



NTNU – Trondheim
Norwegian University of
Science and Technology

Modeling Blowouts During Drilling Using STAMP and STPA

Silje Frost Budde

Master of Science in Product Design and Manufacturing

Submission date: June 2012

Supervisor: Stein Haugen, IPK

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

MASTEROPPGAVE
Våren 2012
for
stud. techn. Silje Frost Budde

MODELLERING AV UTBLÅSNINGER UNDER BORING MED BRUK AV STAMP OG STPA

(Modeling blowouts during drilling using STAMP and STPA)

Eksisterende rammeverk for risikoanalyser ble utviklet for rundt 50 år siden og baserer seg i stor grad på den forståelsen man hadde den gang av ulykkesmodeller og hvordan ulykker skjer. Siden den tid er flere alternative forståelser av spesielt storulykker eller organisatoriske ulykker lansert. Pr i dag har disse imidlertid i stor grad det til felles at de ikke har utviklet gode metoder for å kunne analysere risiko, men i hovedsak er begrenset til å kunne brukes i ulykkesgransking, for å forklare ulykker som har skjedd. Et unntak fra dette er ulykkesmodellen STAMP og den tilhørende metoden STPA.

I denne oppgaven er målet å teste STAMP og STPA på en konkret problemstilling for en offshore installasjon. Problemstillingen er utblåsninger under boring. Formålet er å danne seg en oppfatning av om dette er en mulig alternativ fremgangsmåte, å gjøre seg opp en mening om arbeidsomfang, om man får andre svar enn gjennom en tradisjonell risikoanalyse samt hvilke data som er nødvendige for å kunne gjennomføre slike analyser. Dette vil danne grunnlag for anbefalinger om videre arbeid.

Opgaven skal gjennomføres i følgende trinn:

1. Litteraturstudium – gjennomgang og oppsummering av relevant litteratur om STAMP og STPA samt sette seg inn i problemstillingen.
2. Etablere en modell for utblåsninger, basert på STAMP/STPA. Modellen skal i utgangspunktet være kvalitativ, men målet er at den skal kunne danne grunnlag for kvantifisering.
3. Identifisere databehov for en slik modell og vurdere tilgjengelighet av data som behøves for å kunne kvantifisere risiko.
4. Vurdere modellen som er utviklet og arbeidet som er utført med tanke på:
 - a. Arbeidsomfang, sammenlignet med tradisjonelle analysemetoder

- b. Hvilke nye muligheter for beslutningsstøtte en slik modell gir sammenlignet med tradisjonelle analysemetoder.
 - c. Om kvantifisering er mulig med en slik modell, og i så fall hvilke nye typer data som må fremskaffes for å kunne kvantifisere.
5. Oppsummere og gi anbefalinger for videre arbeid.

Oppgaveløsningen skal basere seg på eventuelle standarder og praktiske retningslinjer som foreligger og anbefales. Dette skal skje i nært samarbeid med veiledere og fagansvarlig. For øvrig skal det være et aktivt samspill med veiledere.

Innen tre uker etter at oppgaveteksten er utlevert, skal det leveres en forstudierapport som skal inneholde følgende:

- En analyse av oppgavens problemstillinger.
- En beskrivelse av de arbeidsoppgaver som skal gjennomføres for løsning av oppgaven. Denne beskrivelsen skal munne ut i en klar definisjon av arbeidsoppgavenes innhold og omfang.
- En tidsplan for fremdriften av prosjektet. Planen skal utformes som et Gantt-skjema med angivelse av de enkelte arbeidsoppgavenes terminer, samt med angivelse av milepæler i arbeidet.

Forstudierapporten er en del av oppgavebesvarelsen og skal innarbeides i denne. Det samme skal senere fremdrifts- og avviksrappporter. Ved bedømmelsen av arbeidet legges det vekt på at gjennomføringen er godt dokumentert.

Besvarelsen redigeres mest mulig som en forskningsrapport med et sammendrag både på norsk og engelsk, konklusjon, litteraturliste, innholdsfortegnelse etc. Ved utarbeidelsen av teksten skal kandidaten legge vekt på å gjøre teksten oversiktlig og velskrevet. Med henblikk på lesning av besvarelsen er det viktig at de nødvendige henvisninger for korresponderende steder i tekst, tabeller og figurer anføres på begge steder. Ved bedømmelsen legges det stor vekt på at resultatene er grundig bearbeidet, at de oppstilles tabellarisk og/eller grafisk på en oversiktlig måte og diskuteres utførlig.

Materiell som er utviklet i forbindelse med oppgaven, så som programvare eller fysisk utstyr er en del av besvarelsen. Dokumentasjon for korrekt bruk av dette skal så langt som mulig også vedlegges besvarelsen.

Eventuelle reiseutgifter, kopierings- og telefonutgifter må bære av studenten selv med mindre andre avtaler foreligger.

Hvis kandidaten under arbeidet med oppgaven støter på vanskeligheter, som ikke var forutsett ved oppgavens utforming og som eventuelt vil kunne kreve endringer i eller utelatelse av enkelte spørsmål fra oppgaven, skal dette straks tas opp med instituttet.

Oppgaveteksten skal vedlegges besvarelsen og plasseres umiddelbart etter tittelsiden.

Innleveringsfrist: 11. juni 2012

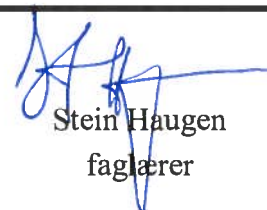
Besvarelsen skal innleveres i 1 elektronisk eksemplar (pdf-format) og 2 eksemplar (innbundet).

Ansvarlig faglærer/veileder ved NTNU: Professor Stein Haugen
Telefon: 73 59 01 11
Mobiltelefon: 934 83 907
E-post: stein.haugen@ntnu.no

**INSTITUTT FOR PRODUKSJONS-
OG KVALITETSTEKNIKK**



Per Schjølberg
førstemanuensis/instituttleder



Stein Haugen
faglærer

“Knowledge rests not upon truth alone, but upon error also.”

Carl Gustav Jung

Preface

This report is written by stud.techn. Silje Frost Budde and is the result of the master thesis *Modeling Blowouts During Drilling Using STAMP & STPA*, given at the department of Production and Quality Engineering at the Norwegian University of Science and Technology (NTNU). The work related to this assignment has been performed during the spring of 2012.

The master thesis has its foundation in the project assignment *Monitoring of Major Accident Risk- blowout and well releases*. The aim of this paper is to get an insight into the methods of STAMP and STPA for a drilling operation.

I would like to express my gratitude to my father, Ole Budde, and my brother, Simen Frost Budde, for their assistance during proofreading. A special thanks my supervisor, Stein Haugen at NTNU for patiently reading and giving good advice during the preparation of this master thesis.

Trondheim, 07.06.2012



Silje Frost Budde

Abstract

The focus of this master thesis has been on modeling the risk of blowouts during drilling using System-Theoretic Accident Model and Processes (STAMP) and System-Theoretic Process Analysis (STPA). The world and technology are changing, but these changes are not reflected in our safety engineering approaches. Many of the basic assumptions of traditional techniques no longer hold for complex, high-technical systems being built today. STAMP is a new model based on systems theory rather than reliability.

The STAMP model is based on three concepts - safety constraints, hierarchical safety control structures, and process models - together with system theory concepts. The systems are considered as interrelated components kept in a state of dynamic balance by feedback control loops. Systems are treated as dynamic processes that are frequently adjusting to attain their ends and to respond to internal changes, as well as changes to their environment.

STPA is a hazard analysis technique, based on the STAMP model that assumes that accidents are caused by inadequate enforcement of constraints on component behavior more precisely than simple component failures. Accidents in complex systems are often caused by unsafe interaction between components that have not failed. STPA includes both component failure accidents and component interaction accidents and may find more causes of hazards than the older techniques. The first step in STPA is to identify the unsafe control actions that can result in hazards. The second step is to specify the potential causes of the unsafe control.

The process of safely extracting hydrocarbons from a reservoir can be divided into three steps. The first step is drilling, where the hole is drilled and reinforced from the sea floor down through the trap layers and into the reservoir zone. The second step is completion, which begins by opening the well bore, this allows hydrocarbons to flow into it. The final

step is production, wherein the hydrocarbons are extracted from the well.

Formation flow during drilling operations is normally referred to as a kick. If a kick is not controlled, it may result in a blowout. Six well kick indicators have to be monitored during drilling; (1) drilling breaks, (2) increase in flow rate, (3) increase in pit volume, (4) variation in pump speed and pump pressure, (5) well flowing during connection, and (6) change of drilling fluid properties.

The STPA model has its basis in the well kick indicators, whereas drilling breaks are the first indication of a well kick. When this is detected, the other five indicators have to be monitored closely to see if a well kick is the case or not. The sensors send information about the parameters to the control panel, where the driller and mud logger monitors the process. If some of the parameters are outside given limits, the pump is stopped to stabilize the process. In case the well condition does not change, the blowout preventer (BOP) is closed to get control over the situation.

A lot of the identified errors are often the same for many of the different control actions. This includes among other control actions “inflow of mud does not stop when provided”, “change in one of the control actions is discovered too late” and “misinformation about one of the parameters”.

There will be a great amount of work related to developing a STPA model. In order to utilize the method, one has to be familiar with the operation and organization. The organization has to be known to obtain a realistic hierarchical control structure and a control structure where the safety constraints to all controllers are identified. If one is unfamiliar with the actual system, some inadequate control actions might be overlooked.

The STPA model is suitable for analysis of well kicks during a drilling operation. This approach is effective to give an understanding of why accidents happen, so that sufficient improvement measures can be implemented to prevent future accidents. A good basis for quantification of human error, together with organizational factors, is to use the Human Error Assessment and Reduction Technique (HEART) to set generic task types with their associated nominal error probability. The activities in the control loops will then be matched with to the generic tasks listed in HEART. Based on the numbers given by HEART, an event tree analysis can be used in modeling and analysis of different accident scenarios for a drilling operation.

Sammendrag

Fokuset for denne masteroppgaven har vært modellering av utblåsninger under boring med bruk av metodene, System-Theoretic Accident Model and Processes (STAMP) og System-Theoretic Process Analysis (STPA). Verden og teknologien ender seg, men disse endringene gjenspeiles ikke i risikoanalysene. Mange av de grunnleggende forutsetningene for tradisjonelle teknikker er ikke egnet for komplekse og høyteknologiske systemer som lages i dag. STAMP er en ny modell som bygger mer på systemteori enn på pålitelighet.

STAMP er basert på tre konsepter - sikkerhetsrestriksjoner, hierarkisk sikkerhetskontrollstruktur og prosess modeller - sammen med systemteori konsepter. Systemene blir vurdert som beslektede komponenter holdt sammen i en tilstand av dynamisk balanse ved hjelp av kontrollsløyfer. Systemene blir behandlet som dynamiske prosesser som blir justeret for å holde sine målparametre og reagere på egne og omgivelsenes endringer.

STPA er en risikoanalyse teknikk, basert på STAMP, som antar at ulykker er forårsaket av utilstrekkelig gjennomføring av restriksjoner på komponenters adferd enn av enkle komponentfeil. Ulykker i komplekse system er ofte forårsaket av farlig vekselspill mellom komponenter som ikke feiler. STPA inkluderer både ulykker basert på komponentfeil og vekselspill mellom komponenter og kan kanskje finne flere årsaker til farer enn eldre teknikker. Det første trinnet i STPA er å identifisere de farlige kontrollhandlingene som kan føre til ulykker. Det andre trinnet spesifiser de mulige årsakene til disse farlige kontrollhandlingene.

Prosessen for sikker ekstrahering av hydrokarboner fra et reservoar kan deles opp i tre trinn. Det første trinnet er boring, hvor hullet blir boret og forsterket fra havbunnen og nedover gjennom forskjellige sedimenter ned til reservoarsonen. Det andre trinnet er ferdigstilling, som starter med å åpne borekronen og tillater hydrokarboner å flyte inn. Det siste trinnet er produksjon, hvor hydrokarboner blir hentet ut fra brønnen.

Ukontrollert innstrømning under boreoperasjoner refereres ofte til som et brønnsпарк. Dersom et brønnsпарк ikke blir holdt under kontroll, kan det resultere i en utblåsning. Det er seks indikatorer som må overvåkes under en bore operasjon; (1) borehastighet, (2) økende strømningsrate, (3) økende “pit” volum, (4) variasjon i pumpehastighet og pumpetrykk (5) innstrømning under tilkobling og (6) forandring i borevæskens egenskaper.

STPA modellen er basert på brønnsпарк indikatorene, hvor endring i borehastighet er den første antydningen på et brønnsпарк. Når dette blir detektert, må de andre indikatorene overvåkes nøye for å se om et brønnsпарк er tilfelle eller ikke. Sensorene sender informasjon om parameterne til kontrollpanelet, hvor en borer og en “mud logger” overvåker prosessen. Dersom noen av parameterne er utenfor de gitte grensene, blir pumpen stoppet for å stabilisere prosessen. Dersom brønnens tilstand ikke endres, blir en sikkerhetsventil mot utblåsning (BOP) brukt for å få kontroll over situasjonen.

Mange av de identifiserte feilene er de samme for de forskjellige kontrollhandlingene. Eksempler på dette er: “innstrømmingen av boreslam stopper ikke når det skal”, “forandring i en av kontrollhandlingene oppdages for sent” eller “feilinformasjon om en av måleparameterne”.

Det er mye arbeid knyttet til utviklingen av STPA modeller. For å kunne utnytte metoden, må man være kjent med både operasjonen og organisasjonen. Organisasjonen må være kjent for å kunne få en realistisk oversikt over kontrollstruktur og identifisere en kontrollstruktur hvor alle sikkerhetsrestriksjoner til kontrollerne er identifisert. Dersom man ikke kjenner det faktiske systemet, kan enkelte viktige kontrollhandlinger ikke bli inkludert i analysen.

STPA egner seg for analysering av brønnsпарк under boreoperasjoner. Denne metoden gir en god forståelse av hvorfor ulykker skjer, slik at man kan identifisere forbedringstiltak for å kunne forhindre fremtidige ulykker. Et godt grunnlag for kvantifisering av menneskelige feil og organisatoriske faktorer er å bruke teknikken, Human Error Assessment and Reduction Technique (HEART) for å knytte nominelle feilsannsynligheter til oppgavetyper. Man kobler dermed aktivitetene i kontrollsløfene til en av oppgavene i HEART. Basert på tallene i HEART, kan man bruke et hendelsestre for å modellere og analysere de ulike ulykkescenariene for en boreoperasjon.

Contents

- Preface** **iii**

- Abstract** **v**

- Sammendrag** **vii**

- 1 Introduction** **1**
 - 1.1 Background 1
 - 1.2 Objectives 2
 - 1.3 Delimitations 3
 - 1.4 Approach 3
 - 1.5 Structure of the Report 4

- 2 STAMP & STPA** **7**
 - 2.1 STAMP 7
 - 2.1.1 Safety Constraints 8
 - 2.1.2 Hierarchical Safety Control Structure 9
 - 2.1.3 Process Model 11
 - 2.1.4 Classification of Accident Causes 12
 - 2.2 STPA 13
 - 2.2.1 The STPA Process 13

- 3 A Drilling Operation** **15**
 - 3.1 Defining the Process 15
 - 3.1.1 Spudding the Well 15
 - 3.1.2 Set the Conductor Casing and Cement Extra Early Casing Stings 16
 - 3.1.3 Lower the Riser and BOP 17

3.1.4	Set the Subsequent Casing Strings	17
3.1.5	Cement the Casing String	17
3.1.6	Production Casing	18
3.2	Well Control	18
3.2.1	Primary Barriers	18
3.2.2	Secondary Barrier	19
3.2.3	Indication of Kicks	19
4	Hazard Analysis For Drilling Operations Based on STPA	21
4.1	System Hazards and System-Level Safety Constraints	22
4.2	Safety Control Structure	25
4.3	Potentially Inadequate Control Actions	28
4.4	Identifying Causal Scenarios	32
4.4.1	Drilling Breaks	34
4.4.2	Increase in Flow Rate	36
4.4.3	Increase in Pit Volume	37
4.4.4	Variation in Pump Speed & Pressure	39
4.4.5	Well Flowing During Connection	41
4.4.6	Change of Drilling Fluid Properties	43
4.4.7	Summary of Causal Scenarios	44
4.5	The Degradation of Controls over Time	45
4.5.1	Feedback Channels	46
4.5.2	Process Model	47
4.5.3	Education and Training	47
5	Evaluation of the Model	49
5.1	Decision Support	49
5.2	Limitations with STAMP & STPA	50
5.3	Workload in STAMP & STPA	51
5.4	Quantification in STAMP & STPA	52
5.5	STAMP & STPA Compared to Other Methods	54
5.5.1	Event Chain Models	54
5.5.2	HAZOP & FMEA	55

5.5.3 FRAM 57

6 Conclusions 59

6.1 Recommendations for Further Work 60

Appendices 63

A List of Abbreviations 63

B Definitions 65

C Pre-Study Report 69

D Progress Report 77

References 81

List of Figures

- 2.1 Operator has Indirect Information About the Process State and Indirect Controls 9
- 2.2 The Communication Channels Between Control Levels 10
- 2.3 Any Controller Needs a Model of the Process Being Controlled 11
- 2.4 A Standard Control Loop 13

- 3.1 A Surface Typical Oil Production Well 16

- 4.1 The Hierarchical Control Structure to Ensure the Safe Operation of Drilling . . 23
- 4.2 The Overall Control Structure for a Drilling Operation 26
- 4.3 The Overall Process Model for the Drilling Operation 31
- 4.4 The Control Loop With All Well Kick Indicators for a Drilling Operation 33
- 4.5 The Control Loop for the Drilling Breaks Indicator 34
- 4.6 The Control Loop for the Flow Rate Indicator 36
- 4.7 The Control Loop for the Pit Volume Indicator 38
- 4.8 The Control Loop for the Pump Speed & Pressure Indicator 40
- 4.9 The Control Loop for the Well Flowing During Connection Indicator 42
- 4.10 The Control Loop for the Drilling Fluid Properties Indicator 43

- 5.1 The Event Sequence for the Well Kick Indicator “Flow Rate” 53

List of Tables

4.1 Safety Related Requirements and Constraints for Each Controller 27

4.2 Identified Hazardous System Behaviors 29

Chapter 1

Introduction

This chapter introduces the basis for this master thesis, with focus on the background and problem description together with limitations, approach and structure of the report.

