NTNU – Trondheim
Norwegian University of
Science and Technology

Modeling process leaks using FRAM

Inger Krohn Halseth

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

NTNU
Fakultet for ingeniørvitenskap og teknologi
Institutt for produksjons- og kvalitetsteknikk

Vår dato 2012-01-09 | Vår referanse SHA/LMS

MASTEROPPGAVE
Våren 2012
for
stud. techn. Inger Krohn Halseth

MODELLERING AV PROSESSLEKKASJER MED BRUK AV FRAM
(Modeling process leaks using FRAM)

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.

I denne oppgaven er målet å se på prosesslekkasjer på offshoreinstallasjoner med utgangspunkt i FRAM-modellen (Functional Reasonance Accident Modelling). Fokus kan om nødvendig avgrenses til lekkasjer som skyldes feil under arbeid på trykksatt utstyr. 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 om kvantifisering er mulig og hensiktsmessig. Dette vil danne grunnlag for anbefalinger om videre arbeid.

Oppgaven skal gjennomføres i følgende trinn:

1. Litteraturstudium – gjennomgang og oppsummering av relevant litteratur om FRAM samt sette seg inn i problemstillingen.
2. Etablere en modell for prosesslekkasjer, basert på FRAM. 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 avviksrapporter. 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
førsteamanuensis/instituttleder

Stein Haugen
faglærer

“Knowledge has to be improved, challenged, and increased constantly, or it vanishes.”

Peter F. Drucker

Preface

This report is written by stud.techn. Inger Krohn Halseth and constitutes the master thesis "Modeling process leaks using FRAM", given at the Department of Production and Quality Engineering at the Norwegian University of Science and Technology (NTNU). The master thesis has its foundation in the project assignment "Monitoring of Major Accident risk - Leaks and Fires". The work related to the thesis has been performed from January to June of 2012.

A lot of guidance and feedback through the entire process of writing this assignment has been given by my supervisor professor Stein Haugen, and for that I am truly grateful. I would also like to thank Ivonne Herrera for a helpful conversation on FRAM, and my sister Anja Halseth for making my thesis better and always cheering me on.

Trondheim, 07.06.2012

Inger Krohn Halseth

Summary

This thesis was written to form an understanding of whether the Functional Resonance Analysis Method (FRAM) is a possible alternative approach to review process leaks on offshore installations and gain some experience on the amount of work involved, whether there are different results compared to conventional methods and if quantification is possible and suitable. To answer this a literature survey was performed, resulting in an explanation of the course of the method. After this, the method was tested on an exemplified operation on pressurized equipment. These results were in turn used to evaluate the method in terms of workload, quantification and the characteristics of the method.

FRAM, when used to analyse risk, contrary to retrospect when considering accidents, consists of four steps. First the system or operation considered is divided into functions. For each function six parameters are defined; input, output, preconditions, resources, time and control. The next step consists of characterizing the potential variabilities of the function, namely the variation of possible performances of a function. In the third step the network is constructed using the defined parameters. The parameters link the functions together before the variations is traced throughout the system identifying functional resonance, this is called following a signal. In the last step barriers for variability are identified, in addition, performance monitoring may also be specified.

The method was tested on a description of an operation taken from the studies of Barrier and Operabiilty Risk Analysis (BORA) where pressurized equipment is closed down to disassemble some equipment. In this case a pump is removed from a separation system. After performing the analysis it was found that the process had several barriers and opportunities for dampening the *Disassembly* function, which is critical in terms of leakages. The other functions critical in terms of leakages, the functions involved in closing down and isolating the system, does not have the same layer of protection. The source of the signal creating resonance in these functions is often found in the functions *Draw up work description* and *Coordination with CCR*, it is therefore natural to direct new barriers towards these functions.

The results of testing the method on this system has shown that FRAM is a suitable method for modeling the cause of process leakages. The method provides the analysts with the tools

to ask the right questions before looking for the answers. The methods lack of assumptions of typical cause-effect relations and decomposition of the system into components opens up for the analysts to see new aspects and connections that might have been overlooked when using more traditional methods.

One of the methods greater disadvantages is that it is, compared to more traditional methods, time consuming. Some of this time can be attributed to the fact that the method is new and requires the user to get accustomed to the method and a new way of thinking. Since the method requires a team effort, this may make the apparent difficulty appear larger. Another element that may add time to the analysis is the lack of a detailed step by step approach portraying how to perform the analysis, which more common and established methods have. The method is extensive, it is important that the constraints and limitations are thoroughly defined and the focus of the analysis well specified and understood. In lack of this, the network would become very large and difficult to handle and it would be easy to miss a possible outcome of a signal. This also applies to the functions, if they are defined covering too much it would be difficult defining the variability and handling this throughout the system.

FRAM is developed as a qualitative method, and for the time being there are no established steps formulated for the method to support quantification. Since the method focuses on the likelihood of function variability rather than the probability of a malfunction or failure, a quantification would require some changes to handle this. It should be possible to mathematically construct the network connections and their variability, the problem is finding good functions representing the variability, in other words data. A possible solution that would not require altering the method as it is today is adding an additional step using the results found when examining the resonance within the network. By doing this the data needed would only be on the variability known to create unwanted events, instead of all the defined variability. A natural method to use would be an event tree, this is however a linear method and some simplification might be necessary when considering each path of resonance pursued in the quantification. Several event trees might be needed to quantify all the different scenarios and data on both technical, organizational and human variations must be documented.

Sammendrag

Denne oppgaven ble skrevet for å undersøke om Functional Resonance Analysis Method (FRAM) er en egnet metode for å se på presselekkasjer på offshoreinstallasjoner. Ved å gjøre dette har en forsøkt å danne seg et overblikk over arbeidet involvert i en slik metode, de ulike resultatene en slik metode kan tilby i forhold til konvensjonelle metoder samt å vurdere mulighetene for kvantifisering. For å besvare dette ble et litteraturstudium utført, presentert som en stegvis forklaring av metoden. Etter dette ble metoden testet på en eksemplifisert operasjon på trykksatt utstyr. Resultatene fra dette ble igjen brukt til å evaluere metoden i form av arbeidsomfang, kvantifisering og egenskapene til metoden.

FRAM, når den brukes til å analysere risiko i motsetning til analyse av ulykker, består av fire trinn. Først blir systemet eller operasjonen som er under analyse delt inn i funksjoner. For hver funksjon defineres seks parametere; input, output, forutsetninger, ressurser, tid og kontroll. Det neste trinnet består av å karakterisere den potensielle variabiliteten i funksjonene. I det tredje trinnet blir nettverket konstruert ved hjelp av de definerte parameterne. Disse danner koblingspunktene mellom funksjonene før den definerte variasjonen spores gjennom systemet for å identifisere funksjonell resonans, dette kalles å følge et signal. I det siste trinnet blir barrierer for å forhindre variasjonen identifisert, i tillegg kan også overvåkingsmuligheter spesifiseres.

Metoden ble testet på en beskrivelse av en operasjon tatt fra en studie av barriere og operasjonell risikoanalyse (BORA) der et trykksatt system blir stengt ned for å demontere utstyr. I dette tilfellet blir en pumpe fjernet fra et separasjonssystem. Etter å ha utført analysen ble det funnet at prosessen hadde flere muligheter for å dempe signaler sendt til funksjonen *Demontering*, som er kritisk i forhold til lekkasjer. De andre funksjonene kritiske i forhold til lekkasjer, funksjonene som er involvert i nedstenging og isolering av systemet, har ikke det samme laget av beskyttelse. Kilden til signalene som kan skape resonans i disse funksjonene er ofte funnet i funksjonene *Utarbeide arbeidsbeskrivelse* eller *Samordning med sentralt kontrollrom*, det er derfor naturlig å rette nye barrierer mot disse funksjonene.

Resultatene fra testing av metoden har vist at FRAM er en egnet metode for modellering av prosesslekkasjer. Metoden gir analytikerne de nødvendige verktøyene som trengs for å stille de riktige spørsmålene før de leter etter svar. Metoden er ikke basert på typiske

årsak-virkning-relasjoner og systemet brytes ikke ned i komponenter, slik mer tradisjonelle metoder gjør. Dette åpner for å se nye aspekter og sammenhenger som kan ha blitt oversett ved bruk av mer tradisjonelle metoder.

En av metodens svakheter er at den, sammenlignet med mer tradisjonelle metoder, er tidkrevende. Noe av denne tiden kan tilskrives det faktum at metoden er ny og krever at brukeren gjør seg kjent med metoden og den nye måten å tenke på. Siden metoden krever et team, kan dette gjøre at disse utfordringene oppleves større. Et annet element som kan øke tidsbruken er analysens mangel på en detaljert forklaring av fremgangsmåten, noe mer etablerte metoder har. Metoden er omfattende, det er derfor viktig at restriksjoner og begrensninger er grundig definert og at fokuset for analysen er godt spesifisert og forstått. I mangel av dette vil nettverket bli svært stort og vanskelig å håndtere, og det vil med dette være lett å overse et mulig utfall av et signal. Dette gjelder også ved utforming av funksjonene, hvis de er definert slik at de dekker for mye vil det være vanskelig å definere variabilitet og håndtere dette i hele systemet.

FRAM er utviklet som en kvalitativ metode, og for tiden er den ikke utformet slik at den støtter kvantifisering. Siden metoden fokuserer på sannsynligheten for variasjon i funksjonene snarere enn sannsynligheten for feil eller svikt, ville en kvantifisering kreve noen endringer for å håndtere dette. Det bør være mulig å matematisk konstruere nettverkstilkoblingene og deres variabilitet, problemet er å finne gode funksjoner som representerer variasjon, med andre ord data. En mulig løsning som ikke ville kreve endring av metoden slik den er i dag er å legge til et ekstra steg i analysen der resultatene funnet når nettverket analyseres for resonans blir brukt videre for å kvantifisere. Ved å gjøre dette vil den nødvendige dataen kun være på variabiliteten kjent for å skape uønskede hendelser, istedenfor alle definerte variabiliteter. En mulig metode å bruke ville være hendelsestrær, dette er midlertidig en lineær metode og noe forenkling kan være nødvendig når man vurderer hvert tilfelle av resonans. Det kan være behov for å konstruere flere hendelses trær for å kvantifisere alle de ulike senarioene og data om både teknisk, organisatorisk og menneskelige variasjoner må fremskaffes.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Background

The existing framework for risk analysis was developed about 50 years ago and is mainly based on the perception of how accidents happened and of accident models at that time. Later, several alternative interpretations of particularly major accidents and 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. New methods including organizational aspects and non-linear relations have been developed, but there is still room for much improvement. The Functional Resonance Analysis Method is one of the new methods focusing on the relations between different functions in the system, and by mapping these, describing outcomes using the idea of resonance arising from the variability of everyday performance.

1.2 Problem formulation

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

1. Literature survey – review and summarize relevant literature on FRAM and become familiar with the assignment.

2. Establish a model for process leaks, based on FRAM. The model will initially be qualitative, but the goal is that it shall form the basis for a quantitative model.
3. Identify the parameters needed for such a model and assess the availability of the data needed to quantify the risk.
4. Assess the model developed and the work performed in terms of:
   (a) The amount of work, compared to conventional methods of analysis.
   (b) Determine new possibilities of decision support given by such a model compared with conventional methods of analysis.
   (c) Determine if quantification is possible given such a model, and if so, the new types of data required to do so.
5. Summarize, conclude and give recommendations for further work.

1.3 Objective

The objective of the assignment is to form an understanding of whether the Functional Resonance Analysis Method is a possible alternative approach to analyse process leaks on offshore installations, gain some experience on the amount of work involved, whether there are different results compared to conventional methods and if quantification is possible and suitable.

1.4 Scope and Limitations

1.4.1 Scope

The term “mainly” will be used to indicate that the main discussion covering the task is in the stated section or sections.

Task 1; Literature survey. The aim of this task is to gain enough knowledge of the method to perform the analysis. The findings from this task will create the foundation for the entire report, particularly task 2. This task will mainly be covered in chapter 3.

Task 2; Establish a model. The aim of this task is to perform a FRAM analysis for process leaks with the possibility of quantification at a later stage. This is the task that will require the most time and resources in the thesis. The task will mainly be covered in chapter 4, 5 and 6.

Task 3; Evaluate quantification The aim of this task is to identify the required data to enable quantification. This task, and subtask c) in task four are overlapping. These tasks are so correlated that they are considered as one and are mainly answered in section 7.1.

Task 4; Evaluate the model. The aim of this task is to evaluate the method in terms of workload, decision support and possible quantification. The task is manly answered in chapter 7. Each subtask is devoted its own section, respectively section 7.1, 7.2 and 7.3 but arguments and discussion on the topics related to the subtasks can be found exceeding these throughout the chapter.

Task 5; Summarize. The aim of this task is to give a summary of the findings and recommendations for further work, this will to some degree be done in chapter 7, but the answer to this task will manly be found in chapter 8, constituting the conclusion of the thesis.

1.4.2 Limitations

The focus of the analysis is limited to leaks caused by errors during operations on equipment under pressure. Leaks can occur during many different processes on the platform for equipment under pressure. To test the method, a general maintenance operation on pressurized offshore equipment is used as an example to test and illustrate the FRAM analysis in relation to process leaks. Several parts of the steps in the method is usually done in teams with operational expertise, knowledge and experience with the process in question. In lack of this, an assessment is done based on the information provided in the process description in this thesis, with the weaknesses this entails.

1.5 Approach

This master thesis is a sequel to the project assignment. The project assignment was mainly performed as a literature study with an aim of clarifying how different perspectives are used to understand accidents and how they happen, methods to monitor accident risk and what methods are used in terms of leaks and fires.

