NTNU – Trondheim
Norwegian University of
Science and Technology

Modeling Process Leaks Offshore Using STAMP and STPA

Filip Hoel

Product Design and Manufacturing
Submission date: June 2012
Supervisor: Stein Haugen, IPK

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

MASTEROPPGAVE
Våren 2012
for
stud. techn. Filip Hoel

MODELLERING AV PROSESSLEKKASJER OFFSHORE MED BRUK AV STAMP OG STPA
(Modeling process leaks offshore using STAMP and STPA)

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

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

Oppgaven skal gjennomføres i følgende trinn:

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

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

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

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

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

Forstudierapporten er en del av oppgavebesvarelsen og skal innarbeides i denne. Det samme skal senere fremdrifts- og 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

Per Schjølberg
førsteamanuensis/instituttleder

Stein Haugen
faglærer

Preface

This is a Master's thesis carried out in the spring semester of 2012 as a part of the Master's degree study in RAMS, at the department of Production and Quality Engineering. The thesis revolves around the emerging risk analysis model STAMP and the belonging method STPA, with the main objective to develop a qualitative and a quantitative model of leakages during maintenance of pressurized hydrocarbon processing equipment. It simulates a real life practical situation, but the thesis is mostly a theoretic study.

I would like to extend my thanks to Professor Stein Haugen for his help and supervision of this thesis, as well as my friends at the office for making this semester enjoyable.

Trondheim, 11.06.2012

Filip Hoel

Summary

The industry is rapidly evolving, and getting more complicated and comprehensive with the time by creating dynamic systems that intertwine technical components with humans. Existing models for risk modeling and assessment are lacking in their ability to include human and organizational error to the necessary extent. Further, they struggle to keep up with the complex interaction between different components of a system as well as the high pace of change, and at the same time assess specific components and directs blame, thus prevent a healthy creation of a safety culture. An accident model that tries to accommodate these challenges is the systems-theoretic accident model and processes (STAMP) and the belonging method system- theoretic process analysis (STPA).

STAMP builds upon three basic principles: Hierarchical safety control structures, safety constraints, and process models. The intention is to view the connection between hierarchical levels as constraints towards the activities below, thus the approach to a safer system is through enforcement of constraints. The STPA is an method developed to include the causal factors identified in the STAMP by utilizing control loops.

To test the STAMP, leakage of hydrocarbons as a result of maintenance work related to pressurized process equipment is chosen as an appropriate hazard to analyze. This hazard has little to no improvement in number of occurrences over the past years, and is recognized as a complex procedure with a lot of human interactions.

A STPA of the maintenance procedure is developed, thus giving the possibility to discuss and assess STAMP to a greater depth. The model present a different view on risk analysis by focusing on surroundings, constraints, and interactions rather than physical components and their specific failure. This affords new opportunities related to decision making support. Concerns are mostly related to the method being resource heavy and demanding on the analyst, with a high possibility of making the models difficult to follow.

The attempted solution of implementing quantitative risk analysis into a STPA involves event trees and reliability block diagrams. It is theoretically plausible, but a challenge is to find suitable data, especially concerning human errors.

Sammendrag

Industrien blir mer komplisert og omfattende med tiden ved å skape dynamiske systemer som endres i hurtig tempo, og integrerer tekniske komponenter med mennesker. Eksisterende modeller for risikoanalyse mangler en tilstrekkelig evne til å inkludere menneskelige og organisatoriske feil. De sliter også med å holde tritt med det komplekse samspillet mellom de ulike komponentene i et system og de hurtige endringene som foregår, samtidig som modellene evaluerer spesifikke komponenter og retter skyld mot den enkelte. Dermed hindres utviklingen av en sikkerhetskultur. En risikomodell som prøver å imøtekomme disse utfordringene er “systems- theoretic accident model and processes” (STAMP) og den tilhørende metoden “system- theoretic process analysis” (STPA).

STAMP bygger på tre grunnleggende prinsipper: Hierarkiske sikkerhetskontrollerende strukturer, sikkerhetsrestriksjoner og prosessmodeller. Hensikten er å benytte koblingene mellom ulike hierarkiske nivåer som restriksjoner mot underliggende aktiviteter, for dermed å oppnå et tryggere system via håndheving av restriksjonene. STPA er en metode utviklet for å inkludere de kausale faktorene i STAMP ved å utnytte reguleringssløyfer.

For å teste STAMP, er det lekkasje av hydrokarboner som et resultat av vedlikeholdsarbeid knyttet til trykksatt prosessutstyr som er valgt å analysere. Denne faren har vist mangelfull forbedring i antall tilfeller de siste årene, og er ansett som en kompleks prosedyre.

En STPA av vedlikeholdsprosedyren har blitt utviklet, og den har gitt muligheten for en grundigere diskusjon og vurdering av STAMP. Modellen presenterer et annet syn på risikoanalyse ved å fokusere på omgivelsene, begrensninger og interaksjoner fremfor fysiske komponenter og deres spesifikke feil. Dette gir nye muligheter knyttet til beslutningsstøtte. Bekymringer er hovedsakelig ressurskrav og utfordrende gjennomføring for analytikeren, med en stor mulighet for at modellene blir uoversiktlig.

Et forsøk for å gjennomføre kvantitative risikoanalyser i en STAMP er gjort ved implementering av hendelsestrær og pålitelighetsnettverk. Det er teoretisk sannsynlig, men en utfordring er å finne egnede data, spesielt for menneskelige feil.

Contents

List of Figures

Chapter 1

Introduction

1.1 Background

Existing frameworks for risk analysis were developed about 50 years ago and are largely based on the understanding of accident modeling and how accidents occur at that time. The industry has evolved a lot since then. Technical systems have become more complex and are more commonly used, humans have more interaction with the machinery and need to work alongside them rather than with, and the organizations that supervise and control the processes are at a greater scale than ever. It has evolved into what is popularly called a sociotechnical system, a highly complex work environment where machinery and humans coexist.

To cope with the sociotechnical system, alternative understandings of accident causation have emerged. New frameworks need to be developed, where interactions and connections between each contribution in the systems are manageable, dynamic adaptability is possible, and reduction of hazards are a result. Major accidents rarely happen, and there is seldom a second chance. That is why the existing models' emphasis on accident investigation need to take a back seat for the actual risk analysis that contributes to accident reduction before they occur. An accident model that tries to fulfill these requirements is the systems- theoretic accident model and processes (STAMP) and the belonging method system- theoretic process analysis (STPA).

1.2 Objectives

In this thesis, the main objective is to test STAMP and STPA on a concrete hazard at an offshore installation. The hazard is leakage of hydrocarbons as a result of maintenance work related to pressurized process equipment. The purpose of this thesis is to:

1. Present relevant literature about STAMP and STPA, and address the challenges.
2. Establish a model for leakage, based on STAMP/STPA. The model should be qualitative, but the goal is to form a basis for quantitative assessment.
3. Identify data requirements for such a model and assess the availability of data necessary to quantify risk.
4. Consider the developed model and the performed work in terms of:
   (a) Work scope, compared with traditional methods of analysis
   (b) New possibilities related to decision making support, compared with traditional methods of analysis
   (c) Whether quantification is possible with such a model, an if so, which new types of data must be provided to quantify the results.
5. Recommendations for further work.

The thesis takes a slightly different turn compared to the initial objectives. Instead of strictly identifying data requirements to a potential quantification process, it is attempted to create a way of quantifying risk by using the STPA as a framework. Hence, the focus of this thesis is more directed at a possible solution to quantify risk, and then use this solution to identify data requirements.

1.3 Approach

Obtaining necessary understanding of the challenges and the STAMP/STPA is the initial goal, but acquiring proper depth about the sociotechnical system is just as important to understand the general challenges. Especially considering that the maintenance procedure has a high risk of experiencing human error, thus the emphasized, additional, focus on human error in this thesis.