1.1 Background

Accident models form the foundation for investigating and analyzing accidents, preventing accidents in the future and specifying whether systems are suitable for use (Leveson, 2004). In accident investigation accident models are used to identify patterns in the accident and the model may affect both the data collected and the factors identified as causative. They also underlie all hazard analysis and risk assessment methods. Because they affect the factors considered in any of these activities, they may either act as a filter and prejudice toward considering only certain events and conditions or they may expand activities by focusing on factors that are often excluded.

Most accident models view accidents as a result of a chain or sequence of events. Models like this work well for losses caused by failures of physical components and for quite simple systems. But the types of systems we are trying to establish and the context in which they are being established have changed.

The existing framework for risk analysis was developed about 50 years ago and is mainly based on the understanding of accident models and how accidents happen. Later, several alternative interpretations of particularly major accidents or organizational accidents have

been launched. As of today, these understandings have in common that no accompanying methods to perform risk assessment have been developed. Generally they are limited to accident investigation and to explain why accidents have happened. One exception from this is the accident model System-Theoretic Accident Model and Processes (STAMP) and the corresponding method System-Theoretic Process Analysis (STPA).

Problem Formulation

The main problem to be addressed, as it was presented in the master thesis, consists of five main tasks, as listed below:

1. Review and summarize STAMP and STPA and become familiar with the problem complex.
2. Establish a model for blowouts based on STAMP/STPA.
3. Identify the parameters needed for such a model and assess the availability of them to be able to quantify risk.
4. Assess the model developed and the work that is performed with focus on:
 - (a) Amount of work,
 - (b) New possibilities for decision support,
 - (c) If quantification is possible, and if it is, what types of data are required.
5. Summarize, conclude and give recommendations for further work.

1.2 Objectives

The aim of this master thesis is to test the STAMP and STPA method for a specific case on an offshore installation. The problem to investigate is blowouts and well releases during drilling operations. The goal is therefore to form an understanding of whether this is a possible alternative approach, together with gaining some experience on the amount of work involved. In addition, whether there are different results compared to conventional methods and list what parameters are necessary to perform these analyses.

1.3 Delimitations

Because of the time frame, some limitations have been made to the assignment text. The master thesis is generally delimited to only cover oil and gas activities on the Norwegian Continental Shelf (NCS). Due to the size and complexity of a drilling operation, the STAMP model is based on the drilling phase. This is an important part of a drilling operation. Many blowouts and well releases occur during this phase, and the aim is consequently to investigate deeper into this phase to try to find errors that could cause blowouts and well releases.

A drilling operation can be executed from many different platform types. The focus for this master thesis has been production platforms, where other activities also are executed at the platform. Thus affects how hierarchical control structure is established.

The established model will be based on general operations and is for that reason not linked to a specific company, but tries to cover the whole oil and gas industry at the NCS. In that way, the model can later be linked to other locations and detect improvement factors. The established model will in addition be a simplification of a real drilling operation. Such an operation is a very complex operation and the simplification is done to get a better understanding of how factors are linked together. The parameters that does not affect a drilling operation is not considered in this analysis.

1.4 Approach

The foundation for the master thesis was laid by the work related to the project assignment - *Monitoring of Major Accident Risk- Blowout and Well Releases* (Budde, 2011), which was performed as a literature study. As Reisman (1988) states, the strategy for this master thesis is based on the transfer of technologies. This is a strategy where one uses what is known in one discipline to model problem domains falling in another discipline.

Task 1 will set the foundation for the master thesis with summarizing STAMP and STPA supported by relevant literature and get a insight into the problem complex regarding drilling on an offshore installation. The model for blowouts in task 2 should be produced based on the findings from task 1, and should be presented in a clear and logic manner. The estab-

lishment of this model will be the main focus for this assignment. The model will initially be qualitative, but the goal is that it will form the basis for a quantitative model.

Both task 3 and 4 have their foundation in the findings presented in task 2. This includes identifying parameters for the STPA model, amount of work, new possibilities for decision support and if quantification is possible. This will be compared to conventional analysis methods such as event chain model and Hazard and Operability study (HAZOP) and Failure Modes and Effects Analysis (FMEA) together with a relatively new method, Functional Resonance Accident Model (FRAM). One have chosen to first introduce STAMP and STPA in relation to these aspects and then compare them to the other methods with emphasize on their differences.

The recommendations in task 5 should be based on all the previous problems. The section should be concluded with recommendations for actions to improve the methods.

Literature Survey

The book *Engineering a Safer World Systems Thinking Applied to Safety*, written by Nancy G. Leveson, is the foundation for this master thesis. In this book Leveson argues that traditional models of causality are inadequate and present a new, extended model of causation, called Systems-Theoretic Accident Model and Processes, or STAMP, and then demonstrate how the new model can be used to create methods for system safety engineering, including accident analysis, hazard analysis, system design, safety in operations and management of safety-critical system. The emphasis in system safety is changed from preventing failures to enforcing behavioral safety constraints.

1.5 Structure of the Report

The structure of this master thesis will be based on the primary task, and follows the order of the tasks. The second chapter introduces a new causality model, called STAMP. This includes both the three main concepts in the model - safety constraints, hierarchical control structures and process models - classification of accident causes implied by the new model together with a new approach to hazard analysis based on the causality model, called

STPA.

The third chapter briefly describes a drilling operation and well control in connection with the drilling phase. Further, chapter four introduces the STAMP and STPA method applied on a general drilling operation at the NCS.

Chapter five begins by evaluating the model presented in the previous chapter in relation to quantification of the model, new possibilities for decision support and limitations together with work load for the methods. In addition, a comparison with event chain model, HAZOP, FMEA and FRAM has been carried out.

The conclusions and recommendations for further work from this report are presented in chapter six.

Chapter 2

STAMP & STPA

Accident models structures the foundation for investigating and analyzing accidents, preventing future ones, and deciding whether systems are appropriate for use (risk assessment) (Leveson, 2004). In accident investigation they take advantage of patterns on the accidents and influence both the data collected and the factors identified as causative. Since they influence the factors considered in any of these activities, they may either behave as a filter and bias toward considering merely certain events and conditions or they may expand activities by forcing consideration of factors that are often excluded.

In traditional causality models, accidents are regarded to be caused by chains of failure event, where each failure directly causing the next one in the chain (Leveson, 2011). Nevertheless, the systems we are trying to build and the context in which they are being built has been changing. Accident causality needs to be expanded outside failure event, so that it incorporates component interaction accident and indirect or systematic causal mechanisms (Leveson, 2004). This chapter present a new model, where the limits to current accident models have been stretching and new approaches are needed.

2.1 STAMP

While traditional accident causation explain accident as a chain of events that leads to an accident, The Systems-Theoretic Accident Model and Process (STAMP) have another approach (Leveson, 2009). To prevent accident it has to 'break the chain' either preventing an event or

by adding extra 'and' gates in the chain to make the existence of the events in the chain less probable.

STAMP consider additional types of accidents and causes by included non-linear, indirect, and feedback relationship between events (Quyang et al., 2010). Accident or unacceptable losses can not only be a result of system component failures, but also from interactions between components- both physical and social- that desecrate system safety constraints.

The principles of this method is based on understanding why an accident happened by deciding why the control was ineffective. Obstruct future accidents demand shifting from a focus on obstruct failures to the extensive goal of designing and implementing controls that will impose the necessary constraints.

The three important concepts in STAMP are safety constraints, hierarchical safety control structure and process models.

2.1.1 Safety Constraints

An important aspect in STAMP is a constraint and not an event (Leveson, 2011). Events that results in losses only happen because safety constraint were not successfully imposed. *Safety constraints* specify the relationship between system variables or components that constitute the non-hazardous or safe system states, such as that power must never be on when the access door to the high-power source is open (Leveson, 2009). It has with time become more difficult to identify and enforce safety constraints in design and operations because of old and less automated systems.

It is divided between *passive* and *active* controls (Leveson, 2011). Passive controls are defined as those that maintain safety by their attendance, such as shields and barriers. Active controls demand some actions to provide protection: (1) monitoring, (2) measurement, (3) diagnosis, and (4) response. All four has to be completed before a loss happens. These actions are normally implemented by a control system.

By introducing electromechanical control the operators can control the processes from a larger distance, than with pure mechanically linked controls (Leveson, 2011). But the distance has resulted in loss of direct information about the process. The system designers have to determine beforehand what information the operator would need under all condi-

tions to safely control the process. Electromechanical controls relaxed constraints on the system design permitting greater functionality, see figure 2.1. But it also creates new possibilities for designers and operator errors that had not existed or were much less probable in mechanically controlled systems.

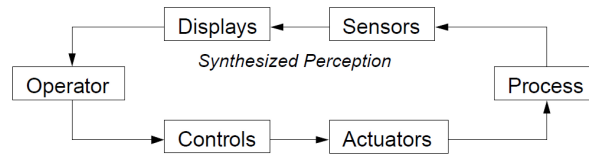


Figure 2.1: Operator has Indirect Information About the Process State and Indirect Controls (Leveson, 2011, p.68)

It is the freedom from constraints that make the design of such systems so complicated. Physical constraints force discipline and limited complexity in system design, structure and modification. The physical constraints also forms system design in ways that efficiently transmits useful physical components and process information to operators and supports their cognitive processes.

2.1.2 Hierarchical Safety Control Structure

The second concept is hierarchical safety control structure, where hierarchies are a basis concept in systems theory (Leveson, 2009). For a hierarchical model of a complex process, it is often possible to describe and comprehend mathematically behavior of individual components when the behavior is totally independent of other components at the same or other levels. Whereas emergent properties such as safety does not fulfill this assumption and demand a description of the acceptable interactions between components at a level higher than the components.

Systems are viewed as hierarchical structures, where each level levies constraints on the activity in the level beneath it (Leveson, 2011). Constraints or lack of constraints at a higher level provide or control lower-level behavior. These are often divided between two basic hierarchical control structures; system development and system operation - with interaction between them.

Control processes function between different levels to control the processes at lower levels in the hierarchy. These control processes impose the safety constraints for which the control

process is responsible. Accidents happen when these processes supply inadequate control and the safety constraints are invaded in the behavior of the lower-level components.

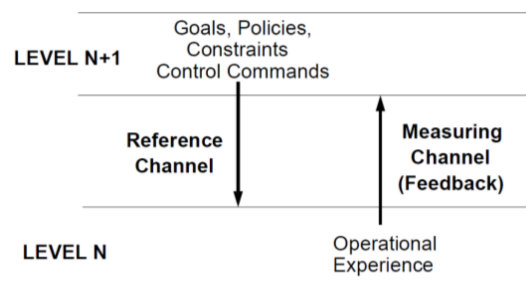


Figure 2.2: The Communication Channels Between Control Levels (Leveson, 2011, p.72)

Between the hierarchical levels of each safety control structure, effective communication channels are needed. This include both a downward reference channel providing the information essential to levy safety constraints on the level below and an upward measuring channel to provide feedback about how effectively the constraints are being fulfilled. This is illustrated in figure 2.2. A critical part in any open system is feedback in order to provide adaptive control. The controller uses feedback to adjust future control commands to more easily achieve its goals.

At each level of the hierarchical structure, insufficient control may result from missing constraints, inadequate safety control commands, commands that were not performed correctly at a lower level, or insufficiently communicated or processed feedback about constraint enforcement. To totally understand the cause of accident and prevent future ones, the system hierarchical safety control structure must be inspected to determine why the controls at each level were inadequate to maintain the constraints on the safety behavior at the level below and the event happened (Leveson, 2009).

When designing a new system or analyzing an existing system with STAMP as the foundation, required safety constraint are identified at the system first level. In addition, a top-down iterative process is utilized to identify required safety constraints that must be levied at each of the lower levels. The whole safety control structure must be carefully designed and assessed to assure that the controls are adequate to continue the constraints on behavior essential to control risk.

2.1.3 Process Model

The third concept used in this model is process models (Leveson, 2011). This is an important part of control theory. There are four conditions demanded to control a process. The first is a *goal*, which is the safety constraints that must be imposed by each controller in the hierarchical safety control structure. The *action condition* are implemented in the control channels while the *observability conditions* is implemented in the feedback or measuring channels. The last condition is the *model condition*, where any controller have to have a model of the process being controlled to control is effectively. This is illustrated in figure 2.3.

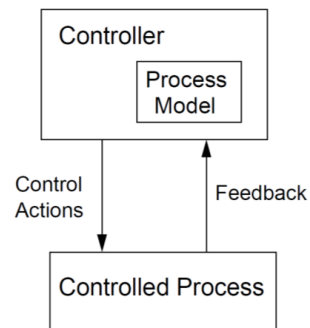


Figure 2.3: Any Controller Needs a Model of the Process Being Controlled (Leveson, 2011, p.75)

Overall, accidents often happen, when the process model used by the controller (automated or human) does not match the actual state of the process and, as a result:

1. Unsafe control commands are given
2. Control actions demanded for safety are not provided
3. Potentially safe control commands are provided at the wrong time (too early or too late), or
4. Control is stopped too soon or applied too long

It can be challenging to design an effective safety control structure that provides feedback and input essential to keep the controller's model compatible with the actual state of the process. Likewise, an important component in understanding accidents and losses include determining how and why the controller was ineffective.

2.1.4 Classification of Accident Causes

With basis in STAMP, the general causes of accidents can be identified using basic system and control theory. Accidents in STAMP are the result of a complex process that results in the system behavior invading the safety constraints (Leveson, 2011). The safety constraints are forced by the control loops between the different levels of the hierarchical control structure that are in place throughout design, development, manufacturing and operations.

When using STAMP causality model, if there is an accident, one or more of the upcoming must have happened:

1. The safety constraints were not enforced by the controller.
 - (a) The control actions necessary to enforce the related safety constraint at each level of the socio-technical control structure for the system were not supported,
 - (b) The necessary control actions were provided, but at the wrong time (too early or too late), stopped too soon, or applied too long, or
 - (c) Unsafe control action were provided that caused a violation of the safety constraints.
2. Suitable control action were provided, but not followed.

These same general factors applied at each level of the socio-technical control structure, whereas the interpretation of the factor at each level may vary, see figure 2.4. Classification of accident causal factors begins by examining each of the basic components of a control loop and deciding how their inappropriate operation may contribute to the general types of inadequate control.

The causal factors in accident can be divided into three general categories: (1) the controller operation, (2) the behavior of actuators and controlled processes, and (3) communication and coordination between controllers and decision makers. When humans are involved in the control structure, context and behavior-shaping mechanisms also play a significant role in causality.

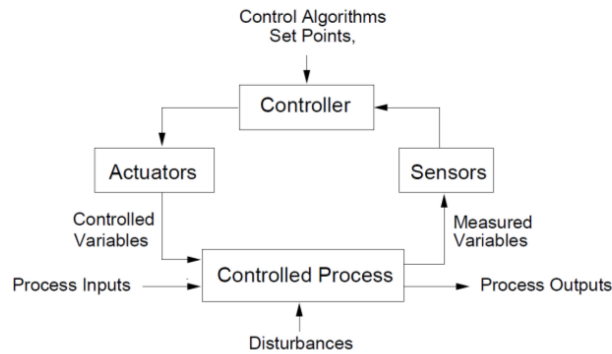


Figure 2.4: A Standard Control Loop (Leveson, 2011, p. 55)

2.2 STPA

Systematic-Theoretic Process Analysis (STPA) is a new approach to hazard analysis, based on the STAMP causality model (Leveson, 2011). To establish new approach to both technical system hazard analysis and organizational risk analysis based on STAMP, one has to identify a set of factors that can lead to contravention of safety constraints, such as inadequate feedback to maintain factual mental models (Leveson, 2009). The reason for developing STPA was to incorporate the new causal factors identified in STAMP that are not treated by older techniques (Ishimatsu et al., 2010).

2.2.1 The STPA Process

This approach can be used at any stage of the system life cycle. The goals for STPA are (1) to identify the system hazards and the safety-related constraints necessary to assure acceptable risk, and (2) to gather information about how safety constraints may be desecrated and use this information to eliminate, reduce and control hazards in the system design and operation (Leveson, 2011).

The method starts with identifying the system safety requirements and design constraints and then assist requirement and safety constraints on individual system components. STPA helps to identify scenarios in which the safety constraints can be desecrated, at both system and component level. The information can be used to eliminate or control the scenarios in the system and component design.

STPA has two main steps:

1. Identify the potential for inadequate control of the system that may lead to a hazardous state. Hazardous states result from inadequate control or imposition of the safety constraints, which can happen because:
 - (a) A control action required for safety is *not* supported or not followed;
 - (b) An unsafe control action *is* supported;
 - (c) A potentially safe control action is supported too early or too late, that is, at the wrong time or in the wrong sequence;
 - (d) A control action required for safety is stopped too soon or applied too long.
2. Determine how each potentially hazardous control action identified in step 1 could happen.
 - (a) For each unsafe control action, inspect the parts of the control loop to see if they could cause it. Design controls and alleviation measures if they do not already exist, or evaluate existing measures if the analysis is being performed on an existing design. For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems.
 - (b) Consider how the designed controls could demote over time and build in protection, including:
 - i. Management of procedures to assure safety constraints are imposed in planned changes.
 - ii. Performance audits where the assumptions underlying the hazard analysis are the preconditions for the operational audits and controls so that unplanned changes that desecrate the safety constraints can be detected.
 - iii. Accident and incident analysis to trace oddities to the hazards and to the system design.

The analysis can be performed in one step, but separating the process into discrete steps reduces the analytical responsibility on the safety engineers and give a structured process for hazard analysis. The information from the first step, identifying the unsafe control actions, is required to carry out the second step ,identifying the causes of the unsafe control actions.

Chapter 3

A Drilling Operation

Blowouts have plagued the petroleum industry since its beginning. Well operations and well control events have resulted in losses of valuable resources, increased drilling costs, environmental damages, increased regulations, injuries to personnel, and loss of life (Schubert, 1995). The majority of all blowouts are often due to human error, and may be avoided if proper well control procedures would have been followed. The purpose of this chapter is to get an overview of a drilling operation together with a presentation of potential well control problems.