The first part of the thesis will consist of a small literature survey where articles applying the FRAM method and other material describing the method will be used to give a short step by step presentation of the method. The database on www.functionalresonance.com displaying all relevant publications on FRAM has been diligently used to find articles and information on the topic. Based on the findings the method is applied to an exemplified operation from the process industry. According to Reisman (1988) the scientific method used in this thesis can be described as a transfer of technology, where a known method is used in a new context. FRAM has to this date mostly been applied in aviation studies in addition to nuclear industry and the health industry, the transfer in technology is quite small, but there are no records of the method being used in analysis of operations in the process industry. The last part of the thesis will consist of a discussion of the findings done when applying the method with regards to quantification, the data needed and new possibilities of decision support given by the method.

Chapter 2

Definitions and abbrivations

2.1 Definitions

Barrier - a hindrance that may either prevent an unwanted event from taking place, or protect against the consequences (Hollnagel, 2004).

Failure - termination of the ability of an item to perform a required function (NS-EN 13306, 2010).

Functional Resonance Analysis Method - refers to the analysis as a whole.

Functional Resonance Analysis Model - refers to the model constructed by connecting the defined functions i.e. the network.

Hazard - source of potential harm (SN-ISO Guide 73, 2009).

Non-linear interactions - a nonlinear system is any problem where the variable(s) to be solved for cannot be written as a linear combination of independent components (Wikipedia, 2012).

Resilience - the ability to meet risk (Herrera et al., 2010).

Risk - effect of uncertainty on objectives (ISO 31000, 2009).

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

Socio-technical system - is loosely referring to a system with interactions between society's complex infrastructures including both technological, organizational and human behavior.

Sub-system - is loosely referring to a part of a system which itself has the characteristics of a system, usually consisting of several components.

2.2 Abbreviations

AC form - Activity and Control form

BORA - Barrier and Operability analysis

CCR - Central Control Room

CPC - Common Performance Conditions

CREAM - The cognitive reliability and error analysis method

FRAM - Functional Resonance Analysis Model/Method, see definitions

HC - Hydro Carbons

HAZOP - Hazard and Operability study

HEART - Human Error Assessment and Reduction Technique

MTO - Human,Technological and Organizational

NCS - Norwegian Continental Shelf

O&M - Operations and Maintenance

PSA - Petroleum Safety Authority

P&ID - Piping and Instrumentation Diagram

QRA - Quantitative Risk Analysis

QA - Quality Assessment

RE - Resilience engineering

RNNP - Risk level in the Norwegian petroleum industry (from Norwegian, Risikonivå i Norsk Petroleumsindustri)

SJA - Safe Job Analysis

SOP - Standard Operating Procedure

STAMP - System-Theoretic Accident Model and Process

THERP - Technique for Human Error Rate Prediction

TRA - Total Risk Analysis

V&B - Valves and Blindings

WO - Work Order

WP - Work Permit

Chapter 3

Functional Resonance Analysis Method

Resilience Engineering (RE) introduces a new concept of viewing risk by taking the focus away from viewing risk only as a reduction or elimination of negative outcomes, but instead focusing on what goes right and with this, producing safety. RE views safety as the ability to succeed under continuous changes in the system and its conditions (Herrera et al., 2010). The term Resilience is defined as the ability to meet risk. It is the system's ability to maintain operations before, during and after changes and disturbances in relation to known and unknown conditions. In this chapter the Functional Resonance Analysis Method will be presented, this is a method based on principles from RE.

3.1 FRAM

FRAM is a functional method in the meaning that it focuses on normal variability in the system and considers variations in the execution of daily operations (Herrera et al., 2010). It is a risk model reviewing non-linear interactions of a sosio-technical system and it is built on reviewing normal operations, when things are working as they should be. By describing operations when they are functioning, this can also be used to understand why things go wrong. The method is based on four principles (Hollnagel et al., 2008):

1. **The principle of equivalence of successes and failures.** This is related to the principle from RE grounded in the view that failures represent the flip side of the adoptions necessary to cope with the real word complexity rather than a failure of normal system

function. Success is measured in the ability of an organization, group or individual to anticipate the risk and critical situations, to recognize them in time and to make appropriate action. Failure is a result of temporary or permanent absence of this ability.

2. **The principle of approximate adjustment.** The conditions of work never completely match what has been specified or prescribed, adjustments must always be made to succeed with the actual resources and requirements at hand. Because the resources always are finite, such adjustments are invariably approximate rather than exact.

3. **The principle of emergence.** This reflects how variability in normal performance rarely is large enough to cause an accident on its own, but how variabilities from multiple functions may combine in unexpected ways, leading to consequences that are disproportionately large, hence produce a non-linear effect.

4. **The principle of functional resonance.** The variability of a number of functions may at some occasion reinforce each other and thereby cause the variability of one function to exceed its normal limits. The consequence may spread through tight couplings rather than via identifiable and enumerable cause-effect links.

3.2 FRAM – Step by step

There are some different opinions to how many steps there are in a FRAM analysis, though the majority consider it to be four, there are those who include an initiating step where the goal of the analysis is defined. This concerning whether the analysis is done as part of a risk analysis or as part of an accident investigation (in retrospect or prospect). The difference in performing a FRAM in retrospect or prospect is little, the only difference is the focus of the analysis, therefore the initiating step is not included.

3.2.1 Step 1; Identifying functions

In order to map the event or scenarios that are under analysis the essential system functions are identified and described. A function is, in terms of FRAM, defined as an activity or a task that is important or necessary for the state of other task or activities (Herrera et al., 2010). Hollnagel (2005) describe each function through six different parameters, these are:

1. **Input (I)** – What the function uses or transforms, this constitute the links to previous functions.
2. **Output (O)** – What the function produces, this constitutes the links to the subsequent functions.
3. **Preconditions (P)** – Conditions that must be fulfilled before a function can be performed. This can for example be that another step or process has been completed or that a specific system condition has been established.
4. **Resources (R)** – What is needed by the function to process the input, this can for example be procedures, software, hardware, energy, manpower etc.
5. **Time (T)** – That affects time availability of the function. Hollnagel (2005) explains this by determening that everything takes place in time and is governed by time. It can also be a constraint in the sense of a time window for an activity (a duration) or it can be considered as a special kind of resource.
6. **Control (C)** – That supervises or adjusts the function. This can be active functions or just plans, procedures and guidelines.

These six aspects of a FRAM function are visualized using a hexagonal representation shown in figure 3.1. These will in a later step be connected together through the parameters defined in this step.

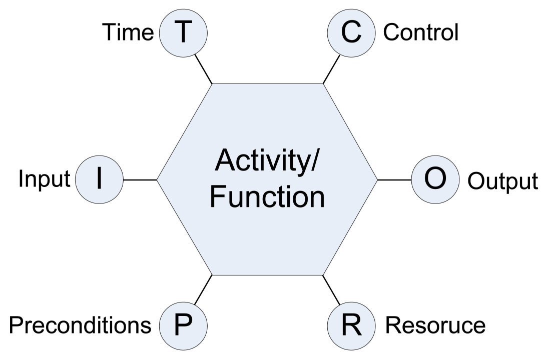


Figure 3.1: Visualization of the six parameters and the FRAM function (Wolter and Hollnagel, 2008).

Macchi (2010) proposes that functions identified in the analysis are classified as either foreground or background functions. The foreground activities are defined as the main focus of the analysis, for example control functions. The background functions are the functions that provide support and means (i.e inputs, controls, resources and preconditions) for the performance of the set of foreground functions. The systemic approach adopted by the

FRAM therefore requires that both foreground and background functions are modeled with the same approach.

3.2.2 Step 2; Identifying variation

In this step the potential variabilities of the functions are characterized. By asking the questions; Which conditions can lead to increased performance variability? Which functions are affected? And how can the variability express itself and how may this affect/be affected by other functions? The variability of the functions are tried deduced.

Step 2 is a good illustration of FRAM being a new method still under development. The original tool suggested used to ease this process was the common performance conditions (CPCs) and variability phenotypes (Nouvel and Travadel, 2007). In this case eleven CPC are identified within FRAM to elicit potential variability. The CPCs address the combined human, technological and organizational (MTO) aspects of each function (Wolter and Hollnagel, 2008). The CPC are used as the main determinant of the variability of the functions, the combined effect of the CPC are non-linear. The variability can be characterized in a qualitative manner or by using equivalent concepts such as stability, predictability, sufficiency and boundaries of performance (Wolter and Hollnagel, 2008). The human/machine failure modes that are related to FRAM can be used to characterize the potential consequences of functional variability in terms of quality of the output. This can be expressed either as failure modes, or variably phenotypes.

A more recent method suggested to replace the old method to characterize the variability, is to asses the function in relation to the three MTO categories: HuMan (M), Technology (T), and Organization (O) (Macchi, 2010). These three categories describe functions of a different nature and with characteristic differences in performance variability.

- Human factors will, because people must adjust their performance to the current working conditions, typically be quite variable. They can vary on a short term basis, but may also have a dampening effect.
- Technological functions that to a large degree depend on the technology implemented in the system are in less subject to variability since they are designed to be stable reliable and predictable, but they do not have the ability to dampen performance vari-

ability.

- Organizational functions have a variability relative to the human functions. The nature of organizational functions have a delayed effect on the human functions. A typical example of this is the production and updating of procedures. The organizational functions are typically a set of background functions.

Hollnagel (2005) illustrates how the CPCs can be classified according to the MTO principle. This is shown in table 3.1. As seen in this table most of the CPC affect the human functions, this creating the most variability. By using the MTO categories and resources with knowledge of the situation, the variability of the method is identified.

Common Performance Conditions	Functions affected		
	M	T	O
Availability of resources	x	x	
Training and experience (competence)	x		
Quality of communication	x		x
HMI and operational support	x		
Access to procedures and methods	x		
Conditions of work	x	x	
Number of goals and conflict resolution	x		x
Available time / time pressure	x		x
Circadian rhythm, stress	x		
Crew collaboration quality	x		
Quality and support of organization			x

Table 3.1: MTO relation to CPC (Hollnagel, 2005).

3.2.3 Step 3; Constructing the network and identifying functional resonance

Simultaneous occurrences of spreading variability may have the effect of resonance, it becomes a signal that spreads throughout the system, it is this phenomenon that may constitute a high risk or vulnerability (Woltjer, 2012). In this step the functional resonance is defined based on the possible couplings between functions and the potential functional variability. The functions defined in step one, may be coupled via their parameters. One functions output may be another functions input, fulfill a precondition, or enforce a control or time constraint. The couplings are found by analyzing the functions and identifying common aspects. By combining these links with the results from step 2 the variability of one

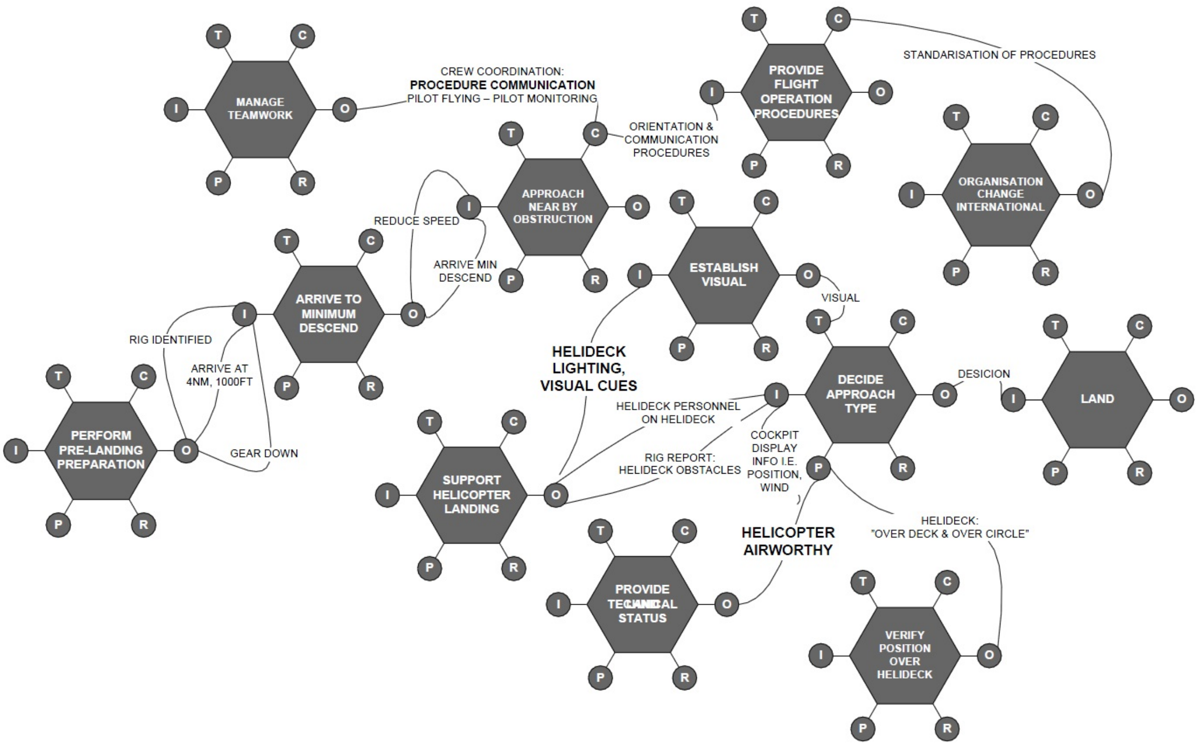


Figure 3.2: A FRAM instantiation for landing on a helicopter deck during night (Herrera et al., 2010, p. 133).

function and how this may spread through the system is mapped. The connections between the functions are modeled using the hexagonal representation of the functions and drawing a line between the parameters to illustrate the link between the parameters of each function to each other, as shown in figure 3.2.

