP) and the toolpusher's control panel(TCP). Each of control panels equipped with two PLCs, sometimes three PLC forming as the triple modular redundant (TMR) subsystem (Cai et al., 2012b). The main function of CCU is to provide electric power when the signals from those control panels on the topside transmitted to the subsea control pods (both blue and yellow pods) through the MUX cables.Besides the electric power supply for control system, there is the hydraulic fluid supply system supplied from the reservoir connected with an HPU. The pod selector valve is able to guide the fluid to the selected pod, and further directs to subsea accumulators after activating the pods. Two identical and redundant subsea electronic modules (SEM): SEM A and SEM B are located in each control pod, and can be activated when the surface fluid supply is directed accordingly.It can be used for energizing the solenoid valves then the high pressure fluid is directed into the shuttle valve.

In addition, the SEMs can monitor and transmit the relevant data from instruments located on the BOP system to the surface for decision-making.

3.2 Function Identification of Blowout Preventer System

The NORSOK standard (D-010, 2004) indicates that *"there should be two well barriers available during all well activities and operations"*. Based on this principle, there are always at least two well barriers, where the fluid column of drilling mud is defined as the primary well barriers and the BOP system then becomes one of the secondary barriers. Others could be the casing, casing cement and the wellhead.

If the BOP is considered as the well barrier, then the essential BOP function is to shut in the well in event of emergency. There are three defined sub-functions of BOP to prevent blowouts and well leaks (NOG-070, 2004):

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

Function 1 above is mostly performed in common situation. Both annular preventers and pipe ram preventers can perform this certain function for the purpose. There can be limitations to when the pipe rams work properly, such as closing on drill collars, tool joints, perforation guns, etc.

Function 2, as indicated before, the blind shear ram can seal the well on the open hole. To be noticed, only when the drilling pipe is not running through the BOP then function 2 is involved.

Function 3 above the drill pipe has to be sheared before the well can be sealed off. Failure in performing this intended function in the BOP system will directly lead to the loss of well control. In subsea drilling operation, the shear rams is of importance to seal and the mud column as the primary barrier is significantly contributed to the wellbore pressure. Factory acceptance testing is performed for the BOP to shear a pipe and is considered as a destructive test.

3.3 Failure Identification of Blowout Preventer System

After presenting the system familiarization and functions identification of BOP, the failure identification of BOP should be required to complete the initial analysis of BOP system. This analysis can be carried out through some qualitative methods such as failure mode, effects and criticality analysis (FEMCA) and hazard and operability study (HAZOP). In this section, the brief summary of failures identification the failure modes identified in (Holand, 1999), (Holand, 1987) and (Holand, 1997) and author's judgment.

The failure modes for each component of the BOP system can be demonstrated separately in following:

- Flexible joints: As Holand (1987) and Holand (1999) indicates that: more failures in flexible joint when the ball joints were used in earlier days. In general, the observed failures in the flexible joints are rare.

- Annular preventers: there are two main failure mode observed in Phase II report (Holand, 1999): *Internal leakage* failure and *Failed to fully open* failure. They both lead to pull up the BOP or the LMRP. Most of the internal leakage failures is observed on the wellhead failure and the rest is occurred on the rig when the BOP was tested prior to running (Holand, 1999). The failure mode 'failed to fully open' is the well-known annular problem and it is not that safety critical but contributes to the rig downtime. According to Holand (1997) and Holand (1997), this type of failure is reduced significantly compared to the 80s.

- Ram-type preventers: there are several types of failure mode in ram preventers:

  Failed to close: This can cause the leakage on the BSR from the shuttle valve and also has the problems with BSR shuttle valve for shearing.

  Failed to open: it is considered as a rare failure mode in previous study, however, several failures are observed in Phase II report.

  Internal leakage (through the closed ram): This failure is in the BSR sealing area.

  External leakage (bonnet/door seal): This can cause the leakage to sea in bonnet sealing areas.

All those failure modes can be summarized as: 1) the internal failure of ram preventer to close (pipe ram), shear and seal (BSR) and shear (CSR); 2) shuttle valve to preventer leaks. According to Holand (1987), however, due to improved preventive maintenance and some minor design modifications, the failure rate of internal and external leakage has decreased significantly during the past years.

- Hydraulic connectors: The *external leakage* to environment and *failed to unlock* are the most frequent observed failures. Failed to unlock LMRP connectors is a most important failure model since the failure in disconnection can cause the riser damage and large rig downtime. To prevent the external leakage in the wellhead is of great importance of controlling a well kick.

- Choke and kill valve: there are basically two types: *internal leakage* and *external leakage*, where the failure mode internal leakage is usually considered as less important since there require the extra leakage to allow the well fluid reach the surrounding if choke and kill valve both in failed state.

- Control systems: there are three main BOP control system principles: MUX control system transmit the MUX pilot signal to pods, pre-charge pilot hydraulic control system can reduce the BOP function response time by pre-charge pressure and pilot hydraulic control system to activate the pilot valves (Holand, 1999). The failure modes could be: surface control valve failure, external leakage in pilot line, fails to select, equipment failure, pilot signal failure from topside and so forth.

- Backup control system: In Norway, the back-up control systems has been required since 80s, however, in countries like Brazil and Italy, the back-up control system is not mandatory. The back-up control system uses the acoustic signal transmission. As suggested by Holand (1987), the typical failure is on the topside acoustic equipment.

Due to the limited pages, the complete list of all the possible failure is not developed in this report. Here recommending reviewing the FTA developed in Phase II report for familiarization of all the possible failures in the BOP system.

3.4 Reviews of Blowout Preventer System Reliability Assessment

After reviewing most of the aspects and conception for SIS reliability assessment and building the basic understanding of the BOP system, then the problem formulation should be carried out. To achieve this objective, it is necessary to have the quick review of the previous BOP reliability studies to show the key contributors and authors for reliability analysis of the BOP system and identify the relevant approach. Besides, the possible weaknesses in these analysis approaches are identified, which trigger for the further discussion and problem formulation.

There is a considerable amount of literature concerning reliability of subsea BOP system. A comprehensive study of Subsea BOP performance in the North Sea between 1978 and 1986 was carried out by Holand (1987). Besides that, SINTEF spent more than two decades to collect data and information of BOP system during this period. The most recent and widely recognized report for BOP reliability studies is the technical report Reliability of Subsea BOP systems for Deepwater Application, Phase II DW written by project leader Per Holand and reviewed and commented by Marvin Rausand (Holand, 1999). It is based on the reliability experience from BOPs that have been used in the US GoM OCS from 1997 to 1998, which provides the reliable data for failure in most components of BOP based on the reliability experience from wells drilled.

The subsequent reliability assessment of the BOP system is based on those literatures in some degree, such as the report for analysis of deepwater kicks and BOP performance (Holand and Skalle, 2001), the report using Markov methods investigating performance of BOP systems (Cai et al., 2012b), the report using Bayesian Networks for evaluating reliability of BOP control system (Cai et al., 2012a). The Phase II report (Holand, 1999) is the most widely used one, since it generates the clear description of failure modes in the BOP system by developing the FTA and provides the reliable data source based on the daily reports.

However, there are some weaknesses existing in the previous approach of BOP reliability assessment, even though in the widely acceptable approach indicated in Phase II report (Holand, 1999). Here, the main difference in the construction of BOP stack, modelling approach and relevant assumption in the calculations method are identified as the weakness in previous study:

- Construction of BOP stack: In Phase II report (Holand, 1999), the BOP stack is similar to the traditional stack without CSR as indicated before. The exclusion of CSR decreases the shearing capacity of the BOP, which result in the lower redundancy level in event of cutting drill pipe.

- Modelling approach: FTA is used in (Holand, 1999)'s report for reliability assessment since FTA is the most common quantitative method in reliability assessment. However, for typical redundant system like the BOP system, the FTA may not be the most suitable model for reliability assessment. (Liu and Rausand, 2011) suggest Markov method because of its flexibility. Some other methods like Petri-net and Bayesian method can also be the alternatives. The further discussion about the potential weakness of FTA would be discussed in the following subchapter 4.3.

- Updating information: due to lacking of generic data, the uncertainty generated from the expert judgement sometimes lead to the imprecise reliability assessment. Bayesian Network provides the diagnostic analysis based on the calculation of posteriors will help for facing this challenge. Besides that, in the on-going pratical situation, the Bayesian Network model will also provide the way for updating the reliability assessment when the test data or faulty state of system, subsystem or components is available for analysis.

Chapter 4

Bayesian Network in Reliability Assessment

4.1 Introdution of Bayesian Network

4.1.1 Basic Conceptions of Bayesian Network

There are three basic causal networks should be introduced before starting the Bayesian networks. According to Jensens' book (Jensen, 1996), they are serial connections, diverging connections and converging connections. In these connections, when there is a link connects the variable A to variable B then variable B is a *child* of variable A, and variable A is a *parent* of variable B. It is obvious that the certainty of variable of parent would have the impact on the child and vice versa. If taking diverging connections as the example, when the certainty function of variable B is increasing, the certainty of variable A will increase inversely; the increased certainty of variable A is expected to have the increased certainty of variable C or D.

For the serial and diverging connection, when the variable V between variables A and B are given evidence, or neither V or descendants of V have received evidence for converging connection, then A and B are called *d-separated*. If A and B are not d-separated then them are called as *d-connected*. For instance, in serial connections of Figure 4.1, if variable B is given, then A and B are called as d-separated or independent. Similarly, B, C, D are d-separated given A in diverging connections, or B, C, D are independent when nothing known about A in converging connections (Jensen, 1996).

Bayesian network (BN), is the widely used method, dealing with representing uncertain knowl-

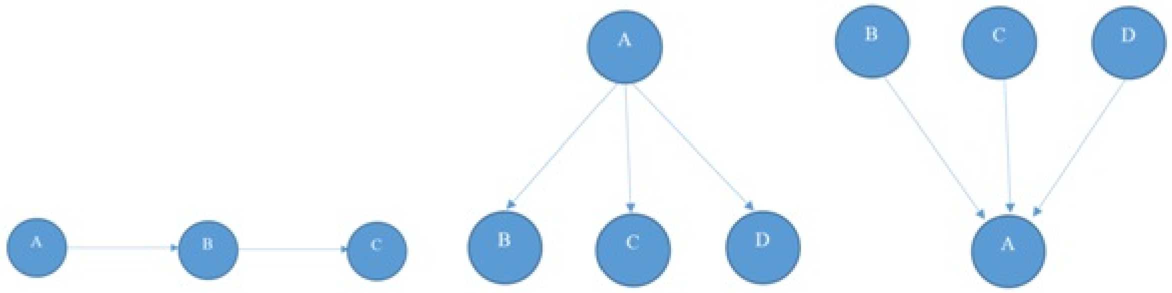


Figure 4.1: Serial, diverging and converging connections

edge of probabilistic systems in a variety of real-world problems. It can be expressed as the graphical representation which consists of a directed acyclic graph (DAG) formed by variables together with the directed edges and conditional probability table (CPT) for conditional probabilities of variables on all corresponding parents (Jensen, 1996). The connected nodes means that they are conditional dependent on the parent nodes, where the nodes that are not connected are conditionally independent of each other. It means if there are variables or nodes without any parent then they are called as the *root nodes* and the unconditional probabilities or *prior probabilities* for such variables should be specified.

Variables in a model which are neither hypothesis variables nor information variables are called mediating variables. Usually mediating variable will increase the precision of model, but there is a risk of increasing the complexity.

The quantitative analysis of BNs relies on the conditional independence assumption and causal dependence between nodes by developing the CPT for each node. The marginal posterior probability $P(X|E)$ for each variable X can be computed by using different classes of algorithms, where a set of variable E called as evidence, which means that the condition or the observation of variables is known. Then for the joint probability distribution of a set of variables $[X_1, X_2.....X_n]$, it gives as follows, where $P[X_i]$ states for the parent of variable X_i:

$$P[X_1, X_2.....X_n] = \prod_{i=1}^{n} P[X_i|P(X_i)] \tag{4.1}$$

The quantitative analysis of BNs can be both forward (or predictive) analysis and backward (or diagnostic) analysis. In forward analysis, the probability calculation of occurrence of any node is based on the prior probabilities of the root nodes and the conditional dependence of each node,

Table 4.1: Conditional probability of P (A|B)

	b_1	b_2	b_3
a_1	0.2	0.3	0.1
a_2	0.2	0.3	0.2
a_3	0.6	0.4	0.7

Table 4.2: Joint probability for variables A and B

	b_1	b_2	b_3
a_1	0.06	0.09	0.04
a_2	0.06	0.09	0.08
a_3	0.18	0.12	0.28

where root nodes are the nodes without parent nodes. In the backward analysis, the calculation of the posterior probability of any given set of variables given some evidence is considered as the instantiation of some of the variables to one of their admissible values (Bobbio et al., 2001).

4.1.2 Probability Calculation of Bayesian network

Conditional probability is the basic concept in Bayesian causal networks. It gives that the statement of probability of event A is $P(A|B)$ given the event B. The basic rule for conditional probability calculation is $P(A|B) \times P(B) = P(A,B)$, where the $P(A,B)$ states for the probability of joint event of A and B. And this formula can also be read as $P(A|B) \times P(B) = P(B|A) \times P(A)$ and this yields the well *Bayes' rule*.

When the variable A has states $a_1, a_2 ... a_n$ and variable B has states $b_1, b_2 ... b_n$ then the probability distributions of variable A and B are $P(A) = (a_1, a_2 ... a_n)$ and $P(B) = (b_1, b_2 ... b_n)$ respectively, where $\sum_{i=1}^{n} a_i = 1$ and $\sum_{j=1}^{n} b_j = 1$. Then the basic rule could be apply for calculate the joint probability and conditional probability for variable A and B. In Table 4.1 for conditional probability of $P(A|B)$, we firstly assign the conditional probability of variables A and B, and it can be easily found that the sum of each column is equal to 1. Then if P (B) = (0.3, 0.3, 0.4), we can get Table 4.2 for joint probability of variables A and B by using basic rule, and we can summarize the $P(A) = \sum_{i=1}^{n}(a_i, b_j) = (0.19, 0.23, 0.58)$. Similarly in Table 4.3, the conditional probability P (B|A) can be calculated by applying Bayes' rule in 4.1, where P (B) = (0.3, 0.3, 0.4) and P (A) = (0.19, 0.23, 0.58).

Table 4.3: Conditional probability of P (B|A)

	b_1	b_2	b_3
a_1	0.32	0.26	0.31
a_2	0.47	0.39	0.21
a_3	0.21	0.35	0.48

Table 4.4: States Identification of Example

Rain soon (true)	It will rain soon
Rain soon (false)	It will not rain soon
Cloudy weather (true)	Cloudy
Non-cloudy weather (false)	Not cloudy
Weather forecast reports rain (true)	Weather forecast reports rain before
Weather forecast reports rain (false)	Weather forecast don't reports rain before
High humidity (true)	humidity increase
High humidity (false)	Feeling that humidity is normal as usual

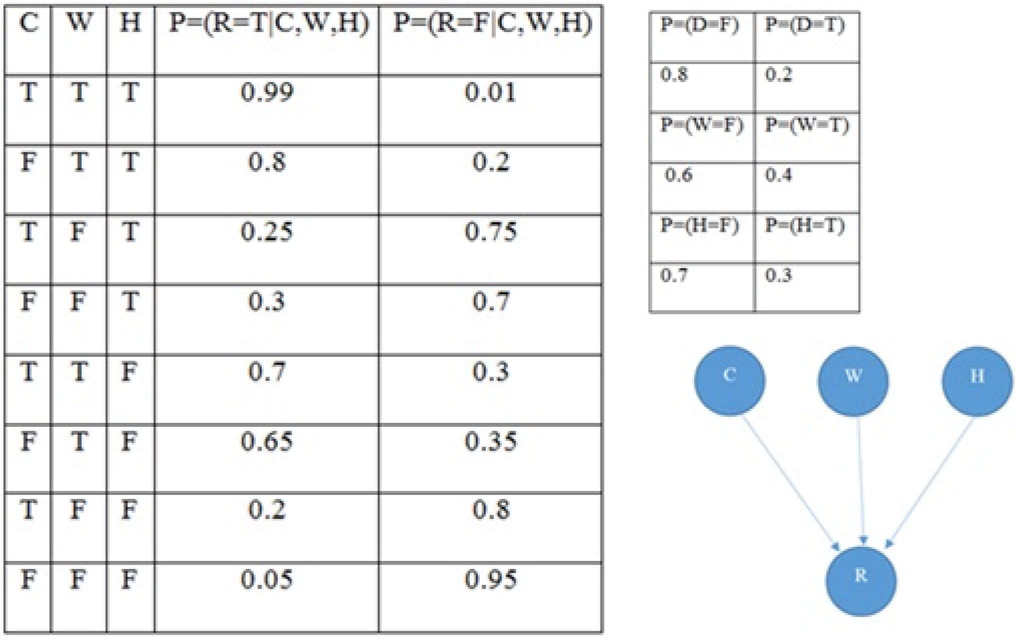
4.1.3 Building Bayesian Network Model

There are generally three steps for organizing the BBN model:

- Identify the hypothesis event
- Provide information variables for certainty estimation
- Build up causal structure after identifying the relationships between variables.