3.1 Defining the Process

There are three phases to safely extract hydrocarbon from a reservoir (Bartlit et al., 2011). The first step is drilling, where the hole is drilled and reinforced from the sea floor and down through the trap layers and into the reservoir zone. The second step is completion, which begins by opening the well bore, this allows hydrocarbons to flow into it. Equipment is then installed at the wellhead to control and collect the hydrocarbons. The final step is production, wherein the hydrocarbons are extracted from the well.

3.1.1 Spudding the Well

The operation starts with lowering the first casing string, typical 36 inch or more, down to the sea floor. This is a part of the structural foundation for the rest of the well. The wellhead

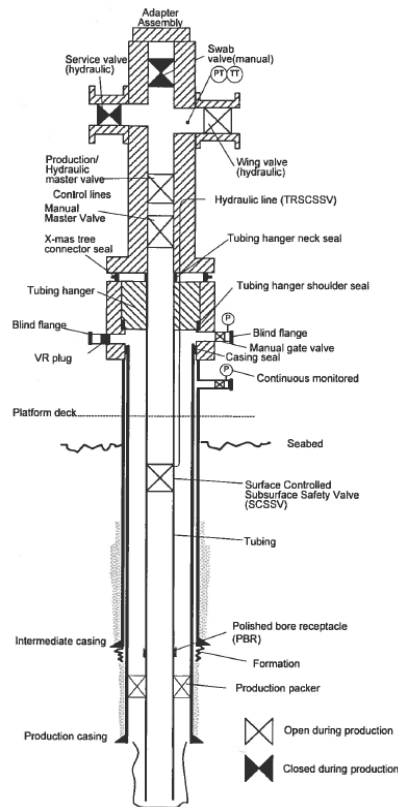


Figure 3.1: A Surface Typical Oil Production Well (Corneliusson, 2006, p.22)

assembly is on top of the conductor casing and is an anchoring point for the future casing strings. The conductor is lowered into place using a drill string and a “running tool” that fasten the drill string to the wellhead. Seawater is pumped down the drilling string at high pressure to “jet” away the sediment at the bottom of the conductor casing.

3.1.2 Set the Conductor Casing and Cement Extra Early Casing Stings

When the conductor casing has been jetted to its depth, a smaller casing string is installed deeper into the seabed. It is drilled with a hole diameter a bit larger than the casing to leave room for the cement that secures it into place. The cement seals the interior of the well from formation outside the casing and anchors the casing to the rocks around. When this is completed, the cement fills the annular space around the casing, reinforcing the casing and establishes the mechanical foundation for additional drilling. The process continues as the hole is drilled using a smaller diameter casing and cementing each in place.

3.1.3 Lower the Riser and BOP

Gradually the dregs at the bottom of the well are too strong to be removed by jetting and starts to use rotary drilling bits or drilling mud. The Blowout Preventer (BOP) is fastened on the wellhead and is connected back to the rig through the Lower Marine Riser Package (LMRP) and riser. When the BOP and riser system are moved down atop of the wellhead, the rest of the drilling operations are done through this. The mud is then circulated down through the drill string, into the well bore, back up the annular space around the drill string, up through the riser and back to the rig.

3.1.4 Set the Subsequent Casing Strings

The drilling mud system and a rotary drill bit are used to drill through the earlier set of casing strings. The open hole is extended below the existing casing strings as far as the pore pressure and fracture gradient allows it, and set subsequent smaller diameter casing strings inside the existing ones.

A new casing string is needed at specific depth and the drill string is removed from the well. After finishing this a running tool is attached to the end of the drill string and the running tool is fastened to the casing hanger. It is then lowered down the riser through the BOP, and down into the well until the casing hanger is position.

3.1.5 Cement the Casing String

The process of cementing the casing strings into place after installing the BOP is a bit different than cementing the earlier casing strings. The mud and cement are split with a water-based liquid spacer. Further is the separating of the spacer and cement done with a plastic wiper plug that travels down the well between the spacer and the cement.

When the bottom plug reaches the float valve assembly near the bottom of the casing string, it breaks, allowing the cement behind to pass through. The top plug lands at top of the bottom plug when all cement have made it through. The mud is blocked and results in increased pressure. The cement fills the annular space around the bottom of the casing string and portion of the casing between the bottom and the float valves.

Pressure tests are done when the slurry has set to ensure that the cement has sealed the casing in place. The process continues by removing the running tool and install a smaller diameter drill bit on the end of the drill string, and lower it back down to the bottom of the well. This is done to drill through the float valves and the cement in the shoe track.

3.1.6 Production Casing

A production well is used to recover oil, while an exploration well is applied to learn about the geology of the area and evaluate if oil or gas are present. After drilling the final section of a production well, a production casing is installed on the open hole section.

3.2 Well Control

Throughout drilling operations rig personnel have to ensure that hydrocarbons do not relocate from the reservoir into the well (Bartlit et al., 2011). Well control is the procedure of monitoring the well and make sure that any hydrocarbon influxes are detected.

The Petroleum Safety Authority (PSA) has establish some regulations related to well barriers (PSA, 2007). During drilling and well activities at least two independent and tested barriers must be available in order to prevent an unintended flow from the well. The well barriers should be designed to ensure well integrity and barriers functions are taken care of during the well's lifetime. NORSOK D-010 (2004) defines a primary well barrier as the first object that prevents flow from a source and a secondary barrier as the second object that prevents flow from a source.

3.2.1 Primary Barriers

To maintain well control one has to establish and maintain barriers inside the well that controls the subsurface pressure and prevent hydrocarbon flow (Bartlit et al., 2011). Some barriers are part of the well design, while others are operational barriers that the drilling crew uses during the drilling process.

A key operational barrier is drilling mud. As long as the drilling mud inside the well exerts pressure on the formation that exceeds the pore pressure, hydrocarbons should not flow out of the formation and into the well. If the pore pressure exceeds mud pressure, the well is underbalanced, which means that the mud pressure is no longer enough on its own to prevent hydrocarbon flow.

Additional barriers can be inside the well to increase the redundancy of the barrier system. For instance, rig personnel can pump cement inside the final casing string of the well to establish cement plugs at different depths inside the well.

3.2.2 Secondary Barrier

A BOP stack is a potential barrier. By closing different individual rams in the BOP stack, rig personnel can close off the well, and prevent hydrocarbon flow up in the well and into the riser. When a BOP ram is closed, it becomes a barrier to flow. It takes from 40 seconds to a minute to close the ram, once activated. The BOP ram can be activated in several ways, manually from the rig, robotically by Remotely Operated Vehicles (ROVs) or automatically.

3.2.3 Indication of Kicks

Formation flow during drilling and well servicing operations is normally referred to as a kick (Grace, 2003). If a kick is not controlled, it may result in a blowout. Well control procedures are planned to safely prevent or handle kicks and reestablish primary well control. A kick is defined as flow of formation fluid and/or gas into the well bore and the effects are generally detected at the surface (API, 2006), (NN, 2009).

There are listed six indications that have to be followed while drilling; (1) drilling breaks, (2) increase in flow rate, (3) increase in pit volume, (4) variation in pump speed and pressure, (5) well flowing during connection, and (6) change of drilling fluid properties.

Drilling Breaks

Normally, the first indication of a well kick is a sudden drilling break or a sudden increase in drilling rate. This is interpreted that a porous formation may have been penetrated.

Increase in Flow Rate

If pumps are running at the same speed, the increase in flow rate out of the well is due to formation fluid entering the well bore downhole, or gas bubbles are expanding in the annulus as they are reaching surface.

Increase in Pit Volume

If active pit or trip tank volume increase without sensible cause from surface activities, the observed extra volume can be formation fluid flowing into the well bore.

Variation in Pump Speed and Pressure

Provided that formation fluid is allowed to flow into the well bore and reduce the hydrostatic pressure in the well, this reduction on bottom hole pressure can influence surface pump pressure.

Well flowing During Connection

In case the well flows during connection, chance are that primary well control is lost.

Change of Drilling Fluid Properties

The first sign of formation fluid entering the well bore might show up as a change in the drilling fluid properties.

Chapter 4

Hazard Analysis For Drilling Operations Based on STPA

The literature presented in the previous two chapters will be helpful to develop a model for a drilling operation based on STAMP and STPA particular.

Accidents in complex systems are often caused by unsafe interaction between components that have not failed. STPA includes both component failure accidents and component interaction accidents, which can potentially find more causes of hazards than the older methods, including causes involving software and human errors which normally not involve failures, but inadequate or unsafe control actions (Ishimatsu et al., 2010).

Since a drill operation is a large operation, the focus will be on the drilling phase. In this step the hole is drilled and reinforced from the sea floor down through the trap layers and into the reservoir zone. This is a significant step for the rest of the operation, and therefore important to do correctly to avoid accidents. Holand (2010) defines a blowout as an incident where fluid flows out of the well or between formation layers after all predefined technical well barriers or the activation of the same has failed. While well release is oil or gas flow from the well from some point where is not was intended and the flow is stopped with use of the barrier system. A well kick is defined as inflow of fluid from the reservoir. A well kick may generate a blowout if well control action is not taken. Blowout situations can occur in complex operations, such as deep, high pressure gas wells and simple shallow operation.

4.1 System Hazards and System-Level Safety Constraints

The first step in the analysis process is to identify accidents or unacceptable loss event, such as loss of life and then determining hazardous states in the system that would permit these accidents to occur.

The hazards for a drilling operation are blowouts and well release of hydrocarbons from the well that could lead to loss or damage to persons, platform or environment. The safety constraint can therefore be defined as preventing flow of hydrocarbons into the well from the reservoir. There are several methods to monitor if hydrocarbons are flowing into the well. In case there is some indication that this safety constraint is violated, the driller will stop the drilling process and shut down the well if necessary. Both the driller and mud logger is monitoring the whole process and the mud logger gives information to the driller if something is unusual. It can be summarized into:

Hazards: Blowouts and well release of hydrocarbons from the well.

Safety Constraints: Prevent flow of hydrocarbons into the well from the reservoir.

Figure 4.1 shows the hierarchical control structure to ensure safe operations of drilling operations in Norway. It starts with the Petroleum Safety Authority (PSA) which give regulations and guidelines to the petroleum industry down to the driller and mud logger involved in a specific drilling operation

The PSA is the regulator for technical and operational safety, which includes emergency preparedness and for the working environment in all phases of the petroleum activity, such as planning, design, construction, use and potential later removal (PSA, 2012). Their duties are to ensure that the petroleum activity and activities relating to it are supervised in an unified way. The PSA also provide information and advice to players in the industry, set up appropriate collaborative relationships with other Health, Safety, and Environment (HSE) regulators nationally and internationally, and impart actively to a transfer of knowledge from the HSE to society in general.

The Offshore Installation Manager (OIM) is responsible for the safety at the installation, personnel on board and all operations in the safety zone that may have implications for the facility security (NWEA, 2009). Through planning the OIM is responsible for that the operations are conducted safely, effectively and without interruptions. He has also the responsible

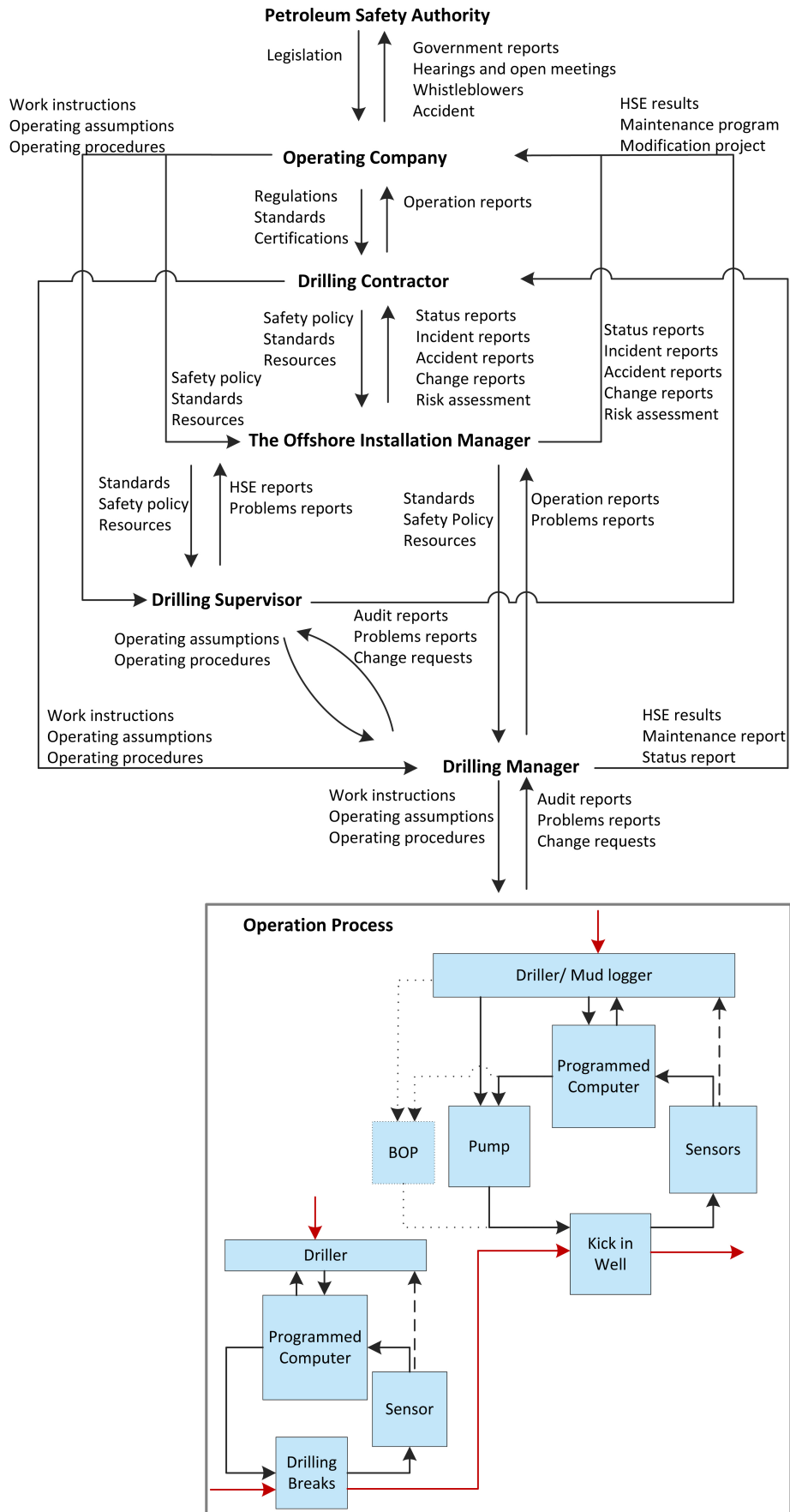


Figure 4.1: The Hierarchical Control Structure to Ensure the Safe Operation of Drilling

for having good overview of all operations performed at the platform.

The operation leader has to have good knowledge of and is responsible for that the operations are well planned and carried out according to the operating company's governing documents, objectives and strategies together with regulatory requirements. He is also responsible for that offshore personnel have the necessary training and knowledge within governing documents.

The drilling supervisor is hired by the operating company. He has a proactive information responsibility against the OIM and operations in connection with drilling at the platform (NN, 2005). It is expected that the drilling supervisor reports status and progress on HSE results, modification projects and maintenance program for the drilling area. Ambiguity and challenges in the daily operation, together with planned future activities should be cleared with the management onshore before presented to the platform management. It is important that the drilling supervisor has a focus on the HSE goals, quality and effectiveness. He shall at all times know how the project is doing in terms of the schedule.

The drilling supervisor must assure a good handover between day and night shift for the drilling supervisor and assistant drilling supervisor, together with drilling contractor personnel and supplier personnel. A written handover should amongst others include relevant data for the drilling operation and time schedule and goal for the coming shift regarding propulsion. The drilling supervisor is reporting according to internal guidelines and should put data into their daily drilling report. Both up- and downtime, activity codes and time ahead of or behind of schedule should be included.

Reports to the OIM are also the drilling supervisor responsibility. This applies to HSE, both personal injury and conditions during the operation that could be a risk for the platform, together with conditions concerning propulsion that could have consequences for the platforms remaining operations.

Both operation company and drilling contractor have their own internal requirements, standards and certifications that have to be followed during all operations at the platform. It is expected that they get informed regarding problem reports and operation report from the drilling manager and drilling supervisor. This is often based on information from the driller and mud logger. This includes incident reports, accidents and change reports. It is significant that changes in plans both for the operating company and drilling company are well

communicated to the drilling supervisor and drilling crew.

The lowest level in the control structure is the driller and mud logger who not only directly controls the drilling operation, but also has the responsibility to provide operation reports and problem reports to drilling manager. The driller controls the drilling operation and has responsibility to monitor some important parameters. While the mud logging engineer is responsible for maintenance together with correct operation of equipment supplied to provide service. He is also responsible for the collation and presentation of the information monitored in accordance with company standard procedures and customer requirements to ensure a high quality service. The mud logger is monitoring the process and gives information to the driller in case something is unusual. The driller often takes action based on the information he gets from the mud logger. In addition, it is nevertheless important that the driller and mud logger have good communication with the drilling manager and consults throughout the drilling operation. The drilling manager has in addition good communication with both the drilling supervisor and OIM throughout the operation.

This control structure for a drilling operation will be used to analyze the causal factors later in this assignment and will thereby provide some improvement measures.

4.2 Safety Control Structure

The next step is to develop a diagram of the safety control structure of the system. Each node in the graph represents a human or machine component in a socio-technical system. Connecting lines demonstrate control actions used to impose safety constraints on the system and feedback that supplies information to the controlling entity.

As illustrated in figure 4.2 a drilling operation is a complex and large operation with many different participants that take part in different phases of the process. The PSA is the highest level in the hierarchal structure and down to driller and mud logger who monitor the drilling process. The arrows in the figure try to illustrate the information flow between the different participants in a drilling operation. It is also exemplified what kind of information the various participants are expected and instructed to get from others.