The acronym FRAM is used for both Functional Resonance Analysis Model and Functional Resonance Analysis Method without any clear distinction between these two concepts. In this thesis the use of method refers to the analysis as a whole while the use of model refers to the model constructed by the functions i.e. the network.

3.2.4 Step 4; Identifying barriers

In the last step barriers for variability are identified, in addition required performance monitoring may also be specified (Nouvel and Travadel, 2007). Hollnagel (2004) defines a barrier as a hindrance that may either prevent an unwanted event from taking place, or protect against the consequences. In FRAM four categories of barrier systems are identified these are; physical, functional, symbolic or incorporeal. A physical barrier, or a material barrier, physically prevent an action from being carried out or an event from taking place (Hollnagel, 2004). A characteristic of the physical barrier is that they do not have to be perceived or interpreted by the acting agent in order to work, this is not the case for the functional barrier. This type of barrier requires a pre-condition to be met before action can be carried out, a good example of this is a lock that requires either a password or a key. A symbolic barrier has the characteristic that they require an act of interpretation in order to achieve its purpose. Examples of such a barrier is the reflective posts in the road indicating the edge of the road and the speed limit. A procedure represent a symbolic barrier system since its warns, cautions and conditions require an act of interpretation to work, but can also be seen as an incorporeal barrier. Incorporeal barriers are not material but depend on the knowledge of the user in order to achieve its purpose. Examples of incorporeal barriers are for example rules, guidelines, safety principles, restrictions and laws.

Chapter 4

Defining the process

The RNNP project monitors the risk level on the Norwegian Continental Shelf (NCS) as a whole, the project was initiated by the Norwegian Petroleum Directorate, now the Petroleum safety Authority (PSA) in 2000 (PSA, 2010). The goal of the project is to monitor and identify the risk level in the Norwegian petroleum industry. Annual reports are published describing the development and based on this the PSA identify areas that need extra attention. In the eight year period 2001-2009, 350 leaks occurred. In the reports from 2004 it was found that along with serious well incidents, damage to supporting structures and marine systems, and ships on a collision course, such leaks occurred for more than 80% of total major accident risk on the NCS. Process leaks is in other words a phenomenon that should be monitored closely and better methods to do this and anticipate when they will occur are always wanted. To test FRAM a general scenario of operations on pressurized equipment taken from the BORA studies is used as the basis when performing the analysis. In this chapter the system under analysis is presented, broken down into functions and the parameters are defined.

4.1 The situation considered

The situation considered for analysis in this paper is an event where a pump is removed for maintenance from a separation system. The Piping and Instrumentation Diagram (P&ID) in figure 4.1 shows how such a system may look like. When operations are carried out on pressurized equipment several procedures and checklists must be followed. Planning, authorization , checklists and briefing meetings must be executed, an example of how this may be done is found in the table given in appendix A, taken from the BORA studies. Here the work description is given, in addition to the people needed for the task, the demands and possible faults. The procedures described in this table forms the basis used for identifying the FRAM functions. The operation can in short be described as planning the process, closing and draining the system before the pump is disconnected. When this pump is repaired it is connected to the system followed by O2-emptying and testing before the system is turned back on.

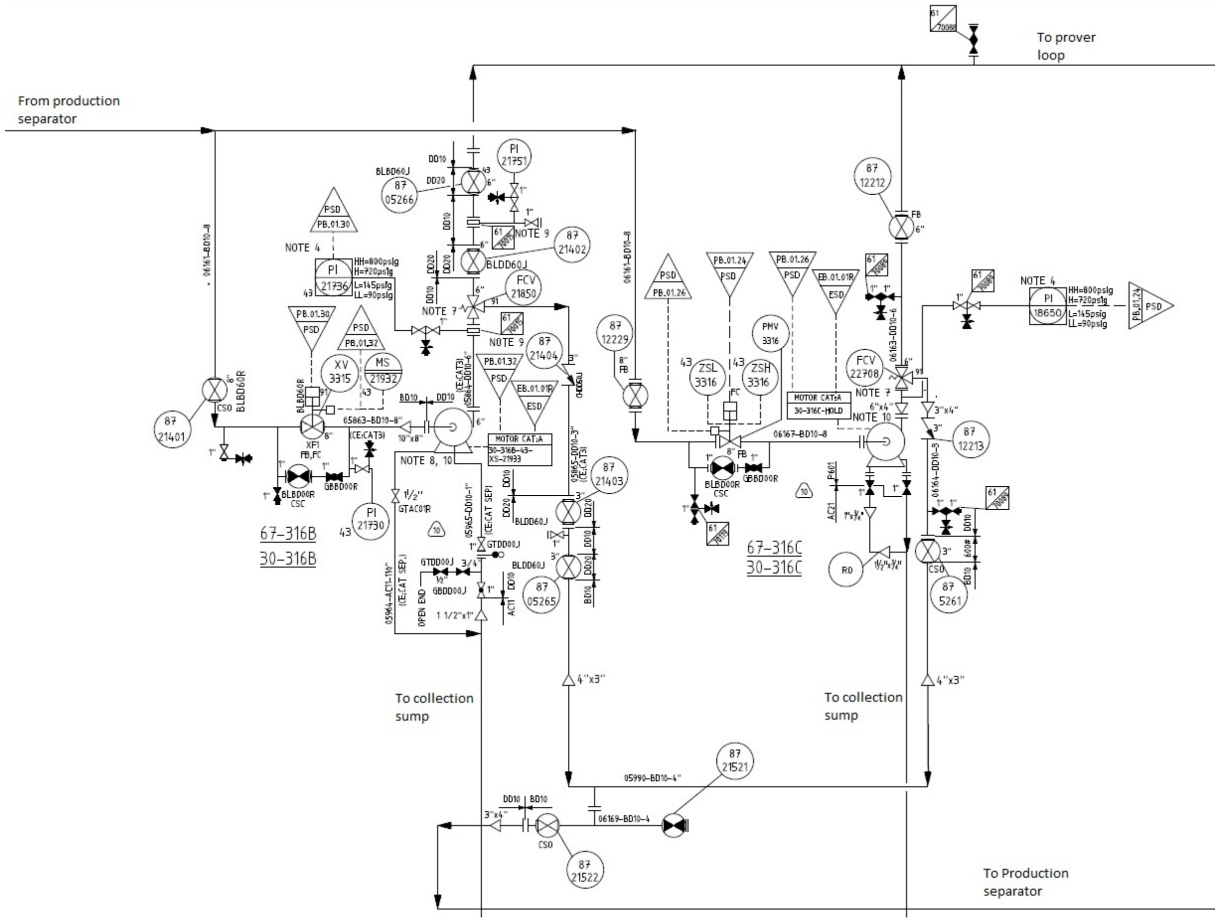


Figure 4.1: P&ID of the system.

4.2 Identifying functions

The first step in FRAM is to identify the functions of the operation in analysis. A more or less chronological list of the function is shown in appendix B.1.2, the numbers following the functions refers to the steps in the process description in appendix A, describing the operation in more detail.

4.2.1 Simplifications

From appendix B.1.2 one can see that 33 functions are identified to describe the operation. To simplify and make the workload more fitting for the next tasks, only the functions up to and including *Disassembly* are considered. The assumption that the operation can be performed by one shift is also made, excluding the handover between shift as part of the analysis. Defining the functions, parameters and variability for each function is usually done in teams with operational expertise, knowledge and experience with the process in question, but in lack of this, an assessment is done based on the information provided in the process description in this thesis, with the weaknesses this entails.

4.2.2 Foreground functions

The identification and choice of the overall functionality or performance that will be the focus of the analysis is what states the foreground of the analysis. Since the activity in analysis is leaks in a pressurized system it is natural to consider the activities that directly can lead to a leak as the focus of the analysis. The foreground functions defined for the operation can be found in table 4.1. The full sett of foreground functions for the entire operations considered can be found in appendix B.1.2.

Foreground functions
Prepare for work (16-18)
Shut down process (19)
Isolate using valves (20)
Drain (21-23)
Isolate (24)
Disconnect equipment (25, 26)
Disconnect safety system (38)
Disassembly (43)

Table 4.1: Foreground functions.

4.2.3 Background functions

The identification of background functions is based on the consistency check of the model and starts from the description of foreground functions. The background functions provide support and means for the performance of the set of foreground functions. The identified background functions for the part of the operation considered are found in table 4.2, the classification of the background functions for the entire operation can be found in appendix B.1.2.

Background functions
Draw up work description (1-12):
Draw up work permit (13-14)
Coordinate with Central Control Room (CCR) (15)
Label equipment. (27-29)
Prepare (30-32)
Quality check and sign Work Permit (WP) (33-35)
Sign splice log (39)
Update (Valves and Blindings) V&B (40)
Supervision; ignition control (41)
Quality control (42)

Table 4.2: Background functions.

4.3 Parameters

For each of the defined functions up to and including *Disassembly* the six different parameters have been identified. Table 4.3 shows and example of the parameters identified for the foreground function *Drain*, parameters identified for the full set of functions are found in appendix C.

FRAM function	Drain
Input	Work Order (WO) , WP, marked P&ID
Output	Empty piping and equipment
Time	
Control	Standard Operating Procedure (SOP)
Preconditions	Draining to closed system
Resources	Area technician, N2/steam

Table 4.3: Parameters for the foreground function *Drain*.

Chapter 5

Function variabilities and connections

One of FRAMs four principles is the principle of Approximate Adjustments which states that situations and conditions never are identical, and adjustments are made to fit the actual conditions. This creates variability. In this chapter the variability for each of the systems defined functions is identified and the FRAM network is constructed.

5.1 Variabilities

Defining the variability of the functions is done by first classifying the functions according to the MTO principle. The MTO categories relate to different CPCs, the original classification used to identify variability in FRAM. How the variation is seen will differ for the different CPCs, in the same way human, technological and organizational variability will differ in its characteristics. In table 5.1 it is shown how Macchi (2010) explain how the MTO categories have different variability and ability to damp the effect of the variability.

	Human	Technological	Organizational
Characteristic performance	Adjust their performance to current working conditions	Function in a stable, reliable and predictable way	Provide support and means to human and technological functions
Variability	Variable (High frequency)	Stable, slowly degrading	Variable (High inertia)
Damping potential	Potential for performance variability damping	No potential for performance variability damping	Provide the means to damp performance variability

Table 5.1: Performance variability and their qualities in relation to MTO (Macchi, 2010, p. 69).

5.1.1 MTO classification

When classifying the functions according to the MTO principle, each function is considered and its nature is identified. It is possible for a function to be classified in more than one category, a manual procedure involving use of technical equipment will be considered both human and technical. An example of this is the function *Shut down process.* This involves the operator interpreting the information giving the order to shut down the system, then performing this command in the control room causing the technical equipment to shut down. In the same way the function *Draw up work permit* includes the manual operation of producing the work permit and the organizational task of getting it approved by all the necessary levels in the organization.

Function	M	T	O
Draw up work description (1-12)	x		
Draw up work permit (13-14)	x		x
Coordinate with CCR (15)	x		
Prepare for work (16-18)	x		
Shut down process (19)	x	x	
Isolate using valves (20)	x	x	
Drain (21-23)	x	x	
Isolate (24)	x		
Disconnect eq. (25, 26)	x	x	
Label eq (27-29)	x		
Prepare (30-32)	x		x
Quality check and sign WP (33-35)	x		x
Disconnect safety system (38)	x	x	
Sign splice log (39)	x		
Update V&B (40)	x		
Supervision; ignition control (41)		x	
Quality control	x		
Disassembly (43)	x		

Table 5.2: MTO classification of process functions.

The result of classifying the function according to the MTO principle can be found in table 5.2. As indicated by the great majority of the functions being classified as human, one can from Macchi's (2010) classification of the different variability expect a variability with a high frequency but also a potential for performance variability damping.

5.1.2 Defining the variability

The next step is to identify each of the functions' variability. By using the MTO classification and asking the questions 1-3, the variability of the functions is tried identified.

1. Which conditions can lead to increased performance variability?
2. Which functions are affected?
3. How can the variability express itself and how may this affect/be affected by other functions?

As mentioned in section 4.2.1, defining the variability for each function is usually done in teams with operational expertise and knowledge of the process in question, but in lack of this, an assessment is done based on the information provided in the process description in this thesis, with the weaknesses this entails. When identifying the variability of each function, the entire function and what the function entails is considered, this being reflected in the MTO classification, and the questions 1-3 are answered. In lack of a team and more experience and knowledge of the process the different CPCs related to the MTO classifications, found in table 3.1, are used as a supplement when identifying conditions that can lead to increased performance variability.

Each of the functions identifed variability can be found in appendix C. Here the questions 1-3 are answered. If there are any special circumstances or other information relevant for the variability this will be found in an additional row in the table labeled “Comment”. An example of this presentation is found in table 5.3, where the parameters and variability of the function *Drain* is shown. In the row describing the control of the function, many of the functions have only the notation SOP written, this refers to Standard Operating Procedure, indicating that there are no known extra measures of control in addition to the operator(s) need to follow preapproved procedures.

5.2 Constructing the network

The work done to construct the network is mostly done when the variability and parameters are defined. The question which functions are affected lists all the functions succeeding the function in question. With this and the defined parameters, the connections between the

FRAM function	Drain
Input	WO, WP, marked P&ID
Output	Empty piping and equipment
Time	
Control	SOP
Preconditions	Draining to closed system
Resources	Area technician, N2/steam
Variability	1. Competence, stress, communication, degradation, work conditions 2. Isolation 3. Wrong valves opened, inadequate draining, inadequate procedures, no flushing, inadequate gas freeing

Table 5.3: Variability and parameters for the function *Drain*.

functions are already identified and the network can easily be drawn. In this thesis a plug-in stencil for Microsoft Visio is used (Woltjer, nd). The result can be found in figure 5.1. The foreground functions are identified using a darker color.