To explain how to build a Bayesian model, here is a simple example starting with two hypothesis events, namely *'rain soon* and *'no rain soon.* Therefore, the hypothesis variable (child) is called as R-soon (rain soon) with states y and n. Then three information variables (parents) are defined as C (Cloudy), W (weather forecast reports rain), H (high humidity) with two states y and n, which will indicate the child variables or be influenced and impacted by child variables. Then the states for all variables are shown in the Table 4.4, in this example, only binary states (true and false) are assigned. Finally, we can estimate simple conditional probability for each variable by subjective estimation based on experience in Figure 4.2.

Noted conditional probability table in this example is relatively small since only three variables with two states have been assigned. In the large-scale BBN model within numerous components, the CPT would enlarge geometrically and the increasing interactions between subsys-



C	W	H	P=(R=T|C,W,H)	P=(R=F|C,W,H)
T	T	T	0.99	0.01
F	T	T	0.8	0.2
T	F	T	0.25	0.75
F	F	T	0.3	0.7
T	T	F	0.7	0.3
F	T	F	0.65	0.35
T	F	F	0.2	0.8
F	F	F	0.05	0.95

P=(D=F)	P=(D=T)
0.8	0.2
P=(W=F)	P=(W=T)
0.6	0.4
P=(H=F)	P=(H=T)
0.7	0.3

Figure 4.2: Causal networks with probabilities for example

Table 4.5: Posterior probability for child variable when Pr (R=T) =1

	Pr(F)	Pr(T)
Variable C	0.7612	0.2388
Variable W	0.1985	0.8015
Variable H	0.5940	0.4060

tems will become too cumbersome to be involved in the computation. Then some software applications are suggested to estimating the probabilities and implement computational model, such as (HUGIN, 2015) suggested by (Jensen, 1996). In this paper, the software (Matlab, 2014) is suggested to be used in computational model.

We can get the marginalized probability of event R by computational software Matlab. Then the probability of event R occurs is $Pr(R = T) = 0.3828$, where the corresponding $Pr(R = F) = 0.6172$, which means that the probability of raining soon is 38.28%. Moreover, the diagnostic analysis can be performed by computing the marginal probability of all parent variables when the evidence is given that it will rain soon. Then the posterior probabilities of parent variables when the evidence of R is given are shown in Table 4.5 and Table 4.6.

Table 4.6: Posterior probability for child variable when Pr (R=F) =1

	Pr(F)	Pr(T)
Variable C	0.8241	0.1759
Variable W	0.8490	0.1510
Variable H	0.7657	0.2343

Table 4.7: Joint probability for example(C,W,H,R)

C	W	H	R	Values
1	1	1	1	0.3326
2	1	1	1	0.0672
1	2	1	1	0.0560
2	2	1	1	0.0168
1	1	2	1	0.1008
2	1	2	1	0.0234
1	2	2	1	0.0192
2	2	2	1	0.0012
1	1	1	2	0.0034
2	1	1	2	0.0168
1	2	1	2	0.1680
2	2	1	2	0.0392
1	1	2	2	0.0432
2	1	2	2	0.0126
1	2	2	2	0.0768
2	2	2	2	0.0228

From the second column of Table 4.5, it can be found out that the posterior probabilities of Pr (C=T) =0.2388, Pr (W=T) =0.8015, Pr (H=T) =0.4060, which means that the severity rank of parent variables is: W>H>C. According to the first column in Table 4.6, the severity rank of parent variables when there is no rain follows the similar rule, but this relationship is not revealed distinctly. In addition, the joint probability could be also computed by Matlab, where the sum of values in Table 4.7 is equal to 1.

4.2 Comparison between Bayesian Network and other methods

In the past, Bayesian network is generally used in development of the artificial intelligence and industrial engineering decision making strategy (Jensen, 1996), since this method can deal with the error and uncertainty in probabilistic computation model when lacking of statistical data for prior probability estimation. Recently, due to the ability of information updating for Bayes' theorem, Bayesian network was starting to be applied in the reliability assessment of large complex system, such as software-based system (Gustav, 2000), simple structural system (Sankaran et al., 2001) or as an alternative for traditional reliability assessment method (Bobbio et al., 2001). However, so far few researchers have performed the reliability assessment in the subsea BOP system.

There are many traditional reliability assessment methods, such as reliability block diagram (RBD), fault tree analysis and event tree analysis. Similar as Bayesian Network, these methods are developed based on the description of the system flow chart of system functions. Compared to those methods, however, Bayesian Network can update the system information or perform the reassessment of reliability when the test data of system or components becomes available. It is one of the biggest differences between the other methods and Bayesian Network: when information or observations are provided for some nodes or the whole system, also called as "given evidence", it can "renew" the performance assessment of any other components or the whole system, which is impossible to obtain by all these methods.

There are some other advanced methods for reliability assessment, like Markov method or Petri-net method, and they are generally used in dynamic analysis of the complex system. However, one of the difficulties is that the reliability engineers should identify all the possible states before building the model. It may be hard for the expert of reliability engineering but who is unfamiliar with the specific system.

4.3 From Fault Tree Analysis to Bayesian Network

In this section, FTA is the one analytically compared to BN by investigating how FTA can be translated into BN without losing any details and obtaining the advanced modelling power simultaneously,and the unreliability of the top event (TE) or subsystem of FTA can be also calculated as the prior probability of target variable in faulty state when given no evidence in BN model, while backward (diagnostic) analysis can also compute the severity ranking of components. Basically, FTA can be analyzed both qualitatively and quantitatively, and minimal cut-sets method is most frequently used in quantitative part.

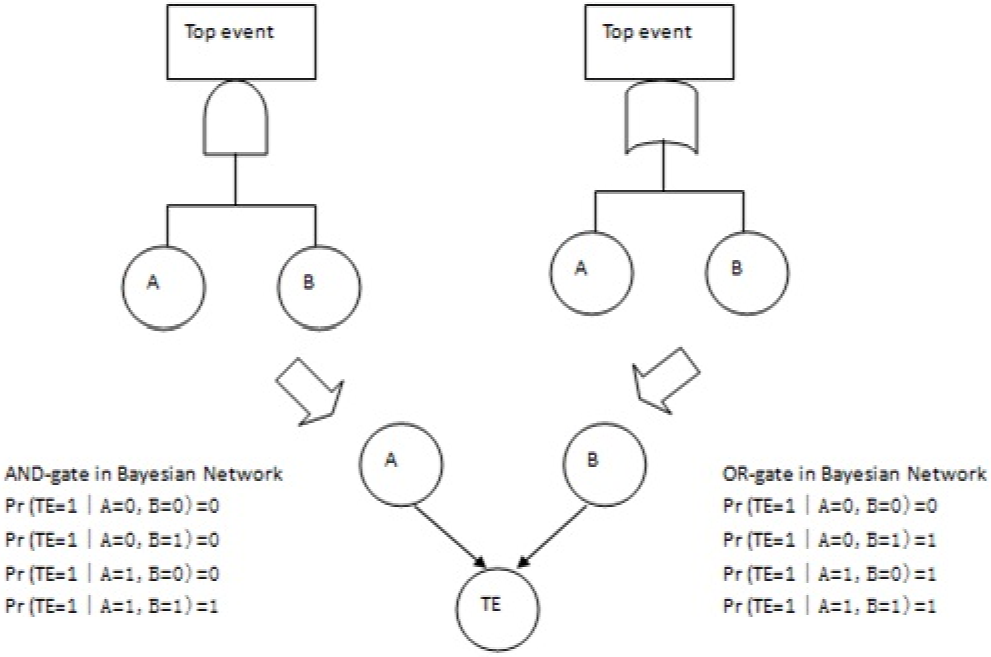


Figure 4.3: AND-gate and OR-gate in Bayesian Network

Compared to FTA which is the mostly applied method in reliability assessment of subsea BOP system in the past decades, BN model can avoid generating duplication of basic nodes or events, which reduce the model size and make the system more easily to be understood, especially in the large and complex system with many components and complicated interrelation between components. Moreover, some unnecessary assumptions in FTA can be removed when translating into BN: (1) the binary gates (AND gate and OR gate) are replaced by the probabilistic gates; (2) the general binary states (survival or failure) for components in FTA are extended to be multiple states in BN; (3) components are no longer statistically independent.

FTA can be translated by an algorithm (Bobbio et al., 2001) or automatically by the software named RADYBAN (Cai et al., 2012a). Kim (2011) also provides the method for mapping RBD into BN. Here taking the algorithm method as the example to show how the AND-gate and OR-gate could be translated into BN nodes.

As Figure 4.3 shown above, we have two basic events A and B, where the value 0 and 1 represent non-fault state and fault state, respectively. It is noticed that the translation of AND-gate and OR-gate from FTA results in the same DAG in BBN but with the different corresponding CPTs.

4.3.1 Common Cause Failure in Fault Tree and Bayesian Network

SIS is widely applied in the oil and gas industry to reveal the hazards and eliminate the consequence to human, material assets and the environment. To achieve this objective, the SIS is often equipped with redundant system with various degrees. For example, in BOP system one can find the control pods has two identical subsystems, yellow pod and blue pod within associated components, forming the most typical redundant system. However, CCFs have serious impacts on the reliability of SIS, lead to simultaneous failures of redundant system. According to Rausand and Lundteigen (2007), CCF cause into root cause and coupling factor. A root cause is a basic cause like extreme environment condition (e.g. bad weather and deep water depth). A coupling factor reveals that failures of components caused by the same root cause (e.g. same design and same maintenance).

Since the subsea BOP system is the typical redundant system, then the CCFs can have a strong impact on the BOP system. It means that the CCF should be treated more carefully in reliability analysis of the BOP system. As Rausand and Lundteigen (2007) argued that, the oil and gas industry should pay more attention on CCFs in the design phase of SISs than the operational phase. Many projects and institutions have contributed to the reliability analysis and data collection. The OREDA project is carried out by oil companies to collect reliability data based on the maintenance reports from single item failure, however, this approach cannot properly collect the information related to CCFs. The Norwegian Petroleum Safety Authority (PSA) is increasingly focused on independence reduction between SIFs (Rausand and Lundteigen, 2007).

There are two methods for inclusion of CCF in FTA: *implicit* and *explicit*. The explicit method is to treat CCF as the separate event in the logic model by adding an OR-gate directly to the top event of FTA; CCF in the implicit method is considered as the term in the minimal cut set, which which implies the cause-effect relationship between failure and some failure cause (Hokstad and Rausand, 2008). According to the literature review for this topic, both methods have their own defects. Generally, there is few high quality data for explicit method, according to Rausand and Høyland (2004), the explicit method will receive the more accurate result than implicit method even with low quality of data. As argued by Lundteigen and Rausand (2009), however, for the system with more than one type of common causes, the implicit method would keep the fault tree simple and avoid incorrect inclusion of dependent events in the FTA. The Markov

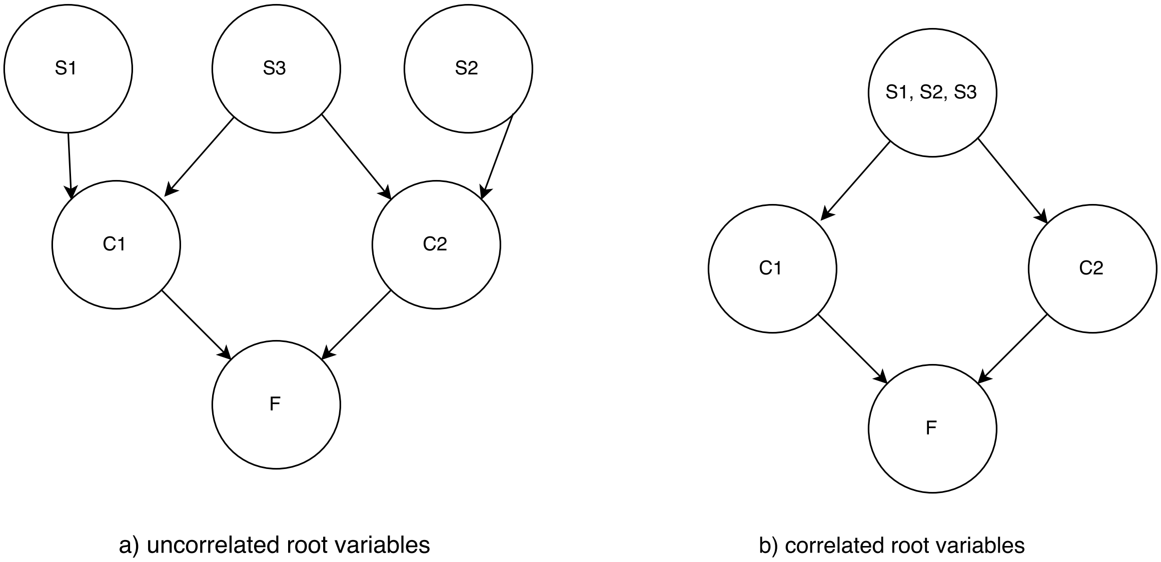


Figure 4.4: Common Cause Failure in Bayesian Network

technique can be used to model both implicit and explicit cause for system consisting of fewer components (Hokstad and Rausand, 2008).

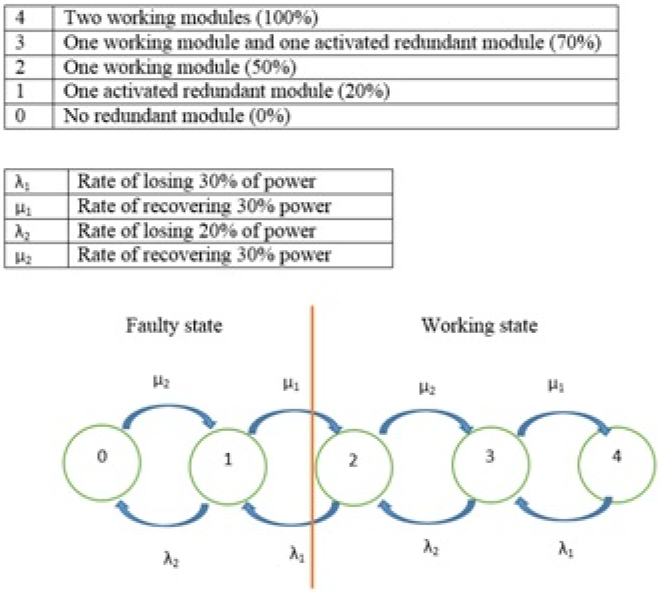
The example for allocating common cause failure in BN model is shown in Figure 4.4, where S$_i$ stands for the root nodes which lead to the failure of component C$_i$ and F stands for the system state. For Figure 4.4 a), the root nodes are uncorrelated, which means that only variable S2 acts as the CCF since it can lead to the failure of both basic variables. For Figure 4.4 b), the root node insists of all the correlated root variables associated with joint probability for computation. In this case study, the uncorrelated root variables are mainly applied for inclusion of CCFs and only one common cause component is considered for each redundant system. According to the property of binary gates in FTA, sometimes the root CCF in BN can be directly linked to the desired event to avoid the repeating

The identical components or the components sharing the same working or desgin mechanism are considered to be dependent and susceptible to the common cause failure, such common cause failures will be indicated as the root variables, for example, when component i and component j share one common cause, then S$_i$ and S$_j$ represent the independent root nodes where S$_{i,j}$ indicates the root node that directed to both child nodes.