Chapter 2 is mostly a worked version of the one used in the authors previous project thesis (Hoel, F. , 2011). The literature used consists largely of work done by the professors James Reason, Jens Rasmussen and Erik Hollnagel. Reason and Rasmussen is regarded as one of the most influential contributors within human error research, and most of the articles containing human error theory have references to them. The same is with Hollnagel regarding resilience engineering theory.

Theory of STAMP/STPA consists mostly from the recently published book by Nancy Leveson, Engineering a Safer World (Leveson, 2011). Being a fairly new addition to the understanding of accidents, the method is largely driven by Leveson. Seeing that she has contributed to a major part of the scientific literature regarding STAMP/STPA, the book is considered as the most updated literature, representing the cumulative work done over the past years, of the STAMP/STPA available for public reading.

Following the initial goal is to gain necessary understanding of the process meant to model. To describe the process of maintenance on pressurized process equipment and how this can lead to leaks, literature and documents has been provided by the supervisor. Some of the documents contain confidential material, thus very little reference is given to support the superficial description of the maintenance procedure.

With the theoretic foundation acquired, an attempt to develop a qualitative and quantitative model is done.

1.4 Limitation

The work done in this thesis is relatively superficial, some part due to the confidential details of a more thorough analysis, but mostly because this is an attempt to see possibilities, opportunities and challenges with the STAMP/STPA, and ultimately learn something from applying theory. This is not necessarily done by a really thorough analysis, and the amount of work would probably be too great concerning the scope of the thesis.

1.5 Overview of the Thesis

The thesis starts out by elaborating the very nature of human error, challenges related to sociotechnical systems, and the emerging philosophy of resilience engineering to give a proper understanding of the fundamentals of the emerging risk analysis paradigm. Further, the thesis describes the theory behind the STAMP and STPA, before a generalized maintenance procedure is described. After elaborating the theory and issues regarding the maintenance procedure, the thesis describes how the specific qualitative STAMP and STPA analysis has been done step by step. Some own modifications to the model have been made, but they are thoroughly described. Following the qualitative model is the attempt of developing a quantitative model. The thoughts surrounding the model and its creation are discussed together with an assessment of the data availability used to quantify risk. In the end, the thesis is concluded and discussed.

In brief, chapter 2, 3, and 4 are constituted by theory, while the models and discussion presented in chapter 5 and 6 represent the author's own contribution to research.

It is worth to mention that most of the figures and models used in the thesis are rather large, so they are placed in the appendix, and some of them in various sizes.

Chapter 2

The New Paradigm

2.1 Normal Behavior

2.1.1 The Human Mind

"The human mind is prone to match like with like. It is therefore natural for us to believe that disastrous accidents must be due to equally monstrous blunders." (Reason , 1997, p 21)

Rarely, human people want to make mistakes. Those with the malevolent or neglecting attitude towards safety stands as an exception, thus the focus will remain on the majority of people who wish others no harm. Reason (1990) argues that the errors these sensible people make can be broadly put in two categories, slips and mistakes. Slips are the errors that emerge from the actions that does not go according to plan, while the mistakes explain those where the plan itself is lacking. Further, the mistakes are split in two categories, rule-based and knowledge-based mistakes, thus creating the three error types (Reason , 1990, p 53), (Reason , 1997, p 70):

- Skill-based slips (SB): Routine, highly-practiced tasks, automatic fashion. This is what people are very good at most of the time.
- Rule-based mistakes (RB): When a need to modify behavior because of some change in the situation. Apply memorized or written rules, like if-then do.
- Knowledge-based mistakes (KB): Only when failing to find some pre-existing solutions.

Given time and forgiving environment, usually good solutions. Not in case of emergency.

SB and RB errors work the brain in one of the two control modes that is named the automatic mode. The automatic mode process actions fast and works in parallel to other thoughts. This runs great for most practiced tasks and known situations. KB errors, on the other hand, is more related to the second of the control modes, the conscious mode: A highly demanding and restricted mode, but potentially very smart (Reason , 1997). This is one of the reasons why safety measures have a tendency towards emphasizing structured and practiced tasks, because in a case of emergency it is a great advantage to be able to use the automatic mode in order to achieve swift and effective actions.

In many events after accidents, investigations discover that there should be enough warning signs to identify, and possibly prevent, the accident. From there on it is a huge commotion in trying to explain/defend how this could have happened. What many people fail to notice is that observers armed with the outcome knowledge of an accident view the events in a complete different perspective than the active participant at the time the accident supposedly should have been avoided. According to Reason (1997, p 38) several studies have shown that:

- people greatly overestimate what they would have known in foresight
- they also overestimate what others knew in foresight
- they misremember what they themselves knew in foresight

Put differently, what might be obvious in present is not necessarily obvious in the past. This is easily recognizable in bigger companies where communication and knowledge of the 'bigger picture' could be very bad. At the same time, while in the automatic mode, as the name suggests, actions could be made without much recognition of what is actually happening. If a hundred workers act at an offshore installation in everyday manner, there is really no reason why they should notice even the enormously big warning signs unless they interfere with their work. This is an argument for initiating work activities that involve either the use of the conscious mode or people especially trained to discover potential dangers.

In order to perform a task correctly there is usually only one or a couple of ways to do this. The same goes for the subtasks needed to perform the task, meaning that there is an opportunity to stray along a multitude of unintended or inappropriate pathways in performing that simple task. But regarding the potential, human error is not that varied or ample. In fact, errors occur in a surprisingly limited number of forms compared to the vast potential, and errors take place much more seldom than correct actions (Reason , 1990). Studies of absentminded slips in everyday life has, according to Reason (1997), shown that the most common omission is 'premature exits' that happens when people get preoccupied with the next task. The top four is as follows (Reason , 2008, p 112):

1. Premature exit
2. Lack of cueing
3. Goal achieved before the last task is complete
4. Out of sight, out of mind

This is one of the reasons why maintenance is a major source of human error, and mostly during the reassembly process. Maintenance is usually strongly based on procedures, and in bigger firms there is no guarantee that the person who began the maintenance will be the one to finish it, making it easy to do small mistakes. On the other hand, by being highly proceduralized, it is in principle easy to identify the most vulnerable steps to omission, although necessary effort is required.

2.1.2 Reaction and Measurement

Whatever the reason, when someone performs badly, other people attribute this to their personality. The observing people might instigate that he/she is stupid, incompetent, careless, reckless, and so on. Because of this, it is easy to blame humans for those 80-90 % on human error, because "humans perform badly". But if they were to confront the person of their behavior, surly they would deny these accusations and blame their behavior on the local situation and circumstances provoking the performance. Of course, the reality is probably somewhere in between, but the point is that it is easy to forget that errors comes in a multitude of shapes, have different psychological origins and happens in different parts of a system that require different methods of management. In this sense, people's behavior is more constrained in these hazardous environments than it is in the everyday life that they are compared to. (Reason , 1997)

From an organizations point of view, the real challenge comes from the method of measurement. A common method is to rely upon negative outcomes to measure safety. Unfortunately, not only is this an unreliable indication of a system's intrinsic safety, but it also emphasize the aspect of blaming the people seemingly responsible for the accident (Reason , 1997). The problem with this method is that accidents (usually) occur seldom, and the feedback from the measurement will not be anything more than "noise" rather than "signal", and therefore not able to recognize pending troubles before it is too late. Measurement of negative outcome would be a valid safety index in an utopia where the managers of a system had complete control over all factors that could possibly create an accident.

Another reason is the aspect of luck. An organization can have the best possible protection against accidents and have a strong safety culture, but still be unlucky and have a major accident. Likewise, an organization could have a disastrous approach to safety management and culture, but still be lucky enough to escape any accidents. It is nice to know, but with that said, luck is not something that can be comprehended to a usable level, implying that it should rarely, if ever, be used as an element in risk management.