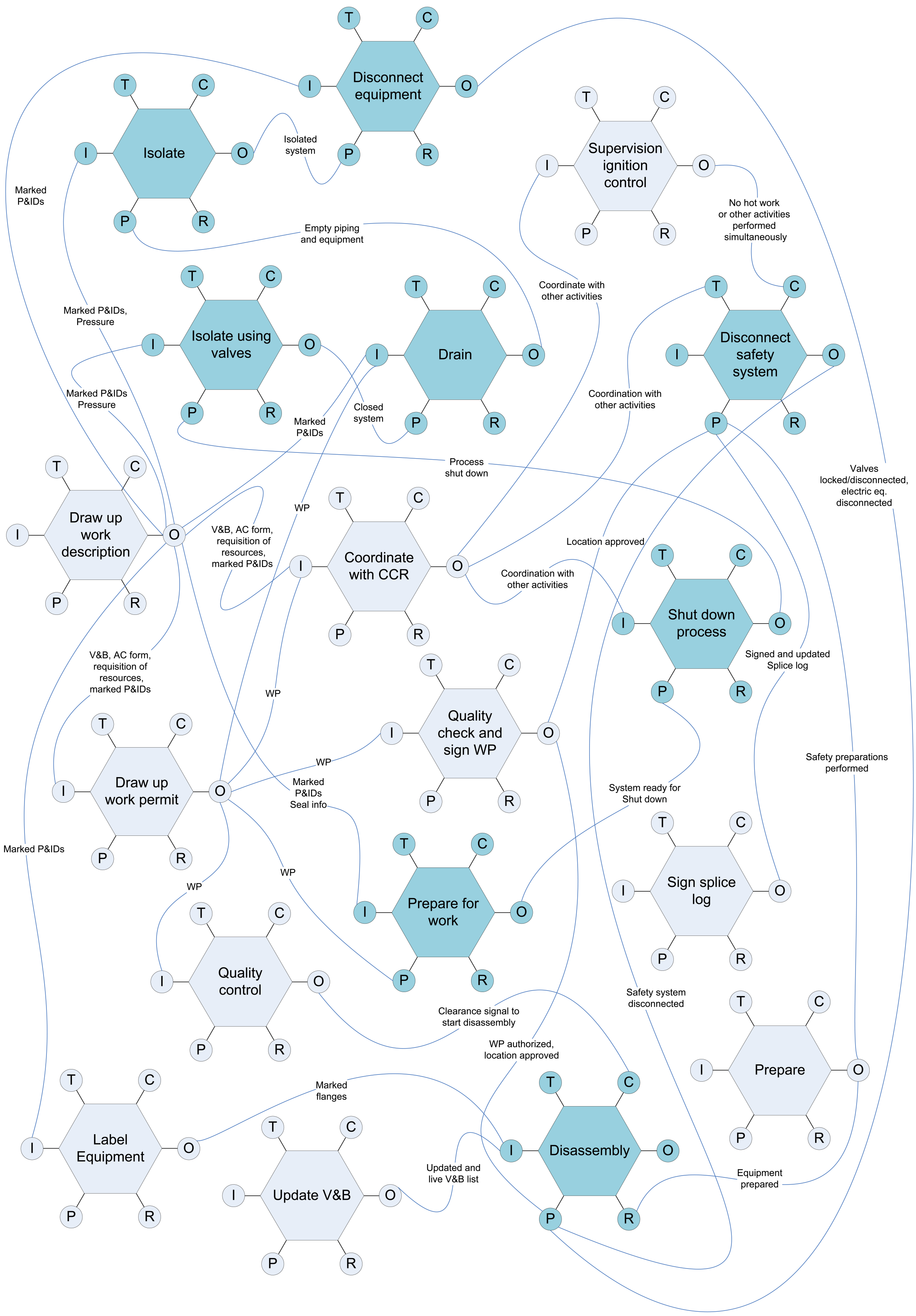


Figure 5.1: The FRAM model for process leaks.

Chapter 6

Identifying functional resonance and barriers

Resilience engineering and the FRAM method is founded on a view that accidents result from unexpected combinations, also known as resonance of normal performance variability. The resonance is a detectable signal that emerges from the unintended interaction of the variabilities of many functions that together may combine in unexpected ways, leading to consequences that are disproportionally large. In this chapter the last step in the FRAM method is performed; identifying the functional resonance in the FRAM model. In addition, a small discussion of the possible barriers to prevent the resonance is included.

6.1 Identifying functional resonance

Identifying the resonance is done by considering the variations defined in the previous chapter and following the possible outcomes of this throughout the network, combining the variations of the different functions to identify all the possible outcomes. An example of how this process is done is described below.

6.1.1 Example of tracking a signal in the network

The example will track a signal and how this may lead to a leak throughout the network. Starting with a signal created in the function *Draw up work description.* This function has a variability affected by stress and workload, this may result in a wrong notation of information regarding valves, pumps, seal, pressure etc. Assuming a wrong notation of the equipment in the process is done, this signal is tracked throughout the network. Each function when considered in relation to the signal will be listed with one or more numbers in brackets. These numbers represent the number of activities passed from the initiating variation starting the signal to the event in consideration. For example will the function *Coordinate with CCR* have both the numbers 1 and 2, denoted (1;2), seeing as its both in direct connection to the starting point in *Draw up work description* but also connected via the function *Draw up work permit,* making it a secondary connection. The connection can be through any of the parameters, not only input/output.

Draw up work permit (1) For this function communication and knowledge are the contributors to variability. Communication can be inadequate and a failure to detect the signal occurs. But it can also go the other way and the signal is detected due to good communication and knowledge of the process and thus working as a damping effect.

Coordinate with CCR (1;2) For this function inadequacies in communication and knowledge may lead to the signal going unnoticed or it may work as a dampening effect and the error is found and corrected. Additional errors increasing the signal can be made by not seeing overlapping processes creating problems as a result of the information on equipment involved in the operation being incorrect.

Prepare for work (1;2) This functions' variability is affected by stress and competence. If knowledge of the system is good the signal may be dampened or the preparations may be inadequate seeing as the information provided is incorrect.

Shut down process (3;3) In this function experience and knowledge may lead to a dampening effect causing the signal to be detected, otherwise the signal will continue into the network.

Isolate using valves (2;4) For this function the signal can result in the system not being isolated seeing as the wrong equipment is operated, degradation may worsen this effect, or the signal could be discovered and dampened. If not, the signal will go unseen and the wrong valves may be shut down.

Drain (3;5) In this function the signal may lead to the system not draining properly or at all caused by the misinformation regarding equipment in the signal. Another possible scenario is draining to the wrong system, as a result of closing the wrong valves. This may result in leakages or disturbances outside the system covered in this analysis.

Isolate (2;4;6) For this function drain is a precondition, if drain is not completed this can result in a leak. Another possibility is that the signal is not spotted and the wrong blindings are isolated, which again may lead to the isolation not fulfilling its function as a barrier.

As seen in figure 6.1 the signal spreads from *Draw up work description* and ends up with a leak, illustrated by a drop of oil in the output of the function *Drain*. Another feature seen by this illustration is how there are several paths to the different functions. The function *Isolate* have both a direct path with only one function between itself and the starting point, and a longer path covering six functions. This will result in more opportunities for making mistakes, but also provide several opportunities for dampening the effect. The signal can be followed throughout the entire system with many different other scenarios, describing this entire process is too time and space consuming and the findings will in stead by summarized in the paragraphs below, both in terms of resonance and dampening effects.

6.1.2 Resonance

By viewing resonance and how this will spread throughout the system with emphasis on leakages it is apparent that the function *Drain* is critical, a leak cannot occur unless there is liquid in the system, therefore any variations leading to the drain function not being fully completed are dangerous in terms of leakages. Another critical point in the process is isolation, more specifically the functions *Isolation* and *Isolation using valves*. If these processes

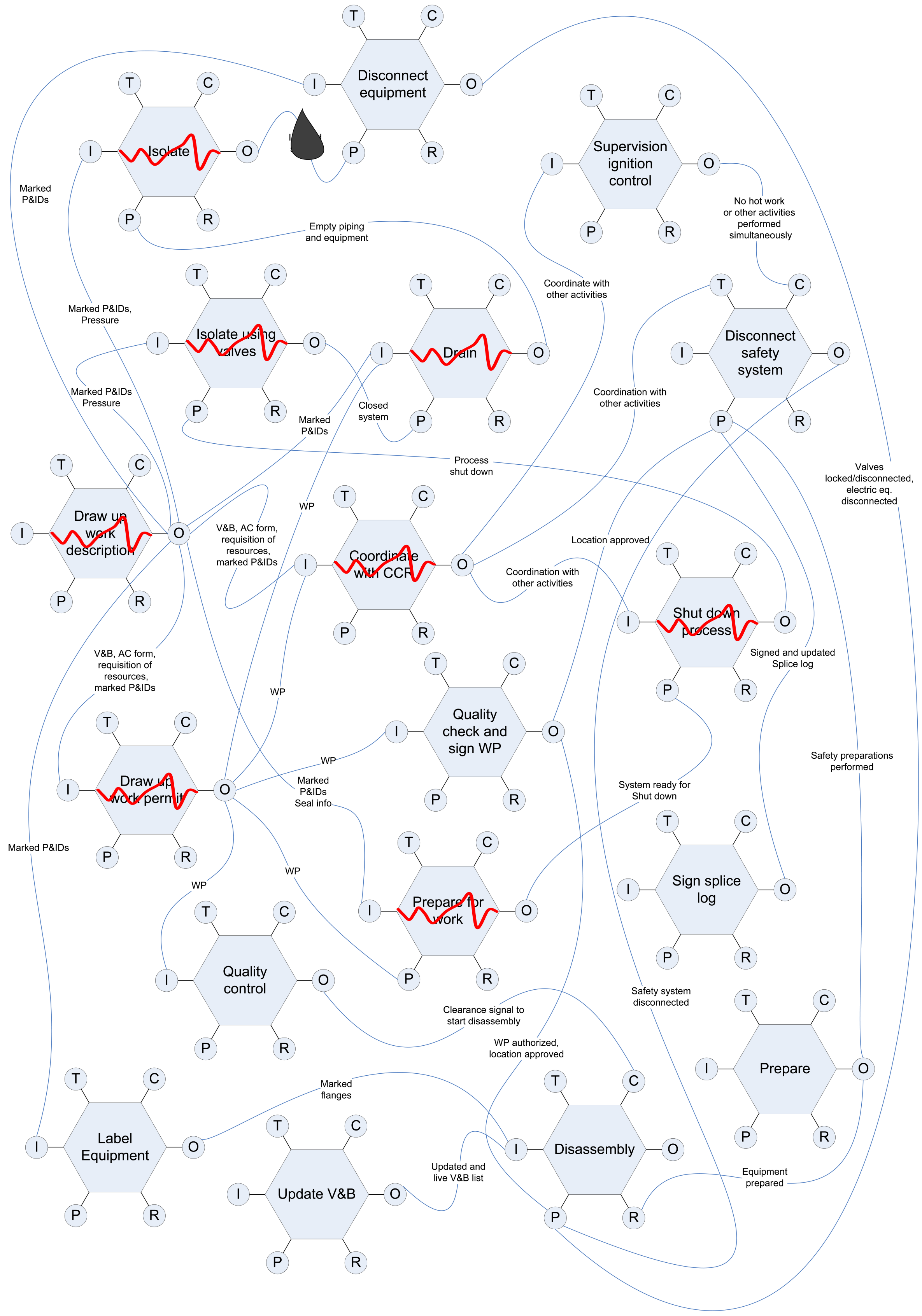


Figure 6.1: Illustration of how a signal may spread in the system until a leak occurs.

are disturbed in a matter causing the barriers to be vulnerable, the possibility of a leak increases. This will manifest itself in either the functions *Disconnect equipment* or *Disassembly*.

The focus of the analysis is leakages, the undesirable events will appear in the sharp end of the system, which to a large degree are the foreground functions. The signal causing a leakage is however not necessarily started in the foreground functions. Studying the network and how the signal spreads it is clear that the background functions *Draw up work description* and *Coordinate with CCR* are the functions constituting the biggest risk of starting a signal, with the possibility of affecting the other functions in such a way that a leak may be the result. A foreground function with much the same ability is the function *Prepare for work*. If there is much variation in this function a signal may be started and manifest itself in the critical functions mentioned above.

If one or more of the functions mentioned above starts a signal, resulting in the wrong valves being shut down in the function *Isolate using valves*, this might lead to draining to the wrong system. This can result in problems in other processes on the plant which are not covered in this analysis.

Following the signal it is clear that not all the functions included in the network will contribute to a scenario involving a leakage, but merely pass the signal on without increasing it any further. The reason for this is that there are many functions that only include updating lists and documenting procedures, and not changing them. An example of this are the functions *Update V&B* and *Sign splice log*. It is possible that the variation in these function might cause trouble in the assembly of the equipment, but this part of the process was excluded when the limitations were set, and is therefore not considered.

6.1.3 Dampening

Many of the functions have little effect on the signal in terms of the function being able to create resonance that may lead to a leak. Instead they serve as an opportunity to discover the signal and with that, the opportunity to dampen it. If dampening does not occur they simply pass the signal "as is" to the latter functions in the network. The functions that in the largest degree serve to this opportunity are:

- *Ignition control*
- *Quality check and sign WP*
- *Quality control*
- *Label equipment*
- *Sign splice log*
- *Update V&B*

These functions must be passed as a mandatory devious route to get to the functions which are more critical in terms of creating leakages, giving the system several opportunities to spot its defaults before they turn into hazardous situations, and by doing this the devious routes functions as a quality check.