4.3.2 Advanced Modelling Power of Bayesian Network Compared to Fault Tree

Accurate reliability estimation requires the high quality of data resource as the input for the classic reliability assessment. However, in the realistic cases, there is limited number of observed data can be obtained from the daily reports. Then the estimated parameters based on the experience and the expert judgement should be provided and contributed significantly, even through the uncertianty of such estimation will generate the inaccurate result. This is one of the common problem among the traditional reliability estimation approaches, however, it can be solved in BN by introducing random variables instead of deterministic values in FTA. In addition, one of the most unique characteristics of BN is the ability for updating the information of occurance probability of the root variables when the certain states of the other variables are observed. BN with this ability is able to deal with the uncertainty of parameter since posterior probability can be updated when new information is provided, then uncertainty will be reduced continuously through re-analysis (Nima et al., 2011).

In addition, it allows multi-state variable to be easily accommodated into DAG, where there are only two states can be taken into account in FTA. In the real case, some parent variables may not always have or have no effect on the child variables, for example, assumed that there is an additional variable called "human interface" has three states: positive, irrelevant, negative, where irrelevant means that variable has no effect on its child variables. Sometimes variables may have the different levels of effect, for instance, a processing system may have two modules as the redundant system. Assumed power supply spends 50% of total working voltage for each modules and there will be the abnormal performance in defective working state when only one module can work (one working module can support to perform the desired function sufficiently but the redundant module is not activated, where redundant module is activated when abnormal voltage is provided for it). Suppose this variable has five states with different percentages of power: 100%, 70%, 50%, 20% and 0%, with respect to two working modules, one working module with one activated redundant module, only one working module, only one activated redundant module and no redundant system, respectively. Obviously, compared to FTA, the multi-states in BBN model is closed to the real case and can be easily applied in the large complicated redundant system. This kind of analysis is allowed in some dynamically analysis method such as Markov method, as shown in Figure 4.5. However, there would be at least three nodes for the



4	Two working modules (100%)
3	One working module and one activated redundant module (70%)
2	One working module (50%)
1	One activated redundant module (20%)
0	No redundant module (0%)

λ_1	Rate of losing 30% of power
μ_1	Rate of recovering 30% power
λ_2	Rate of losing 20% of power
μ_2	Rate of recovering 30% power

Figure 4.5: Markov model of processing system

description of one component with three states, which makes an extremely large Markov model with a large number of components.

Another advantage of BBN is that it can remove one basic assumption in FTA, when means that it allows one to find the dependent failures between variables. From the example about power supply above, it is known that the modules will stop working due to the loss of power supply, but it may also induce the other variables besides modules to break down, such as sensors. This kind of dependence between failure of power supply and failure of sensors is not possible to be allocated in FTA. However, this can be modeled in BN model by assuming corresponding states and adding entries of CPT.

4.4 Example: Fault Tree based Bayesian Network Model

Here providing a simple example for mapping FTA into BN model. The original example is summerized from the part of FTA in the Appendix 1 of PhaseII report (Holand, 1999), where the top event is the "The control system is not operative" and the input data is estimated by author's judgement and generic data, which is not very realistic but that is enough for demonstrating how the model works. The contruction and corresponding analysis for FTA are carried out by

Table 4.8: Prior probability and posterior probability of basic events

Basic Event	Priors (Example1)	Posteriors (Example1)	Priors (Example2)	Posteriors (Example2)
CPODEX	0.007293	0.5981	0.0071	0.5870
PODEXBP	0.065633	0.3952	0.065633	0.4045
PODEXYP	0.065633	0.3952	0.065633	0.4045
SELECT	0.0005208	0.0427	0.0005208	0.0439
Accumul	0.041675	0.04168	0.041675	0.04168
IVYP	0.004687	0.00469	0.004687	0.00469
IVBP	0.004687	0.00469	0.004687	0.00469
CSELE	0.0000521	0.0043	0.000051	0.0042
SELEBP	0.000469	0.0028	0.000469	0.0029
SELEYP	0.000469	0.0028	0.000469	0.0029
ACPVEL	0.0005208	0.000521	0.0005208	0.000521
CIV	0.0005208	0.000521	0.00051	0.0006

the software program (CARA, 1996) developed by SINTEF, and the corresponding FT-based BN model is generated by software (HUGIN, 2015).

In this example, assumed that components sharing the same working mechaism or design principle (IVYP and IVBP, SELEBP and SELEYP and PODEXBP and PODEXYP) would have only one common cause failure, then the FT can be simplified with explicit inclusion of CCF and established as Figure 4.6 shown. All the components are assumed to be non-repairable and the experimental time is assumed as 5000 hours, so prior probabilities calculated as as probabilities on demand are shown in first column of Table 4.8.

Firstly, according to the analysis of CARA Fault Tree, one can find that there are nine cut sets for this fault tree, where the cut set means that the top event will occur when all the compoenents in one cut set are in the faulty state. According to Holand (1999), the unavailability is calculated as the mean fractional deadtime (MFDT) of the component, considering the component within a constant failure rate λ and the failures are assumed to be found at the fixed test interval τ:

$$\text{MFDT} = (\lambda \times \tau)/2, \text{assumed that } \lambda\tau \ll 1 \tag{4.2}$$

Noted that in practical case, the test interval will rarely be fixed and some systems are redundant system (each singel components will be tested simultaneously), which means that this formula will get the optimistic results in both case. In addtion, Holand (1999) indicated that some fail-

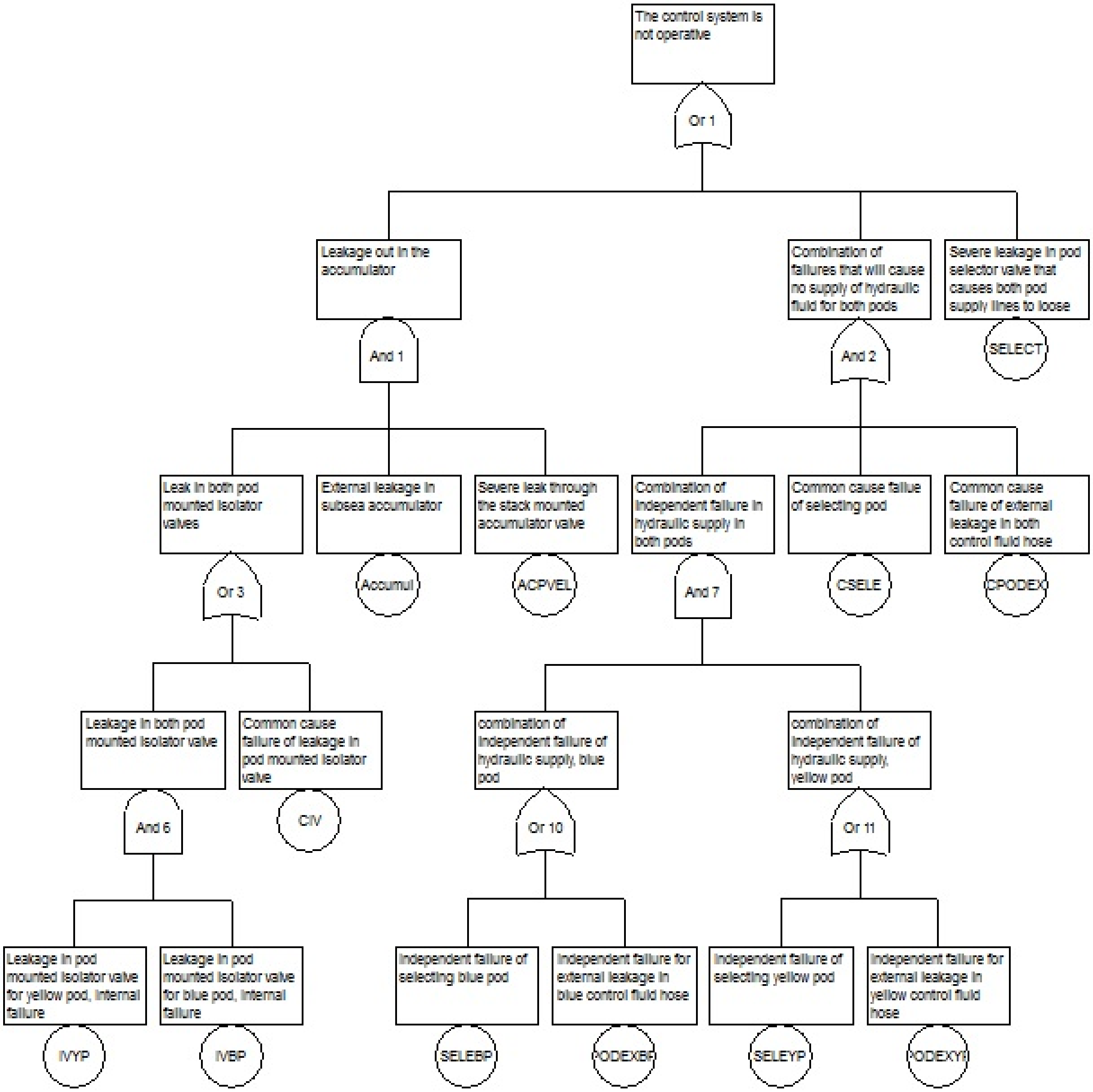

The control system is not operative
Or 1
Leakage out in the accumulator
Combination of failures that will cause no supply of hydraulic fluid for both pods
Severe leakage in pod selector valve that causes both pod supply lines to loose
And 1
And 2
SELECT
Leak in both pod mounted isolator valves
External leakage in subsea accumulator
Severe leak through the stack mounted accumulator valve
Combination of independent failure in hydraulic supply in both pods
Common cause failue of selecting pod
Common cause failure of external leakage in both control fluid hose
Or 3
Accumul
ACPVEL
And 7
CSELE
CPODEX
Leakage in both pod mounted isolator valve
Common cause failure of leakage in pod mounted isolator valve
combination of independent failure of hydraulic supply, blue pod
combination of independent failure of hydraulic supply, yellow pod
And 6
CIV
Or 10
Or 11
Leakage in pod mounted isolator valve for yellow pod, internal failure
Leakage in pod mounted isolator valve for blue pod, internal failure
Independent failure of selecting blue pod
Independent failure for external leakage in blue control fluid hose
Independent failure of selecting yellow pod
Independent failure for external leakage in yellow control fluid hose
IVYP
IVBP
SELEBP
PODEXBP
SELEYP
PODEXYP

Figure 4.6: Simple example for FTA, modified from Appendix 1 of Phase II report(Holand, 1999)

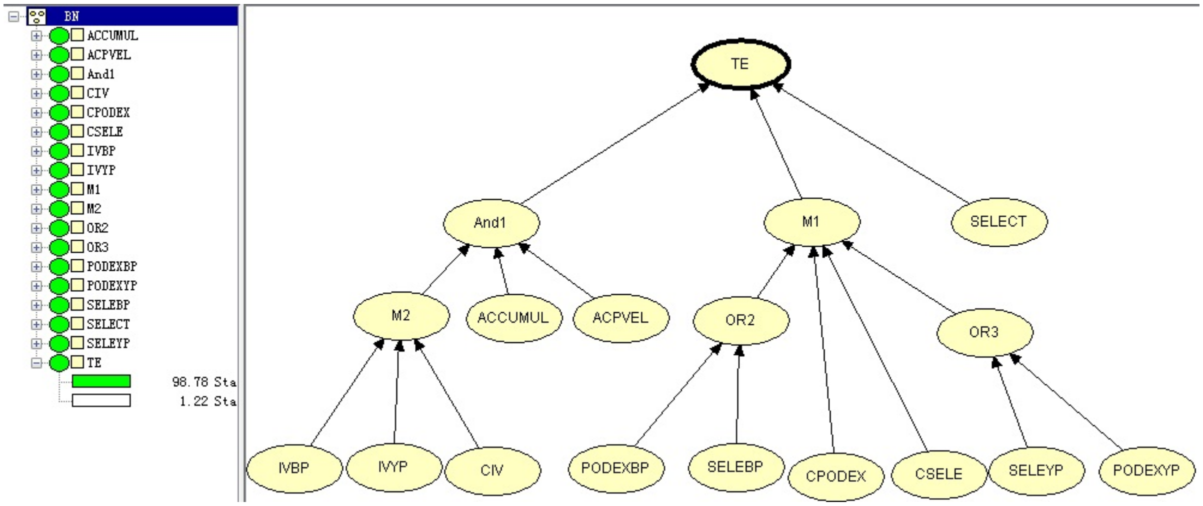


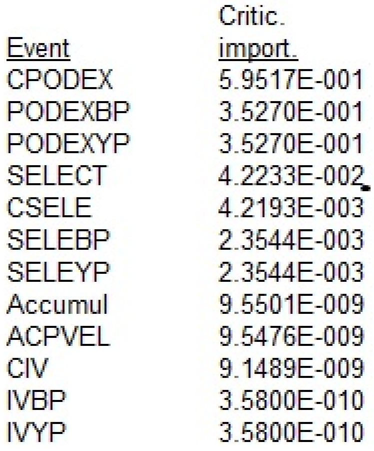
Figure 4.7: FT-based BN model for Example 1 in software HUGIN

ures in control system are observed when they occur, not only during the testing. So that the calculated results will be conservative.

4.4.1 Example 1: Updating information and Severity Ranking

According to the result of CARA Fault Tree, the unavailability of top event is equal to 1.2192×10^{-2} when the test interval is 5000 hours. Based on this fault tree, Example 1 is created in the HUGIN as shown in Figure 4.7. One can find out that the size of model is reduced because of the employment of probabilistic gate by modifying CPTs. And the unavailability is calculated as the 0.0122 based on prior probabilities, which yields the same result using tranditional method FTA.

The marginal posterior probability for each single basic event given the total system is malfunction can be computed and reported in the second column of the Table 4.8. Noticed that the posterior probabilities of "CPODEX","SELECT","PODEXBP","PODEXYP","SELEBP","SELEYP" and "CSELE" increase when compared to corresponding prior probabilities. This measure sometimes can be explained as the indication of the criticality of component given faulty system, where the variable within high posterior probability indicates that it is more vulnerable than others. One can see that CCFs have serious influence to the system: the posteriors of CCF in this example are higher than corresponding posteriors for independent failure of components, even though priors are much lower.