At the same time, luck or not, the best people tend to make the worst mistakes. This can be explained by their urge to push the limits of existing practice by trying out new techniques, multi-tasking and generally trying to be as effective as possible, thus making them easily distracted or preoccupied (Reason , 2008). In theory, this might be wrongdoing in the eyes of the managers, but in practice this is exactly what you wish from a co-worker.

2.1.3 Weakness of the Total System

A major feature involving human fallibility is the fact that similar situations provoke similar types of error and recurrent accident patterns involving different people . If we are to understand and prevent these situations from occurring, it is necessary to look beyond the actions on the spot and examine the weakness of the total system (Reason , 2008). For example, one of the most common elements in all types of human error is under-specification, whether it is inattention, forgetting, incomplete knowledge, ambiguous feedback from sensory data to mention some. Of course, you could tell the people to straighten up and get it together, but this would in most cases not work. It would probably be more productive to analyze the situation and see if there are any changes to the system that might help with specification.

According to Reason (1997) the cognitive system is good at remembering regularities and reapply them whenever they are needed. This is why proper training in specific situations is stressed in creating a safety culture. People are also quite good at ignoring irrelevant events in their immediate surroundings and rather focus their attention on the task at hand. At the same time, people manage to process two physically distinct concurrent sources of information if the ambiguity is low, but switching attention takes time and results in an interval where accidents are more prone to happen (Reason , 1990).

What is strange about these facts, is that most of them are well known, but still many models used by the risk managers approaches safety issues from a top-down perspective focusing on the component level, and not the operators that operate them, and neglecting these simple facts when creating the rules and methods. These models can be very useful to support actors and decision makers in an isolated perspective, but not very useful for analyzing the presence and operation mode of the total system (Rasmussen, 1997).

> *"Control of activities and their safety by the classic prescriptive command-and-control approach deriving rules of conduct top-down may be effective in a stable society where instruction and work tools at all levels can be based on task analysis. In the present dynamic situation, this approach is inadequate and a fundamentally different view on system modeling is required."* (Rasmussen, 1997, p 185)

2.1.4 Safety Space

Compared to earlier years, today's society revolves at a very fast pace of change. The innovation and development of new technology in the operative level of the society constantly changes, and this pace of change is much faster than the pace of change a rigid management structure is able to follow. At the same time, the scale of industrial installations steadily increases, same with the integration level and couplings of different systems, thus potentially making the consequence of a single fault decision highly dramatic. Combine this with the fact that companies today have to endure a very aggressive and competitive environment, and we have a model for disaster, not risk reduction. A consequence of this is that laws, rules, practices and instructions from the management system are outdated and practically never followed to the intended extent, probably securing a huge contribution to accidents in the name of "human error" (Rasmussen, 1997).

To fight this management challenge, Reason (1997), (2008) and Rasmussen (1997) introduces a method Reason conveniently names "safety space". Rasmussen (1997) argues that human behavior have many degrees of freedom in how to successfully perform a job, but they are constantly pushed around by administrative, functional and safety related constraints, creating a tiny space of movement freedom. In this movement space the workers are supposed to do their work the way experience have taught them to do it, the most efficient, practical and safe way unrelated to the strict regulations and rules.

Rasmussen's model (see figure 2.1) suggests that the actors within an organization is confined by the surrounding boundaries, which is the economic, work load and acceptable work performance. At the same time, different forces pushes the actors around inside this safety space the boundaries create, such as managers wish for efficiency, workers wish for least amount of effort, and campaigns for increased safety (Rasmussen, 1997).

Reason (1997) mention the organizations placement in the safety space, thus creating an oval which represent the boundaries of possibilities (see figure 2.2). The right side represents the most vulnerable state concerning safety, while the left side the most resistant state. The thought behind the oval structure is that most organizations find themselves in the middle, and fewer stay to either extremes.

By modeling the accidents according to the safety space view changes the approach to system performance improvement. Instead of fighting irregularities and deviations from a strictly pre-planned path, the attention should be given to make the boundaries as distinctive as possible and develop coping skills at boundaries (Rasmussen, 1997). This practice would not remove the accidents from happening, but it would keep the company more flexible to change and, in theory, strengthen the adaptability to risky situations. This is because what produces stable outcome, concerning safety, is the constant change rather than continuous repetition, if one changes a system parameter it must be compensated for by changes in other parameters (Reason , 1997).

Fast and constant changes are also the reason why very few organizations occupy fixed po-

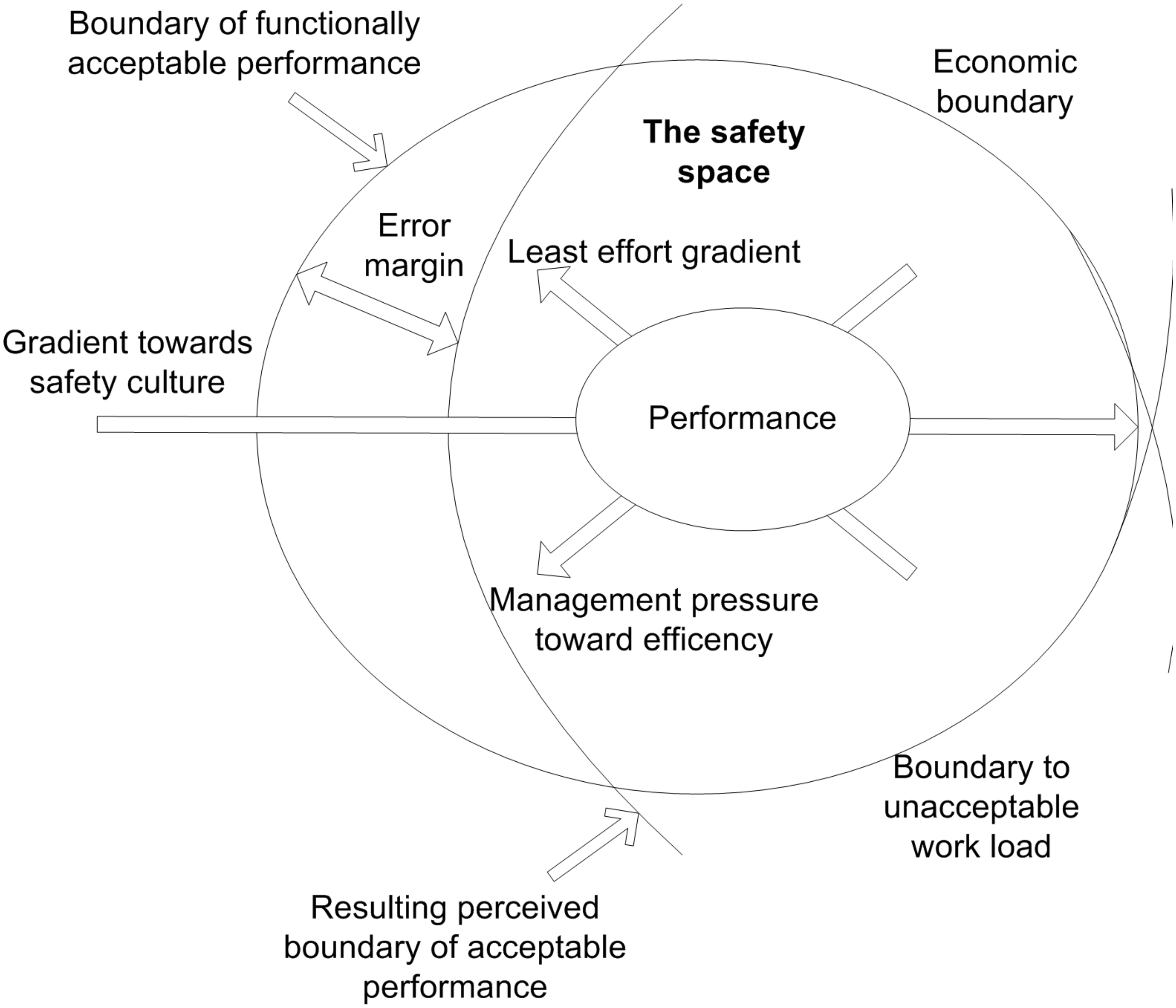

Boundary of functionally acceptable performance
Economic boundary
The safety space
Error margin
Least effort gradient
Gradient towards safety culture
Performance
Management pressure toward efficency
Boundary to unacceptable work load
Resulting perceived boundary of acceptable performance