It is not given that the functions with a larger potential for creating resonance can not create dampening. In the functions where resonance may occur it is also a possibility that the signals are discovered before an unwanted event occurs. An example of this is if a wrong notation is made in the P&IDs in the function *Draw up work description*, the function *Coordinate with CCR* can instead of making the wrong decisions based on this, detect the signal and correct the error. In the example of tracking a signal the different numbers of activities passed are listed for each activity, as one can see from this there are three different paths to the function *Isolate*, giving several opportunities to dampen the signal.

6.2 Identifying Barriers

A barrier can either prevent an unwanted event from taking place, or protect against the consequences. In the system considered there are several functions that serve as a barrier. The function *Disconnect equipment* is a physical barrier preventing work accidents by eliminating the possibility of the equipment starting up at the wrong time. This is not a barrier with main focus on leakages, but there are several of these. The function *Ignition control* is a functional barrier set up to protect against the consequences if there is a leak in terms of hindering it igniting. *Quality Control* is a function where a Safe Job Analysis (SJA), work place control and approval is performed before the work permit is signed, this is a series of procedures and can therefore be seen as a symbolic or incorporeal barrier according to Hollnagel's classifications. Other functions that consists of procedures that must be carried out are *Sign* *splice log*, *Update V&B* and the function *Quality Control* where the flange is controlled to be the right one and it is ensured that the system is emptied of HC.

In figure 6.2 the functions with barrier purposes are marked in red and the output is followed into the system. As one can see from this figure the only function determined as critical in section 6.1.2 properly protected by these functions is *Disassembly*, leaving the other critical functions *Isolation*, *Drain* and *Disconnecting equipment* unprotected. It is therefore natural that if new barriers are recommend that they are centered towards these functions. Seeing as the *Draw up work description* and *Coordination of CCR* are the functions that can create the most trouble for these functions, it is natural to direct the barriers towards these functions. A function reviewing and quality proofing the procedures to be performed is a good solution for a barrier for these functions, seeing as the signal often is based on misinformation etc. In terms of barriers this would be a physical or functional barrier that can stop a signal created in these functions.

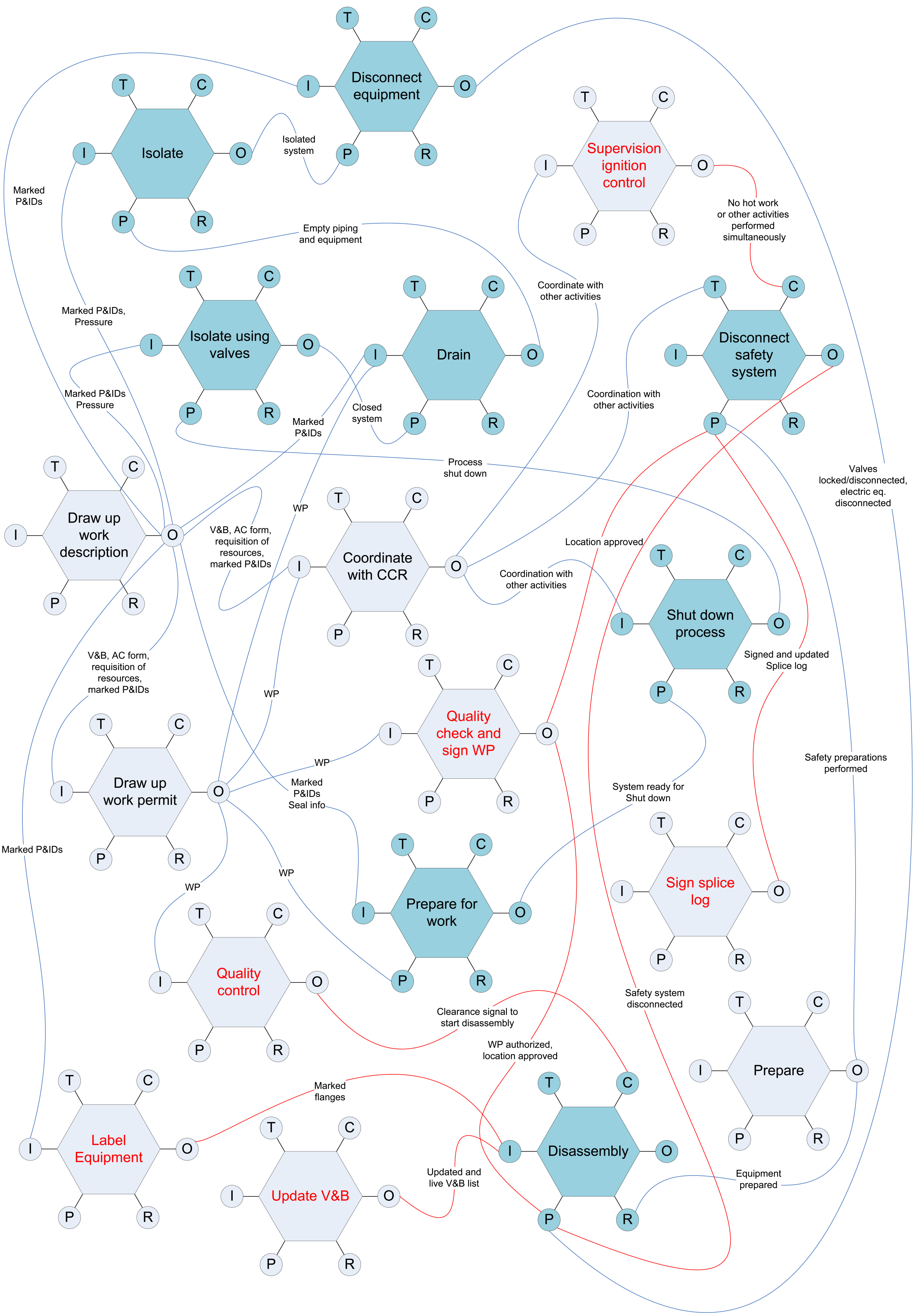


Figure 6.2: Illustration of how quality control is centered around *Disassembly* and *Disconnecting safety system*.

Chapter 7

Evaluation of the method

In this chapter the possibility of quantification will be discussed before the workload in FRAM is considered. Then the strengths and weaknesses are discussed before some general comments are made.

7.1 Quantification

FRAM is developed as a quantitative method, and for the time being there are no established steps formulated for the method to support quantification. There are however some obstacles, making the usefulness of applying the method as means to quantify scenarios questionable. One of the four principles FRAM is founded on is the principle of emergence. This reflects how the variability of normal performance rarely is large enough to be the cause of an accident, but how variabilities from multiple functions may combine in unexpected ways, leading to consequences that are disproportionately large. Since the method focuses on the likelihood of function variability rather than the probability of a malfunction or failure, a quantification would require some changes to handle this. If the cost of the changes are considered worth while, a quantification is very possible, but the quality and accuracy of it might be questionable, since the nature of the network makes it hard to determine the uncertainty in addition to the difficulties of finding good data.

It should be possible to mathematically construct the network connections and their variability, the problem is finding good functions representing the variability, in other words data. The formula would be complex and hard to handle because the model is non-linear. A possible solution that would not require altering the method as it is today is adding an additional step using the results found when examining the resonance within the network. By only using the results found to create resonance that may result in undesirable outcomes and quantifying these, a lot of the trouble of tackling non-linearity and multiple outcomes is avoided. A natural method to use would be an event tree, this is however a linear method and some simplification might be necessary when considering each path of resonance pursued in the quantification.

An example of how such an event tree would look is shown in figure 7.1. This is based on the example of tracking the signal described in section 6.1.1, where the signal is a wrong notation in a P&ID with the possible outcome of isolating with flanges in the wrong place. Using this method, several event trees must be constructed to include all the possible chain of events. An example of this can be seen in the function *Coordinate with CCR* which can find or pass on the signal, or increase it by making decisions based on the wrong information worsening the situation, which in turn can combine in different ways with the latter functions. Both outcomes may result in a leak, but the path to the leak is different. This path, and other paths, would be modeled in another tree. The frequency of leakages is found by calculating the sum of each tree's contribution to the probability of a leak. Using this method it is important that the constraint and limitations are thoroughly set and the focus of the analysis well specified and understood, so the undesired event does not cover to much which would result in large amount of event trees to cover the quantification.

7.1.1 Data

The main obstacle in procuring data for quantifying FRAM is that the method focus on the likelihood of function variability rather than the probability of a malfunction or failure. In most risk analysis the data needed is either probability of success or failure, but in FRAM it is the variability that must be quantified, in other words all possible performances of a function and the distribution of these. By doing this, only the probability of a function varying in a specified way must be quantified. Even with this simplification, finding good data is always a challenge when doing risk analysis.

The probability of equipment failing or malfunctioning is data often given by the supplier

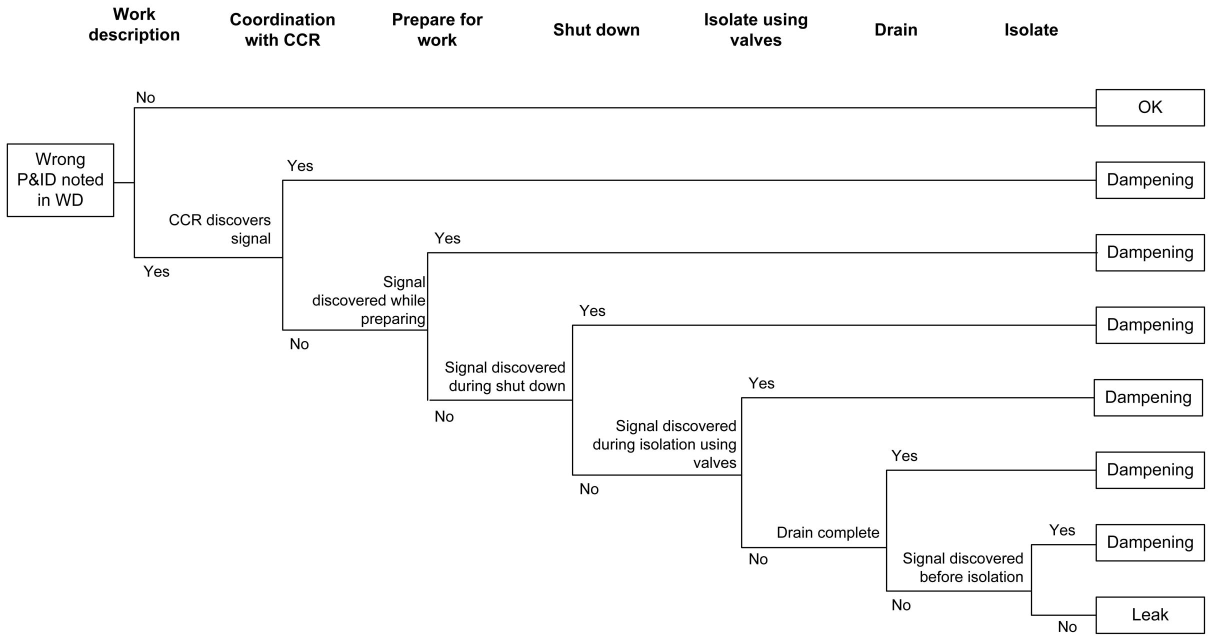


Figure 7.1: Eventtree of FRAM results.

or it can be found by using historical data, the bigger challenge often lies in finding good data for human and organizational failures. Here, a solution could be to borrow some techniques from human reliability assessment methods and organizational factors in risk analysis. Human reliability analysis were developed to provide input to quantitative risk analysis and to integrate human factors into risk analysis. The distinct similarity between classical human reliability analysis and FRAM is how these methods strive to identify performance shaping factors and how these will affect the system. One of the most resent methods in the field, CREAM (The cognitive reliability and error analysis method), also uses common performance shaping factors (CPCs). Another example of finding the data could be using the generic tasks and associated error probabilities from the Human Error Assessment and Reduction Technique (HEART) developed by Jermey Williams (Reason, 1997). This method classifies generic tasks in nine groups that range from totally unfamiliar, performed at speed with no idea of likely consequence to miscellaneous task for which no description can be found. For these groups the nominal error probabilities with 5th to 95th percentile bounds are given. If these classifications are used, a challenge here will be breaking down the functions small enough for this to be applicable.

7.2 Workload in FRAM

Performing a FRAM analysis is a difficult and time consuming process, much of the time used can however be related to the fact that FRAM is a new method, this requires the user to get accustomed to a new way of thinking and will require extra effort. In addition, the method is based on team work, meaning there are several people who need to get acquainted with the method which can make the apparent difficulties of the method appear larger. The method is still not finished, it is still under development and weaknesses are still being worked out and adjusted. With the lack of a detailed step by step explanation of how the method is applied, which more established and tested methods have, it is natural that the method will aquire more time. With more knowledge and experience in using the method it is expected that it will go a lot faster.

Compared to conventional methods such as event trees and fault trees, FRAM is a very time consuming method and it requires more resources. But the extra effort also provides a different output, which can be argued to be of a richer nature. An event or fault tree only considers the connections and dependencies defined (or imagined possible) by the applicant and is performed to quantify these, while using FRAM new connections and dependencies might be discovered. In terms of the output and resources FRAM has more similarities to a hazard and operability study (HAZOP). A HAZOP is a structured and systematic examination of a planned or existing process or operation in order to identify and evaluate problems that may represent a risk. This method, like FRAM, uses teams with knowledge of the method and the system considered and the output is knowledge of how the system may react in certain situations.

7.3 New possibilities of decision support

One of FRAMs greatest strengths is that it provides a good understanding of how the system works. By breaking down the system into functions and seeing how these will affect each other instead of braking it down to components that are considered in solitude with regards to their characteristics, the trap of finding a solution to each cause is avoided and the emphasis is made on providing a more comprehensive view of the interactions and the system as a whole.