Event	Critic. import.
CPODEX	5.9517E-001
PODEXBP	3.5270E-001
PODEXYP	3.5270E-001
SELECT	4.2233E-002
CSELE	4.2193E-003
SELEBP	2.3544E-003
SELEYP	2.3544E-003
Accumul	9.5501E-009
ACPVEL	9.5476E-009
CIV	9.1489E-009
IVBP	3.5800E-010
IVYP	3.5800E-010

Figure 4.8: Component importance of basic events

Moreover, one can compute the component importance, which can measure how the change in the reliability of component will result in the comparatively change in the reliability of the total system. As shown in the Figure 4.8,the criticality importance for each component is calculated and ranked by CARA Fault Tree. The component i is called critical if the other components of the system are in such states that the system is functioning if and only if component i is functioning. Then the critical importance $I^{CR}(i|t)$ of component i is the probability that component i is critical and failed at time t when the failure of system at time t is known (Rausand and Høyland, 2004). In FTA, since $Q_0(t)$ denotes the unavailability of the top event and $q_i(t)$ denotes the unavailability of the component i, then the critical importance could be calculated based on following equation :

$$I^{CR}(i|t) = \frac{\partial Q_0(t)}{\partial q_i(t)} \times \frac{q_i(t)}{Q_0(t)} \tag{4.3}$$

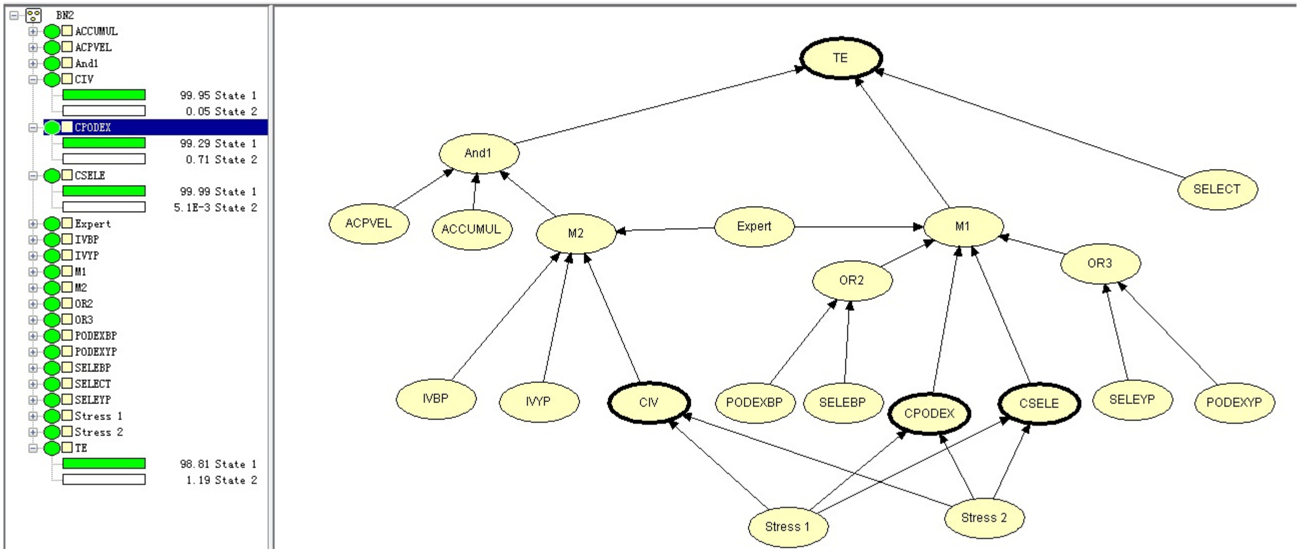
However, we can noticed that the severity ranking based on marginal posterior probability is a little bit different from the component importance computed by FTA, for example, "Accumul" seems more critical than "SELEBP" and "SELEYP" based on ranking of marginal posterior probability but reverse based on the criticality importance. This situation could be explained away: one can observe from Table 4.8 that the posterior probabilities of components change after providing information the faulty of TE except variables "Accumul", "IVBP", "IVYP" , "CIV" and "ACPVEL". It means that those components become independent to the top event because the related cut sets [Accumul, ACPVEL, CIV] and [Accumul, ACPVEL, IVYP, IVBP] are almost imposible to happen and those variables do not conribute to malfuntion of system. Since the value of Accumul is higher than values of "SELEBP" and "SELEYP" , then it will provide the wrong information of indication of criticality. One solution is to reset the failure rate of "Accumul" to become lower than "SELEBP" and "SELEYP" . The new result shows that this change of prior probability has no influence on the unavailability of system and the identification of critical events based on marginal posterior probability and minimal cutset will finally become the same.

In fact, the joint posterior probability for each single component given system failure as evidence is able to provide the more useful and precise diagnostic analysis than the analysis based on marginal posterior probability or based on criticality importance. In the Bayesian Network, there is a direct method to get the most probable one of all possible states of variables given evidence, which is also called as most probable explanation (MPE). The BN model is able to obtain the most probable state of all root nodes and non-root nodes through MPE. In this case, when using the MPE concept, the most probable state is faulty state of root variables "CPODEX" and functioning state of other root variables. Then the joint posterior probability of MPE (only concerns root nodes) is shown as follows, where the variable within overline represents the variable is in the functioning state:

$$\mathrm{Pr} = \mathrm{Pr}[\mathrm{CPODEX}, \overline{(\text{other root nodes})}|\mathrm{TE}] = \frac{\mathrm{Pr}[\mathrm{CPODEX}, \overline{(\text{other root nodes})}, \mathrm{TE}]}{\mathrm{Pr}[\mathrm{TE}]} = 0.4945 \quad (4.4)$$

The obvious benefit of MPE is to find the desired result without obtaining all possible states, in this case the state size is $2^{12} = 4096$, where 12 root nodes are involved. To be noticed, MPE implies the most likely state is not always the same as the result of minimal cutset method (Nima et al., 2011). In addition, MPE also implies that the other variables have little contribution to the failure of the syatem.

Posterior probabilities obtained through the calculation of Example 1 could be used for information integration, combining with the judgments of experts, generic data and test data during development. Then the impact of uncertainty from expert judgement or simulation results



```
BN2
ACCUMUL
ACPVEL
And1
CIV
    99.95 State 1
     0.05 State 2
CPODEX
    99.29 State 1
     0.71 State 2
CSELE
    99.99 State 1
   5.1E-3 State 2
Expert
IVBP
IVYP
M1
M2
OR2
OR3
PODEXBP
PODEXYP
SELEBP
SELECT
SELEYP
Stress 1
Stress 2
TE
    98.81 State 1
     1.19 State 2
```

Figure 4.9: FT-based BN model for Example 2 in software HUGIN

would be gradually lower by repetition of generating BN model. For more details of information intergation and updating approach, please check the methods proposed by Peng et al. (2013).

4.4.2 Example 2: Multiple State and Dependent Failure

As we discussed before in section 4.3.2, advantage of modeling power for BN model, the application of multi-state and dependent failure, can be demonstrated by the modification of the Example 1.

Since control pods with blue and yellow pods have the associated redundant components:"IVYP" and "IVBP", "SELEBP" and "SELEYP" and "PODEXBP" and "PODEXYP", then assumed that there are two variables within different-levels of stress: "Stress 1" (High stress, Normal stress, Low Stress) and "Stress 2"(High stress, Low Stress) for estimation of effect for CCFs. The corresponding model for inclusion of such variables is shown in Figure 4.9.

Besides, assumed there is a group "Expert" within two experts (exp1 and exp2) to estimate the probabilities that the component will survive under the occurrence of CCFs. To be noticed, the occurrence and new assigned values of CCFs become independent to the internal or independent failure of related components and the survival probabilities estimated by experts only has influence on the CCFs. The related assigned values for "Stress 1" & "Stress 2" and "Expert" are reported in Table 4.9 and Table 4.10, respectively, where "Stress 1" has prior as [High (0.3), Nor-

Table 4.9: CPT of root nodes "Stress 1" and "Stress 2"

Stress 1	Stress 2	CIV	CPODEX	CSELE
High	High	0.0010416	0.014586	0.00010416
Normal	Low	0.0003906	0.00546975	0.00003906
Low	High	0.0005208	0.007293	0.0000521
High	Low	0.0005208	0.007293	0.0000521
Normal	High	0.0007812	0.0109395	0.00007812
Low	Low	0.0002604	0.0036465	0.00002604

Table 4.10: Simplified CPT of root node "Expert"

Expert	CIV and CPODEX and CSELE	M1 and M2
exp1	one CCF (M2)	0.01 (survive)
exp2	one CCF (M2)	0.05 (survive)
exp1	two CCFs (M1)	0.05(survive)
exp2	two CCFs (M1)	0.1 (survive)

mal (0.2), Low (0.5)], "Stress 2" has prior as [High (0.4), Low (0.6)], "Expert" has prior as [exp1 (0.6), exp2 (0.4)]. Since the CPTs for M1 and M2 would be increasly enlarged, here the assumption is made that the effect of different CCFs are treated equally and the states for non-CCFs follows the rule of AND-gate to avoid the long table.
Through the analysis result generated by HUGIN, one can easily find out that:

1. After introducing two stress variables, the priors of CCFs of Example have been decreased a little bit. The posteriors of "CPODEX" and "CSELE" in Example 2 are lower than the posteriors in Example 2, however, the posterior of "CIV" becomes higher and no longer independent as in Example 1.

2. Posteriors for all the other non-CCF variables have a bit increase compared to Example 1, except the cut-set [Accumul, ACPVEL, IVYP, IVBP].

3. After calculating the posteriors, the information variables "Expert", "Stress 1" and "Stress 2" have been updated to [0.6058(exp1),0.3942(exp2)], [37.56(H),20.84(N),0.4160(L)],[0.5008 (H), 49.92(L)], respectively. One may conclude that the reliability for each expert remians the same. There is a increase in High degree in "Stress 1" while Low degree decreases, and degrees of "Stress 2" get balanced.

4. After the modification, the prior probability of leaf node "TE" decreases from the 1.22% to

1.19%, indicating the effect of uncertainty in the model. And the MPE configuration within probability as 0.045 indicates that the state of informative variables "Expert", "Stress 1" and "Stress 2" become exp1, High and High, respectively.

By reviewing these examples, one may conclude that the FT-based BN model can update the reliability prediction when the component-level or system-level test data become available. In fact, when the new information on any variables are provided in Bayesian Network, the probabilistic peformance of all the other variables would be updated. In addition, the advanced modeling power of BN, probabilistic gates, multiple states and the inclusion of correlations among variables (especially for common cause failure) can also be revealed by these two examples.

Chapter 5

Case study: Reliability Assessment of BOP System in Base Case

The objective of this case study is to demonstrate the application of Bayesian Network in reliability assessment of the BOP system with different configuration stack under the most demanding situation, mainly focus on the effect of pressure conditions of the wellbore. Based on the discussion of two examples in the last chapter, the reliability predicition and the analysis for criticality ranking based on updated performance when given information can be carried out in this case study.

5.1 Case Introduction

5.1.1 Description of Case Study

According to the subchapter 3.2, there are three essential functions in BOP system:

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

For the most frequent situation as recorded by Holand and Skalle (2001) within largest proportion (85.4 precent), all the annulars and pipe rams can seal around the drill pipe (Function 1) and the CSR and the BSR are able to shear drill pipe and seal off well (Function 3) when needed (the open hole situation requiring the Function 2 is only recorded as 4.2 precent of cases). Considering the operation of sealing off the well results in the huge downtime and possibility of closing the well entirely, then the first attempt is always to perform the Function 1 instead of Function 3.

Performing Function 1 always starts with closing annulars. If both annulars fail to close, then the forward operation is to close one of the pipe rams (normally to close the lower ram first to keep the hydrocarbon as far as away from the rig). If the BOP fails to perform the Function 1, then the activation of BSR is required for Function 3. The relevant reliability block diagrams for Function 1 and Function 3 are reported in Figure a Reliability block diagram for the base case and Figure b Reliability block diagram for the base case , respectively. However, if the pressure in the wellbore is too high, the redundancy of the BOP system is therefore lost from 1oo5 to 1oo3. Since the working pressure of annular preventers is only 5000 psi, which is much lower than the working pressure of ram preventers (15000 psi), then the high pressure situation may result in the malfunction of annular preventers. Besides that, it is assumed that under the high pressure situation, the drill pipe or casing is becoming heavy, then performing Function 3 may requires BSR and CSR works at the same time since the CSR is designed to have larger shearing ability than BSR. Then the reliability block diagrams for Function 1 and Function 3 under high pressure situation are reported in Figure c Reliability block diagram for the base case and Figure d Reliability block diagram for the base case , respectively.

Different configurations of the BOP stack are presented in Table 5.1, where one may find out that only Deepwater Horizon (DWH) stack is equipped with CSR but "losing" one pipe ram (the pipe ram is converted to test ram, which largely reduces the preparing and resume time for pressure testing on BOP system but loses the redundant sealing function). Equipping with CSR will have the better performance and higher probability for the successful shearing since the CSR is designed to shear the heaviest drill pipe and casing.

Performing the BOP function normally requires that subsystems of BOP system are functioning mutually :

- Control panels (Toolpusher's control panel is acting as the secondary barrier to Driller's control panel) with PLC system can send electronic signal for command "activiting shear

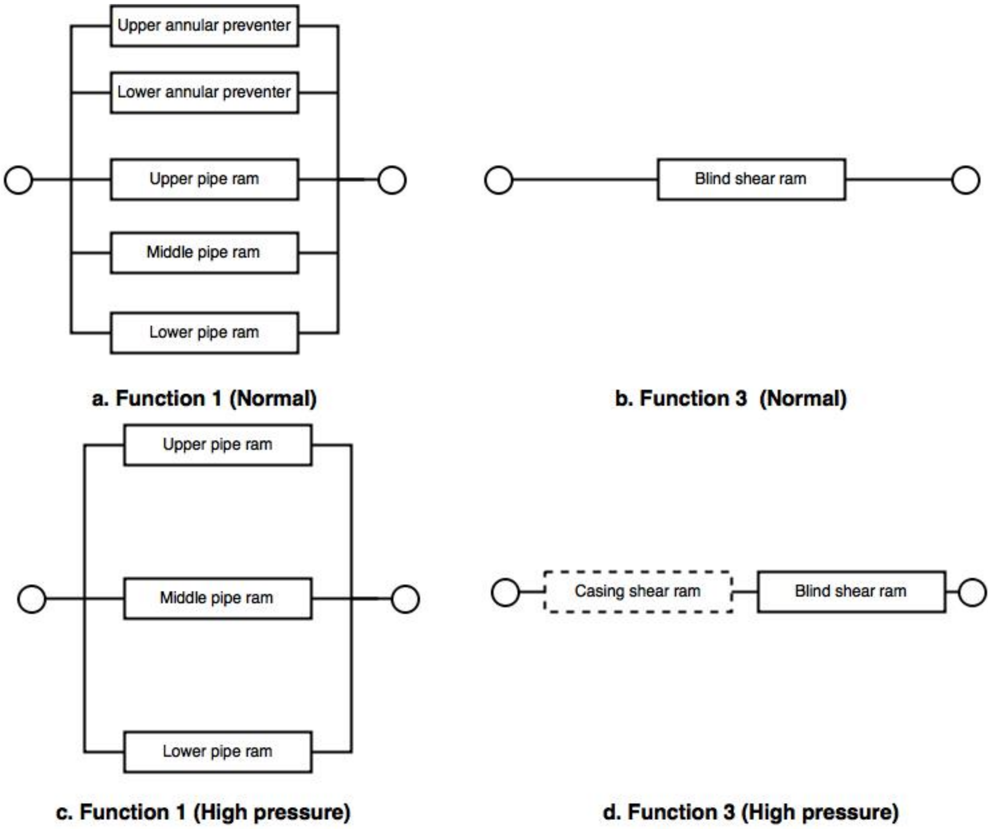


Figure 5.1: Reliability block diagram for the base case

Table 5.1: Different configurations of the BOP stack

	Annular preventer(AP)	Blind shear ram (BSR)	Pipe ram (PR)	Casing shear ram (CSR)
Classical	2	1	3	0
Modern	2	2	3	0
DWH	2	1	2	1

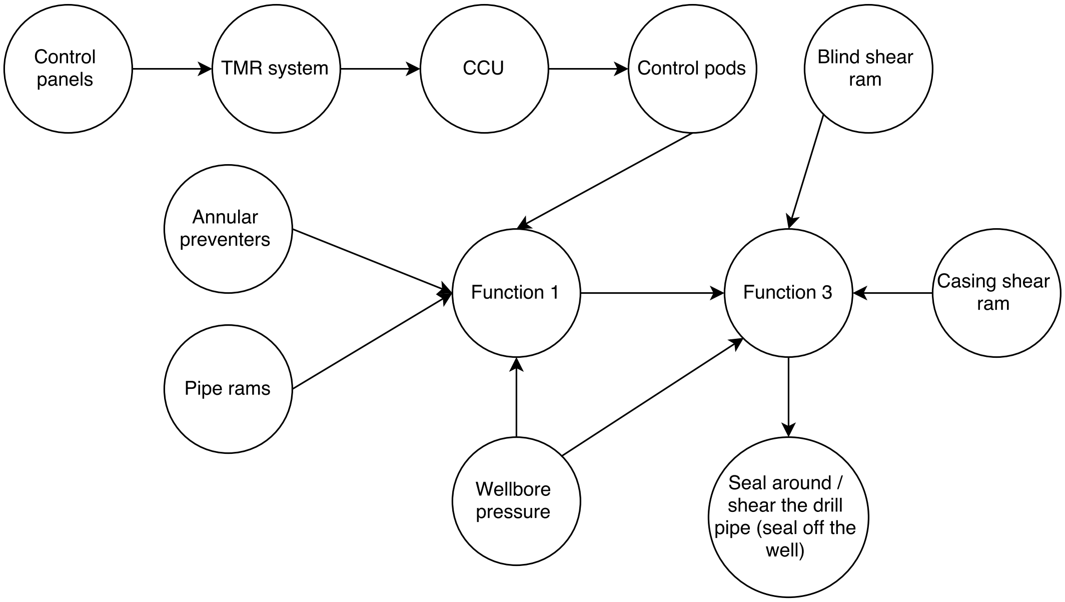


Figure 5.2: Bayesian Network model for case study

ram", through the MUX cables to the control pods, where CCU provides electric power supports for this process.