Figure 2.1: Rasmussen's safety space (Rasmussen, 1997, p 190)

sitions in the safety space (Reason , 1997). A major point in the safety space model is that just gaining a greater safety position is not that difficult, but the real challenge is to sustain this position. This is why having both reactive and proactive measures are important to have as "navigational aids" from both the conditions at work, and the different defenses/barriers. (Reason , 1997, p 115)

With that said, an important feature to the safety space model is that it seeks an attainable safety level within its boundaries, not zero accidents. Many organizations approach safety management the same way they treat production, just in a negative view. The main purpose is to create a focus on the positive side of safety (not number of deaths, accidents, near accidents

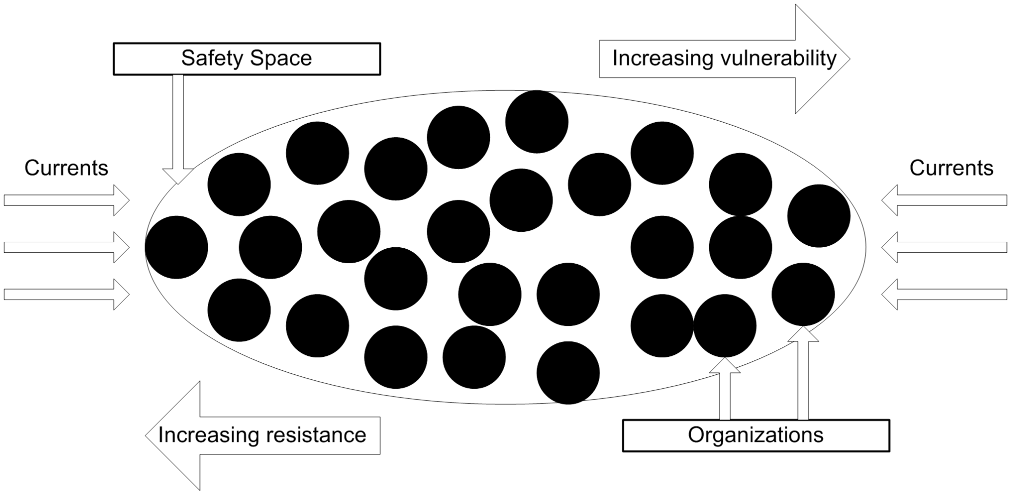


Figure 2.2: Reason's version of the safety space (Reason , 1997, p 111)

and so on), that relates to the system's intrinsic resistance to its operational hazards. Instead the organizations should improve the basic processes that are known to influence the probability of accidents, like design, maintenance, planning, procedures, budgeting, communication and scheduling to mention a few (Reason , 2008, p 267,275)

To navigate towards the "righteous" end of Reason's safety space, there are three driving forces, "the three Cs", pushes the organization: Commitment, competence and cognizance. Commitment is whether decision makers will act properly, and includes two main components: Motivation, whether the to strive to be a role model or merely keep one step ahead of regulatory sanctions, and resources, not just money but also the caliber and status of those who are assigned to the risk management task. Competence is not necessary the knowledge, but also the skills and know-how to act quickly and effectively in the work context. Cognizance is the understanding of the struggle for enhanced resilience, for example that a lengthy period without events is not necessary safe enough (Reason , 2008), (Rasmussen, 1997). Further, there are "the four Ps" of organizational management (Principles (philosophy), Policies, Procedures, Practices), devised by Degani, A. and Wiener, E. L. (1994), that in combination with the "Cs" makes twelve sets of indicators that can be used to navigate the safety space (e.g. principles combined with commitment: Safety is everyone's responsibility and a primary goal. Management accepts errors and safety is a high level meeting on a regular basis).

Conveniently, the twelve indicators can be expressed as one: Create a safety culture. Easily said, although *"few things are so sought after and yet so little understood."* (Reason , 1997, p 191). All the indicators can be categorized by the four critical subcomponents of a safety culture that is a reporting, a just, a flexible and a learning culture. The easiest way to implement such a culture is to apply continuous pressure on achieving this mindset of everyone involved. This is not easily done, however, but the awards could just be worth it.

2.2 The Existing Methods

The thoughts generated around the safety space have spurred a paradigm shift in the way to approach risk analysis from looking at specific component failure to failure of the system as a whole. The new paradigm have an urge to consider what is called a sociotechnical system, a system where humans and their habits are an integrated part of the technical system, thus the need for a joint optimization of both the technical and social aspects of the system to meet the organizational objectives (Qureshi , 2008). The existing models based on the barrier concept (such as FTA and ETA) are terrific at the specific component part with a binomial status (work/fail), but really struggle to keep up with the sociotechnical systems.

The greatest advantage of the existing methods lies in their simplicity. They are easily performable, understanding the methods are usually simple even for those who have not performed the work, and the methods are mostly versatile enough to combine with each other. This is also the core of their greatest weakness. With the development of more complicated high-tech systems combined with a fast pace of change, these methods struggle to keep up. Of course, the simplicity could make up for the pace of change if the system is less complicated, but a more intricate system seldom needs the addition of some branches to the fault tree. To recreate a complete system for each possible situation demands valuable resources, so having a method with the possibility of easy update and evolve with the system would be a great advantage. This multiplies if you consider the system to be at the dynamic level of a sociotechnical system. A constant change in status and situation is not applicable with the existing methods, especially if human and organizational behavior is involved, because the multitude of possible actions is too great to assess with a simple binomial failure approach.

This brings forth another challenge related to the existing models, the lacking ability to actually analyze complex systems. They were developed mainly as a tool to recognize and calculate component failure, but have a hard time to recognize interactions and indirect relationship between specific failures and their influencing factors needed to understand why accidents occur. Other than human errors, the existing methods do for example not work very well for software errors, system design errors, management flaws, and they must work hard to recognize component interaction accidents and organizational factors (Leveson, 2011). Of course, it is possible to include human behavior in the analysis, for example as a basic event in a fault tree or a barrier in an event tree, but mapping this the same way as a component failure easily directs the focus on the specific human failure, and not the weakness of the total system. This way it is imminent to alter the perspective towards blaming humans for their mistakes, and this is not a great contributor in creating a safety culture.

A real challenge lies in capturing the essence of a dynamic system. To be able to keep up with a huge complex system, including both highly technical components and humans with fluctuating behavior, and at the same time keeping in touch with a diverse network of possible interactions and relationships, is by no means an easy task. Most of the existing models approach system failure at a component level, and assess the failures in a binary way that does not represent real life situations. To get the grasp of a sociotechnical system it might be a good idea to take a step back from the specificity, to rather gain an impression of the total system. And if the system where to be understood as a complex, dynamic flow, in contrary to a work/fail methodology, it could be wise to discard the binary approach to risk assessment.

With a new paradigm, there is a necessity of new models able to cope with the demands. The main criteria for a new framework should be to comprehend a dynamic system and recognizing the connection between different functions, including both the human and technical. A very important detail is to include this in a way that does not delegate blame, but strengthen the rise of a safety culture. Further, discarding a binary approach to the risk assessment to accommodate the complexity of the systems could prove to be useful. Lastly it needs, of course, to find the risks and help increase safety, assisting in the creation of a safety culture.

With that said, it does not mean that the existing models have no use in the new paradigm. Yet again, the simplicity is a key factor, because this makes them easier to evolve into, or become a part of, a new, more suitable method.