It is important that the work plan is updated and according to actual work being done. Often,

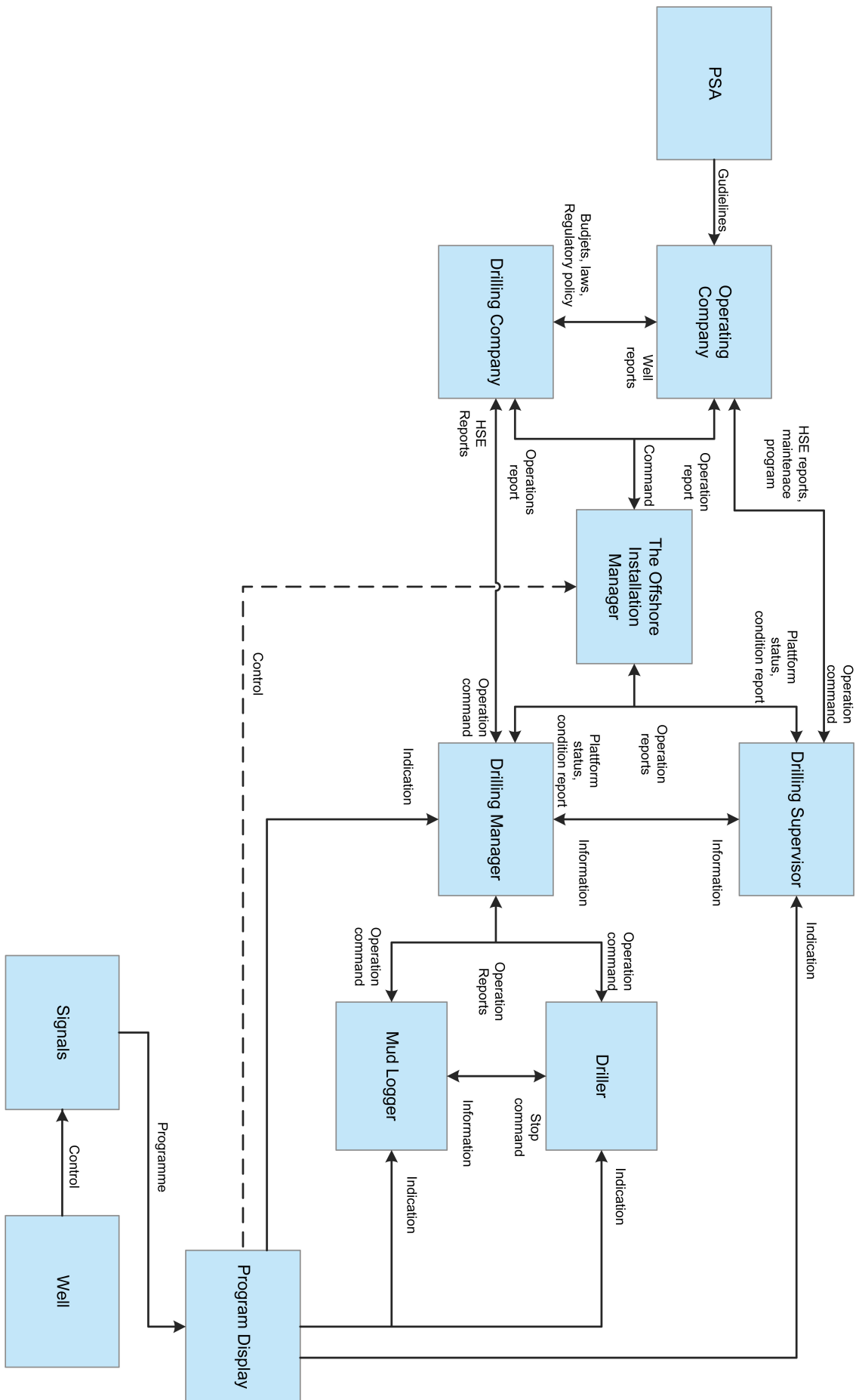


Figure 4.2: The Overall Control Structure for a Drilling Operation

Table 4.1: Safety Related Requirements and Constraints for Each Controller

Controller	Safety Constraints
PSA	Establish guidelines to ensure offshore operation safety.
Operating Company	Establish program for future operations Establish training requirements for all platform crew Verify the context of received control commands Support oversight and feedback loops to make sure that platform manager is doing his job adequately Provide oversight and feedback loops to ensure that each platform administration is doing their job adequately
Drilling Contractor	Establish program for future drilling operations Ensure that those in charge of the drilling operation are competent to carry out their responsibility Enact legislation, regulations and policies to ensure the safe performance of drilling Adjust the work plan according to the drilling condition, establish a file for the adjustment, and send the file to the drilling company and PSA Provide oversight and feedback loops to ensure that each drilling crew is doing their job adequately Establish routines for all drill crew in relation to a drilling operation Establish training requirements for all drilling crew
OIM	Monitor operations and enforce the legislations, regulations, and policy applying to a safe operation of local platform system Establish feedback channels for problems found by the driller or mud logger and the files and control commands issued by them
Drilling Supervisor	Adjust the work plan according to the well condition and information reports from the driller
Drilling Manager	Establish the temporary control command according to the well conditions and information reported by driller and mud logger at the platform Send the temporary control command to all driller and mud logger Adjust the work plan according to the well condition and information reports from the driller
Driller	Pay attention to identification of kick and operate the well according to this. Notice the drilling display and operate the well according to the inflow signals. Operate well according to work plan issued by the scheduler in drilling company. Confirm the actual work plan with the drilling manager or OIM.
Mud logger	Pay attention to the identification of kick during drilling operation Notice the drilling display during the entire drilling process

all decisions being made both before, during and after the drilling process are discussed with people onshore. This also includes work plans that have to be approved again if something unexpected occurs and changes are made compared to the original plans. The different participants have different safety requirements and safety constraint that they have to deal with during the entire operation.

Table 4.1 exemplifies the safety constraints and requirements to each controller. As seen for the table, there are many requirements that controllers have to consider throughout the drilling operation.

4.3 Potentially Inadequate Control Actions

The system control structure for a drilling operation have been outlined, the next step specifies how the controlled system can get into a hazardous state. A hazardous state is defined as a state that desecrates the safety constraints that are defined for the system. As mentioned in chapter 2, inadequate control is divided into four general categories;

1. A required control action to maintain safety is not provided.
2. An incorrect or unsafe control action is provided that induced a loss.
3. A potentially correct or adequate control action is provided too early, too late or out of sequence.
4. A correct control action is stopped to soon.

The accident to consider is blowouts and well release of hydrocarbons from the well, where the consequence of this is injury to persons, environment or platform. The system-level hazards relevant to this definition of an accident include blowouts and well release of hydrocarbons.

Table 4.2 presents the identified hazardous system behaviors for a drilling operation. The table contains the various hazardous types of behavior that needs to be considered. Incorrect but non-hazardous behavior is not included in the table, such as providing inflow of mud to close too soon is non-hazardous event that is not dangerous for blowouts and well release of hydrocarbons from the well.

As seen from table 4.2 there are many different scenarios that could occur. Based on the different identified hazardous system behaviors, a pattern can be drawn. Most of the errors that are listed in the table can then be found for many of the other control actions. It includes “inflow of mud does not stop when provided”, “change in one of the control actions is discovered too late” or “misinformation about one of the control actions”.

Another error that are considered is “sensor giving misinformation” or “feedback from the sensor is delayed”. This is considered for all control actions. In addition, “driller or mud logger not following the work plan for the drilling operation provided” may cause an error.

The last barrier to prevent a blowout or well release in the well is to activate the BOP. It may fail in many different ways, such as “does not close when provided” or “shutting down too

Table 4.2: Identified Hazardous System Behaviors

Control Action	Not Providing Causes Hazard	Provide Causes Hazard	Wrong Timing or Order Hazard	Causes Stopped Too Soon Applied Too Long
Inflow Stops	<ul style="list-style-type: none"> - The BOP does not close when it is provided - The driller and mud logger does not follow the work plan provided - Information about deviations is not given 	<ul style="list-style-type: none"> - Misinformation about kicks - Misinformation from the sensors 	<ul style="list-style-type: none"> - The BOP is shutting down too late - The feedback from the sensors is delayed 	<ul style="list-style-type: none"> - Not hazardous
Drilling Breaks	<ul style="list-style-type: none"> - The driller does not follow the work plan provided - Information about deviations in well is not given 	<ul style="list-style-type: none"> - Misinformation about status regarding drilling breaks - Misinformation from the sensor 	<ul style="list-style-type: none"> - Drilling breaks discovered too late - The feedback from the sensor is delayed 	<ul style="list-style-type: none"> - Not hazardous
Change in Flow Rate	<ul style="list-style-type: none"> - The inflow of mud does not stop when it is provided - Information about deviations in flow rate is not given -The driller and mud logger does not follow the work plan provided 	<ul style="list-style-type: none"> - Misinformation about change in flow rate - Misinformation from the sensor 	<ul style="list-style-type: none"> - Change in flow rate discovered too late -The feedback from the sensor is delayed 	<ul style="list-style-type: none"> - Not hazardous
Change in Pit Volume	<ul style="list-style-type: none"> - The inflow of mud does not stop when it is provided - Information about deviations in pit volume is not given - The mud logger does not follow the work plan provided 	<ul style="list-style-type: none"> - Misinformation about change in pit volume - Misinformation from the sensor 	<ul style="list-style-type: none"> - Change in pit volume discovered too late - The feedback from the sensor is delayed 	<ul style="list-style-type: none"> - Not hazardous
Variation in Pump Speed & Pressure	<ul style="list-style-type: none"> - The inflow of mud does not stop when it is provided - Information about deviations in pump speed & pressure is not given - The mud logger does not follow the work plan provided 	<ul style="list-style-type: none"> - Misinformation about variation in pump speed and pressure - Misinformation from the sensors 	<ul style="list-style-type: none"> - Variation in pump speed & pressure discovered too late - The feedback from the sensors is delayed 	<ul style="list-style-type: none"> - Not hazardous
Well Flowing During Connection	<ul style="list-style-type: none"> - The inflow of mud does not stop when it is provided - Information about deviations is not given - The driller does not follow the work plan provided 	<ul style="list-style-type: none"> - Misinformation about well flowing during connection - Misinformation from the sensors 	<ul style="list-style-type: none"> - Well flowing during connection discovered too late - The feedback from the sensors is delayed 	<ul style="list-style-type: none"> - Not hazardous
Change of Drilling Fluid Properties	<ul style="list-style-type: none"> - The inflow of mud does not stop when it is provided - Information about deviations in drilling fluid properties is not given - The mud logger does not follow the work plan provided 	<ul style="list-style-type: none"> - Misinformation about changes in drilling fluid properties - Misinformation from the sensor 	<ul style="list-style-type: none"> - Change in drilling fluid properties discovered too late - The feedback from the sensor is delayed 	<ul style="list-style-type: none"> - Not hazardous

late”.

In addition, there are still some other scenarios one must keep in mind. Although it is not dangerous to stop the inflow of mud too early it could develop into a hazard. It may for instance arise wear on equipment that is not detected before it is too late and one could have a blowout accident.

The identified hazardous behaviors in table 4.2 can be translated into safety constraints for the system component behavior. It is a bit difficult to develop good safety constraints for this operation. The reason for this is that the constraints are often connected to the design and modification phase. The focus for a drilling operation should therefore be to increase the reliability of the sensors and introduce redundancy. Based on this, four constraints that can be enforced by the driller or mud logger have been identified.

1. The “flow closes” command must be provided within x seconds after an indication of well kick is observed.
2. The command “BOP closes” command must be provided within x minutes, if the condition has not changed.
3. Two drilling persons must approve the plan before proceeding with a critical phase.
4. Implement a sensor system with one out of three (1oo3) or two out of four (2oo4) sensors to increase redundancy.

An important aspect of a drilling operation is well control. A well control plan is a program prepared in advance that will accomplish the objective of keeping a well under control during the well phases (API, 2006). To be successful, subsurface condition must be forecast, detected and controlled. One has to consider all conditions to be encountered, the equipment to be used, the procedures to be followed and training of the crew. Checklist items depend on the drilling depth, company policy, government regulations and the anticipated use of well control. All the six well kick indicator must therefore be evaluated in a well control program. The first step will therefore be to construct available data, then assess and predict what can happen and prepare contingency plans.

To get a good overview of the process, figure 4.3 illustrates an overall process model for the entire drilling process. As seen from the figure, the first indication of a well kick is drilling breaks. When the driller notices drilling breaks, some other well kick indicators has to be

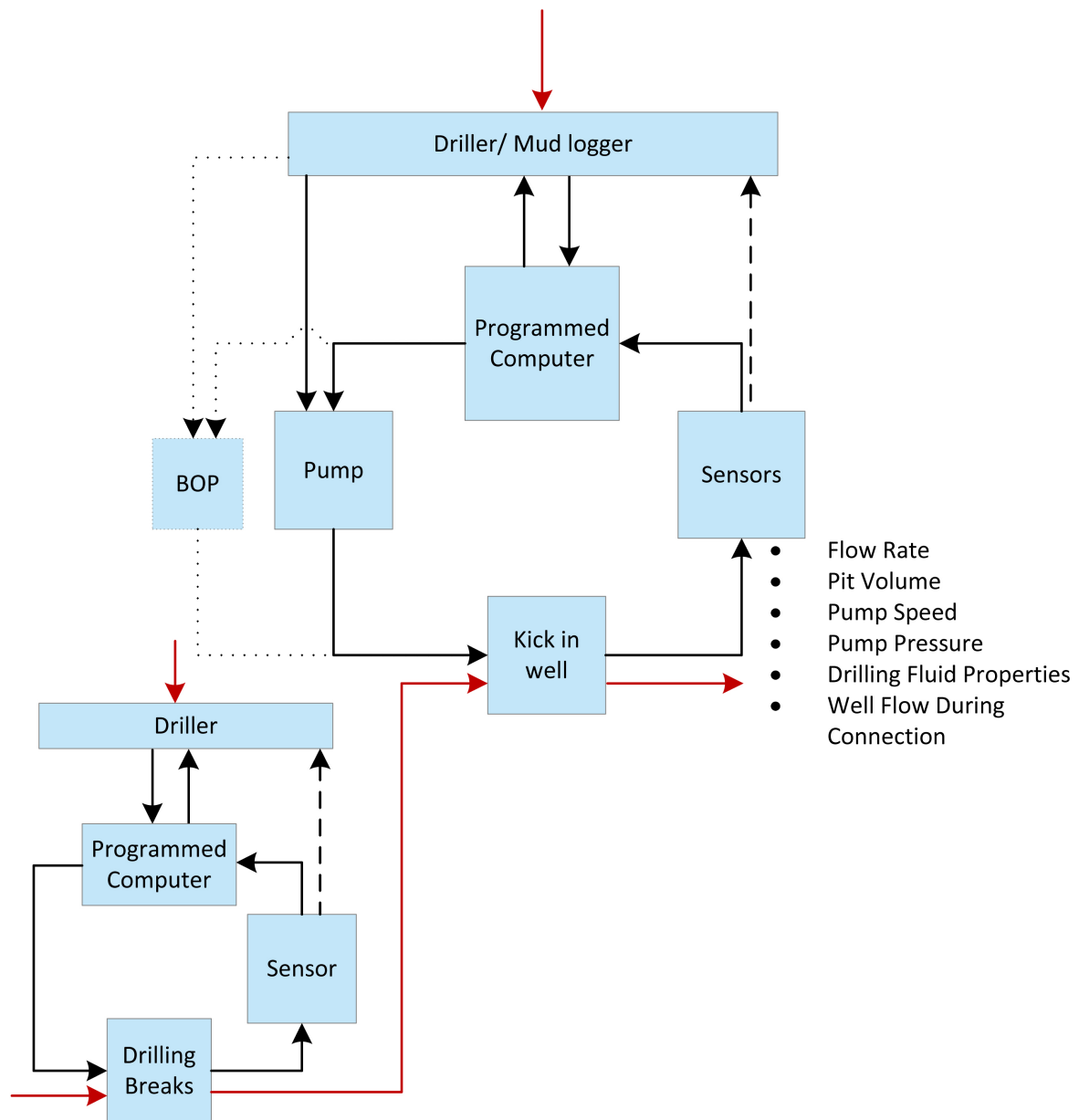


Figure 4.3: The Overall Process Model for the Drilling Operation

monitored closely for some time, such as flow rate, pit volume, pump speed and pressure, drilling fluid properties and well flowing during connection. The driller and mud logger monitor all these parameters, and if they notice something unusual the pump must be stopped. In case the situation is not stable after this action, the BOP is used to hopefully get control over the situation and avoid a blowout or well release of hydrocarbons from the well. The red lines indicate the external conditions that can influence the process, such as control input or external information together with process input and output.

4.4 Identifying Causal Scenarios

The first part of step two identifies the scenarios in a drilling operation leading to hazardous control actions that violate the component safety constraints. Based on the hazardous control action identified in step 1, the next step include identifying how it could occur. The information about how the hazard could happen is gathered and the control loop for each hazardous control action is inspected to specify if they could cause or impact it.

Figure 4.4 illustrates the overall control loop for a drilling operation, where all six well kick indicators are connected to each other. There are several sensors connected to a drilling operation and they monitor different parameters.. This includes information about penetration rate, flow rate, pit volume, pump speed and pressure together with specific weight. In case inflow of mud is stopped and well conditions do not change, the BOP is applied to get control over the situation. Even though one of the well kick indicators is observed and handled in the right way, an accident could happen because some other factors in the process model are failing or not noticed by the driller or mud logger.

Nevertheless, figure 4.4 is a simplification of a real drilling operation. As one got deeper into parameters dependency and procedures of the operation, one discovered that many of the well kick parameters were more connected to each other than were reflected in the beginning. Provided that one should have changed it, the model would have been more complex. Because of the time limit, the model was not changed, but one can still get a picture of the most essential inadequate control action.

Any time the Bottom Hole Pressure (BHP) drops below the formation pressure and one have the essential formation permeability to allow flow of the formation, it is a possibility of taking a kick (Schubert, 1995). Early detection of kicks is peremptory for safe and efficient handling of kick. Provided that a kick is not detected early, and shut in properly, loss of control of the well (blowout) may happen. For each of the kick warning parameters a specific control loop is exhaustive, and all inadequate control actions are identified and discussed.