- The electronic signal can be converted to the hydraulic signal by activited control pods, then require the fluid supply transporting to the subsea components for BOP functions.
- The operation of the activited control pod requires the surface control valve and solenoid valve in the chosen pod works simultaneously, and the shuttle valve can direct the fluid for actuate relevant control valve.

Based on the descriptions from previous sections 3.1.2 and 3.1.3, Bayesian nodes with logic arrangement of performing the BOP function under the base case is then shown in the Figure 5.2. Only two control panels, TMR system, CCU, two redundant control pods, two shear rams (CSR and BSR), two or three pipe rams and two annular preventers are mainly investigated. Noticed that subsystems control panels, control pods, shear rams, pipe rams with n redundant components are forming as the 1oo$n$ connections, where the number of components for each subsystem is not presented, then the Figure 5.2 can present the BOP system with different configuration stack.

5.1.2 Software for Analysis

Since the number states and nodes in this case study exceeds the limit of the trial version of HUGIN (2015), then the common-used mathmatical software Matlab (2014) with Bayesian Network toolbox is suggested to handle the analysis of case study. Due to some updated version problem, the Bayesian Network toolbox may not be able to create the graphical demonstration. The relevant codes for the case study are shown in Appendix. Besides that, the professional software GRIF (2014) is suggested for quick calculation for probabilities of different states of nodes in Mavkov model.

5.1.3 Assumptions and Calculations for Input Data

As shown in Figure 5.2, Control panels, TMR system, CCU and control pods are forming as the serial connection to initial the Function 1, since the single failure of each subsystem results in failing to performing desired function. This serial connection may reduce the working load for setting input data (If these four subsystems forming as the OR-gate to the event Function 1 then the matrix for Function will be significantly increased), however, it may be impossible for calculating posteriors of these four subsystems individually. According to the research review, annulars, pipe rams and shear rams are of most importance for reliability,then such model is acceptable and available for analysis of case study focusing on the different configuration stack

.

This case study focusing on the performance of different configuration of BOP stack under the most demanding situations and the effect of the wellbore pressure. In order to avoid the unnecessary repetitive modelling work and simplify the calculations, some assumptions should be made as follows:

1. Initial states for all components and system are assumed to be perfect.
2. Both failure rate and repair rates are considered in this case study and assumed as the constant over the experiment time and are statistically independent.
3. Failures are assumed to be detected immediately and there is not any undetected failure.

Table 5.2: Estimated C-value for CCFs of component i

Component	C-value (C_i)
Control panels (CPL)	0.15
Control pods (CPD)	0.15
Annular preventers (AP)	0.1
Pipe rams (PR)	0.1
Blind shear ram (BSR)	0.1

4. For the common cause failure, only the components sharing the same working mechanism and design principle are considered to fail simultaneously under the shock. The repair actions for homogeneous components failed under shock are independent.

5. The repair actions are only taken when subsystem fails, and the repaired component is assumed to be as good as the new one.

6. To avoid the large-scale model, some components are omitted, such as kill and choke lines. Only the main subsystem and associated components are considered.

As discussed before, common cause failures are dominant for system reliability in the accident scenario. The most common model for common cause failures is the beta-factor model, which is also recommended by (IEC-61508, 2010). Here the C-factor model is suggested, which is essentially the same as the beta-factor model but the failure rate for CCF is defined as $\lambda^{(c)} = C \times \lambda^{(i)}$ (Rausand and Lundteigen, 2014). The estimated value for C based on the author's judgement is given in the Table 5.2, where i stands for CPL, CPD, AP, PR and BSR, respectivelly. And the individual failure rate and repair rate obtained based on the collected data and research review (Holand, 1999; Holand and Awan, 2012; Cai et al., 2012b)) for all the components is given in Table 5.3, where j stands for CPL, CPD, AP, PR, BSR,CSR, CCU and TMR, respectivelly.

The corresponding Markov model are proposed for 1oo1, 1oo2 and 1oo3 in Figure 5.3. It is noticed that: CPL, TMR, CCU and CSR are 1oo1 system; AP, PR(DWH) and BSR (Modern) are 1oo2 system; PR (Modern and Classical) are 1oo3 system.Based on the state transition digarms, the transition rate matrices can be obtained as follows in Eqs.(5.1) - (5.3): (Rausand and Lundteigen, 2014)

Table 5.3: Failure rate and repair rate for single component

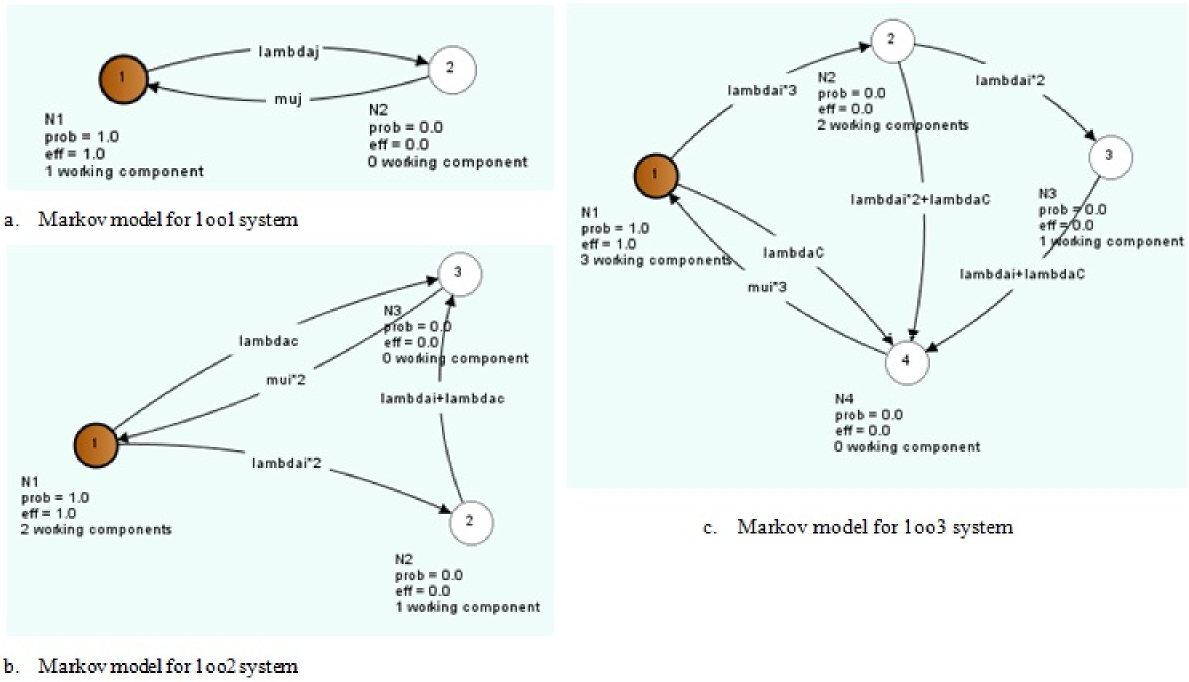
Component	Failure rate λ_j (per hour)	Repair rate μ_j (per hour)
Control panel (single)	1.6667×10^{-4}	1.429×10^{-1}
Control pod (single)	1.1433×10^{-4}	8.621×10^{-3}
Annular preventers (single)	2.059×10^{-4}	6.944×10^{-3}
Pipe rams (single)	1.5590×10^{-4}	6.944×10^{-3}
Blind shear ram (single)	1.8708×10^{-4}	6.944×10^{-3}
Casing shear ram (CSR)	1.8708×10^{-4}	6.944×10^{-3}
CCU	1.000×10^{-7}	1.000×10^{-2}
TMR controller	8.255×10^{-6}	8.333×10^{-2}

$$P_{1oo1} = \begin{bmatrix} -\lambda_j & \lambda_j \\ \mu_j & -\mu_j \end{bmatrix} \tag{5.1}$$

$$P_{1oo2} = \begin{bmatrix} -(2\times\lambda_i+\lambda_C) & 2\times\lambda_i & \lambda_C \\ 0 & -(\lambda_i+\lambda_C) & (\lambda_i+\lambda_C) \\ 2\times\mu_i & 0 & -2\times\mu_i \end{bmatrix} \tag{5.2}$$

$$P_{1oo3} = \begin{bmatrix} -(3\times\lambda_i+\lambda_C) & 3\times\lambda_i & 0 & \lambda_C \\ 0 & -(4\times\lambda_i+\lambda_C) & 2\times\lambda_i & (2\times\lambda_i+\lambda_C) \\ 0 & 0 & -(\lambda_i+\lambda_C) & (\lambda_i+\lambda_C) \\ 3\times\mu_i & 0 & 0 & -3\times\mu_i \end{bmatrix} \tag{5.3}$$

Then probability for each state can be calculated by GRIF (2014) and input into the Bayesian Network Model. The starting state matrix for all the components is $[1,0,0..0]$, which implies that all the operations start perfectly. Based on the calculation from GRIF, the priors for each subsystem can be obtained as shown in Appendix B.1, where the experimental time is 8760 hours (one year) and the step time is 438 hours.



a. Markov model for 1oo1 system

b. Markov model for 1oo2 system

c. Markov model for 1oo3 system

Figure 5.3: State transition digarm for case study (1oo1, 1oo2, 1oo3)

5.2 Bayesian Network Modelling

5.2.1 Conditional Probability Tables for Model

As shown in Figure 5.2, there is a information variable mamed "Wellbore pressure" (WP) for indicating different CPTs of Function 1, Function 3 and effectiveness of BSR. To simplify the analysis and calculation, some assumptions are made as follows for explaining the relevant CPTs for Function 1 and Function 3 are shown in Table 5.4 and Table 5.5, respectively:

1. For each redundant subsystem except BSR,if there is at least one working component for this subsystem, then the subsystem is assumed to be "Working", otherwise the state is "Faulty". And there are three states for BSR: "Working(1)","Working(2)" and "Faulty", which suggest the different influences on the child node "Function 3".

2. For the Classical and Modern stack which are not equipped with CSR, the state for CSR is always treated as "Faulty".

3. There are two states for "Wellbore pressure": "High" and "Normal". When the state of

Table 5.4: Simplified CPTs for Function 1

AP	PR	WP	Function 1 (Working)	Function 1 (Faulty)
Working	Working	High	1	0
Faulty	Working	High	1	0
Working	Faulty	High	0	1
Faulty	Working	High	0	1
Working	Working	Normal	1	0
Faulty	Working	Normal	1	0
Working	Faulty	Normal	1	0
Faulty	Working	Normal	0	1

Table 5.5: Simplified CPTs for Function 3

BSR	CSR	WP	Function 3 (Working)	Function 3 (Faulty)
Working (1)	Working	High	0.95	0.05
Working (2)	Faulty	High	0.85	0.15
Faulty	Working	Normal	0	1
Working (1)	Faulty	Normal	1	0
Working (2)	Working	High	0.999	0.001
Faulty	Faulty	High	0	1
Working (1)	Working	Normal	1	0
Working (2)	Faulty	Normal	1	0
Faulty	Working	High	0	1
Working (1)	Faulty	High	0.45	0.55
Working (2)	Working	Normal	1	0
Faulty	Faulty	Normal	0	1

"Wellbore pressure" is "High", the estimated probabilities for performing the Function 3 by using one BSR, two BSR or combination of BSR and CSR based on the shearing ability are shown in Table 5.5. For example, if the wellbore pressure is too high, there is still a small chance estimated as 0.001 for failing to perform Function 3 by using two BSRs.

4. For the serial connection, the failure of the parent node results in the failure of child node (This also could be explained as: the information of failure from the previous transfers to the next-level through the child node without considering states of child node). Then in the Table 5.4, only the working state of CPD is considered; and in the Table 5.5, the simplified CPTs are provided given the faulty state of Function 1.

5.2.2 Analysis and Discussion of Results

Three different configurations of BOP stack were investigated in this case study, considering the effect of information variable "Wellbore Pressure". According to D-010 (2004), the BOP should be recertified every five years. In this case study, however, the experimental time (also called as the mission time) sets as 8760 hours (one year) since the reliability of BOP in base case reaches the "steady" value before five years. The generic data is obtained from the technical reports and the research review (Holand, 1999; Holand and Awan, 2012; Cai et al., 2012b), and there are also some data like C-value for CCFs estimated by author, which may not be very realistic because of lacking pratical experience.The codes for generate BN model (taking Classical configuration stack as example) for case study in Matlab are reported in Appendix B.2.

To investigate the performance of the BOP system within different configuration stack, both reliability and availability are evaluated. The availability is the probability that the system performing the desired function at the given time point or over time period and the reliability is maily for evaluation of the non-repariable system (Rausand and Høyland, 2004). In order to get the priors for reliability evaluation, the repair action should be removed from the Markov model. The reliability and availability analysis for different configuration BOP stack are given in Figure 5.5 and Figure 5.4, where the variable WP is set as [0.25(High), 0.75(Normal)] and the relevant analysis result is reported in Appendix B.3.

By reviewing the Figure 5.4, one can easily conclude that availability of DWH type is higher and is faster to reach the "steady" value than the other two. The results suggest that even with lower redundancy of pipe ram subsystem, the inclusion of CSR still has the better performance regarding availability than introducing one addtional BSR. However, comparing the reliability as shown in Figure Reliability for different configuration BOP stack when WP=[0.25, 0.75], Modern configuration BOP stack is more reliable than DWH BOP stack and Classical BOP stack, which indicating that the repair action is of great importantance for BOP system within DWH configuration stack. And one can resonably predict that the difference of reliability between DWH and Classical could be omitted if experimental time becomes longer than one year, which means the negative effect of absence of one pipe ram is not fully masked by inclusiopn of CSR for long working period without any repairs or imperfect repair. In the pratical situation, if the proper repairing strategy is applied, the BOP system with DWH type of stack is still expected to have

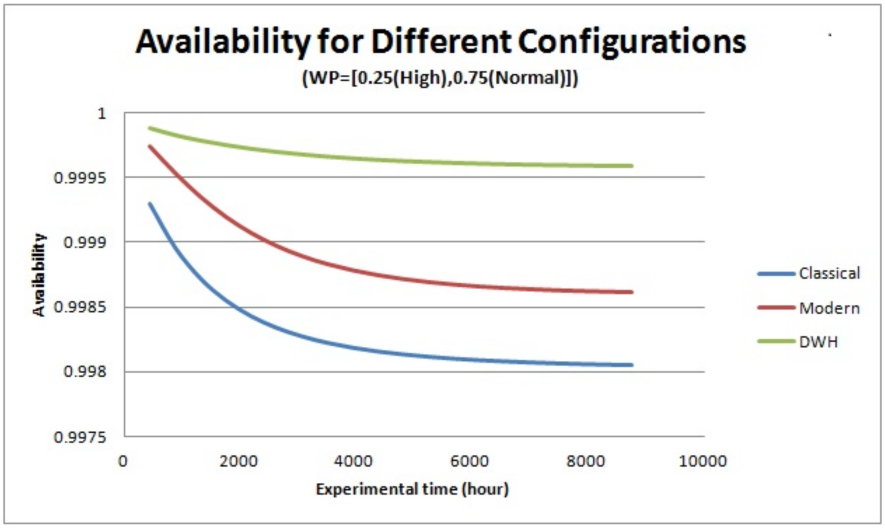


Figure 5.4: Availability for different configuration BOP stack when WP=[0.25, 0.75]

better performance under the most demanding situations.