2.3 Resilience Engineering

Resilience engineering is a perspective on risk management emphasizing proactive monitoring, and creating flexible and robust processes that cope with real life complexity. Both failure and success are the outcome of normal performance variability, and performance variability is both normal and necessary. That is why safety must come by controlling performance variability rather than constrain it, and the focus should be on studying the causes to failures and success to try and alter the variability of the outcomes, preferably in a positive manner. A resilient system is a practitioner of this principle, and is defined by its ability to adjust its functioning prior to or following changes and disturbances. This results in a system that is capable to continue its functions even after interruptions and in presence of continuous stresses. (Hollnagel et al., 2008a)

According to Hollnagel et al. (2008a), (2008b), resilience engineering is about the factual, the critical and the potential, thus the quality of resilience within a system can be defined by the four following abilities, also known as the four cornerstones of resilience:

1. The ability to respond to regular and irregular threats as well as various disturbances. Ready-made responses and tends to differ from actual situations and expectations, so the challenge is to apply a prepared response that matches the terms and needs of a situation.

2. The ability to monitor the systems status, and to avoid being immobilized by routines and working habits. Proper monitoring could help in dealing with short-term challenges.

3. The ability to be predictive of situations and consequences. In contrary to monitoring, this helps dealing with mid- to long-term potential challenges.

4. The ability to make use of previous experience and learn.

Further Hollnagel et al. (2008a) introduces five fundamental, but challenging, issues regarding a safety management system:

1. Target

2. Control options

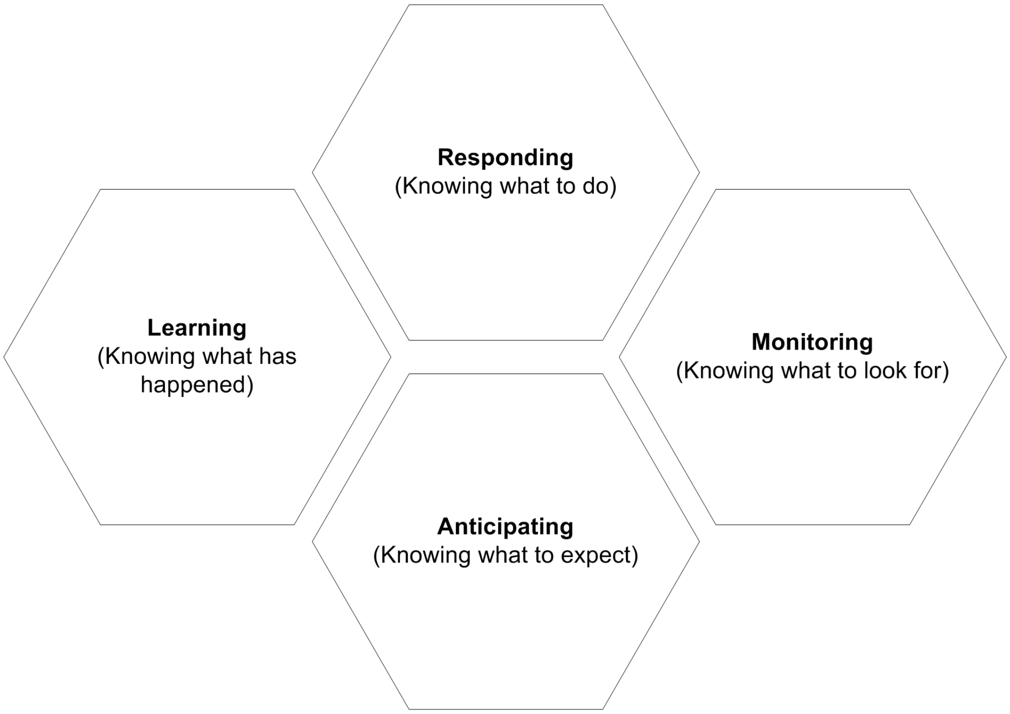


Figure 2.3: The four cornerstones of resilience

3. Process model

4. Nature of threats

5. Measurement

A target is obviously to improve safety, but measuring this improvement is usually delegated to a reduction in number of occurrences. The problem is a paradox that fewer occurrences produce less data to adjust the performance variability, making the measured process uncontrollable. This would of course not be a problem following the ideology that zero accidents is possible, but that is not so in a resilience engineering perspective, thus making the system unpredictable and more out of control considering accidents. This is why, in choosing a target, it is recommended to choose a goal that has a positive increase in output while safety increases.

By control options, it is meant the actions taken when irregularities in the system have been recognized. The challenge is not to just fix what has been broken, but to improve safety by altering the way the organization functions in these situations. Unfortunately, there is usually no easy, single solution to the issue, apart from a thorough review of the organization's safety assumptions and safety culture.

Resilience engineering considers safety as a product of an activity, meaning that it must be actively and continuously be considered and worked with. The process model regards the nature of the safety activity, the activities that "produce" safety. *"Safety is therefore different from, and more complex than, the absence of risk."* (Hollnagel et al., 2008a, p 73). The most resilient activities are the analyzing and predictive ones that helps in accident prevention rather than patching up accidents that has already happen.

The issue with the most attention and experience, thus the one with the most knowledge, is the nature of threats. Since experience plays such an important role in figuring out the sources and reoccurring tendencies, it is critical that the conclusions from previously investigated occurrences are correct and usable as data. Blaming on human error rarely gives enough information to build up resilience.

The fifth, and final, issue concerns the measurement of performance. This issue might sound like the easy challenge, just figure out number of accidents, lost work hours and so on, but these measures rarely gives any meaningful data. As stated earlier, it is not plausible to say that a low number of accidents results in a good safety culture. Hollnagel et al. (2008a) states that finding measures that emphasize the presence of safety rather than the absence could provide a positive flow in the system, considering the initially positive psychological side of striving after a safe work environment.

Not surprisingly, the issues regarding targets and nature of threats are the ones that most safety management systems cope with, although usually limited to the most generic and simple level. The other three issues, though, tends to be troublesome areas for many safety management systems (Hollnagel et al., 2008a). A thought is that a good risk analysis model could help with the safety management system, but finding models that manages to assist in achieving beneficial results concerning these issues is a challenge in itself. Although, a few of them exists, and one of them that takes a shot at creating a resilient system is STAMP.

Chapter 3

Systems- Theoretic Accident Model and Processes

3.1 The STAMP approach

"It's never what we don't know that stops us; it's what we do know that just ain't so" (Leveson, 2010, p 5)

Systems- theoretic accident model and processes (STAMP), first introduced by Nancy Leveson in 2004, is a model that builds upon three basic constructs: Hierarchical safety control structures, safety constraints, and process models (Leveson, 2011). The hierarchical safety part resembles Rasmussen's (1997) hierarchical model of the sociotechnical system involved in risk management. The hierarchical model is supposed to represent a bureaucratic perspective on risk management, stating that safety comes from the upper levels and gets passed down to the ones utilizing actions, with various feedback from the lower levels.

The catch with the STAMP approach, is to view the levels in the hierarchy as constraints towards the activities below it. This implies that the constraints at the higher level control the activity below, thus urges the necessity of having proper constraints to enforce safe behavior. At the same time, the constraints must show adaptability to cope with changes in processes. Examples of controlling actions, that leads to constraints, from the upper levels could be in the form of policies, laws and regulations. It is also possible that feedback leads to constraints.