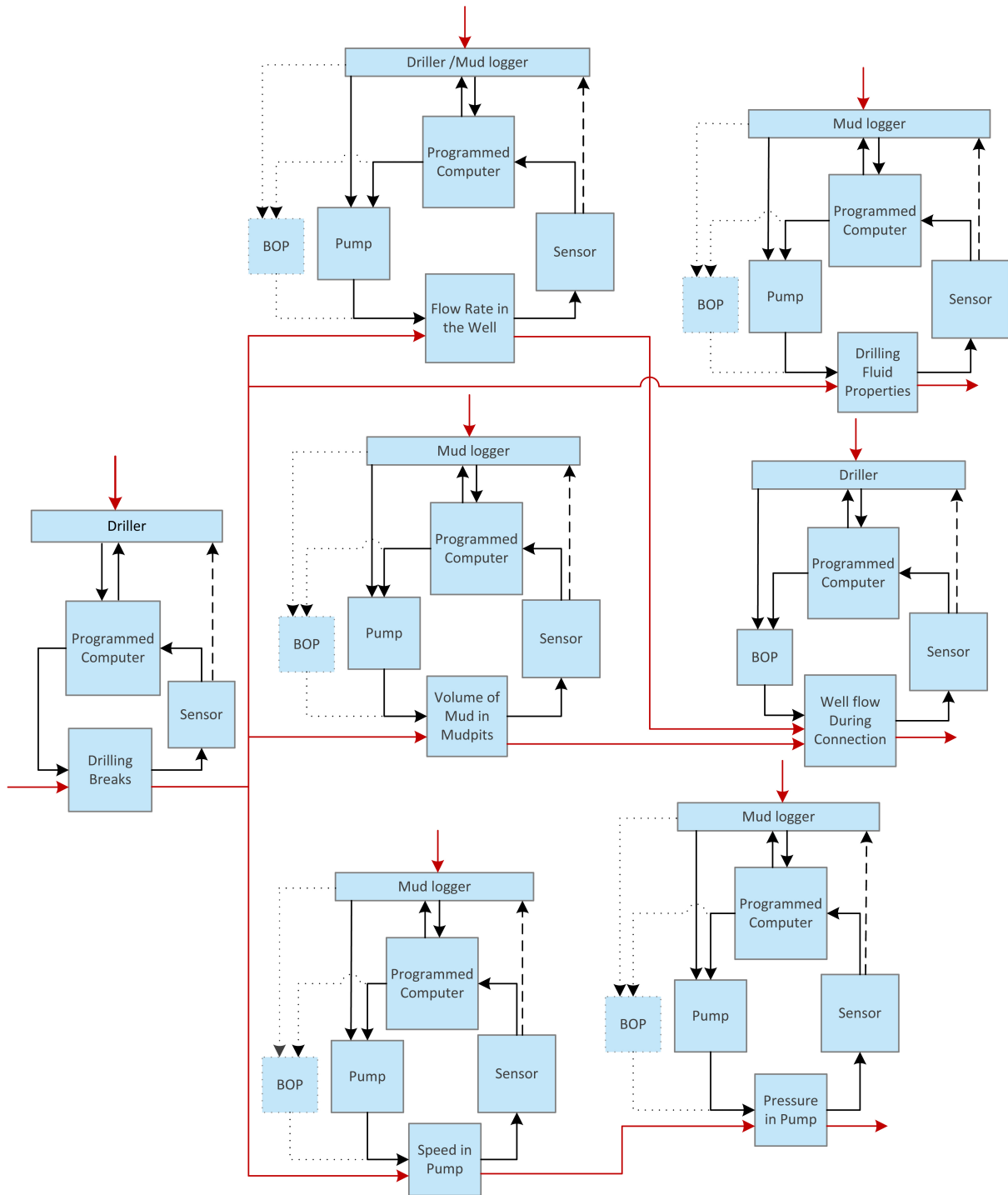


Figure 4.4: The Control Loop With All Well Kick Indicators for a Drilling Operation

4.4.1 Drilling Breaks

Drilling breaks or a sudden increase in drilling rate is the first indication that something may be incorrect in the well. This is illustrated in figure 4.5. The sensor can give inaccurate measurements of penetration rate. Furthermore, it may also give incorrect or no information about the penetration rate or discovering fluctuations in penetration rate too late or not at all. These are errors that have to be under control.

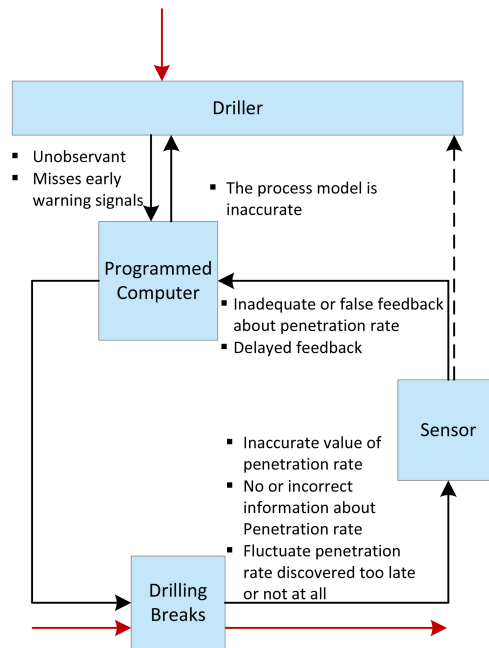


Figure 4.5: The Control Loop for the Drilling Breaks Indicator

The sensor send information about penetration rate to a programmed computer that is monitored by the driller throughout the process. The error connected to the sensor may be that the sensors are submitting incorrect or false feedback about the drilling breaks. In addition, the feedback may be delayed and misses the signal before it is too late and a well kick develops.

The driller has the responsibility to control this process and the drilling breaks indicator. During the operation he can be unobservant and thus miss early warnings signals that can indicate a well kick. The reason for inattentiveness may be that the driller has the responsibility for too many other assignments or is exhausted and tired during the operation. If the model produces many false positive the driller may overlook real drilling breaks and the early warning is lost. So it is important that the model does not have too frequent false positive. In addition, if there are too many false positive a culture of ignoring or overlooking indica-

tors may develop amongst the drilling operators. As a result of this, a well kick can develop without being noticed early.

The model used to monitor the drilling breaks indicator may be inaccurate. This cause either false positive as discussed above or false negative where real well kicks are not detected. Usually a drilling break indicates a change in lithology, such as drilling from a shale into a sand (Schubert, 1995). The detection method is to look for a step in drilling rate, that is how fast the drill is rotating. The step is a result of the lower resistance that comes when the driller shorten at the break. Assuming the power used to rotate the drill is constant, a change in rate will either come from break or tip of the drill reach different material (rock vs. sand vs. gas etc.). Rock bits normally drill faster in sand. The formation change does not automatically mean that the well is kicking, but one can drill a shale underbalanced without an influx of formation fluid into the well bore due to lower permeability of shales. Sand will have a high enough permeability to flow if the BHP is less than the formation pressure. It is possible to drill underbalanced in many shales without taking a kick, but as soon as the top of a permeable sand is cut, the well will start to flow.

A gradual increase in drilling rate while drilling a shale can indicate an increased formation pressure. If this is the case, it is important to pay particular attention to any drilling break. The magnitude of the step in drilling rate is one indication that it is drilling break or softer material. The step function will not be a perfect step, but have a gradient much higher than normal variation. The driller and/or the computer program will look for patterns (a step) with change in drilling rate higher than what can be expected at the location together with a gradient higher than what can be expected. Therefore, the limits for step and gradient must be set based on experience data and may be a function of depth. Failure to set these values will result in either false positive or false negative.

Too many stops of the drilling operation may lead to delays in the operation and the operating company can lose a lot of money. But if the driller misses the one time he should have noticed something incorrect, an early warning signal is missed out.

In case driller notices that something is incorrect, a command from the programmed computer will be sent to observe the remaining five parameters that may indicate a well kick for some time. As a result of this, drilling break is a sign of well kicks and is an input where other parameters have to be investigated afterwards to see if this is the case.

4.4.2 Increase in Flow Rate

Increasing flow rate is one of the indicators that have to be observed throughout a drilling operation. An illustration of how the different controls flows are connected to each other is shown in figure 4.6. There are a variety of errors that may occur in relation to measuring flow rate, such as inaccurate measurement of flow rate, incorrect or no information about flow rate or discovering fluctuate flow rate too late or not at all. These scenarios have to be under control in order to prevent blowouts and well releases.

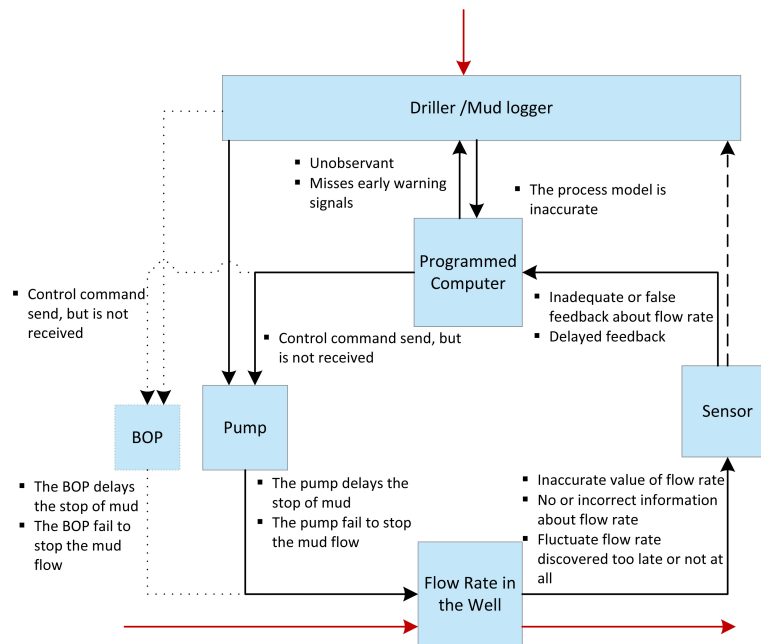


Figure 4.6: The Controll Loop for the Flow Rate Indicator

Information about the flow rate is sent from the sensor to a programmed computer observed by both the driller and mud logger all through the operation. The sensor may submit incorrect or false feedback about the flow rate or the feedback is delayed and the signals are missed until it is too late. All these events could imply that a kick is detected too late.

Both the driller and mud logger are required to monitor the flow rate indicator during the drilling process. The same consideration regarding tired or overworked operators that were discussed in chapter 4.4.1 applies here too.

The model utilized to observe the flow rate indicator may be inaccurate. The detection method is to look for increase in flow rate during the drilling operation. During the drilling the pump is running at a steady speed and a constant volume of fluid should go into the hole with an equal and constant volume of fluid coming out (Schubert, 1995). Provided that mud

returns increase without an increase in pump speed, it could be due to formation fluid dislodging mud from the annulus as it flow from the formation into the well bore, or gas bubbles that expand in annulus when it attain the surface. The model has it basis in a defined maximum flow rate. One also has to consider for how long time the flow rate can be above this value before the drilling has to be stopped. A decrease in the flow rate indicate for instance a pump error and is not a indication of well kicks. The flow rate will have small variation and the maximum flow rate might be a function of other drilling parameters like mud specific weight. The driller and mud logger together with the computer program will therefore look for patterns where the flow rate is above a threshold for a given time. These parameters (threshold and time) must be configured based on experience and local variation and may vary during the drilling operation.

The inflow of mud will be stopped in case the driller or mud logger discovers that something is incorrect. A command is then sent to the pump that stops the inflow of mud into the well. On the other hand, may the stop command be sent but not received by the pump. This case leads to the inflow into the well not being stopped.

As mentioned, the pumps main task is to stop the inflow of mud when a kick is observed. The pump may fail by delaying the stop of inflow or does not stop the inflow of mud. The first thing to do when an indication of increasing flow rate is observed is to stop the inflow of mud. In case the condition remains unchanged, the BOP is used to stop the inflow to the well and hopefully prevent a blowout. The errors connected to the BOP is therefore that the control command is sent, but it is not received. In addition, the BOP may fail by either delaying or not at all stopping the inflow of mud.

4.4.3 Increase in Pit Volume

Increase in pit volume is another indicator that has to be monitored all through the drilling operation. The relationships between the various parameters are illustrated in figure 4.7. There are some errors connected to measurement for pit volume, such as inaccurate measure of pit volume or incorrect or no information about pit volume together with change in pit volume is noticed too late or not at all.

The sensors task is to transmit information about the pit volume to a programmed computer,

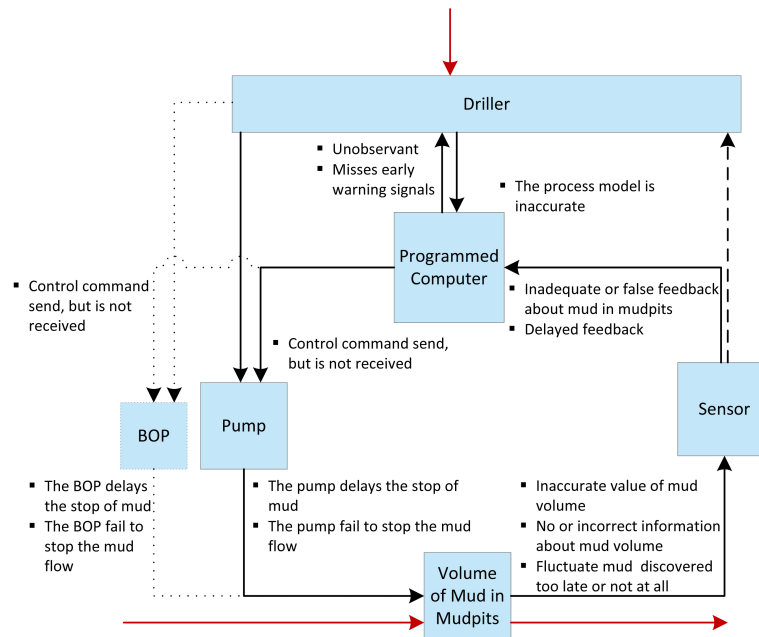


Figure 4.7: The Control Loop for the Pit Volume Indicator

which is monitored by the driller throughout the process. However, the sensor may send incorrect or false feedback regarding the pit volume. Another error connected to the sensor is delayed feedback and the signals are not notice until it is too late to prevent a blowout.

It is the drillers responsibility to observe the pit volume indicator throughout the drilling process. The same consideration regarding exhausted or overworked operators that were discussed in chapter 4.4.1 is relevant here too.

The model used to monitor the pit volume indicator may be inaccurate. Unexplained variation in pit volume has to be detected. Increase in pit volume may be a formation fluid entering into the well bore and it causes more drilling fluid to the annulus than is pumped down the drill string, consequently the volume of fluid in the pit increases (Schubert, 1995). An increase in pit volume could also indicate addition of water, barite or some other material, or moving mud from one pit to another. The driller should therefore be informed of any such operation that could lead to increase in pit volume. On the other hand, the driller should never assume that a increase in pit volume is not from a kicking formation.

A defined pit volume value is the basis in this model. In addition, there have to be defined some variation limits for pit volume before the drilling stops. A decrease in the pit volume indicates outflow of mud in the reservoir. This may lead to that the mud column decreases and the pump pressure is thereby reduced. The pit volume will have small variation and the

maximum pit volume might be a function of other drilling parameters such as pump pressure. It is the driller and/or computer program task to look for patterns where the pit volume is over the threshold for a given time. Both these parameters have to be configured based on experience data together with local variation and it may vary during the operation.

Provided that the driller notices something extraordinary a command is emitted to the pump to break off the inflow of mud into the well. Consequently, the stop command may be emitted, but not received by the pump. This may lead to that the inflow of mud is not being stopped when needed.

The pumps assignment is to stop the inflow of mud. However, errors may still occur, such as postponement of inflow or not stops the inflow of mud. When an indication of increase pit volume is notice, the inflow has to be stopped. Provided that nothing changes, the BOP is used to stop the inflow into the well and successfully avoid a blowout. The same consideration regarding BOP errors that were discussed in chapter 4.4.2 applies here too.

4.4.4 Variation in Pump Speed & Pressure

Variation in pump speed and pressure is an important indicator that has to be supervised throughout a drilling operation. Figure 4.8 show how the various parameters are connected to each other. The pump speed is an input into the pressure pump indicator, together with the other parameters. In connection with measuring of pump speed and pressure there are some errors that may happen, such as inaccurate measure of both pump speed and pump pressure, incorrect or no information about the pump speed or pump pressure together with change in pump speed or pump pressure is notice too late or not at all. These scenarios have to be under control to prevent blowouts or well releases.

As figure 4.8 illustrate the sensors transfer information about the pump speed and pressure to a programmed computer monitor by the mud logger throughout the process. Nevertheless, the sensor can send incorrect or false feedback considering pump speed and pressure. A different error is delayed feedback and the kick signs are not discover until it is too late to avoid a well kick.