The unique and important ability for diagnostic analysis of Bayesian Network Model is the calculation of posteriors. As indicated in Table 5.6, the posteriors for root nodes BSR, AP,PR and CSR are generated, where the time point is 8760 hours, WP is set as[0.25(High), 0.75(Normal)] and the repair action is taken into account. Noticed that for three different configuration BOP stack, the initiation for performing Function 1 and Function 3 is the same. Then the nodes CPL,TMR,CCU and CPOD are treated as the serial connection before activating Function 1 therefore it worth nothing for posteriors calculation of such nodes.

One observation is that the root node PR has the highest increase yields the calculation result of MPE, which indicating that the pipe ram is the most critical component given scenario in all types of BOP stack. When comparing Classical stack and Modern stack, the additional BSR slightly improve the reliability of Function 3 as the last barrier, while the pipe ram becomes more critical since Function 1 is more likely to be "blame" given the failure of system. Based on the comparsion between DWH type and Modern type, the introduction of CSR has siginificantly reduced the posterior of PR even with higher priors. However, the posterior of BSR is increased dramatically compared to Classical, which indicating the losing redundancy of Pipe ram subsystem causes the failure of Function 3 should be more responsible for the faulty state of total system. As the Figure 5.4 indicated, this kind of modification still increase the availability of the BOP system.

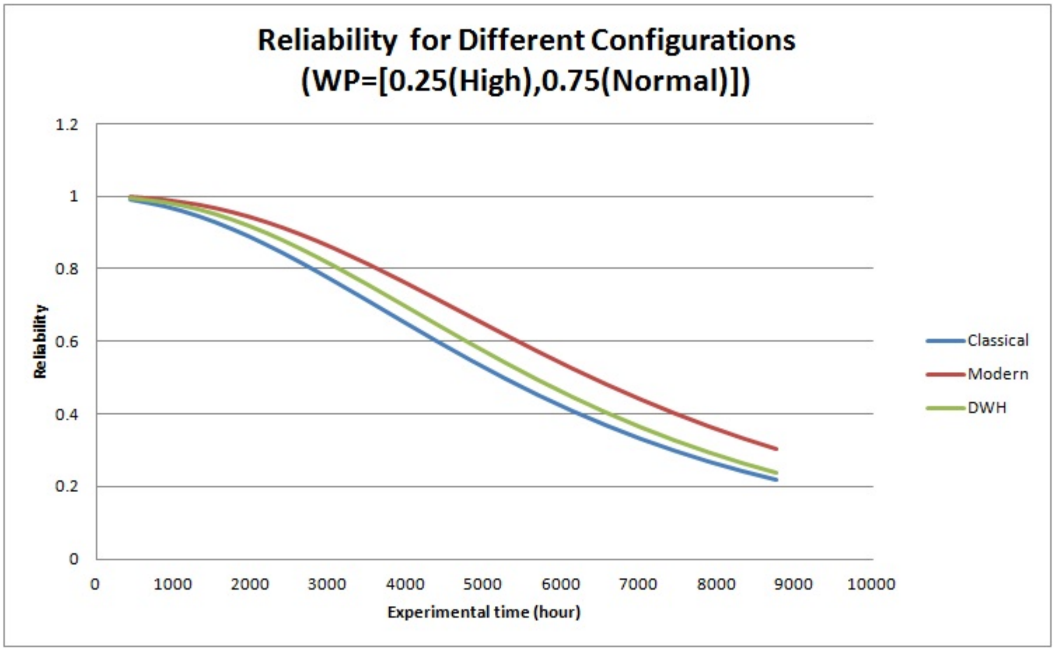


Figure 5.5: Reliability for different configuration BOP stack when WP=[0.25, 0.75]

For the reliability analysis of three configurations, since there is not any repair actions to lower the priors of the each subsystem,the model within increasing priors are not very suitable for such diagnostic analysis based on posterior probabilities. The alternative method then could be the MPE method. The most probable state given the scenario is the faulty state of pipe ram subsystem at very beginning; then the most probable one becomes the failure of BSR and CSR, which indicating the Function 3 is malfunction when priors get higher; Finally, when the experimental time comes to approximate half year, all the components or subsystem trends to be faulty given accident since priors are too high.

Generally, the annular preventers contribue little to the failure of total system, while the pipe rams are considered to have larger contribution than blind shear ram. To be noticed, in some cases, the root nodes with the higher posterior is not implied as the most probable node to happen given fault.

The influence of wellbore pressure is mainly indicated in Figure 5.7 and Figure 5.6. One may observe that the DWH stack has a slighter decrement of availability when the value P decrease from 0.9 to 0.15, which implies that DWH stack is more stable and reliable than the others under the high pressure situation. The similar conclusion can also be draw based on the observation of Figure 5.6, the effect of increasing wellbore pressure still has smallest impact on the perfor-

Table 5.6: Priors and Posteriors for some root nodes, when WP=[0.25, 0.75] and time = 8760 hrs

	Classical		**Modern**		**DWH**	
	Priors	Posteriors	Priors	Posteriors	Priors	Posteriors
BSR	0.026234	0.1009	0.3552(W2), 0.00989 (F)	0.1253(W2), 0.0533 (F)	0.026234	0.4883
AP	0.010892	0.01171	0.010892	0.01132	0.010892	0.01509
PR	0.0075741	0.54693	0.0075741	0.56189	0.008191	0.44278
CSR	-	-	-	-	0.026234	0.12977

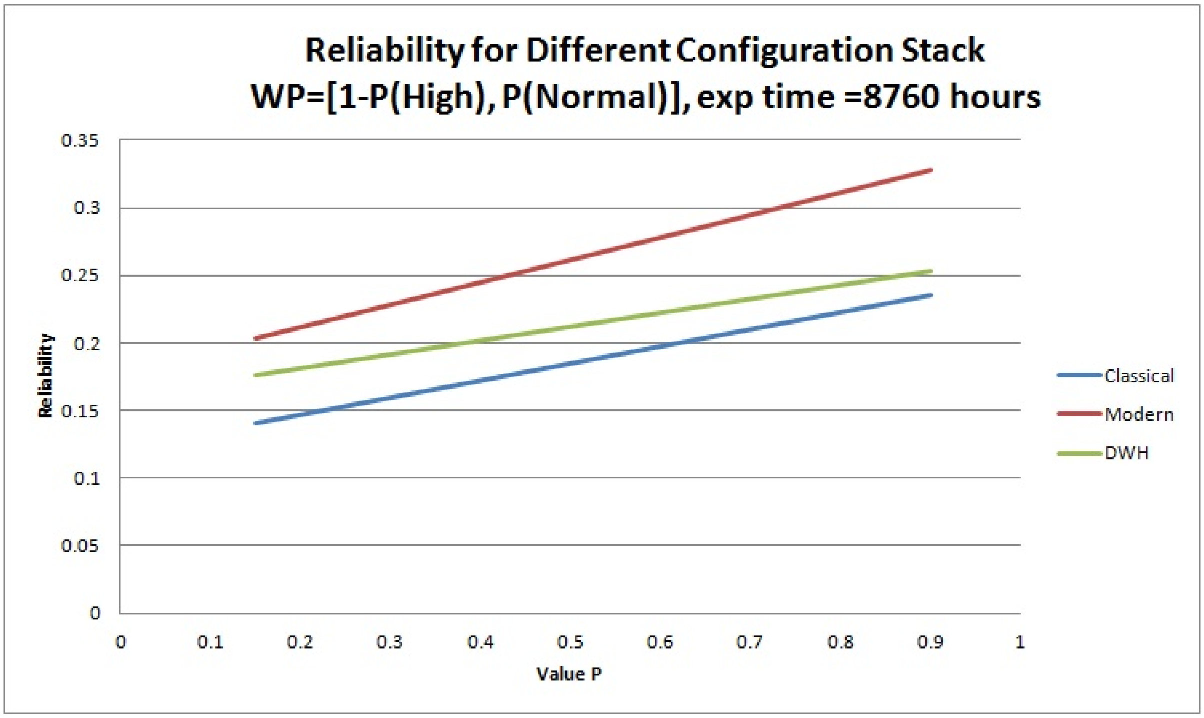


Figure 5.6: Reliability for different configuration BOP stack when WP=[1-P,P]

mance of DWH BOP stack, which indicating that the installation of CSR can effectivelya against the high pressure conditions. Besides that, even the Modern configuration BOP stack is most reliable under high pressure condition as shown in Figure 5.6, the wellbore pressure still has the greatest influence on its reliability. It suggests that the increasing redundancy of BSR subsystem is not working, since the high wellbore pressure conditions requires the high shearing ability when performing Function 3, which generall only provided by CSR.

As shown in Figure 5.8, the posterior *P* of DWH stack is more sensitive: when wellbore pressure trends to be high, the system is more likely to fail due to the loss of redundancy; when wellbore pressure trends to be normal, then the effect of additional CSR is greater than the effect of losing

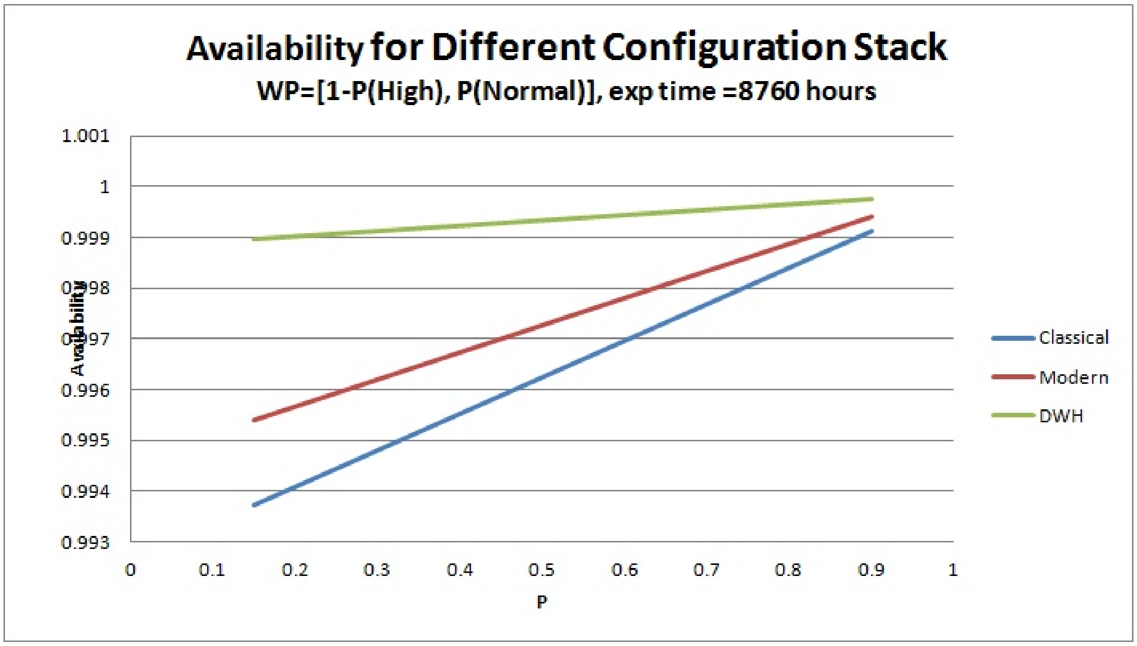


Figure 5.7: Availability for different configuration BOP stack when WP=[1-P,P]

one pipe ram. This could be also explained by using MPE method: when the P is set as 0.9 which implies that wellbore pressure is very impossible to be high, then MPE tells that the most probable component in faulty state given the failure of total system is the BSR instead of pipe ram.

5.3 Validation of Model

Normally the senstivity analysis should be carried out fulfill the validation of model. According to the literature review regarding demonstrating the created model is reasonable,three requirment should be fulfilled (Jones et al., 2010; Cai et al., 2012b,a):

1. A slight increase/decrease in the prior subjective probabilities of each parent node should certainly result in the effect of a relative increase/decrease of the posterior probabilities of child nodes.

2. Given the variation of subjective probability distributions of each parent node,its influence magnitude to child node values should keep consistent.

3. The total influence magnitudes of the combination of the probability variations from x

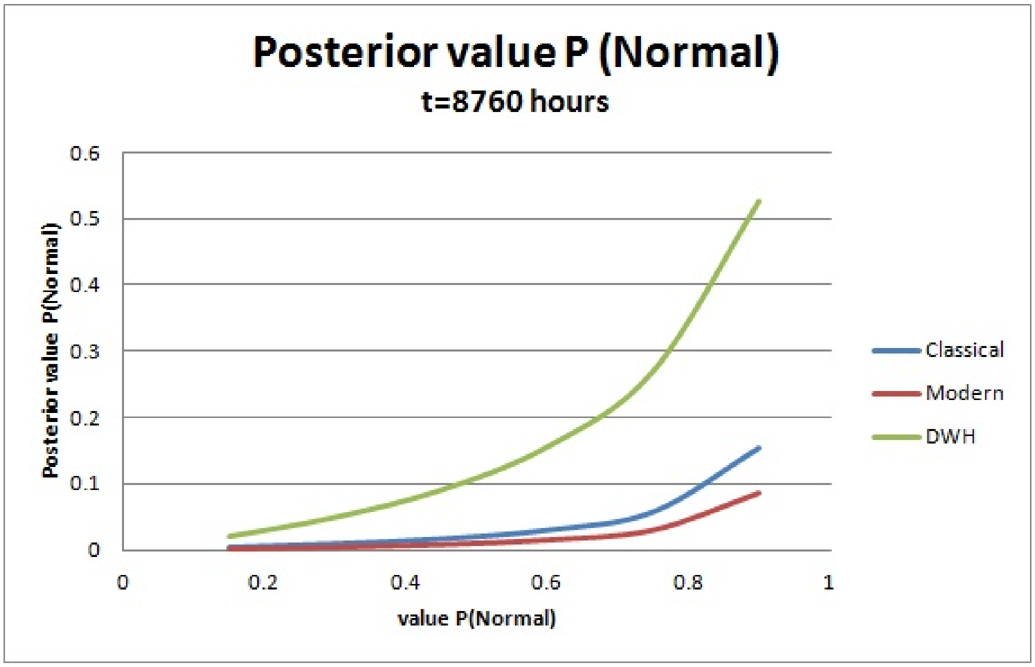


Figure 5.8: Posteriors of value P (within repair actions)

attributes on the values should be always greater than the one from the set of $x–y$ ($y \in x$) attributes.

If taking DWH stack as the example, as shown in Fugure 5.8, when the prior of value P increased from 0.15 to 0.3, the corresponding posterior increases from 0.02129 to 0.05018; As indicating in Figure 5.4, when the prior of root node PR increase from 0.0022870 to 0.0081910, the unavailability increases from 0.000122 to 0.000412. If P is set as 0.45 instead of 0.75, then unavailability increases from 0.000412 to 0.000727612. Those observation satisfy the requirements for validation of model.