FRAM does not include assumptions about specific or typical cause-effect relations, but instead starts with a clean sheet and requires the analysts to identify these. The analysis helps the team ask the right questions before looking for answers, this opens up for the analysts to see new aspects and connections that might have been overlooked when using more traditional methods. In contrast, one of the most used and applied cause-effect relation is the energy and barrier principle which is limited by its view of accidents being caused by uncontrolled energy and layers of protection failing to handle this.

The analysis is not limited to any specific performance or activity, and can be used to model any kind of performance or activity. Already it has been used on “typical” topics from a risk analysis perspective such aviation and nuclear activities. But it has also been used in analysis of a local post office and in the handling of pharmaceuticals in pharmacies.

Imagination is another of the methods great strengths. The construction of the method opens for possibilities and if imagination is used it can give results that otherwise would be unconsidered, limited by automation of the method. The analysis guide the users instead of automating it. By not restraining the thinking to use specified guide words or pre-defined methodology to find the variation and resonance (as HAZOP does), the limitations of thinking are not reduced and provides the analysis with clues as to where to look, but not the answers.

7.4 Limitations and troubles encountered

One of the biggest challenges with the method is, as already mentioned, that it is still quite new and no complete description of the approach exists. The method is also dependent on a team, and as most people who have ever worked in a team knows, teamwork can add great value with several heads thinking better than one, but teamwork is time consuming and the apparent difficulty of FRAM may appear larger in teams.

The methods lack of a definite step by step approach was especially difficult to handle when defining the variability of the functions, since few examples with any detail of how to strategically perform this were found. In most articles describing the use of FRAM, only the results are presented. In addition, the method first used to define variability when FRAM was created, using CPCs, has been replaced by a new method, leaving much of the early examples of uses of FRAM outdated. Some of this difficulty can also be attributed to the fact that describing the variation is based on expert judgment and that there is no right answer, this will always create uncertainty.

When performing a FRAM analysis it is essential to have good knowledge and experience with the process under analysis. The analysis performed in this thesis was done with no hands on knowledge of the process, in addition to no team, this naturally set its limits to the results. A good FRAM analysis is dependent on good knowledge of the process and all the different possible variations of performance. Without personal experience in the process the different “quick fixes” and nuances performed to handle variation in the functions is therefore difficult to know of. The signal followed is therefore limited to the imagination and mostly result in following errors and how they may resonance throughout the system.

Imagination is mentioned as one of the methods strengths, but it can also function as a restraint. Without the ability to free oneself from thinking of only right and wrongs and trying to think out of the box to find new connections and ways of the signal to spread the analysis will end up with a poor result. The analysis is constructed in such a way that it will guide the analyst to where to look for answers, but the analysts are the ones who must conjure the answers. A good FRAM is therefore much relient on good analysts.

The FRAM network can easily become very big, and with this, difficult to handle. There is no strategic way of following a signal throughout the system, and if the network is large with many connections throughout, it is easy to miss a connection and with that, a possibility of resonance can go unnoticed. To handle this it is therefore important to limit the system and functions making the system more manageable. Another obstacle concerning the size of the network and functions was to break the functions down to small enough sub-processes. If the function is “too big” there will be many contributors to the variation and quantification of this will be extensive, making it more likely to miss one.

It is likely to think that the introduction of foreground and background functions was made to handle some of the difficulty of having a big network. However, the experience from testing the method in this thesis the definition of foreground and background gave little contribution in the handling of the network other than making the focal point of the network easier to notice once it was constructed.

When the functions are identified they are described through the six different parameters; input, output, precondition, resources, time and control, which also functions as the connection between the functions as one functions output can be another functions input, precondition etc. Some uncertainties between the differences of some of these parameters were experienced. The parameter precondition is defined as the conditions that must be fulfilled before a function can be performed. The parameter resources is defined by what is needed by the function to process the input, this can for example be procedures, software, hardware, energy, manpower etc., while the parameter input is what the function uses or transforms. When the work description is written marked P&IDs and information on pressure in the system is one of the outputs, this information is needed in the function *Isolate using valves*. If this function does not have this information the function can not be performed, but does it qualify as something needed to process the input, a condition that must be fulfilled to perform the process, or as what the function transforms? There is little problem in finding arguments for this information to fit all of these three parameters. This created some confusion, but since no problems were encountered as a result of functions being connected with either one of the parameters, the conclusion was made that the important aspect is to clearly consider what affects and concerns the function and to understand the dependencies between the functions. As long as this is understood and considered, the choice of parameter used will not affect the result of the analysis noticeable.

7.5 FRAM in relation to STAMP

The history of risk assessment started with the simple linear models focusing on technology, before human factors were included, followed by organizational factors. New methods are developed as new needs are identified an the old methods prove insufficient. FRAM is a new method, but in no way revolutionary and is inspired by many other methods, here some similarities to System-Theoretic Accident Model and Process (STAMP) are presented.

7.5.1 STAMP

The System-Theoretic Accident Model and Process, views safety as a control problem (Leveson, 2004). The model is based on the believes that to prevent accidents, systems need to be controlled so that no system constraint is violated. Instead of thinking in terms of events, STAMP uses constraints as its very basic concept. A hierarchy of control based on adaptive feedback mechanisms, called loops, is constructed to map the behavior of the system and the constraints set to handle this behavior. The system is broken down into several loops, each controlling a phase, action or subprocess in the system. STAMP considers the following system components: hardware, software, people, technical organizational, societal and organizational structures, engineering activities and dynamic factors in modern complex systems. Instead of focusing on certain system components, STAMP analyzes those components in terms of their interactions to each other (Setiadi, 2012).

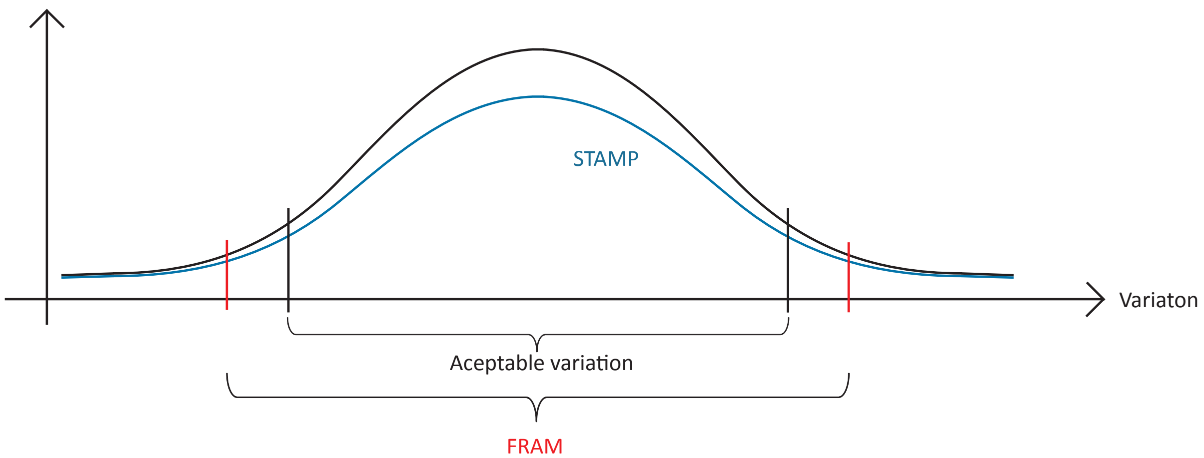


Figure 7.2: Illustration of the difference in handling variability in STAMP vs FRAM.

Much like FRAM, STAMP models the system as non-linear function where the system is broken down to smaller parts and a model of the system is constructed based on the interactions of the different subprocesses defined. The parameters of each system are different; FRAM classifies input, output, time, control, precondition and resources for each subprocess, called functions in FRAM, while the parameters for STAMP are the controller, the activator and the sensors. Both methods constructs a model to identify how the different subsystems may affect each other and how this may result in unwanted events. Both methods also consider the variability and strive to handle this, but how they handle it is somewhat different. STAMPs focus is set on what may go wrong and how to stop this while FRAM, as a method based on RE, focuses more on understanding the system and how a failure occurs, and by doing this increasing the ability to respond to disturbances and irregular and regular threats, and the ability to flexibly monitor whats going on. An illustration of this difference is made, seen in figure 7.2. The figure shows how the variation is reduced using STAMP while the limits of acceptable variation are moved using FRAM.

Chapter 8

Conclusions and further work

8.1 Conclusions

This thesis set out to determine if the Functional Resonance Analysis Method was a suitable model for analysis of process leakages. The method was tested on a description of an operation taken from the BORA studies where pressurized equipment is closed down to remove equipment. In this case a pump is removed from a separation system. The results of testing the method on this system has shown that FRAM is a suitable method for modeling the cause of process leakages. The method gives the analysts the possibility of gaining greater knowledge of the system. One of the great advantages of the method, that separates it from more traditional methods, is its lack of assumptions of typical cause-effect relations and decomposition of the system into components. This opens up for the analysts to see new aspects and connections. This advantage is reinforced by the methods ability to provide the tools for the analysts to ask the right questions before looking for the answers.

The method does, however, have some weaknesses. The method, compared to traditional methods, is time consuming and requires a team effort. Some of the time can be related to the fact that the method is new, this requires the user to get accustomed to the method and a new way of thinking. The fact that FRAM requires a team, may make this apparent difficulty appear larger. The lack of a detailed step by step approach portraying how to perform the analysis does not exist, which can create some confusion and add time to the method. The method is very thorough. When using it, it is important that the constraint and limitations are thoroughly set and the focus of the analysis well specified and understood, so the undesired event does not cover too much which would result in a large network. If the network becomes large it will be difficult to handle. There is no strategic way of following the signal throughout the system, and covering all possibilities can be difficult. This is also important when defining the functions. If the functions cover too much, defining the variability and handling this becomes difficult.

FRAM is developed as a quantitative method, and for the time being there are no established steps formulated for the method to support quantification. Since the method focuses on the likelihood of function variability rather than the probability of a malfunction or failure, a quantification would require some changes to handle this. It should be possible to mathematically construct the network connections and their variability, the problem is finding good functions representing the variability, in other words data. A possible solution that would not require altering the method as it is today is adding an additional step using the results found when examining the resonance within the network. A natural method to use would be an event tree, this is however a linear method and some simplification might be necessary when considering each path of resonance pursued in the quantification. By doing this, the data needed would be on the variability known to create unwanted events. Several event trees might be needed to quantify all the different scenarios and data on both technical, organizational and human variations must be documented.

8.2 Recommendations for further work

FRAM has to this date mostly been applied in aviation studies in addition to nuclear industry and the health industry. The results of this thesis indicate that FRAM is a method suited for process leakages. It would be interesting to test the method on a real system and see if the result will give the workers better understanding of the system and if this again can reduce the leak probabilities. Testing the method on a physical system will also open the possibility of seeing if the quantification provides useful results that coincide with the experience of leakages in the system.

Appendix A

The process in detail

In this appenix the description of the operation taken from the BORA studies is listed.

Work description		Executor	Demands	Possible Faults
		Planning		
1	Receives Work Order (WO)	Planner	Piping and Instrumentation Diagram (P&ID) + Aactivity and control form (AC-form)	
2	Draw up work description	Planner		
3	Requisite resources, materials etc. after need	Planner		
4	Draw up plan for shutdown/start-up	Area-/ operator manager		
5	Draw up valves and blindings -package (V&B)	Planner	V&B drawn up based on WR0218	V&B- list not drawn up, V&B-list is wrong
6	Split point marked in the P&ID	Operations system manager	All connections mounted/demounted must be marked in the P&ID	Split position not noted, Wrong split position noted
7	Draw up V&B list		V&B must include a V&B-list	V&B list not drawn up, V&B list is wrong
8	Valve position marked in P&ID		Valve position described and marked in P&ID	Valve position not noted, Wrong valve position noted
9	Mark blindings on P&ID	Area-/ operator manager	Blindings described and marked in P&ID	Blinding not noted, Wrong blinding noted
10	Draw up AC-form	Planner	Moment values for flange assembly, type of seal and relevant tool info included in the AC-form	AC-form not drawn up Wrong seal type specified, Wrong pump pressure specified, Wrong moment specified

11	Identify and mark common barriers		Common barriers should be marked with ref. to V&B-package and be identified with orange rectangular labels	Common barriers not marked
12	Control and sign V&B package	Area-/ operator manager	Independent QA on the plans with the (Operations and maintenance (O&M) operator	(Quality Assurance) QA not performed, Fault in V&B package not identified
13	Draw up Work Permit (WP), level 1	Planner	WP must be at level 1	WP not drawn up, Inadequate WP
14	Pre-approval of WP	Area-/operations manager, 1st manager, Platform manager	WP at level 1 must be approved by: Manger (onshore) and area manager or the person in place of the area manager. The WP must be treated at the onshore daily meeting before coordination of WP and other simultaneous activities	WP not pre-approved
15	Coordinating with (Centeral Control Room) CCR and other activities	Area-/ operations manager, CCR		Inadequate coordination, No coordination
Preparing equipment/system				
16	Provide the necessary tools, etc.	Technician	The person responsible for the execution is also responsible for the provision of necessary equipment for splitting and assembly, lifting tools and jigs, tools for flange assembly and lubrication	Hydraulic tool not calibrated
17	Finds the correct seal	Technician	The person responsible for the execution must see too that the right seal is available	Chooses the wrong seal
18	Perform operation and maintenance preparation according to the WP	Area technician	Necessary operation- and safety preparations must be done according to the WP and procedures	
19	Process shut down	CCR		
20	Isolate equipment using shutdown valves	CCR / Area technician	Isolate the equipment by closing the specified shutdown valves	Closes the wrong valves, Valve in wrong position
21	Pressure release to torch or other system	CCR	Reduce the pressure by ventilating to the torch	Opens the wrong valve