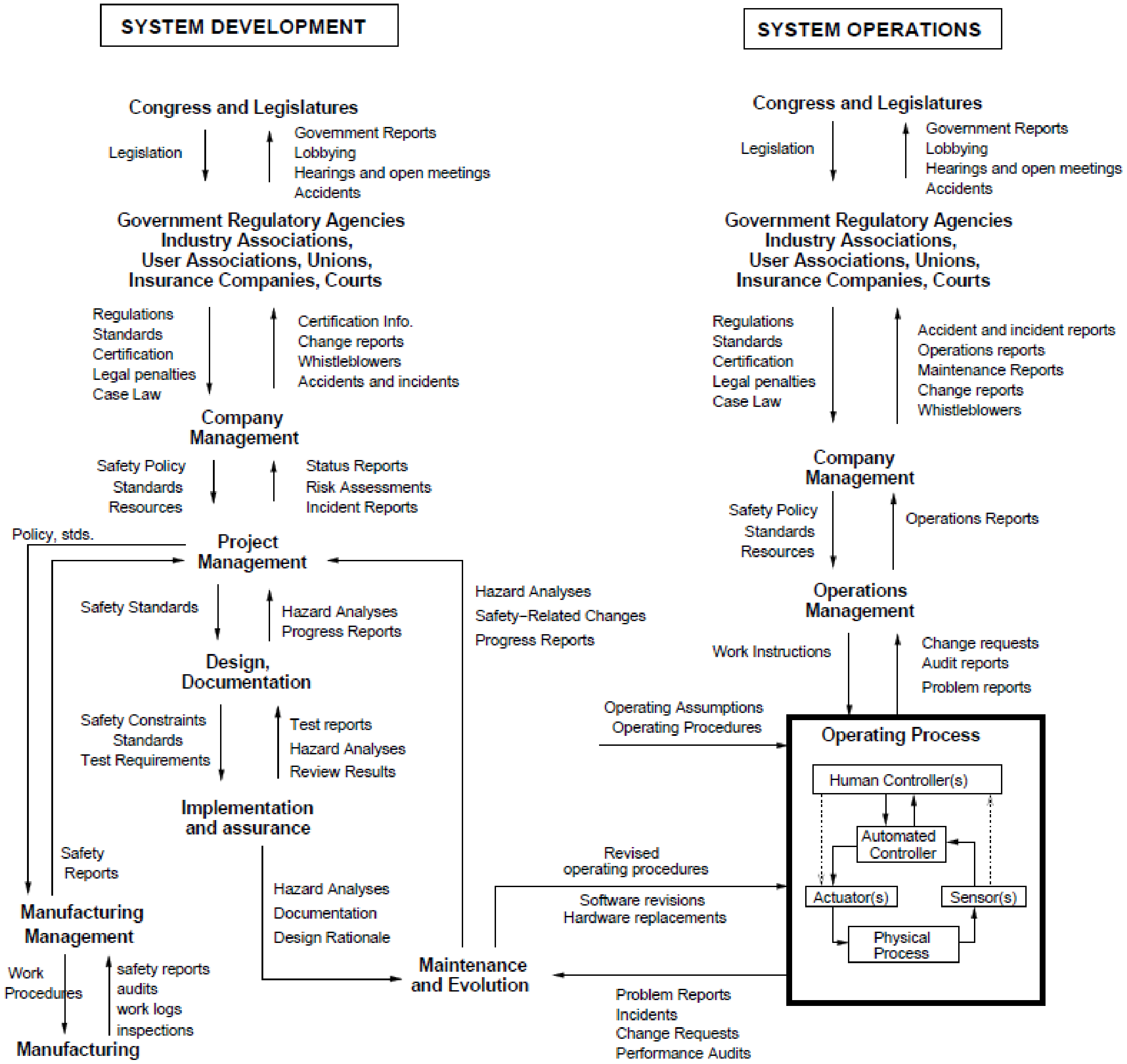


Figure 3.1: Example of a hierarchical structure in a sociotechnical system (Leveson, 2011, p 82)

The feedback in itself tends to be weaker constraints on their own, but, of course, might lead to constraints from the upper levels. Examples of feedback might be success, complaints from interest groups and unions, or accidents. (Qureshi , 2008)

STAMP's approach to accidents as lack of constraints, rather than a result of events, means that the accidents can be explained by flaws in the control loops between the system components in the hierarchy. These flaws are the keys in risk management to assist in the identification of factors involved in the accidents (Qureshi , 2008). To identify these flaws Leveson (2011) states a need for process models, which is the last of the three basic foundations of STAMP. This model is necessary when trying to control the processes, either manually or automatically, to comprehend the required relationship among the system variables. Regardless of whether a controller is automatic or human, the need for an exact model to control the processes exactly enough is still present, it just needs different interface to the process. The reason for the importance of a process model, and belonging control, is because systems are treated as dynamic processes, thus the need for adaptive skills in a risk management perspective.

Because of the way STAMP defines safety management, as the lack of constraints, the best approach to a safer system is obviously through enforcement of constraints. This allows for a more sophisticated approach considering the possible implementation of human-, organizational- and component error, instead of just component failures. By using constraints, accidents occur as a result of flawed process interactions between the different activities and players in the system, like human workers, technical components and organization policies. This means that accidents can be understood by identifying the violated safety constraints and failed system control, thus generating feedback in the sociotechnical hierarchy. Such a hazard analysis technique encourage a greater variety of risk reducing measures than the traditional redundancy-adding, or overcompensation of design to handle component failures Leveson (2011).

3.2 System- Theoretic Process Analysis

The system- theoretic process analysis (STPA) is an analysis method developed to fit the STAMP approach to safety management. STPA resembles HAZOP in the way that it uses "guide words" to assist the analysis process, but that is just a part of the method. STPA utilizes functional

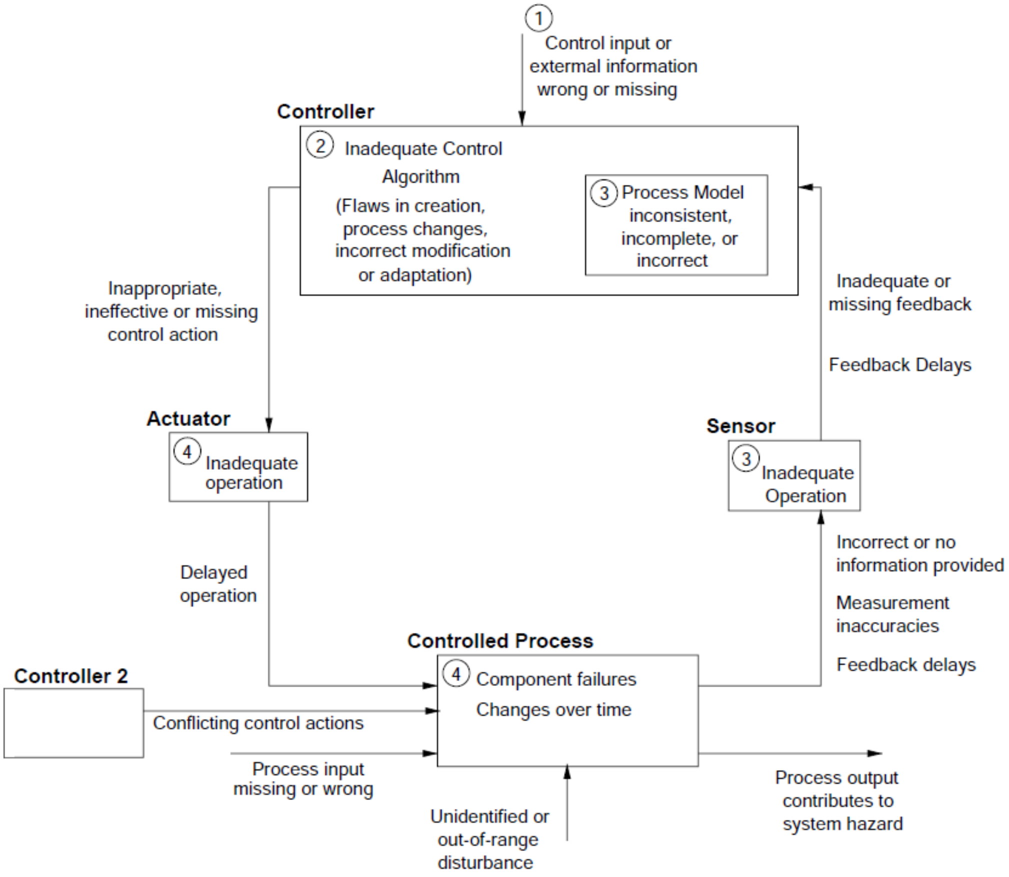

1
Control input or external information wrong or missing
Controller
2 Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)
3 Process Model inconsistent, incomplete, or incorrect
Inappropriate, ineffective or missing control action
Inadequate or missing feedback
Feedback Delays
Actuator
4 Inadequate operation
Sensor
3 Inadequate Operation
Delayed operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Controlled Process
4 Component failures
Changes over time
Controller 2
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Figure 3.2: Example of how to use a functional control diagram (Leveson, 2011, p 223)

control diagrams (control loops) (see figure 3.2) in combinations with the system requirements, hazards, safety constraints and components to acquire information about how the safety constraints can be violated. Its main strength is in systems that already exists, but still Leveson (2011) express that STPA can be used to help in the design process of a system, rather than just a optimization tool to be used on existing systems.