Chapter 6

Summary and Recommendations for Further Work

6.1 Summary and Conclusions

This thesis firstly presents a method of translating Fault Tree into Bayesian Network without losing any details, in addtion with the more advanced modelling power: effectively building the large scale model, applying probabilistic gates, solution for uncertainty and inclusion of the multiple states for nodes. Then the case study is carried out, in order to propose the improved reliability and availability assessment about BOP system within different configurations, based on Bayesian Network model. According to the generated results from Example 1, Example 2 and case study, the main conclusion of the thesis can be summarized as follows:

1. Fault-Tree based Bayesian Network model is proven to update the priors when the new information of the system is taken into account and the updated information could be very useful for diagonstic analysis. And the most probable explanation method of Bayesian Network is also proven to have the more precise severity ranking of components characteristics than the minimal cut-set method provided by Fault Tree Analysis, since MPE configuration considering the occurrence and non-occurrence of root nodes simultaneously.

2. Due to the limited number of the generic data, the uncertainty from the expert knowledge

is unavoidable. Then Bayesian Network is implied as the suitable method for re-estimate the mutual informations probabilistically. However, the detailed method for solving such kind of challenge is not covered in this master thesis.

3. Bayesian Network is proven to carry out the more detailed analysis than the traditional method such as Fault Tree Analysis.Every Fault Tree can be tranlating into Bayesian Network as indicated in Chapter 4. Therefore some assumption of Fault Tree can be removed to investigate more complicated situations, within the ability of handle multiple states and dependent failures.

4. The classical BOP stack is still in use in many offshore locations around the world, the analysis result from case study suggest that the industry should generally moving towards the DWH BOP stack since it is more reliable under high wellbore pressure condition, which means the shearing ability for BOP system becomes more important. According to updated posteriors, the pipe ram subsytem is most critical, however, the implementation of casing shear ram in DWH BOP stack is proven to compensate for losing redundancy of pipe rams. Moreover, the correct choice of suitable and effective repair strategy is very critical for improving availability of DWH BOP stack.

6.2 Research Prespectives

According to the current results, here gives some recommendations for possible extensions of research work in this or similiar filed as follows:

- Short-term: some additional informative variable could be added into the model in the case study, such as the diameter of pipe. If it is too large, then the fixed pipe rams (usually upper pipe ram and lower pipe ram) is not able to perform the Function 1, then redundancy of Function is reduced from 1oo5 to 1oo3 (middle pipe ram and two annular preventers), where the shearing ability remains the same. The introduction of the informative variable about pipe diameter in the Bayesian Network model is able to perform a more detailed and precise reliability/ availability assessment of BOP systems within different configurations stack.

- Long-term: some other modeling power of Bayesian Network could be applied to carry out a more detailed analysis which closed to the pratical situations, such as Dynamic Bayesian Network. As discussed before, there are a few researchers have discussed the suitable method for re-estimate the priors which originally generated by domain experts. Such analysis can be applied in the real industry or in the decision-making strategy regarding BOP system or some other similar large-scale safety critical systems.

Appendix A

Acronyms

BOP Blowout preventer

CCF Common cause failure

BN Bayesian Network

EUC Equipment under control

E/E/PE Electrical,electronic,or programmable electronic

SIS Safety Instrumented System

PLC Programmable logic controller

SIF Safety-instrumented function

DU Dangerous undetected

DD Dangerous detected

SU Safe undetected

SD Safe detected

PFD Probability of failure on demand

PFH Frequency of dangerous failure per hour

MRT Mean repair time

MTTR Mean time to restoration

SIL Safety integrity level

HFT Hardware fault tolerance

SFF Safe failure fraction

FTA Fault tree analysis

LOPA Layer of protection analysis

ETA Event tree analysis

RAMS Reliability, availability, maintainability, and safety

LMRP Lower marine riser package

LAP Lower annular preventer

UPR Upper pipe ram

MPR Middle pipe ram

LPR Lower pipe ram

BSR Blind shear ram

CSR Casing shear ram

OD Outer diameter

VBR Variable bore rams

HPU Hydraulic power unit

DWH Deepwater Horizon

MUX Multiplexed

CCU Central control unit

DCP Driller’s control panel

TCP Toolpusher’s control panel

SEM Subsea electronic modules

FEMCA Failure mode, effects and criticality analysis

HAZOP Hazard and operability study

DAG Directed acyclic graph

CPT Conditional probability table

RBD Reliability block diagram

MFDT Mean fractional deadtime

TE Top event

MPE Most probable explanation

PSA Norwegian Petroleum Safety Authority

AP Annular preventer

TMR Triple modular redundancy controllers

PR Pipe ram

CPOD Control pods

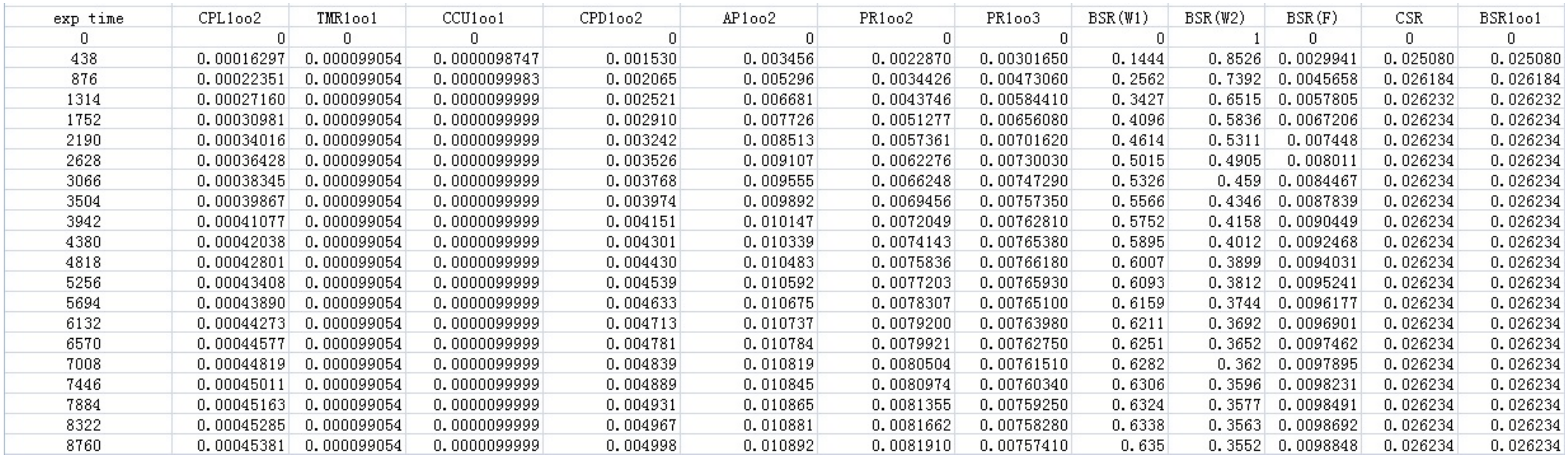
WP Wellbore pressure

CPL Control panels

Appendix B

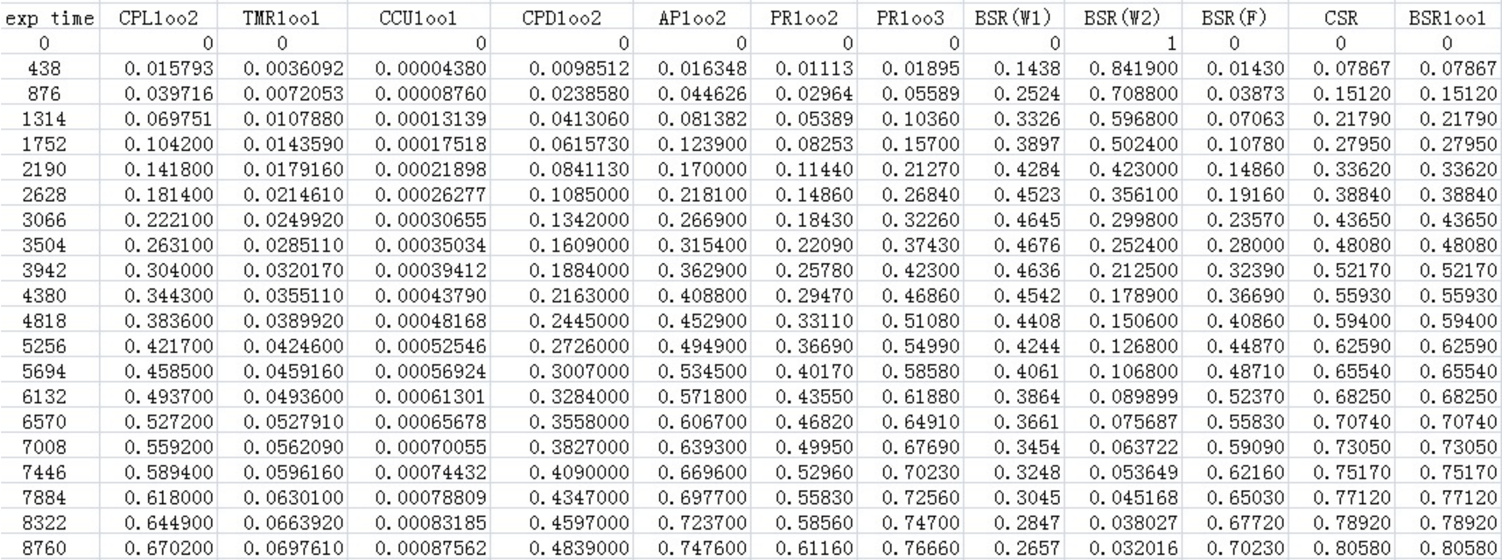
Relevant Data and Code for Case Study

B.1 Priors data for each subsystem in case study



exp time	CPL1oo2	TMR1oo1	CCU1oo1	CPD1oo2	AP1oo2	PR1oo2	PR1oo3	BSR(W1)	BSR(W2)	BSR(F)	CSR	BSR1oo1
0	0	0	0	0	0	0	0	0	1	0	0	0
438	0.00016297	0.000099054	0.0000098747	0.001530	0.003456	0.0022870	0.00301650	0.1444	0.8526	0.0029941	0.025080	0.025080
876	0.00022351	0.000099054	0.0000099983	0.002065	0.005296	0.0034426	0.00473060	0.2562	0.7392	0.0045658	0.026184	0.026184
1314	0.00027160	0.000099054	0.0000099999	0.002521	0.006681	0.0043746	0.00584410	0.3427	0.6515	0.0057805	0.026232	0.026232
1752	0.00030981	0.000099054	0.0000099999	0.002910	0.007726	0.0051277	0.00656080	0.4096	0.5836	0.0067206	0.026234	0.026234
2190	0.00034016	0.000099054	0.0000099999	0.003242	0.008513	0.0057361	0.00701620	0.4614	0.5311	0.007448	0.026234	0.026234
2628	0.00036428	0.000099054	0.0000099999	0.003526	0.009107	0.0062276	0.00730030	0.5015	0.4905	0.008011	0.026234	0.026234
3066	0.00038345	0.000099054	0.0000099999	0.003768	0.009555	0.0066248	0.00747290	0.5326	0.459	0.0084467	0.026234	0.026234
3504	0.00039867	0.000099054	0.0000099999	0.003974	0.009892	0.0069456	0.00757350	0.5566	0.4346	0.0087839	0.026234	0.026234
3942	0.00041077	0.000099054	0.0000099999	0.004151	0.010147	0.0072049	0.00762810	0.5752	0.4158	0.0090449	0.026234	0.026234
4380	0.00042038	0.000099054	0.0000099999	0.004301	0.010339	0.0074143	0.00765380	0.5895	0.4012	0.0092468	0.026234	0.026234
4818	0.00042801	0.000099054	0.0000099999	0.004430	0.010483	0.0075836	0.00766180	0.6007	0.3899	0.0094031	0.026234	0.026234
5256	0.00043408	0.000099054	0.0000099999	0.004539	0.010592	0.0077203	0.00765930	0.6093	0.3812	0.0095241	0.026234	0.026234
5694	0.00043890	0.000099054	0.0000099999	0.004633	0.010675	0.0078307	0.00765100	0.6159	0.3744	0.0096177	0.026234	0.026234
6132	0.00044273	0.000099054	0.0000099999	0.004713	0.010737	0.0079200	0.00763980	0.6211	0.3692	0.0096901	0.026234	0.026234
6570	0.00044577	0.000099054	0.0000099999	0.004781	0.010784	0.0079921	0.00762750	0.6251	0.3652	0.0097462	0.026234	0.026234
7008	0.00044819	0.000099054	0.0000099999	0.004839	0.010819	0.0080504	0.00761510	0.6282	0.362	0.0097895	0.026234	0.026234
7446	0.00045011	0.000099054	0.0000099999	0.004889	0.010845	0.0080974	0.00760340	0.6306	0.3596	0.0098231	0.026234	0.026234
7884	0.00045163	0.000099054	0.0000099999	0.004931	0.010865	0.0081355	0.00759250	0.6324	0.3577	0.0098491	0.026234	0.026234
8322	0.00045285	0.000099054	0.0000099999	0.004967	0.010881	0.0081662	0.00758280	0.6338	0.3563	0.0098692	0.026234	0.026234
8760	0.00045381	0.000099054	0.0000099999	0.004998	0.010892	0.0081910	0.00757410	0.635	0.3552	0.0098848	0.026234	0.026234

Figure B.1: Priors for each subsystem within repair action



exp time	CPL1oo2	TMR1oo1	CCU1oo1	CPD1oo2	AP1oo2	PR1oo2	PR1oo3	BSR(W1)	BSR(W2)	BSR(F)	CSR	BSR1oo1
0	0	0	0	0	0	0	0	0	1	0	0	0
438	0.015793	0.0036092	0.00004380	0.0098512	0.016348	0.01113	0.01895	0.1438	0.841900	0.01430	0.07867	0.07867
876	0.039716	0.0072053	0.00008760	0.0238580	0.044626	0.02964	0.05589	0.2524	0.708800	0.03873	0.15120	0.15120
1314	0.069751	0.0107880	0.00013139	0.0413060	0.081382	0.05389	0.10360	0.3326	0.596800	0.07063	0.21790	0.21790
1752	0.104200	0.0143590	0.00017518	0.0615730	0.123900	0.08253	0.15700	0.3897	0.502400	0.10780	0.27950	0.27950
2190	0.141800	0.0179160	0.00021898	0.0841130	0.170000	0.11440	0.21270	0.4284	0.423000	0.14860	0.33620	0.33620
2628	0.181400	0.0214610	0.00026277	0.1085000	0.218100	0.14860	0.26840	0.4523	0.356100	0.19160	0.38840	0.38840
3066	0.222100	0.0249920	0.00030655	0.1342000	0.266900	0.18430	0.32260	0.4645	0.299800	0.23570	0.43650	0.43650
3504	0.263100	0.0285110	0.00035034	0.1609000	0.315400	0.22090	0.37430	0.4676	0.252400	0.28000	0.48080	0.48080
3942	0.304000	0.0320170	0.00039412	0.1884000	0.362900	0.25780	0.42300	0.4636	0.212500	0.32390	0.52170	0.52170
4380	0.344300	0.0355110	0.00043790	0.2163000	0.408800	0.29470	0.46860	0.4542	0.178900	0.36690	0.55930	0.55930
4818	0.383600	0.0389920	0.00048168	0.2445000	0.452900	0.33110	0.51080	0.4408	0.150600	0.40860	0.59400	0.59400
5256	0.421700	0.0424600	0.00052546	0.2726000	0.494900	0.36690	0.54990	0.4244	0.126800	0.44870	0.62590	0.62590
5694	0.458500	0.0459160	0.00056924	0.3007000	0.534500	0.40170	0.58580	0.4061	0.106800	0.48710	0.65540	0.65540
6132	0.493700	0.0493600	0.00061301	0.3284000	0.571800	0.43550	0.61880	0.3864	0.089899	0.52370	0.68250	0.68250
6570	0.527200	0.0527910	0.00065678	0.3558000	0.606700	0.46820	0.64910	0.3661	0.075687	0.55830	0.70740	0.70740
7008	0.559200	0.0562090	0.00070055	0.3827000	0.639300	0.49950	0.67690	0.3454	0.063722	0.59090	0.73050	0.73050
7446	0.589400	0.0596160	0.00074432	0.4090000	0.669600	0.52960	0.70230	0.3248	0.053649	0.62160	0.75170	0.75170
7884	0.618000	0.0630100	0.00078809	0.4347000	0.697700	0.55830	0.72560	0.3045	0.045168	0.65030	0.77120	0.77120
8322	0.644900	0.0663920	0.00083185	0.4597000	0.723700	0.58560	0.74700	0.2847	0.038027	0.67720	0.78920	0.78920
8760	0.670200	0.0697610	0.00087562	0.4839000	0.747600	0.61160	0.76660	0.2657	0.032016	0.70230	0.80580	0.80580