The mud logger has the responsibility to monitor the pump speed and pressure indicator during the whole drilling process. The same consideration regarding tired or overworked

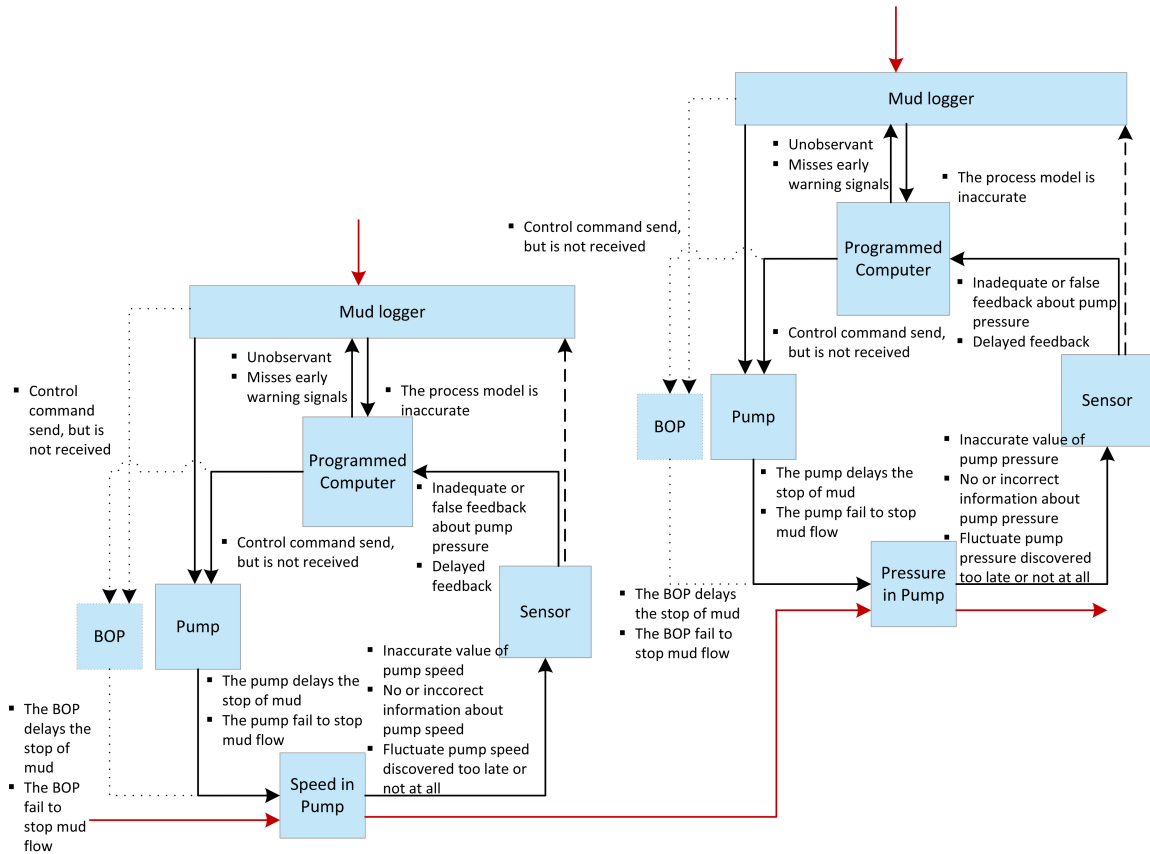


Figure 4.8: The Control Loop for the Pump Speed & Pressure Indicator

operators that were deliberated in chapter 4.4.1 is applied here too.

The model used to monitor the pump speed and pressure indicators can be inaccurate. Variation in pump speed and pressure have to be detected. A decrease in pump pressure or increase in pump speed occur as a result of decrease in hydrostatic pressure of the annulus as the formation fluid flows into the well bore (Schubert, 1995). This reduction on the BHP can effect the pump pressure. As lighter formation fluid flows into the well bore, the hydrostatic pressure exerted by the annular column of fluid decreases, and the drilling fluid in the drill pipe tends to U-tube in the annulus. When this happen, the pump pressure will fall, and the pump speed will increase. Lower pump pressure and increased pump speed symptoms can also indicate a hole in the drill string, often referred to as a washout. Until a verification can be made whether a washout or a well kick has happen, a kick should be assumed.

The model has it's foundation in defined minimum values for pump pressure and maximum value for pump speed. There has to be done some consideration for how long time the pump speed or pressure can be above or below the given value before the drilling has to be stopped. The mud logger and computer program will look for specific patterns where the pump speed

and pressure is above or below a threshold for a given time. Both parameters has to be configured based on experience data and local variation that may vary during the process.

In case the mud logger discovers something unusual a command is transmitted to the pump to stop inflow of mud into the well. On the other hand, the command to stop the inflow may be sent, but not received by the pump. This may lead to that inflow of mud is not stopped and it can develop into a well kick.

The pumps main task is to stop inflow of mud. Nevertheless, errors can still occur, such as delayed stop of the inflow of mud or does not stop the inflow of mud into the well. When a indication of variation in pump speed or pressure is observed, the drilling has to stop. In case the condition stays unchanged, the BOP is used to stop the inflow to the well and hopefully prevent a blowout. The same consideration regarding BOP errors that were discussed in chapter 4.4.2 applies here too.

4.4.5 Well Flowing During Connection

Well flowing during connection is an indicator that has to be supervised all through a well connection. The relationships between the various parameters are illustrated in figure 4.9. One can both monitor the flow rate or pit volume to consider indication of well kicks. It is therefore important to have a good overview of both parameters during the connection. There are some errors connected to measuring well flowing during connection, such as inaccurate measure of flow rate and pit volume, incorrect or no information about flow rate and pit volume together with notice change in flow rate and pit volume too late or not detected at all.

Information about the flow rate and pit volume is sent from the sensors to a programmed computer monitor by the driller throughout a well connection. The sensors may submitting incorrect or false feedback considering the pit volume or flow rate or the feedbacks is delayed and signals are missed until it is too late to prevent a kick. All these events could initiate an accident in connection to well kicks.

The driller has the obligation to monitor both the flow rate and pit volume indicator during a well connection. The same consideration concerning exhausted or overworked operators that were discussed in chapter 4.4.1 is relevant here too.

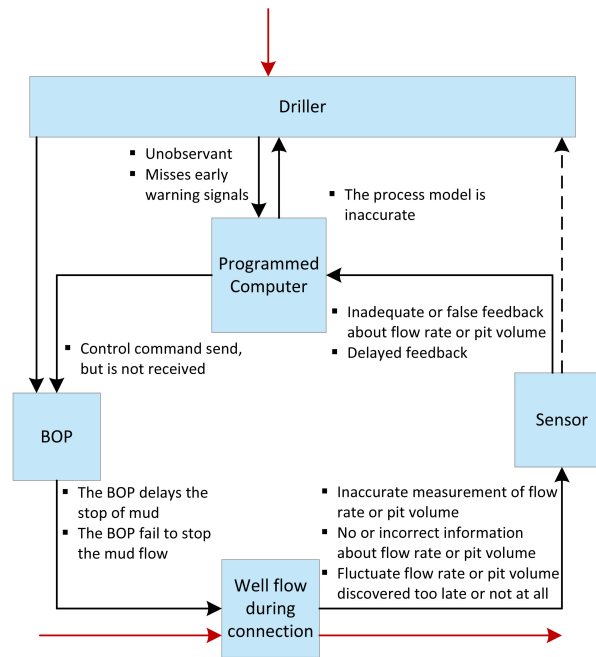


Figure 4.9: The Control Loop for the Well Flowing During Connection Indicator

The model used to observe the well flowing during connection may be inaccurate. Well flowing during connection is a result of that the primary well control is lost. If one discovers returns over the bell nipple, it is often due to well flowing (Schubert, 1995). It is important that one does not assume that the well is U-tubing due to unbalanced mud, or the formation is “giving mud back”. In case the mud is U-tubing, or the well is giving mud back that was lost to the formation, the flow should reduce. Provided that one experience a kick, the flow will not slow down, it will either remain constant or increase. The detection method is to look for constant or increase in flow rate or decrease in pit volume. The model has it basis in a defined flow rate and pit volume during the connection. One also has to regard for how long time these parameter are above or below the given values before the BOP is used. Both the pit volume and flow rate will have small variation and minimum and maximum values might be a function of other drilling parameters. The driller together with the computer program will therefore look for pattern where either the pit volume or flow rate is above, below or constant at a threshold for a given time. These parameters has to be configured based in experience data and local variations.

When an indication of increased or constant flow rate, or decreased pit volume is observed, the BOP is used to shut down the well and hopefully prevent a blowout. The same consideration regarding BOP errors that were discussed in chapter 4.4.2 applies here too.

4.4.6 Change of Drilling Fluid Properties

Change of drilling fluid properties is an important indicator that has to be monitored throughout a drilling operation. Figure 4.10 illustrates how the different parameters are connected to each other. There are many various drilling fluid properties that can be monitored, but specific weight is one of the most important ones. In connection with measuring specific weight there are some errors, such as inaccurate measure of specific weight or incorrect or no information about specific weight together with change in specific weight is discovered too late or not detected. All these errors have to be under control in order to prevent blowouts.

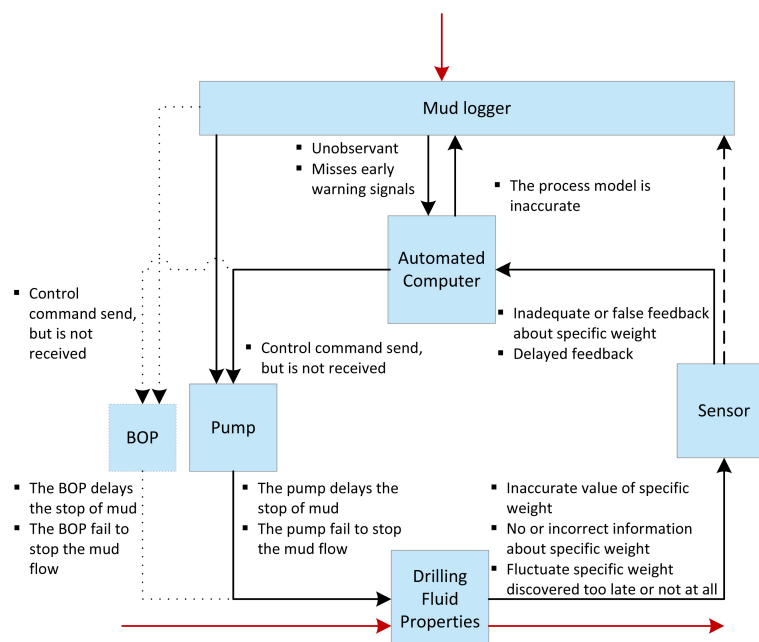


Figure 4.10: The Control Loop for the Drilling Fluid Properties Indicator

As figure 4.10 illustrates the sensor transmit information about specific weight to a programmed computer supervised by the mud logger all through the drilling operation. Nevertheless, the sensor may send incorrect or false feedback regarding the specific weight. Another error is delayed feedback and the change in specific weight is not discovered until it is too late or not detected at all.

It is the mud loggers commitment to observe the specific weight indicator throughout the drilling process. The same consideration concerning exhausted or overworked operators that were discussed in chapter 4.4.1 is applied here too.

The model used to supervise the drilling fluid properties may be inaccurate. Change in drilling fluid properties may be the first sign of formation fluid entering the well bore. The

detection method is to look for change in specific weight in mud and especially decrease. The model has the foundation in a defined specific weight during drilling. There has to be done some evaluation for how long time this parameter can be above or below the given value before the drilling stops. The specific weight might have some variation during the operation and minimum and maximum values might be a function of other drilling parameters. The mud logger with help from the computer program will look for patterns where the specific weight is either above or below a threshold for a given time. Usually, these parameters have to be configured based on experience data and local variations.

In case the mud logger discovers some unusual pattern at the computer a command is transmitted to the pump to stop the inflow of mud into the well. On the other hand, the command to stop the inflow may be sent, but not received by the pump. This can lead to that a well kick is developed before the drilling is stopped.

The pumps assignment is to stop the inflow of mud. Nevertheless, errors may still occur, such as postponement of inflow or the pump does not stop when provided. When an indication of increase specific weight is discovered, the drilling will be stopped. Provided that nothing changes, the BOP is used to stop the inflow into the well and successfully prevent a blowout. The same consideration regarding BOP errors that were discussed in chapter 4.4.2 applies here too.

4.4.7 Summary of Causal Scenarios

Throughout an entire drilling operation the rig personnel has to ensure that hydrocarbons do not start flowing from the reservoir into the well. Well control is therefore an important procedure of monitoring the well and making sure that any hydrocarbon influxes are detected (Bartlit et al., 2011).

The developed control loops can be used to enhance well control by proper planning and execution and consequently avoid a kick. In addition, the model emphasize what inadequate control actions need to be under control and be attentive with to prevent a well kick. The identified inadequate control actions, in connection to a drilling operation, are often similar whereas the only different is the parameter one consider. It may therefore be easier to find constraint that reduce similar inadequate control actions. These control loops can also be

used to try to decrease potentially inadequate control actions and hopefully prevent more well kick.

In this study has it been much focus on the process model that are used to monitor the different well kick indicator. If they are inaccurate, it does not matter how good the driller and mud logger are to interpret signal provided that the models are incorrect.

A large number of personnel and disciplines are involved in a drilling operation. It is important that all involved parties understand the objectives, procedures and hazards. The driller and mud logger have different work assignments and area of responsibility during a drilling operation. Since they have different indicator to monitor during the operation, it is important that it is a good communication flow between them. The mud logger only monitor some of the indicators, but it is drillers responsibility to shut down the well if there is indication of a well kick.

4.5 The Degradation of Controls over Time

The final part of step two consider how the designed control could degrade over time and how to build in protection against it (Leveson, 2011). It is important to consider the interactions between development and operations. At the end of the development process, the safety constraints, the results of the hazard analyses together with documentation of safety related design features, should be handed over to those with responsibility for maintenance and modifications of the system. This information establishes the basis for safe operations. However, operational feedback on trends, incidents, and accident should activate reanalysis when needed.

The design of the operational safety controls are based on assumptions regarding the condition during a drilling operation. It is difficult to make assumptions regarding how the drilling crew will operate the system and the environment (both social and physical) in which the system will function. All these conditions may change. Consequently, not only must the assumptions and design basis be communicated to those who operates the system, but there needs to be protection against change over time or ways to discover changes that invalidate those assumptions. For instance may the equipment be degraded or not maintained properly or human behavior and priorities often changes over time.

The control loops presented in chapter 4.4 can be used to identify and handle flaws in the original hazard analysis and system design together with detection of unsafe changes in the system during operations before the changes results in losses.

A drilling operation is a very large and complex operation there may therefore be some challenges attached to this, such as interpretation of information. There is much uncertainty connected to the various parameters that is monitored during the operation. This can for instance be weak signal or misinterpretation of the signals. Accidents have happened because of interpretations of signal and this is something that everyone has to have in their mind while monitoring a drilling operation.

Since a drilling process is a operation and not a technical system, it may be problematic to improve the process through the design phase. It is difficulties to redesign a the system since there may be many different unanticipated conditions that were not consider during the design phase. Based on the control loops presented in this assignment, the most advantageous best choice is to to reduce the probability for blowout and well releases may be to increase the reliability to the sensors and pump. This can be done by introducing redundancy, for instance a one out of three (1oo3) or two out of four (2oo4) system.

An improved practice to handle the complexity of the operation and tired operators may be to introduce a debriefing after every drilling operation. This may help to detected errors before they can initiate into hazardous states. By getting several people to review the operation, it is more likely that they discover if something is unusual.

The overall goal for companies should be to change the culture from a *fixing orientation*-identifying and removing deviations or symptoms of deeper problems - to a *learning orientation* where systemic causes are included in the search for the source of the safety problems (Leveson, 2011).

4.5.1 Feedback Channels

Feedback is a fundamental part of STAMP and of treating safety as a control problem. Information flow is a basis in maintaining safety. Poorly defined feedback can lead to a reduction in safety. For example an incentive to reduce the number of accidents with rewards to they who have the lowest reported incidents, can have the opposite effect. Such rewards can cre-

ate an incentive to evade information about small accident and near misses and is therefore not investigate and remove the causes. Under-reporting of incidents can create an illusion that the operation has become safer, when, instead, the risk has increased. This may lead to not taking necessary control actions to reduce risk. As an alternative, reporting of accidents should therefore be rewarded.

The hazard and safety constraints, together with the causal information from STPA, forms the founding for deciding what feedback is necessary to supply the controllers with information they need to satisfy their safety responsibilities. Besides, there must be mechanisms to assure that the feedback channels are functioning effectively.

A drilling operation is a very special operation, whereas driller and mud logger together with other drill crew cannot see the actual process down in the well. The information about the condition down in the well is transmitted through a control display and the driller and mud logger have to trust the information the sensor have sent to the programmed computer. The feedback channels are consequently important for the process and have to be updated at all times to avoid and prevent blowouts and well releases.

4.5.2 Process Model

Based on the inadequate control actions presented in chapter 4.4, the process model may be introduced for some improvements. An important aspect is to avoid the uncertainty related to if a well kick is about to happen or not. A warning system may be introduced to forecast the driller and mud logger if some of the well kick indicators are outside the specific limits for a given time. In addition, the model should be general and specific parameter for the platform or surrounding environment should be added at the platform.

4.5.3 Education and Training

It is important that everyone in the safety control structure, not just the driller and mud logger at the lowest level understands their roles and responsibilities with respect to safety and why the system, including the organizational aspects of the safety control structure, was designed the way it was.

Both managers and operators need to understand the risk they are taking in the decisions they make in connection with a drilling operation. Often are bad decisions made because the decision makers have an incorrect assessment of the risk being presumed, which has consequences for training. It is significant that the driller and mud logger knows exactly what signals to look for, not just be told to look for “weak signals”. Everyone involved in controlling a possible dangerous process at the platform needs to have safety training, not just the controllers and operators. It is important that the training include not only information about the hazards and safety constraints implemented in the control structure, but also about priorities and decisions about safety are to be made.

Training should not be a one-time event for employees, but should be frequent during their employment, if only as a reminder of their trustworthiness and the system hazards. The focus for the training should be on knowledge of recent events and trends.

Chapter 5

Evaluation of the Model

This chapter evaluates the model presented in the previous chapter and adds decision support, limitations and work load together with quantification to the model. In addition, there is a comparison to traditional hazard analysis techniques and a systematic method.

5.1 Decision Support

The STAMP model provides help in understanding accidents. The goal with this new approach was to change the focus from “preventing failures” to “impose behavioral safety constraints,” (Leveson, 2011). The method is built on an expanded model of accident causation that incorporate more than the traditional models, attach those factors that more and more are causing accidents today. It permits us to deal with much more complex systems.

STPA analyzes hazards and causal factors in a systematic way. It consider not only component themselves, whereas the interactions between components or among operators and components (Leveson, 2004). The use of safety control and a general control flaws classification to analyze causal factors of each identified hazard may contribute to find more failure modes and causal factors.

An accident model should support a comprehensive view of accident mechanisms that expands the investigation beyond the proximate events. A limited focus on operator actions, physical component failures, and the technology can lead to disregarding some of the most significant factors in terms of preventing future accidents. STAMP and STPA is therefore well

suited, where the entire socio-technical system is included.