22	Drain fluid to closed system (including all low points and instrumental pipes)	Area technician	Drain fluid to closed system and drain all low points/inst. Pipes of oil/condensate too closed system and flush with N2 and/or steam	No draining, Inadequate draining, Contact with other HC systems (valve in wrong position/ opens wrong valve/ inadequate procedures)
23	Freeing gas	Area technician		No gas freeing, Inadequate gas freeing
24	Isolation with blindings	Area technician	Requirements for isolation: P<10 Barg: closed and locked, P> Barg: DB&B or blinding	
25	Lock/disconnect valves	Area technician, Instrument technician	Valves are locked where this is necessary	Valve not locked/disconnected, Inadequate locking
26	Disconnect pumps, heat cables etc.	Electro		El. equipment not disconnected, Wrong el. equipment disconnect
27	Label valves	Area technician	All unlabelled valves should be marked in the field. The need of labelling tagged valves in the field is evaluated by the operation system manager. All valves used for isolation shall be durable, clearly and unambiguously labeled	Valve not labelled, Wrong valve labelled
28	Label blindings	Area technician	All blindings affected in the field must be labelled. All blindings used for isolation shall be durable, clearly and unambiguously labeled	Blinding not labelled, Wrong blinding labelled
29	Label flanges to be split	Area technician, Technician	All flanges shall be labelled with WO nr and P&ID nr as a minimum	Flange not labelled, Wrong flange labelled
30	Sign WO form	Area technician		WO form not signed, WO form singed without the equipment being prepared
31	Draw up SJA	Area/ operation manager, Area Technician, CCR, Technician	Evaluate the need of a SJA	SJA not performed, Inadequate SJA, Inadequate involvement
32	Perform operation and maintenance preparations according to the WP	Technician	Technician must perform operations and safety preparations according to the WP and procedures	

33	Work place control and sign WP	Technician	Perform control and through sign confirm that orders will be/ are done	Shortcomings not found
34	Approve work location and sign work permit	Area technician	Control work permit	
35	Authorize WP (activate in SAP)	CCR	CCR evaluates if the work can be started in relations to on-going activities. The authorization to start is given by activating the WP in SAP	
36	Before work call/ review WP	Area technician, Technician	Check that one is on the right equipment, System manager must control draining and that the system is pressure free, Approved WP must be in the work location and a review of this must be done with the personnel involved before the work is started.	
37	Handover between shifts		Requirements in relation to shift change. Communication and coordination meeting held and important decisions documented. Review of planned and on-going activities performed. Ensure that the new shift gets all information on status	Inadequate communication
38	Disconnect safety system	Area technician, CCR	Disconnection of safety system and disconnection/locking of electric equipment must be registered on the WP form or isolation document	Safety system not disconnected
39	Sign splice log			Splice log not signed
40	Keep V&B-list in central space		Updated V&Bs are kept in central place of the plant. Changes in status in V&B are continuously reported in the V&B	
41	Control of spark and ignition sources			Inadequate control of spark and ignition sources

Conduction of maintenance				
42	Control that the flange is the one in question, and that the system is emptied of HC	Area technician, Technician	Operational system manager and technician should ensure that WO is approved, the flange in question Is the correct one, that isolation/binding is performed correctly and that there is no pressure or HC left in the system etc.	
43	Disassembly of flanges	Technician		Work done on wrong system, The system opened still contains pressure
44	Supervision of opening flanges	Area technician	Area tec. should be present when splitting of HC systems is performed. Work in adjacent areas should be stopped.	
45	Sign AC-form	Technician	AC-form signed	
46	Venting tank	Production technician		Inadequate venting, No venting
47	Gas measurement	Area technician		
48	Control of flanges, seal surfaces and tracks.	Technician	Flanges, seal surfaces and tracks are controlled for injuries, corrosion and wear. Control that bolts and nuts are the right material and tagged according to specifications	Damages not discovered on flanges, seal surfaces or tracks.
49	Work performed according to WO	Technician		Work not performed according to WO, Wrong operation of valves
50	Sign form for “work performed”	Technician	If the tank or drum has been opened, the form “internal inspection” must be filled out and approved before the tank is closed.	
51	Control seal, bolts and tracks	Technician	Control that the right type of seal is used and the quality of the material	Wrong seal not discovered, Damages on bolts and tracks not discovered

52	Assembly of flanges	Technician	Skills required: - 3 day course in flange assembly, - Experience with supervision, - > 1 yr since the last course, if its more than 1 yr since the last course, an E-course may be taken	Flange not assembled, Preload to low, Preload to high, Askew assembly, Bolts not locked, Missing seal in flange, Wrong seal in flange, Damage on seal in flange, Inadequate or wrong lubrication of metal gasket
53	Label assembled flanges	Technician	Old labelling is removed and replaced by a new tag on the flange connection with the WO nr. Moment, date, name and sign.	Flange not labelled, Flange wrong labelled
54	Fill inn AC form	Technician	The person responsible for the assembly should fill inn and sign the AC form continuously as the flanges are assembled.	AC form not filled out, AC form inadequately filled out.
55	AC-form saved for a week at minimum.	CCR	The AC-form must be saved for at least a week after the system is in operation	
56	Clean work area	Technician		
57	Sign form " check out before returning equipment after completed work"		The responsible person should fill in the form	Form not filled in, Form wrongly filled in
58	Perform final inspection, sign WP	Technician	Technician should perform a final inspection in the work place and by signing this confirm that the workplace is cleaned and secure	Wrong assembly not discovered
59	Connect safety system	CCR, Area technician	CCR should perform a reconnection with disconnected safety functions where this is relevant and register this in the WP form	Safety system not connected
60	Sign splice log	CCR		Splice log not signed
Resetting system and production start up				
61	Removes blindings	Technician		Forgets to movie blindings
62	Resetting valves	Area technician		Valves not reset
63	Removes labelling on valves and blindings	Area technician	All labels in the field should be removed	Labels not removed

64	O2-freeing	Area technician	O" must be removed to achieve inert atmosphere before tank or equipment is ready for start up, N2 used as flushing gas	O2 not removed, Wrong valve operated
65	Leak test performed	Area technician, CCR	Leak testing should always be performed according to approved specifications/procedures	Leak test not performed, Wrong assembly not discovered in leak test (ex. Wrong seal used)
66	Connect hoses	Area technician	Requirements to standard couplings, labelling, inspection, pressure testing	Use of un approved hoses, Hose not correctly connected
67	Reset valves	Area technician		Valves not reset
68	Disconnect hoses	Area technician		Hoses not disconnected
69	Log possible leakages in relation to the leak test	CCR	All leakages during testing should be logged in a separate system	Leakages not logged
70	Unlock border valves	Area technician, Instrument technician		Valves unlocked before system is cleared, Valve in wrong position, Transmitters not calibrated
72	Connect pumps, heat exchangers etc.	Electrician		Electric equipment not connected
73	Open border valves			Border valves not opened
74	Remove labels on border valves		Labels must be removed	Labels not removed, Labels removed without valve being opened
75	Perform final control and sign WP	Area technician	The area technician should perform the final control on the work place after the work is done. By signing he/she confirms that the work place is acceptable, in addition to the tagging, locks and equipment being removed and is ready for operation	Final control not performed, Inadequacy not discovered
76	Authorize work, sign WP, complete SAP	CCR	CCR will by signing, confirm the completion of the work is authorized by the CCR	Work authorized without being completed, Work completed without being authorized
77	Debriefing			Debriefing not performed
78	Start-up of normal production	Area technician, CCR		Start-up not according to procedures.

Appendix B

Defined FRAM functions for the process

B.1 All functions

In the list below all functions are presented in a more or less chronological order, the number(s) in brackets refers to the activity in the process description found in Appendix A.

1. Draw up work description (1-12):
2. Draw up work permit (13-14)
3. Coordinate with CCR (15)
4. Prepare for work (16-18)
5. Shut down process (19)
6. Isolate using valves (20)
7. Drain (21-23)
8. Isolate (24)
9. Disconnect equipment (25, 26)
10. Label equipment (27-29)
11. Prepare (30-32)
12. Quality check and sign WP (33-35)
13. Disconnect safety system (38)
14. Sign splice log (39)
15. Update V&B (40)

16. Supervision; ignition control (41)
17. Quality control; empty of HC and the flange in question (42)
18. Disassembly (43)
19. Supervision; of opening (44)
20. Status updating; Sign AC form (45)
21. Repairing pump (46-50)
22. Assembly of flanges (51-52)
23. Label assembled flange (53-54)
24. Clean area (56, 57)
25. Final inspection (58)
26. Connect safety system (59)
27. Sign splice log (60)
28. Reset system (61-62)
29. Remove labels; valves and blindings (63)
30. Testing (64-66)
31. Resetting equipment (67, 71, 72, 73)
32. Remove labels; border valves (74)
33. Final control (75-78)

B.1.1 Foreground functions

The following functions are defined as foreground functions:

- Prepare for work (16-18)
- Shut down process (19)
- Isolate using valves (20)
- Drain (21-23)
- Isolate (24)
- Disconnect equipment (25, 26)
- Disconnect safety system (38)

- Disassembly (43)
- Repairing pump (46-50)
- Assembly of flanges (51-52)
- Connect safety system (59)
- Reset system (61-62)
- Testing (64-66)
- Resetting equipment (67, 71, 72, 73)

B.1.2 Background functions

The following functions are defined as background functions:

- Draw up work description (1-12):
- Draw up work permit (13-14)
- Coordinate with CCR (15)
- Label equipment (27-29)
- Prepare (30-32)
- Quality check and sign WP (33-35)
- Sign splice log (39)
- Update V&B (40)
- Supervision; ignition control (41)
- Quality control; empty of HC and the flange in question (42)
- Supervision; of opening (44)
- Status updating; Sign AC form (45)
- Label assembled flange (53-54)
- Clean area (56, 57)
- Final inspection (58)
- Sign splice log (60)
- Remove labels; valves and blindings (63)
- Remove labels; border valves (74)

- Final control (75-78)

Appendix C

Function parameters and variability

In this appendix the different functions and their parameters are specified. In the table below an explanation of the different parameters and the questions answered in terms of variation is listed.

FRAM function	Name of function
Input	Here the input the function uses or transforms is listed, this constitute the links to previous functions
Output	Here the output the function produces, this constituting the links to the subsequent functions is listed
Time	Here what affects time availability of the function is listed.
Control	Here what supervises or adjusts the function is listed. This can be active functions or just plans, procedures and guidelines.
Preconditions	Here conditions that must be fulfilled before a function can be performed are listed. This can for example be that another step or process has been completed or that a specific system condition has been established.
Resources	Here what is needed by the function to process the input is listed, this can for example be procedures, software, hardware, energy, manpower etc
Variability	In this cell the three questions below are answered 1. Which conditions can lead to increased performance variability? 2. Which functions are affected? 3. How can the variability express itself and how may this affect/be affected by other functions?
Comment	If there is any special circumstances or other information relevant for the variability this is described here.

C.1 Function parameters and variability

C.1.1 Foreground functions

FRAM function	Prepare for work
Input	Marked P&ID
Output	System ready for shut down
Time	
Control	Seal must be the correct one, standard operating procedure (SOP)
Preconditions	Work Permit (WP)
Resources	Tools, technician
Variability	1. Competence, stress 2. Process shut down will not be initiated if the system is not prepared, or the isolation will be inadequate 3. Wrong tools, no tools, tools not calibrated, operations not performed according to WP, wrong seal

FRAM function	Shut down process
Input	Coordination with other activities
Output	Process shut down
Time	
Control	SOP
Preconditions	System preparation done
Resources	Central Control Room (CCR)
Variability	1. Work conditions, degradation, communication 2. Pressure release, draining and isolation 3. Process not shut down, wrong process shut down.

FRAM function	Isolate using valves
Input	Marked P&IDs, Pressure
Output	Closed system
Time	
Control	SOP
Preconditions	Process shutdown
Resources	CCR, Area technician
Variability	1. Work conditions, degradation, communication, competence, stress 2. Draining and isolation 3. Wrong valves closed, valve in wrong position

FRAM function	Drain
Input	Work Order (WO), WP, marked P&ID
Output	Empty piping and equipment
Time	
Control	SOP
Preconditions	Draining to closed system
Resources	Area technician, N2/steam
Variability	1. Competence, stress, communication, degradation, work conditions 2. Isolation 3. Wrong valves opened, inadequate draining, inadequate procedures, no flushing, inadequate gas freeing

FRAM function	Isolate
Input	WO, Marked P&ID, Pressure
Output	System isolated with blindings
Time	
Control	SOP
Preconditions	System drained
Resources	CCR, Area technician
Variability	1. Competence, stress, availability of resources 2. Disconnecting equipment 3. Inadequate isolation, wrong flange isolated, isolation not fitted according to pressure.

FRAM function	Disconnect equipment (valves, electric eq. etc.)
Input	Marked P&ID
Output	Valves locked/disconnected, electric eq. disconnected
Time	
Control	SOP
Preconditions	Isolated system
Resources	Area technician, instrument technician, electro, keys
Variability	Inadequate or not locked/disconnected valves/electric equipment 1. Competence, stress, communication, degradation, work conditions 2. Disassembly 3. Wrong equipment disconnected, equipment not disconnected
Comment	The process of disconnecting may cause leakages when it is performed, but this procedure is mostly done to prevent work accidents

FRAM function	Disconnect safety system
Input	Coordination with CCR
Output	Safety system disconnected
Time	No hot work or other activities can be performed simultaneously.
Control	Ignition control
Preconditions	Must be registered on the WP form or isolation document. Splice log signed and SAP activated. Safety preparations performed, signed WP, Location approved
Resources	CCR
Variability	1. Work conditions, degradation, communication, competence, stress 2. Disassembly 3. Safety system not disconnected

FRAM function	Disassembly
Input	Marked flanges, updated V&B list
Output	Pump released from system
Time	
Control	Supervision of opening by area technician
Preconditions	Valves locked/disconnected, electric eq. disconnected
Resources	Tools, technician, equipment prepared
Variability	1. Competence, stress, communication, work conditions. 2. * 3. Work done on wrong system, system still contains pressure, work not done according to WP
Comment	*This function is the last performed in the sequence considered in this analysis and the output is therefore not relevant for any of the functions considered in this analysis. But this may not be the case if the entire process is considered.