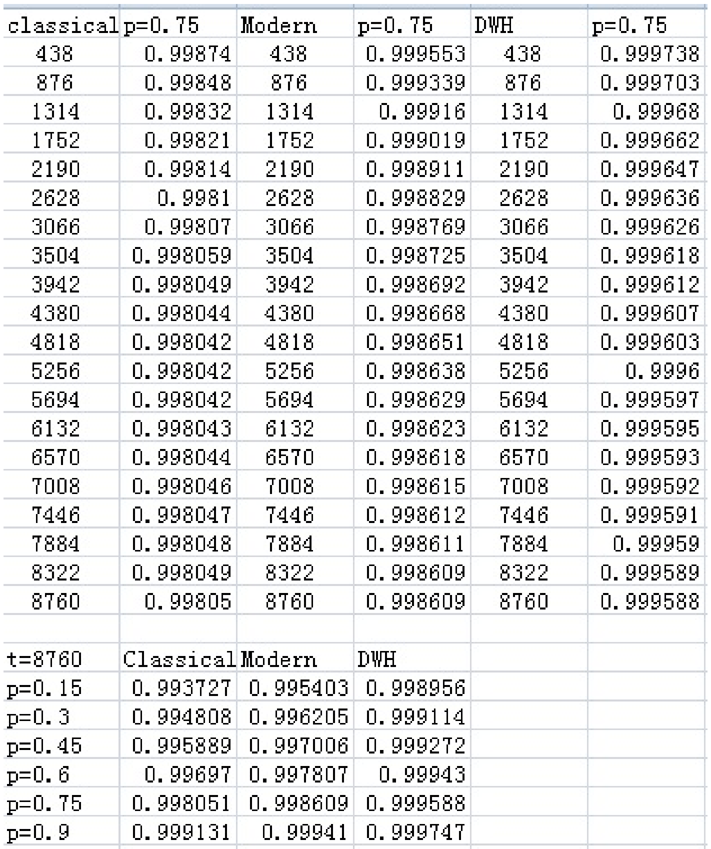
Figure B.2: Priors for each subsystem without repair action

B.2 Codes for Matlab

```
N = 12
dag = zeros(N,N)
BSR= 1; CSR= 2; AP= 3; PR = 4; WP =5;CPL = 6; TMR = 7; CCU = 8;CPOD = 9; F1 = 10; F3 = 11; BOP
= 12;
dag(AP,F1)= 1
dag(PR,F1)= 1
dag(WP,F1)= 1
dag(CPOD,F1)= 1
dag(BSR,F3)= 1
dag(CSR,F3)= 1
dag(WP,F3)= 1
dag(F1,F3)= 1
dag(CPL,TMR)= 1
dag(TMR,CCU)= 1
dag(CCU,CPOD)= 1
dag(F3,BOP)= 1
discrete_nodes = 1:N
node_sizes = [3 2 2 2 2 2 2 2 2 2 2 2 ]
P=0.75;
t=438 ;CPL1oo2=0.00016297 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000098747 ;CPD1oo2=0.0015298
;AP1oo2=0.0034561 ;PR1oo3=0.0030165 ;CSR1oo1=1 ;BSR1oo1=0.02508;
t=876 ;CPL1oo2=0.00022351 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099983 ;CPD1oo2=0.0020647
;AP1oo2=0.0052957 ;PR1oo3=0.0047306 ;CSR1oo1=1 ;BSR1oo1=0.026184;
t=1314 ;CPL1oo2=0.0002716 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0025208
;AP1oo2=0.006681 ;PR1oo3=0.0058441 ;CSR1oo1=1 ;BSR1oo1=0.026232;
t=1752 ;CPL1oo2=0.00030981 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.00291
;AP1oo2=0.0077255 ;PR1oo3=0.0065608 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=2190 ;CPL1oo2=0.00034016 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0032423
```

```
;AP1oo2=0.0085131 ;PR1oo3=0.0070162 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=2628 ;CPL1oo2=0.00036428 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0035258
;AP1oo2=0.0091069 ;PR1oo3=0.0073003 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=3066 ;CPL1oo2=0.00038345 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0037679
;AP1oo2=0.0095546 ;PR1oo3=0.0074729 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=3504 ;CPL1oo2=0.00039867 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0039744
;AP1oo2=0.0098922 ;PR1oo3=0.0075735 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=3942 ;CPL1oo2=0.00041077 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0041507
;AP1oo2=0.010147 ;PR1oo3=0.0076281 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=4380 ;CPL1oo2=0.00042038 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0043012
;AP1oo2=0.010339 ;PR1oo3=0.0076538 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=4818 ;CPL1oo2=0.00042801 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0044296
;AP1oo2=0.010483 ;PR1oo3=0.0076618 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=5256 ;CPL1oo2=0.00043408 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0045392
;AP1oo2=0.010592 ;PR1oo3=0.0076593 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=5694 ;CPL1oo2=0.0004389 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0046328
;AP1oo2=0.010675 ;PR1oo3=0.007651 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=6132 ;CPL1oo2=0.00044273 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0047126
;AP1oo2=0.010737 ;PR1oo3=0.0076398 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=6570 ;CPL1oo2=0.00044577 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0047808
;AP1oo2=0.010784 ;PR1oo3=0.0076275 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=7008 ;CPL1oo2=0.00044819 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.0048389
;AP1oo2=0.010819 ;PR1oo3=0.0076151 ;CSR1oo1=1 ;BSR1oo1=0.026234;
t=8760 ;CPL1oo2=0.00045381 ;TMR1oo1=0.000099054 ;CCU1oo1=0.0000099999 ;CPD1oo2=0.004998
;AP1oo2=0.010892 ;PR1oo3=0.0075741 ;CSR1oo1=1 ;BSR1oo1=0.026234;
bnet = mk_bnet(dag, node_sizes, 'discrete', discrete_nodes)
bnet.CPDBSR = tabular_CPD(bnet, BSR, [1-BSR1oo1 0 BSR1oo1])
bnet.CPDCSR = tabular_CPD(bnet, CSR, [1-CSR1oo1 CSR1oo1])
bnet.CPDAP = tabular_CPD(bnet, AP, [1-AP1oo2 AP1oo2])
bnet.CPDPR = tabular_CPD(bnet, PR, [1-PR1oo3 PR1oo3])
bnet.CPDWP = tabular_CPD(bnet, WP, [1-P P])
bnet.CPDCPL = tabular_CPD(bnet, CPL, [1-CPL1oo2 CPL1oo2])
bnet.CPDTMR = tabular_CPD(bnet, TMR, [1-TMR1oo1 0 TMR1oo1 1])
bnet.CPDCCU = tabular_CPD(bnet, CCU, [1-CCU1oo1 0 CCU1oo1 1])
bnet.CPDCPOD = tabular_CPD(bnet, CPOD, [1-CPD1oo2 0 CPD1oo2 1])
bnet.CPDF1 = tabular_CPD(bnet, F1, [1 1 0 0 1 1 1 0 0 0 0 0 0 0 0 0 1 1 0 0 0 1 1 1 1 1 1 1 1])
bnet.CPDF3 = tabular_CPD(bnet, F3, [1 1 1 1 1 1 1 1 1 1 1 1 0.95 0.999 0 0.45 0.85 0 1 1 0 1 1 0 0 0
0 0 0 0 0 0 0 0 0 0 0.05 0.001 1 0.55 0.15 1 0 0 1 0 0 1])
bnet.CPDBOP = tabular_CPD(bnet, BOP, [1 0 0 1])
engine = jtree_inf_engine(bnet);
evidence = cell(1,N);
evidenceBOP= 2
[engine, ll] = enter_evidence(engine, evidence);
[mpe, ll] = calc_mpe(engine, evidence)
mpe
marg = marginal_nodes(engine, BOP);
marg.T
```

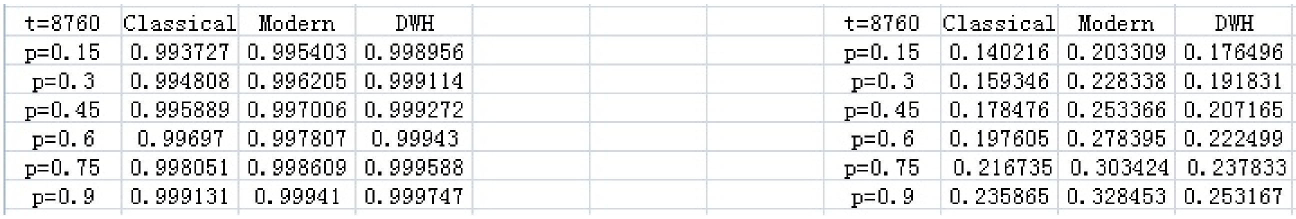
B.3 Analysis results of BN model



classical	p=0.75	Modern	p=0.75	DWH	p=0.75
438	0.99874	438	0.999553	438	0.999738
876	0.99848	876	0.999339	876	0.999703
1314	0.99832	1314	0.99916	1314	0.99968
1752	0.99821	1752	0.999019	1752	0.999662
2190	0.99814	2190	0.998911	2190	0.999647
2628	0.9981	2628	0.998829	2628	0.999636
3066	0.99807	3066	0.998769	3066	0.999626
3504	0.998059	3504	0.998725	3504	0.999618
3942	0.998049	3942	0.998692	3942	0.999612
4380	0.998044	4380	0.998668	4380	0.999607
4818	0.998042	4818	0.998651	4818	0.999603
5256	0.998042	5256	0.998638	5256	0.9996
5694	0.998042	5694	0.998629	5694	0.999597
6132	0.998043	6132	0.998623	6132	0.999595
6570	0.998044	6570	0.998618	6570	0.999593
7008	0.998046	7008	0.998615	7008	0.999592
7446	0.998047	7446	0.998612	7446	0.999591
7884	0.998048	7884	0.998611	7884	0.99959
8322	0.998049	8322	0.998609	8322	0.999589
8760	0.99805	8760	0.998609	8760	0.999588

t=8760	Classical	Modern	DWH
p=0.15	0.993727	0.995403	0.998956
p=0.3	0.994808	0.996205	0.999114
p=0.45	0.995889	0.997006	0.999272
p=0.6	0.99697	0.997807	0.99943
p=0.75	0.998051	0.998609	0.999588
p=0.9	0.999131	0.99941	0.999747

Figure B.3: Analysis results of BN model in case study



t=8760	Classical	Modern	DWH
p=0.15	0.993727	0.995403	0.998956
p=0.3	0.994808	0.996205	0.999114
p=0.45	0.995889	0.997006	0.999272
p=0.6	0.99697	0.997807	0.99943
p=0.75	0.998051	0.998609	0.999588
p=0.9	0.999131	0.99941	0.999747

t=8760	Classical	Modern	DWH
p=0.15	0.140216	0.203309	0.176496
p=0.3	0.159346	0.228338	0.191831
p=0.45	0.178476	0.253366	0.207165
p=0.6	0.197605	0.278395	0.222499
p=0.75	0.216735	0.303424	0.237833
p=0.9	0.235865	0.328453	0.253167

Figure B.4: Analysis results of BN model in case study (2)

Bibliography

Bobbio, A., Portinale, L., Minichino, M., and Ciancamerla, E. (2001). Improving the analysis of dependable systems by mapping fault trees into bayesian networks. *Reliability Engineering and System Safety*, 71:249–260.

British-Petroleum (2010). Deepwater horizon investigation report-appendix h. description of the bop stack and control system. Technical report.

Cai, B., Liu, Y., Liu, Z., Tian, X., Dong, X., and Tu, S. (2012a). Using bayesian networks in reliability evaluation for subsea blowout preventer control system. *Reliability Engineering and System Safety*, 108:32–41.

Cai, B., Liu, Y., Liu, Z., Tian, X., Zhang, Y., and Liu, J. (2012b). Performance evaluation of subsea blowout preventer systemm with common cause failures. *Reliability Engineering*, 90–91:18–25.

CARA (1996). Cara-faulttree application version.

D-010, N. (2004). *Well integrity in dirlling and well operations.* International Electrotechnical Commission, Norway.

Deepwater-Horizon-Study-Group (2008). Final report on the investigation of the macondo well blowout. Technical report.

GRIF (2014). Grif trial version 2015. http://grif-workshop.com/.

Gustav, D. (2000). Combining disparate sources of information in the safety assessment of software-based systems. *Nuclear Engineering and Design*, 195:307–319.

Hauge, S. (2013). Reliability prediction method for safety instrumented system: Pds method handbook. Technical report.

Hokstad, P. and Rausand, M. (2008). Common cause failure modelling: Status and trends. *Handbook of Performability Engineering*, 93:621–640.

Holand, P. (1987). Reliability of subsea bop systems. *Reliability Engineering*, 19:263–275.

Holand, P. (1997). Reliability of subsea bop system for deewater application. Technical report.

Holand, P. (1999). Reliability of subsea bop system for deewater application- phase ii dw. Technical report.

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

Holand, P. and Skalle, P. (2001). Deepwater kicks and bop performance. Technical report.

HUGIN (2015). Hugin expert software trial version 8.1. http://www.hugin.com.

IEC-61508 (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*. International Electrotechnical Commission, Geneva.

IEC-61511 (2003). *Functional safety - Safety instrumented systems for the process industry sector*. International Electrotechnical Commission, Geneva.

Jensen, F. (1996). *An Introduction to Bayesian Networks*. UCL Press, Aalborg University, Denmark.

Jin, H., Rausand, M., and Lundteigen, M. A. (2011). Reliability performance of safety instrumented systems: A common approach for both low-abd high-demand mode of operation. *Reliability Engineering and System Safety*, 96:365–373.

Jones, B., Jenkinson, I., Yang, Z., and Wang, J. (2010). The use of bayesian network modelling for maintenance planning in a manufacturing industry. *Reliability Engineering and System Safety*, 95:267–277.

Kim, M. (2011). Reliability block diagram with general gates amd its application to system reliability analysis. *Annals of Nuclear Energy*, 38:2456–2461.

Liu, Y. and Rausand, M. (2011). Reliability assessment of safety instrumented systems subject to dfferent demand modes. *Journal of Loss Prevention in the Process Industries*, 24:49–56.

Lundteigen, M. and Rausand, M. (2009). Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and case study. *International Journal of Reliability: Quality and Safety Engineering*, 16:187–212.

Matlab (2014). Matlab version 2014b. http://se.mathworks.com/products/matlab.

Matlab (2015). Bayesian network toolbox for matlab. https://code.google.com/p/bnt/. Online; accessed 10-June-2015.

Nima, K., Fasisal, K., and Paul, A. (2011). Safety analysis in process facilities: Comparison of fault tree and bayesian network approaches. *Reliability Engineering and System Safety*, 96:925–932.

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

Peng, W., Huang, H., Li, Y., Zuo, M. J., and Xie, M. (2013). Life cyclereliabilityassessmentofnew-products—a bayesianmodel updating approach. *Reliability Engineering and System Safety*, 112:109–119.

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

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

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

Sankaran, M., Ruoxue, Z., and Natasha, S. (2001). Bayesian networks for system reliability reassessment. *Structural Safety*, 23:231–251.

Transocean (2011). Macondo well incident report-transocean investigation report-volume i. Technical report.