There are two main steps to carry out a STPA (Leveson, 2011, p 213):

1. Identification of the potentially lacking system control that could lead to hazardous situations. These situations could befall because of:

    - A required safety control action is not provided or followed
    - The provided control action is unsafe
    - The potentially safe control action is provided at the wrong time or sequence

- A safety control action is either stopped too soon or too late

2. Determine how the hazardous situations identified could occur by:

    - Examine the parts of the control loop to see if this is the source. If there are multiple controllers for the same component or constraint, additional resources must be put to finding possible conflicts and coordination problems.
    - Consider degradation of designed controls.

To be able to utilize the STPA, a thorough understanding of the system is necessary, like what kind of functional requirements, hazards and safety constraints is bound to the system, as well as different roles of the hierarchy and feedback mechanisms. This is why performing the main steps is not enough on its own, but need to be complemented with proper study of the system; the method demands a strong insight and knowledge of the overall process that is assessed.

Although most of the experience with the STPA is based on lower levels of safety control structures, it is usable on organizational and management levels as well (Leveson, 2011). A big challenge in analyzing organizational and management levels is the complexity of the constraints during decision making. Typically there are a multitude of controllers responsible for the same safety requirements, but even with big redundancy it still manages to create gaps where errors are made. This makes it difficult to map who or what is controlling or being controlled at the necessary moments. To accommodate this, a suggestion from Leveson (2011) is to change the functional control diagram into a less "technical" approach, and more into an "affinity" version (see figure 3.3). The affinities are described as pros and cons to determine whether the decision will be made or not.

A major advantage with the STPA is the possibility to treat humans just like automated components in the first step, making it easier to identify the challenges created by human contributions. Modeling human contribution and behavior in the control loop, and analyzing the system works naturally as if humans are an integrated part of the system. However, because of the complexity of a human controller, the detailed analysis and detailed scenario generation is equally as complex to accomplish. Considering STAMP, the reason is that humans should have knowledge about both the specific process they are controlling, and the system they operate in, compared to a automated component that only need to know its specific task.

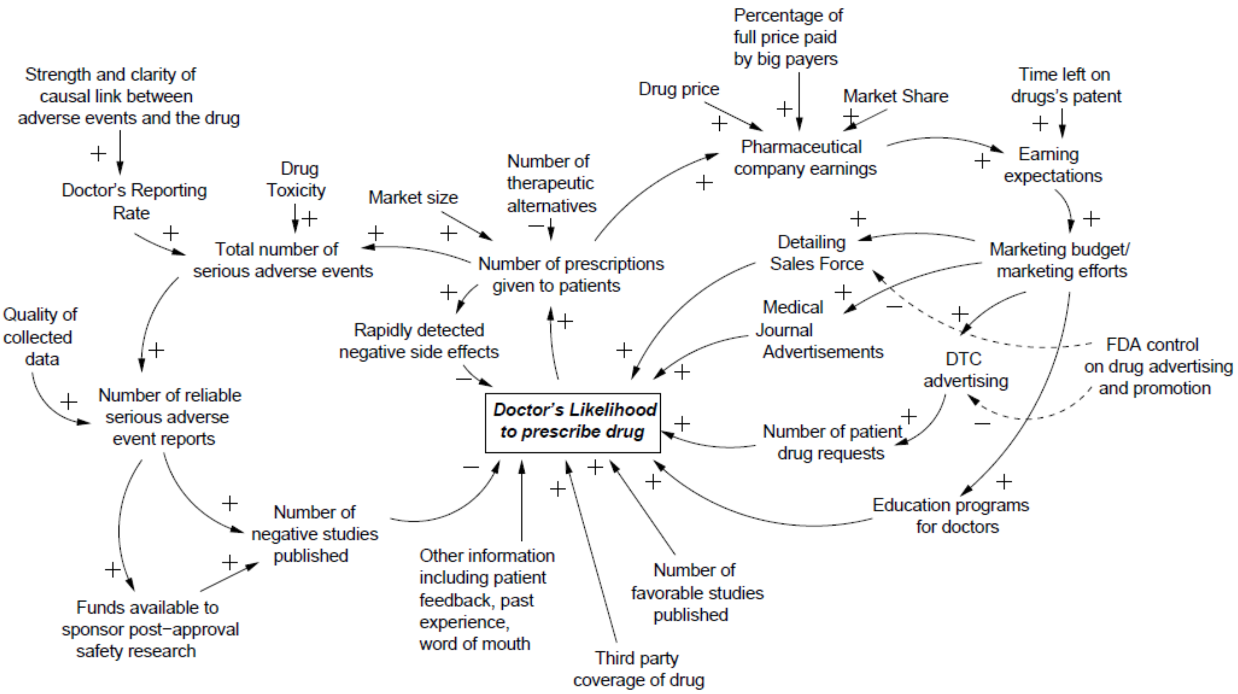

Percentage of full price paid by big payers
Drug price
Market Share
Time left on drugs's patent
Pharmaceutical company earnings
Earning expectations
Strength and clarity of causal link between adverse events and the drug
Doctor's Reporting Rate
Drug Toxicity
Market size
Number of therapeutic alternatives
Total number of serious adverse events
Number of prescriptions given to patients
Detailing Sales Force
Marketing budget/ marketing efforts
Medical Journal Advertisements
Quality of collected data
Rapidly detected negative side effects
DTC advertising
FDA control on drug advertising and promotion
Number of reliable serious adverse event reports
Doctor's Likelihood to prescribe drug
Number of patient drug requests
Number of negative studies published
Education programs for doctors
Other information including patient feedback, past experience, word of mouth
Number of favorable studies published
Funds available to sponsor post−approval safety research
Third party coverage of drug

Figure 3.3: Example of "affinity" use of STPA: Constraints affecting a doctors likelihood of prescribing drugs (Leveson, 2011, p 247)

Another strong side of the STPA is the feasibility to assess different levels of depth of a system. You can start out by taking a broad, non-detailed approach to a system, gaining a general overview. From here it is possible to go more into detail of each and every constraint, or be selective of which constraints to explore. This gives a level of freedom and opportunity to focus on the more important constraints if necessary. Given that STPA is easy to update, just add constraints and direct influence to established constraints, this is a great advantage for large complex systems where prioritizing attention might be an issue.