C.1.2 Background functions

FRAM function	Draw up work description
Input	WO, P&ID
Output	V&B, AC form, requisition of resources, marked P&IDs
Time	
Control	QA on plan performed by area manager
Preconditions	
Resources	Area manager, planner
Variability	1. Stress and workload may affect the variation 2. Isolate, draw up work permit, coordinate with CCR, Isolate using valves, prepare for work and quality control, drain 3. Wrong notation of blinding/P&ID, seal type, pump pressure moment, split position etc. Common barriers not marked.
Comment	The Work description forms the basis for the entire operation and the output is used in several parts of the process, also in functions proceeding disassembly, which is not considered in this analysis.

FRAM function	Draw up work permit
Input	WO, marked P&IDs
Output	WP
Time	
Control	Approval of WP by area manager and platform manager
Preconditions	
Resources	Planner, Area Manager
Variability	1. Quality of communication, team collaboration quality 2. Quality control, coordinate with CCR, Quality check and sign WP, Prepare for work, Drain 3. Inadequate work permit

FRAM function	Coordinate with CCR
Input	Work description, WP
Output	Coordination with other activities
Time	Dependent on situation, continuous activity competing with other activities
Control	Experience, knowledge of other situations
Preconditions	Other activities known and registered
Resources	Area manager CCR
Variability	1. Work conditions, communication, competence, stress, conflicting goals, available resources 2. Process shut down, disconnect safety system, ignition control 3. Inadequate information/communication, wrong interpretation of information
Comment	Available resources can mean competence caught up in other activities/operations, necessary tool etc.

FRAM function	Label Equipment
Input	Marked P&ID
Output	Marked flanges
Time	
Control	SOP
Preconditions	
Resources	Area technician
Variability	1. Stress, communication 2. Disassembly 3. Wrong, inadequate or no labeling of blinding/valves/flanges

FRAM function	Prepare
Input	
Output	SJA, Equipment prepared, safety preparations performed
Time	
Control	Experience, knowledge to perform SJA
Preconditions	
Resources	Technician CCR, Area technician
Variability	1. Work conditions, communication, competence, stress, conflicting goals, available resources 2. Disconnecting and disassembly 3. WO form not signed, singed but equipment inadequately prepared. Inadequate or no SJA, safety preparations not performed according to WP

FRAM function	Quality check and sign WP
Input	Authorization of WP, Location approved, signed WP, WP activated in SAP
Output	
Time	
Control	
Preconditions	
Resources	CCR, Area technician, Technician
Variability	1. Work conditions, communication, competence, stress, conflicting goals, available resources 2. Disconnecting safety system and disassembly 3. Shortcomings not found, inadequate communication

FRAM function	Sign splice log
Input	Splice log
Output	Updated and signed splice log
Time	
Control	SOP
Preconditions	
Resources	CCR
Variability	1. Communication, stress 2. Disconnect safety system 3. Splice log not signed

FRAM function	Update V&B
Input	Splice log, P&ID
Output	Updated and live V&B list
Time	Must be updated continuously when changes in status of V&B occur
Control	SOP
Preconditions	
Resources	Area, area technician
Variability	1. Communication, stress 2. Disassembly 3. Changes not updated in the list, the list is not kept in a central place ensuring access to all people involved

FRAM function	Supervision ignition control
Input	Coordination with other activities
Output	Control of spark and ignition sources
Time	
Control	
Preconditions	Automatic system functioning
Resources	Ignition control system, CCR
Variability	1. Degradation of system, availability of resources 2. Disassembly 3. Inadequate ignition control

FRAM function	Quality control
Input	WP, P&IDs
Output	Clearance signal to start Disassembly
Time	
Control	
Preconditions	
Resources	Area technician, Technician
Variability	1. Communication, stress, qualifications 2. Disassembly 3. Errors on flange found, Remaining HC in system not found

Appendix D

Pre-studyreport

Pre-study report

Inger Krohn Halseth
inger.halseth@stud.ntnu.no

30. mai 2012

1 Preface

This report constitutes the prestudy of the master thesis - Modeling process leaks using Functional Resonance Accident Modeling (FRAM), written at the Norwegian University of Science and Technology, department of Production and Quality Engineering during the spring of 2012.

The foundation of the master thesis was laid by the work related to the project assignment - Monitoring of Major Accident Risks - Leaks and Fires, which was performed as a literature survey.

2 Background

The existing framework for risk analysis was developed about 50 years ago and is mainly based on the understanding at that time of how accidents happen and the accident models constructed. 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.

2.1 Main objective

The main objective of this master thesis is to deliver a report that reviews process leaks on offshore installation using FRAM. The report should have a focus on understanding if this is an alternative approach, and gaining some experience on the amount of work involved, whether there are different results compared to conventional methods and if quantification is possible and suitable.

3 Project description

The master thesis should be performed as a project, with focus on proper planning and project management throughout the project period. As well as the final report, reports on progress and nonconformance should be produced.

3.1 Problems to be addressed

The master thesis is divided in five tasks listed below with a short comment of how the work is planned to be executed and/or challenges.

1. Literature survey – review and summarize relevant literature on FRAM and become familiar with the assignment.

This task will give a better understanding of the method and is an important foundation for the thesis. Hollnagels books and papers on applied FRAM will be the main source of information.

2. Establish a model for process leaks, based on FRAM. The model will initially be qualitative, but the goal is that it shall form the basis for a quantitative model.

This task is the biggest one and will demand the majority of time spent on the master thesis. The major challenge in this problem is gaining a thorough enough understanding of how leakages occur to be able to model them.

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

This task will be done in parallel with task two seeing as this is information that will be provided while working on problem 2.

4. Assess the model developed and the work performed in terms of:

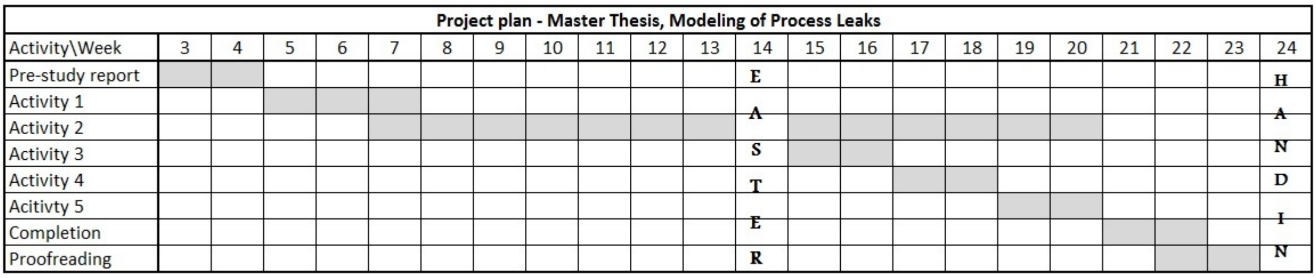
- **a)** The amount of work, compared to conventional methods of analysis.
- **b)** Determine new possibilities of decision support given by such a model compared with conventional methods of analysis.
- **c)** Determine if quantification is possible given such a model, and if so, the new types of data required to do so.

This, like task 3, will be done in parallel with task 2.

5. Summarize, conclude and give recommendations for further work

4 Work Scope

The master thesis is done over 20 weeks, how these weeks will be distributed between the tasks, completion and proofreading is shown in the table below. The activity planning includes start up, planning the project and writing the pre-study report. Completion consists of writing the preface, introduction, abstract and conclusion. How the time is distributed between the different activities is shown in the table below.



Figur 1: Distribution of resoruces

4.1 Mile stones

Seeing as task 3 - 5 will be written as a biproduct of task two, they are not assigned a given finish date. The following milestones are thus established:

06.02.12 Hand inn of pre-study report

30.03.12 Hand inn of progress report

17.02.12 Task 1 completed

18.05.12 Task 2 completed

01.06.12 Done producing text

11.06.12 Hand in

Appendix E

Progress report

Progress report

Inger Krohn Halseth
inger.halseth@stud.ntnu.no

May 30, 2012

Progress

The work that has been done has not yet deviated from scheduled plan as presented in the pre-study report. Some changes have however been made to the plan, as seen in figure 1.

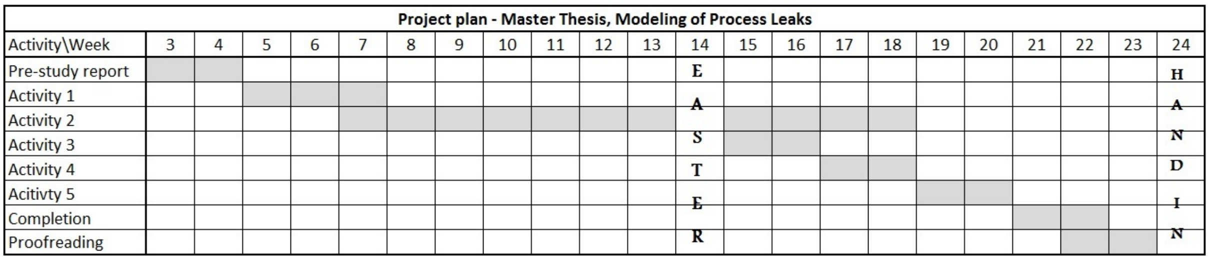


Figure 1: Changes in the progress plan

The work on the literature study has gone according to plan, but the time used to understand and break down the process considered has been more time consuming than first anticipated. Task 2 is the most time consuming task in the thesis, as reflected in the project plan. The extra time used to understand and breakdown the process is not reflected in the project plan because this is only a small part of task 2. To make up for this time there will be made no changes in the project plan, but the remaining time on task 2 must be spent more efficiently to make up for this.

The finishing time of task 2 is reduced, this change does not mean that less time will be spent on task 2, but is made to reduce the amount of multitasking, seeing as the need to finish this and focus on the following tasks is pressing. Task 3-5 all depend on task 2, and it is therefore important that this task does not change much when the consequent tasks are started. By moving the deadline for task 2, time used working on several tasks at once is reduced, and focus can be made on one task at the time.

Mile stones

The only change in the revised milestones is that the milestone concerning the finishing of task two moved two weeks back.

06.02.12 Hand inn of pre-study report

30.03.12 Hand inn of progress report

17.02.12 Task 1 completed

07.05.12 Task 2 completed

01.06.12 Done producing text

11.06.12 Hand in

References

Herrera, I. A., Håbrekke, S., Kråkenes, T., Hokstad, P. R., and Forseth, U. (2010). Helikoptersikkerhetsstudie 3 (HSS-3). Technical report, SINTEF Teknologi og samfunn.

Hollnagel, E. (2004). *Barriers and Accident Prevention*. Ashgate Publishing.

Hollnagel, E. (2005). Functional resonance accident model, method and examples. In *The Open Initiative for Next Generation of Probabilistic Safety Assessment*.

Hollnagel, E., Pruchnicki, S., Woltjer, R., and Etcher, S. (2008). Analysis of comair flight 5191 with the functional resonance accidentmodel. In *Paper published at the 8th International Symposium of the Australian Aviation Psychology Association, Sideny*.

ISO 31000 (2009). *Risk management - Principles and Guidelines*. International Standards.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Sience*, 42:237–270.

Macchi, L. (2010). *A Resilience Engineering approach to the evaluation of performance variability: development and application of the Functional Resonance Analysis Method for Air Traffic Management safety assessment*. PhD thesis, ParisTech.

MIL-STD-882D (2000). *Standard Practice for System Safety*. Department of Defense, United States of America.

Nouvel, D. and Travadel, S. (2007). Introduction of the consept of functional resonance in the analysis of a near-accident in aviation. In *Author manuscript published in 33rd ESReDA Seminar: Future challenges of accident investigation, Ispra, Italy*.

NS-EN 13306 (2010). *Maintenance, Maintenance terminology*. Standard Norge.

PSA (2010). Risikonivå i norsk petroliumsvirksomhet – sammendragsrapport – utviklingstrekk 2010 – norsk sokkel. Technical report, Petroleum Safety Authority Norway.

Reason, J. (1997). *Managing the risks of orgnizational accidents*. Ashgate Publishing Limited.

Reisman, A. (1988). On alternative strategies for doing research in the management and social sciences. *IEE Troansactions Engineering Management*, 35:215–220.

Setiadi, R. (2012). Stamp accident model for safety engineering: A critical analysis. Website: http://www.robertsetiadi.net/articles/stamp_analysis.htm.

SN-ISO Guide 73 (2009). *Risk management, Terminology*. International Standards.

Wikipedia (2012). Nonlinear-systems. Website: http://en.wikipedia.org/wiki/Nonlinear_system.

Wolter, R. and Hollnagel, E. (2008). Functional modeling for risk assessment of automation in a changing air traffic management environment. In *Paper presented at the 4th International Conference Working on Safety, Crete, Greece*.

Woltjer, R. (2012). Resilience assessment based on models of functional resonance. Website: http://www.resilience-engineering.org/RE3/papers/Woltjer_text.pdf.

Woltjer, R. (n.d.). *Functional Resonance Accident Model plug in for Microsoft Visio*. Linkjöping University.