In addition, components in the control structure can be complex such that it may have its own logic or algorithm model, or even its own control structure. Even if they occur in another control structure, may it be further developed by following the same process.

Automated assistance may be provided in form of procedural checklists and guides for the drilling operation, especially non routine operations such as startup, shutdown, and various types of emergency operation as blowouts and well releases. The procedures are not totally automatic since the driller and mud logger monitor the well kick parameters at a control panel. An important aspect is therefore that they cannot only rely on the computer guidance. This may reduce operator vigilance and it is significant that both the driller and mud logger understands the process.

When designing the process model used to monitor the well kick parameters it is essential to distinguish between providing help and taking control. By simplifying the driller and mud logger work can increase the risk of human errors. Automated guidance might best be provided only when requested, and one should in the design phase try to keep human for becoming overly dependent. Operators need to feel that they are in charge of the operation (Leveson, 1995).

It is difficult to give the driller and mud logger practice in decision making. Without this practice, human often lack credence or skills to intervene when the automation fails or error are detected.

5.2 Limitations with STAMP & STPA

Although STAMP and STPA have many advantages, they still have some subjective aspects. For various people, safety control structure might be different since their comprehension of the system might be different. In addition, the identification of hazards and causal factors might be dissimilar. The more one appreciate the system, the more hazards and causal factors one may find and the more accurate and useful they could be.

There are always a numerous of goals and constraints for any system. The challenge in engineering design and risk management is to determine and analyze the conflicts, to make

suitable trade-offs between the conflicting requirements and constraints, and to discover ways to increase system safety without reducing system reliability.

As of today, the method is more suitable for technical systems than operations. It is difficult to come up with new constraints to improve an operation because there are many different participants involved and that needs to be considered throughout the operation. Technical systems can be redesigned to improve the reliability of the equipment. The method therefore has to be improved before it is well suited for operations.

A improvement could be to create a tool to help the analyst create control structures and automate hazards and causal factors results. Development of such a tool might be beneficial for people working with safety-critical systems.

In addition, an improvement of the general classification for identifying potentially inadequate control action together with the classification of control flaws for identifying causal factors can be created.

5.3 Workload in STAMP & STPA

The STAMP and STPA methods have an exhaustive explanation and definition of what shall be included in all steps, together with examples of actual scenarios. Nevertheless, it is important that the method follows the defined steps to get full value of the hazard analysis. The analysis may take some time, and one must know both the system and the whole organization to utilize this method. The organization has to be known to be able to make a realistic hierarchical control structure and control structure where all safety constrains to all controllers are identified. In addition, the identified inadequate control actions have to be inspected based on control loops of the system. If one is unfamiliar with the actual system, some inadequate control actions may be missed out.

This method helps the whole organization to get a good overview of the process together with better knowledge of the actual process. It may find errors that are not included or found in other hazard analysis. In addition, this method have a different approach that may give the analyst another way to consider the operation.

5.4 Quantification in STAMP & STPA

Safety analysis ranges from quite simple qualitative methods to advanced quantitative methods in which numerical values for risk are derived. Although quantitative methods are used, they must be preceded by qualitative analyses where hazards and their causal factors are identified before numerical values can be allocated to them (Leveson, 1995). Consequently, the quality of the quantitative analysis relies on how good the qualitative one was.

A good foundation for quantification of human errors, together with organizational factors, is to use the Human Error Assessment and Reduction Technique (HEART) to set generic task types with their associated nominal error probability (Reason, 1997). The basis is therefore to match the activities discussed in chapter 4.4 to the generic tasks listed in HEART.

For instance the inadequate control action “unobservant driller or mud logger” can be linked to the generic task “fairly simple task performed rapidly or given scant attention” with a nominal error probability at 0.09. The next step is to consult the list of error-producing conditions (EPCs) and determine which condition(s) are likely to affect the performance of the activity. Then the nominal error probability is multiplied by a suitable judged proportion of the relevant EPC factors.

Based on the numbers given by the HEART method, an event tree analysis can be used to model and analyze different accident scenarios for a drilling operation. It is consequently important to identify all possible accident event sequences resulting in accidents and take an appropriate measure to estimate the accident probability. The “accident occurrence” conditions have to be found and its correctness has a large effect on the validity of analysis results. The STAMP- based analysis is useful to get an objective judgment of accident occurrence conditions related to drilling operations.

The different control loops presented in chapter 4.4 are be the basis for developing event trees. It is difficult to generate a model based on all control loops, but a possible starting point is to make separate event trees for the different well kick indicators.

The control loop in figure 4.6 is the foundation for the drilling operation where the driller has to change the flow rate to prevent a potential well kick. The relationship for the flow rate indicator can be described by the event tree inn figure 5.1. The first branch on the event tree represent whether the sensor sends a signal or not. If the sensor does not send a signal, it

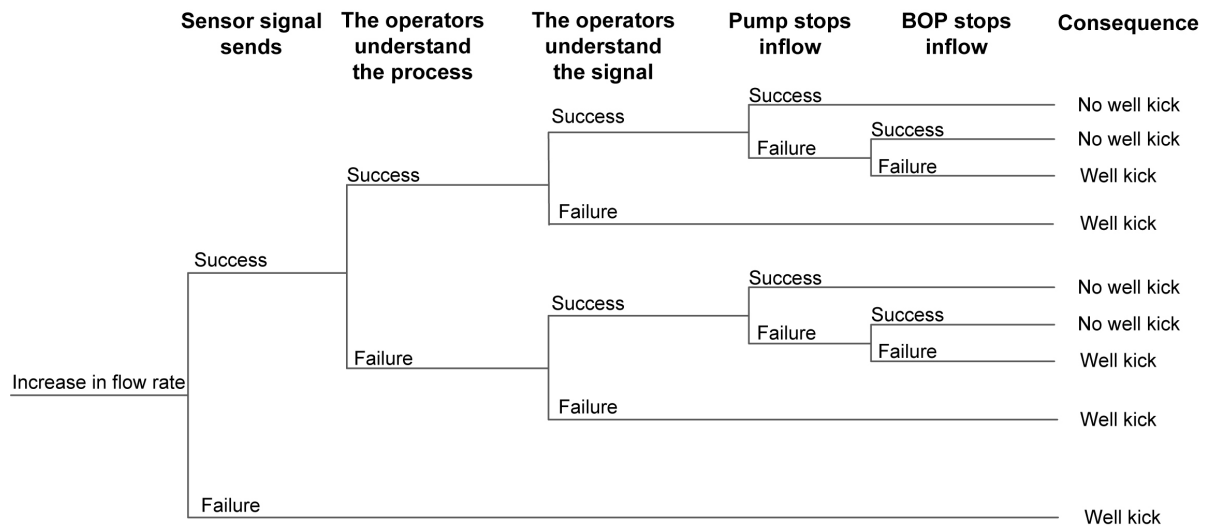


Figure 5.1: The Event Sequence for the Well Kick Indicator “Flow Rate”

does not matter if the driller and mud logger understand the process, since there is no signal to analyze. This is directly influenced by understanding of the process and one may have a well kick. Whether the driller and mud logger actually understands the process when a sensor signal is sent, is directly influenced by their ability to detect the change in flow rate before it is too late. The next branch is defined as the pump stops the inflow of mud. If this control action does not change the condition, the BOP is the last resort to prevent a well kick. There are a total of five factors modeled in the event tree in connection with the well kick indicator “flow rate”.

All results for quantitative risk analysis (QRA) are uncertain to some degree (Rausand, 2011). In some cases, the uncertainty may be large and the conclusion may therefore be questionable. The uncertainty related to quantification of STAMP and STPA may be related to inadequate models and data to misinterpretation of inadequate control actions and failure to identify all inadequate control actions.

Nevertheless, the models presented in chapter 4.4 requires a lot a data. Systems theory is a new way of regarding accidents where accidents are considered as arising from the interactions between system components (Leveson, 2011). In addition, single causal variables or factors are usually not specified. The focus in STAMP is constraints and inadequate control actions. As of today there has not been done much work in quantifying data required for such analysis. It can therefore be difficult to obtain relevant data for the actual process and give a good quantification for the specific hazards.

5.5 STAMP & STPA Compared to Other Methods

Most hazard analysis and other safety engineering techniques deal with systems and their environment as a static design (Leveson et al., 2004). Nevertheless, systems are never static, they are constantly changing and adapting to attain their ends and to change within themselves, in their goals, and in their environment.

There are currently four analysis techniques often used worldwide: Fault Tree Analysis (FTA), Event Tree Analysis (ETA), FMEA and HAZOP. STPA was developed to include the new causal factors identified in STAMP that was not treated by the older techniques.

Together with STPA, FRAM is a comparative new method that has a new way of thinking. The philosophical problem in searching for causes to accidents is that “nothing comes from nothing” (Hollnagel and Goteman, 2004). This means that even an initiating event or “root cause” requires an explanation.

5.5.1 Event Chain Models

Event-based accident models describe accidents in terms of multiple events sequenced as chains over time. The event considered almost always incorporate some type of component failure, human error, or energy-related event (Leveson, 2004).

Event-based models support limited understanding of causality and linear causality relationships are emphasized, but it is difficult to incorporate non-linear relationship which include feedback. Moreover, some important causal factors are problematic to fit into basic event models (Leveson, 2011).

In event-based models, the causal factors identified rely on the events that are considered and the selection of the conditions connected to those events. Nevertheless, other than the physical events directly preceding or immediately involved in the loss, the selection of events to incorporate is subjective and the selection of conditions to describe the events is even more so.

Event-based models works best for accidents where one or several components fail, conducting to a system failure or hazard (Leveson, 2011). Accident models and explanations including only simple chains of failure events can easily miss understated and complex couplings

and interactions between failure events and exclude completely accidents including no component failure at all. Consequently, the event-based models developed to describe physical phenomena are inadequate to describe accidents including organizational and social factors and human decisions and software design errors in complex socio-technical systems, such as drilling operations.

The foundation for an accident is often laid years before. One event may activate the loss, but if the event had not occurred, another one would have activated it. The safety control may degrade over time without any specific single decision to increase the risk, but simply as a series of decisions that move the plant gradually towards a situation where any minor error will lead to a major accident. This may be difficult to model in event based model, whilst STAMP emphasize inadequate control action that may lead to a accident.

A strength with using FTA (and ETA) is that the method can handle complex systems and several errors at the same time. STPA consider only one inadequate control action at the time and is therefore not suitable for systems and operations where it is likely that several errors happen at the same time.

5.5.2 HAZOP & FMEA

A Hazard and Operability study (HAZOP) is a systematic hazard identification process that is completed by a group of experts to investigate how the system or a plant may diverge from the design intent and establish hazard and operability problems (Rausand, 2011). The analysis is done in a series of consultations as a guided brainstorming based on a set of guide-words, process parameters and different checklists.

The system or plant is divided into a number of study nodes that are examined one by one. For each study, the design intent and the normal state are outlined. Guidewords and process parameters are used to brainstorm to give proposal for potential deviations in the system.

Failure Modes and Effects Analysis (FMEA) was developed by reliability engineers to allow them to forecast equipment reliability (Leveson, 1995). The goal is to establish the overall probability that the product will operate without a failure in a specific duration, or that the product will operate a certain duration before failure.

FMEA is effective for analyzing single units or single failure to improve individual item integrity. It can be used to identify redundancy and fail-safe design requirements. However, FMEA puts little attention to human errors in operating procedures or hazardous characteristics of the equipment. Although environmental conditions are regarded in identifying the stresses that could cause hardware to fail, the probabilities of occurrence of such environmental stresses are seldom used.

Both HAZOP, FMEA and STAMP provide more guidance to the analysts. However, HAZOP uses a set of guidewords to inspect each part of a plant piping and instrument diagram, such as *more than*, *less than* and *opposite*. Guidance in performing the process together with a definite model of the physical structure of the plan are for that reason available.

Similar to HAZOP, STPA works on a model of the system and has “guidewords” to help in the analysis, but since in STAMP accidents are seen as consequences of inadequate control, the model used is a functional control diagram rather than a physical component diagram. Nevertheless, the set of guidewords is based on lack of control rather than physical parameter deviations. Engineering expertise is even now required, but guidance is provided for the STPA process to give some certainty of completeness in the analysis.

FMEA reviews many component, assemblies, and subsystems to identify failure modes, causes and effects of such failures (Rausand, 2011). For each component, the failure modes and their following effects on the rest of the system are entered in to a specific FMEA worksheet.

The HAZOP process focuses on identifying single failures that can result in accidents of interest. A FMEA does not usually consider effects of multiple failures, where each failure is treated as an independent event with no relation to other failures in the system except for subsequent effects it might produce (Leveson, 1995). Whereas STAMP includes how the different control loops are affecting each other and may discover hazard that the HAZOP analysis does not catch.

The big difference between FMEA, HAZOP and STAMP is basically what is considered in the analysis. A HAZOP analysis considers the process, while FMEA take a closer investigation at component level. Whereas the STAMP method has it foundation in safety constraints and control loops.

5.5.3 FRAM

The Functional Resonance Accident Model (FRAM) uses the principle of stochastic resonance in a system context. The model can be used both to account for complex accidents and to identify risk in dynamic systems (Hollnagel and Goteman, 2004). The basis is to describe the functional entities that are significant for the given scenarios or tasks. The method is based on an understanding of system functions and the entities are therefore more likely to be characteristic or recurrent functions than system structures or physical units.

FRAM is performed by dividing a process in a number of interacting functions consisting of inputs, outputs, preconditions, control constraints, timing constraints and resources (Greenwood and Sommerville, 2011). The possible variability of functions is recognized and the implication of this variability is determined by identifying its consequences on the outcome of the process. In STAMP, the process is instead divided in many different control loops that are connected to each other through inputs and outputs.

An important strength of the method is that it provides a way to develop an overall understanding of how a socio-technical system works or should work (Hollnagel, nd). FRAM does not break a system down in components or component characteristics that are considered one by one. It is therefore not a goal to find a solution to each cause, but have emphasis on the complete system. FRAM is therefore for identifying risks at a process level, whilst STAMP may be used to identify risk at an institutional level.

In addition, FRAM helps the analysis team ask questions before looking for answers. The method does not incorporate a model for any system or assumptions about specific or typical cause-effect relations.

FRAM does not provide a final explanation to why accidents occur, but can serve as a useful analogy to think about accidents and understand how large effects can accrue, and consequently how to prevent them (Hollnagel and Goteman, 2004). This is different from STAMP, which is about enforcing behavioral safety constraint, instead of preventing failures.

The difference between STAMP and FRAM is the way they handle variation in established processes. For a given process there are always some defined acceptance criteria that have to be met. In STAMP, safety constraints are introduced to reduce the variation between the acceptance criteria in the process. Whilst FRAM emphasize on being inside the given limits

and thereby deal with the problems this reveals during operations.

Chapter 6

Conclusions

Every hazard analysis technique is based on a model of accident causation. Most of the traditional accident models consider accidents as results from a chain or sequence of events, such models may be used to assign blame for the accident and could be ineffective to prevent future ones.

The STPA model helps us to understand processes in different ways and to find hazards that could not be found using traditional accidents models. Blowout accidents can be understood using this model. It helps to determine why the controls that were in place did not prevent or discover maladaptive changes. It also examines the safety constraints that were violated and determines why the controls were inadequate when enforcing them.

There will be a considerable amount of work related to developing a STPA model. In order to utilize the methods, one has to be familiar with both the operation and organization. The organization has to be well known to obtain a realistic hierarchical control structure and a control structure where the safety constraints to all controllers are identified. If one does not know the actual system, some inadequate control actions might be overlooked. It is essential that the defined steps are followed to get full effect of this hazard analysis.

Different individuals might model the safety control structure differently due to their own unique comprehension of the system. In addition, the identification of hazards and causal factors might be different. The deeper ones knowledge about the system is, the more hazards and causal factors one could find, which will make the methods much more accurate and useful.

It is an important topic to reduce the risk of major accidents and more still needs to be learned, especially with respect to safe system design for human controllers. Systems for offshore installation are designed and built by engineers and then operated by different people. Enforcing safety constraints on system behavior requires that the information needed for decision making is available to the right people at the right time, whether during system development, operations, maintenance or engineering.

With basis in HEART, the human and organizational factors can be quantified. The initial focus will be to match the inadequate control actions for the different well kick indicators with generic tasks listed in HEART. Using the numbers given by the HEART method as a foundation, an event tree analysis can be used to model and analyze the various accident scenarios for a drilling operation. As of today there has not been much work done in quantifying data required for such analysis. It can therefore be difficult to find relevant data for the actual process and give a good quantification of specific hazards.

6.1 Recommendations for Further Work

As of today, most studies in the field of system theory together with STAMP and STPA have focused on mostly technical systems within other industries than the offshore industry. This includes industries such as pharmaceutical testing, hospitals and the air transportation system. Although extensive research has been carried out on STAMP, no single study exists which adequately covers in particular the oil and gas industry within the subject of drilling.

Based on the findings in this assignment, some future tasks that will improve the methods is listed below.

- Further analysis for the whole drilling operation.
- Compare with a traditional hazard analysis.
- Introduce a tool that can help to establish control structures.
- Improve classifications of control actions and causal factors.
- More research within each method.

In terms of the case study, additionally analysis can be done for the whole drilling operation. Due to the time limit and constraints listed in the beginning of this study, only a

small example of a drilling operation has been developed to demonstrate how to use STPA. If additional material and time were available, each component in the system-level control structure might be further developed to have its own logic model, or even its own control structure.

To gain a better understanding of whether STPA covers hazards that are not included in traditional methods, one should also perform a traditional hazard analysis based on a drilling operation. Based on previous discussions, a HAZOP or FMEA would be most suitable for this case study.

One improvement could be to create a tool to aid the analyst in creating control structures, automating hazards and causal factors results. STAMP and STPA are relatively new and a mature tool support is missing. Development of such a tool could be beneficial to people working with safety-critical systems.

In addition, an improvement of the general classification for identifying potentially inadequate control action together with the classification of control flaws for identifying causal factors must be created. More research might be conducted to demonstrate the completeness and the correctness of identification of hazards and causal factors. As STAMP and STPA is founded based on control structures, it might be useful to employ some knowledge related to control theory.

Appendix A

List of Abbreviations

BHP Bottom Hole Pressure

EPC Error-Producing Condition

ETA Event Tree Analysis

FMEA Failure Modes and Effects Analysis

FTA Fault Tree Analysis

FRAM Functional Resonance Accident Model

HAZOP A Hazard and Operability study

HEART Human Error Assessment and Reduction Technique

HSE Health, Safety, and Environment

LMRP Lower Marine Riser Package

NCS The Norwegian Continental Shelf

OIM Offshore Installation Manager

PRA Probabilistic Risk Assessment

PSA The Petroleum Safety Authority (Petroleumstilsynet)

ROV Remotely Operated Vehicle

STAMP System-Theoretic Accident Model and Processes

STPA System-Theoretic Process Analysis

QRA Quantitative Risk Analysis

Appendix B

Definitions

Accident (Rausand, 2011): A sudden, unwanted, and unplanned event or event sequence that leads to harm to people, the environment and other assets.

Annulus (API, 2006): The space between the drill string and the inside diameter of the hole being drilled, the last string of the casing set in the well, or the marine riser.

Barrier (Rausand, 2011): Physical or engineered system or human action (based on specific procedures or administrative controls) that is implemented to prevent, control, or impede released energy from reaching the assets and causing harm.

Blowout (API, 2006): An uncontrolled flow of well fluids and formation from the well bore.

Blowout Preventer (BOP) (API, 2006): A device attached to the casing head that allows the well to be sealed to the confine the well fluids to the well bore.

Bottom Hole Pressure (BHP) (API, 2006): Depending upon the context, either a pressure exerted by a column of fluid contained in the well bore or the formation pressure at the depth of interest.

Drilling Break (API, 2006): A change in the rate of penetration that may or may not be a result of the penetrating a pressured reservoir.

Fail Safe (MIL-STD-882D, 2000): A design feature which ensures that a system remains safe, or in the event of a failure, causes the system to revert to a state that will not cause a mishap.

Hazard (MIL-STD-882D, 2000): Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.

Initiating Event (Rausand, 2011): An initiating event is the beginning of an accident scenario. It is an event that triggers subsequent chains of events.

Kick (API, 2006): Intrusion of formation fluids into the well bore.

Quantitative Risk Analysis (QRA) (Rausand, 2011): A risk analysis that provides numerical estimates for probabilities and/or consequences – sometimes along with associated uncertainties.

Redundancy (IEC 61508-4, 1997): Existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information.

Reliability (ISO 8420, 1986): The ability of an item to perform a required function, under given environmental and operational conditions and for a stated period of time.

Risk (AS/NZS 4360, 1995): The chance of something happening that will have an impact upon objectives. It is measured in term of consequences and likelihood.

Root Cause (Rausand, 2011): The root cause if a specified failure is the most basic cause that, if corrected would prevent recurrence of this and similar failures.

Safety (MIL-STD-882D, 2000): Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Socio-Technical System (Fischer and Herrmann, 2011) Socio-technical systems can be understood as the systematic integration of two kinds of phenomena that have very diverging, partially contradictive characteristics. Socio-technical systems are composed both of computers, networks, and software, and of people, procedures, policies, laws, and many other aspects.

System Safety (Rausand, 2011): The effort to make things as safe as possible by systematic use of engineering and management tools to identify, analyze, and control hazard.

U-tubing (Schubert, 1995): The well bore acts essentially like a u-tube, with one leg repre-

senting the drillpipe and the other leg representing the annulus. The drillpipe and the annulus are connected at the bottom of the u-tube. The sum of all the pressures on the drillpipe equals the total pressure at the bottom of the hole and the sum of all pressures on the annulus equals BHP. The sum of the pressures on the drillpipe is therefore equals the sum of the pressures on the annulus.

Underbalance (API, 2006): An uncontrolled flow of formation fluids from a subsurface zone into a second subsurface zone.

Appendix C

Pre-Study Report

Pre-study Report

Silje Frost Budde

budde@stud.ntnu.no

6. February, 2012

Contents

1 Preface	2
2 Background	2
2.1 Main Objectives	2
2.2 Success Criteria	3
3 Project Description	3
3.1 Problem to be Addressed	3
3.2 Limitations	4
4 Work Scope	4
4.1 Resource Distribution	5
4.2 Milestones	5
4.3 Progress Meetings	6
4.4 Work Method	6

1 Preface

This report constitutes the pre-study of the master thesis - *Modeling Blowouts During Drilling Using STAMP and STPA*, written at the Norwegian University of Science and Technology (NTNU), department of Production and Quality Engineering during the spring of 2012. The foundation for the master thesis was laid by the work related to the project assignment - *Monitoring of Major Accident Risk- Blowout and Well Releases*, which was performed as a literature study.

2 Background

The existing framework for risk analysis was developed about 50 years ago and is mainly based on the, then current, understanding of accident models and how accidents happen. Later, several alternative interpretations of particularly major accidents or organizational accidents have been launched. As of today, what these understandings have in common is that no accompanying methods to perform risk assessment have been developed. Generally they are limited to accident investigation and to explain the chain of events that led to the accidents occurring. One exception from this is the accident model STAMP and the corresponding method STPA.

2.1 Main Objectives

The overall objective of this master thesis is to gain an understanding of blowouts during drilling at an offshore installation using STAMP and STPA. The goal is to find out whether this method is a possible alternative approach. As well as gaining some experience on the amount of work involved and necessary parameters to perform these analyses.

2.2 Success Criteria

Success criteria related to this master thesis is based on the availability of relevant literature, my understanding of the STAMP and STPA methodology and my analytical abilities.

3 Project Description

The master thesis will be performed as a project, with focus on good planning and project management throughout the period. The progress report and non-conformance will be produced and included with the final report.

The project consists of five problems that will be answered and these are presented below.

3.1 Problem to be Addressed

In order to get a rigorous understanding of the scope of this master thesis, each of the problems in the assignment is analyzed.

1. Review and summarize STAMP and STPA and become familiar with the problem complex.

Approach: This task will set the foundation for the master thesis. Summarizing STAMP and STPA supported by relevant literature and give a insight into the problem complex regarding drilling at an offshore installation.

2. Establish a model for blowouts based on STAMP/STPA.

Approach: The model for blowouts should be produced based on the findings from task 1, and should be presented in a clear and logic manner. The model will initially be qualitative, but the goal is that it will form the basis for a quantitative model.

3. Identify the parameters needed for such a model and assess the availability of them to be able to quantify risk.

Approach: Identifying the parameter for the model should have a basis in findings from task 2.

4. Assess the model developed and the work that is performed with focus on:

- (a) Amount of work
- (b) New possibilities for decision support
- (c) If quantification is possible, and if it is, what types of data are required.

Approach: Based on the model developed in task 2, the assessment will focus on amount of work, new possibilities for decision support and if quantification is possible. This should be compared to conventional analysis methods such as, HAZOP and fault tree.

5. Summarize, conclude and give recommendations for further work.

Approach: The recommendations should be based on all the previous tasks. A discussion on the developed model compared with conventional analysis methods will be present. The section should be concluded with recommendation for action to improve the methods.

3.2 Limitations

The focus will be on the left side of the bow-tie model. Which would only concern itself with prevention rather than decreasing the potential amount of damage in the case of an accident. The model will be based on a specific section of a drilling operation.

4 Work Scope

The master thesis counts for all 30 credits during the spring semester of 2012, with a duration of 20 weeks. This calculation is based on a project period from the 16th of January to the 11th of June, including one week Easter holiday.

4.1 Resource Distribution

Figure 1 shows the distribution of the four different work packages; (1) pre-study report, (2) literature study, (3) main report and (3) project management. Each work package has then been divided into several activities.

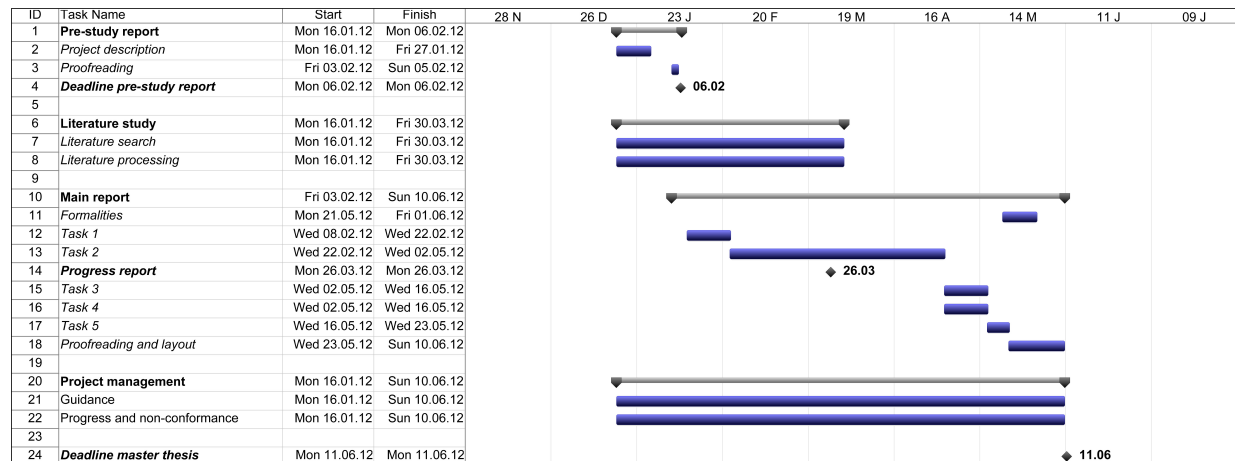


Figure 1: GANTT diagram

As seen from figure 1, task 2 is given most time and resources. This activity is important for the remaining activities in the master thesis. Task 2 therefore has to be completed before considering the rest of the tasks. While working with task 2, keywords will be written down in order to move onto the next tasks with the least amount of difficulties. The activity *formalities* includes writing preface, summary, introduction and concluding remarks of the master thesis report.

4.2 Milestones

In order to have a good overview and even amount of work throughout the spring, the following milestones have been defined:

06.02.2012 Deadline pre-study report

26.03.2012 Hand in progress report

11.06.2012 Deadline master thesis

4.3 Progress Meetings

To get useful input and motivation through the period, meeting with supervisor Stein Haugen should take place every second week.

4.4 Work Method

This master thesis will be performed as a literature study. Based on experience from the project assignment, some of the literature search and processing will be performed in parallel with the production of the master thesis report.

Appendix D

Progress Report

Progress Report

Silje Frost Budde

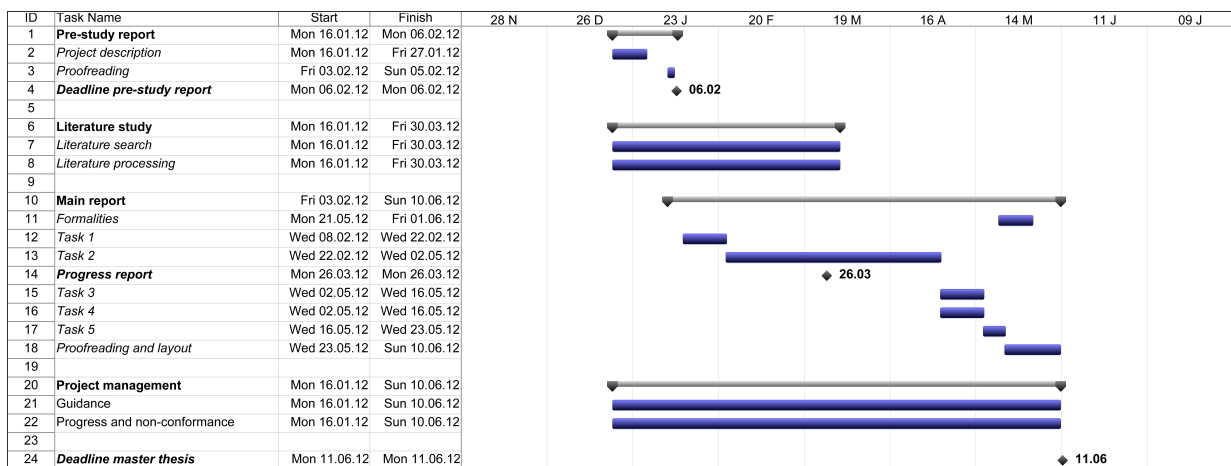
budde@stud.ntnu.no

30. March, 2012

Progress per 30.03.2012

Table 1 illustrates the planned progress outline in the pre-study report. The GANTT diagram explains the scheduled resource use distributed in the different work packages.

Figure 1: Planned Project Progression



As illustrated by table 1, the deviation in progress between planned- and actual progress is approximately 2 weeks. This can be seen as a normal deviation in a project process. The pre-study report was handed in on time and took the time that was planned to do.

The literature study has taken much more time than expected, partly because there were many articles and books to read about this subject and get a good overview of the methods.

Task 1 has successfully been executed within a longer period of time than planned. It was necessary to get a good overview of the method that is basis for the rest of the master thesis. Even though time than originally planned is used, especially with literature study and task 2, was this necessary and the efficiency has increased throughout the project. While working with task 2, keywords have been written down in order to move onto the next tasks with the least amount of difficulties.

Table 1: Project progress per 30.03.2012

Activity	Planned progress	Actual progress	Deviation
Pre-study report	2	2	0
Literature study	8	9	-1
Task 1	3	3.5	-0.5
Task 2	4	3	- 1
Task 3	-	-	-
Task 4	-	-	-
Task 5	-	-	-
Completion	-	-	-
Total deviation			-2.5

The resources available at the university's and literature database have been used in order to get supplementing literature. Some time has also used to create an overview of literature available for later use.

Several guidance meetings with supervisor at NTNU have provided constructive input, perspective and motivation for further work.

Concluding Remarks

In regards to the deviation the plan is revised to add some extra effort and to catch up with the original schedule in two weeks. This requires some work with task 2. Because of all delays the previous milestones have been updated. The milestones are listed below.

04.05.2012 Complete task 2

18.05.2012 Complete task 3 & 4

25.05.2012 Complete task 5

11.06.2012 Deadline master thesis

Even though it is hard to precisely measure exact project progress, the overall impression is that the progress at this point is satisfactory.

References

- API (2006). *Recommended Practice for Well Control Operations : Upstream Segment*. American Petroleum Institute.
- AS/NZS 4360 (1995). *Risk Management*. Standards Association of Australia, Sidney, Australia.
- Bartlit, F. H., Sankar, S. N., and Grimsley, S. C. (2011). Chief Counsel's Report. Technical report, National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling.
- Budde, S. F. (2011). *Monitoring of Major Accident Risk - Blowout and Well Releases*. NTNU. Project Assignment.
- Corneliussen, K. (2006). *Well Safety- Risk Control in the Operational Phases of Offshore Wells*. PhD thesis, Norwegian University of Science and Technology.
- Fischer, G. and Herrmann, T. (2011). Socio-Technical Systems - A Meta-Design Perspective. *International Journal for Sociotechnology and Knowledge Development*, 3(1):1–33.
- Grace, R. D. (2003). *Blowout and Well Control Handbook*. Elsevier.
- Greenwood, D. and Sommerville, I. (2011). Responsibility Modeling for the Sociotechnical Risk Analysis of Coalitions of Systems. *CoRR*.
- Holand, P. (2010). Blowout and Well Release Characteristics and Frequencies, 2010. Technical report, SINTEF.
- Hollnagel, E. (n.d.). The Functional Resonance Analysis Method for Modelling Complex Socio-Technical Systems. <http://www.functionalresonance.com/>. (Accessed 10th of May 2012).
- Hollnagel, E. and Goteman, Ö. (2004). The Functional Resonance Accident Model. In *Cognitive Systems Engineering in Process Control*.

- IEC 61508-4 (1997). *Functional Safety of Electrical/Electronic/programmable Electronic*. International Electrotechnical Commission, Geneva.
- Ishimatsu, T., Leveson, N. G., Thomas, J., Katahira, M., Miyamoto, Y., and Nakao, H. (2010). Modeling and Hazard Analysis using STPA. In *Presented at the Conference of the International Association for the Advancement of Space Safety, Huntsville, Alabama*.
- ISO 8420 (1986). *Quality Vocabulary*. International Standards Organization, Geneva.
- Leveson, N. G. (1995). *Safeware : System Safety and Computers*. Addison-Wesley.
- Leveson, N. G. (2004). A New Accident Model for Engineering Safer Systems. *Safety Science*, 42:237–270.
- Leveson, N. G. (2009). *Safety-Critical Systems: Problems, Process and Practice*, chapter 1, pages 3–20. Springer.
- Leveson, N. G. (2011). *Engineering a Safer World- Systems Thinking Applied to Safety*. MIT Press.
- Leveson, N. G., Daouk, M., Dulac, N., and Marais, K. (2004). A Systems Theoretic Approach to Safety Engineering. *Aeronautics Astronautics Department*.
- MIL-STD-882D (2000). *Standard Practice for System Safety*. Department of Defense, United States of America.
- NN (2005). Internt dokument: Forventninger til boreledere. Technical report, "Company one".
- NN (2009). Internal Document: Well Control Manual – Drilling. Technical report, "Company one".
- NORSOK D-010 (2004). *Well Integrity in Drilling and Well Operations*. Standards Norway.
- NWEA (2009). NWEA Guidelines For the Safe Management of Offshore Supply and Rig Moving Operations. Technical report, The North West European Area.
- PSA (2007). Forskrift om Utforming og Utrustning av Innretninger med mer i Petroleumsvirksomheten (Innretningsforskriften). Technical report, The Norwegian Petroleum Safety Authority.

- PSA (2012). Rolle og ansvarsområde. <http://www.ptil.no/rolle-og-ansvarsomraade/category129.html>. (Assessed 28th of April 2012).
- Quyang, M., Hong, L., Yu, M.-H., and Fei, Q. (2010). STAMP-based analysis on the railway accident and accident spreading: Taking the China-Jiaoji railway accident for example. *Safety Science*, 48:544–555.
- Rausand, M. (2011). *Risk Assessment – Theory, Methods and Applications*. John Wiley & Sons.
- Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate Publishing.
- Reisman, A. (1988). On alternative strategies for doing research in the management and social sciences. *Engineering Management, IEEE Transactions on*, 35(4):215–220.
- Schubert, J. J. (1995). *Well Control*. Texas A&M University MEng Report for well control".