Chapter 4

Release of Hydrocarbons

4.1 The Risk Level Project

As authorities increase their focus on risk reduction, a simultaneous increase in number of risk reducing research and development projects have been started. One of these is the risk level project (RNNP) initiated in 1999 by the Norwegian Petroleum Directorate (NPD) to establish a realistic picture of, and hopefully improve, the human, environment and safety level of the offshore industry in Norway. The RNNP was later transferred to the Petroleum Safety Authority of Norway (PSA) and the project was extended to contain both offshore and onshore petroleum plants and activities. One of the hazardous situations they collect data about is hydrocarbon leaks, and all companies operating on the Norwegian Continental Self are obliged to report process leaks with release rate in excess of 0.1 kilogram per second. It is worth noticing that the data analysis used further excludes leaks from risers, pipelines and well blowouts, because they are represented by other categories in RNNP, as well as non-processing equipment leaks such as hydraulic and diesel oil leaks. (Haugen et al., 2011)

Analysis of the data collected have shown a solid reduction of total hydrocarbon leaks through the collecting period, but appears to be stabilizing on ten to fifteen leaks per year. There is a telling difference in initiating events that causes the hydrocarbon leakages, with human intervention operation failures rising as the leading cause, followed by technical failures with less than half the number of accidents. These two categories have both had a steady falling tendency in occurrence, although the interesting part comes when further divide the human errors into normal operation and maintenance requiring intervention. Normal operation have had a significant reduction, but maintenance intervention have hardly been reduced. Further, differentiation between hydrocarbon leakages can be made between leaks more and less than 1 kg/s, and the results shows marginal reduction in leakages of more than 1 kg/s. This outlines an area of potentially significant improvement. (Haugen et al., 2011)

4.2 Pressurized Hydrocarbon Processing Equipment

As stated in section 4.1, vulnerability to hydrocarbon leakage is high during maintenance. An area of improvement is during the maintenance of pressurized equipment containing hydrocarbons used in oil and gas processing. On a superior level, these maintenance procedures usually involve isolating the equipment from the rest of the process line, remove any hydrocarbons inside, perform maintenance, and reconnect the equipment to resume normal process. The need to halt the production requires some major planning and involvement of several levels of management to carry out such a maintenance process, and gives extra pressure on the workers chosen to execute the process to accomplish the task swiftly and correctly. Considering the comprehension of the task there is a multitude of possible errors to occur resulting in hydrocarbon leakage, as well as other accidents, thus representing a great opportunity to explore the potential of a new risk analysis model.

4.2.1 Description of the Maintenance Procedure

The first step is to have necessary planning and certification. To help coordinating the procedure a work permit and an activity and control form (AC/WP) are required which includes permissions, descriptions and specifics, as well as attached assisting information such as drawings, that follows the work from start to finish. Planning operations include evaluation of safety and hazards, choosing the right isolation area, choosing the right valves and flanges, and marking of the right valves and flanges by use of a piping and instrumentation diagram (P&ID). The results must be approved by proper managers at the site before initiated.

The hydrocarbon processing is stopped, and items used for isolation purposes are tagged with unique labels, and valves additionally secured by padlocks, before the isolation and bleed-out procedure begins. It is worth mentioning that each tag is marked with corresponding numbers in the AC/WP and P&ID, and signed with the initials of a person, making the isolator personally responsible for correct tagging and utilization. All valves controlled by electronic solutions must be disconnected to prevent accidental reopening. There are four different methods to isolate and bleed out a system: Single valve, double valve, double valve and bleed, and finally positive isolation.

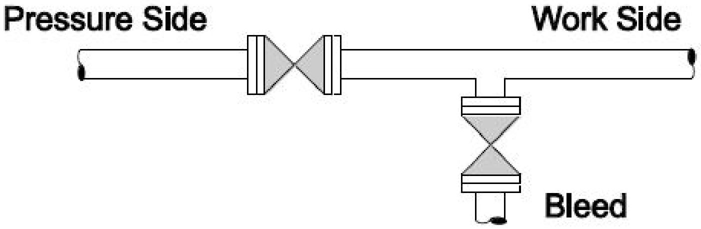


Figure 4.1: Single Valve Isolation

The single valve isolation is tested by closing the valve and bleeding the pressure on work side to atmospheric pressure. After this the bleed vent is closed for some minutes, then reopened to check for pressure build up.

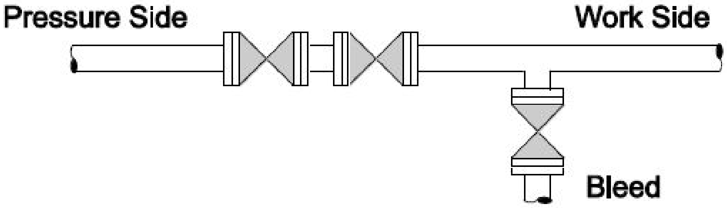


Figure 4.2: Double Valve Isolation

The same goes for the double valve isolation, only this time the procedure is done twice to check the sealing of each of the pressure side valves. Starting off with the work side valve, bleeding and checking for pressure build up, then the pressure side valve, before closing both.

Double valve and bleed isolations are tested by first doing the same procedure as single valve isolation on the work side, then do a similar procedure on the pressure side valve and bleed.

The last isolation method is positive isolation (zero potential of energy/absolutely no system flow) by either removing of pipe spool and bolting live ends, or insertion of plates/blindings. This is the method of use if the maintenance is performed in confined space and isolations

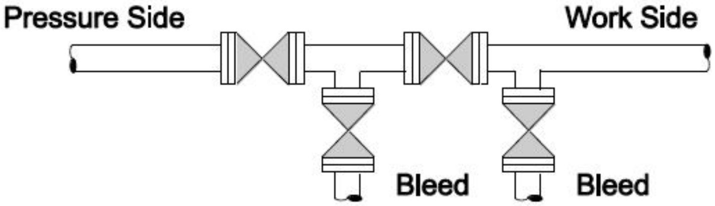


Figure 4.3: Double Valve and Bleed Isolation

with long duration. The selection of isolation method in general however, is chosen by common sense, technical judgment and experience. Though, it is possible to use a risk matrix combined with available parameters and data as assistance, but this is not to be used blindly. Single valve isolation method is suitable for the least hazardous situations and requires least amount of work, then double valve, double valve and bleed, and ultimately positive isolation as the best suitable method for the most hazardous situations, but requires the most effort to carry out.

Prior to the drainage, gas is usually ventilated to the torch to relieve the system of pressure. If gas is the main hydrocarbon in containment, it is sufficient to just have a controlled purging. A typical way to clean the system of liquid hydrocarbon is to flush it thoroughly with water. It is effective for most systems, but has a hard time against sludge and especially complex pipe work. Besides, not all pipe work can withstand such a huge weight addition of water, both concerning stability and actual weight. A huge amount of water is also necessary to acquire. For those systems, relying on inert gas, like nitrogen, is a common practice. However, nitrogen creates low temperature, potentially cracking the pipes or damage human workers if used unfortunately.

When the system is isolated and all of the hydrocarbons are removed, it is ready to proceed with the maintenance. When the work is done, blindings must be removed and resetting of valves must be done to assemble the system back to its former self. It is advised to test run the system for leakages before resuming normal production, and an evaluation of the job for further improvement.

Chapter 5

Performing a STAMP and STPA Analysis

5.1 The Approach

By establishing an overall understanding of the system, it is time to dive deeper into the specifics and finally perform a STAMP and STPA analysis of the maintenance procedure of pressurized equipment containing hydrocarbons used in oil and gas processing. At first, there is a need to create a hierarchical structure of the system. Excluding external contribution from government and different organizations, there are eight people directly participating in the maintenance procedure: A platform manager and an operations manager that prepares the P&ID and the AC/WP, but is not a part of the operating process that physically does the maintenance. The people being in the operating process are the central control room (considered to be a person), the three mechanics being executing professional, the electrical engineer and the instrument technician, and finally the two maintenance personnel being the area technician and the production technician.

5.2 The Hierarchical Structure

At the top of the hierarchy for this process is the government. They distribute fundings to different departments and directorates that create and assess rules, standards and similar. These standards and rules are constraints on the organizations to arrange for proper maintenance procedures. An AC/WP is made, with the platform manager being the main responsible, and assessed together with the operations manager. Once the AC/WP is approved, the operations manager marks up the P&ID, and pass them on to the operating process (this process is illustrated as “creating P&ID”, although a P&ID is not created as such, but altered to the intended use). In the hierarchical structure, the people within the operating process are regarded as being on the same level, and by that ending the hierarchical structure (see figure 5.1).

5.3 The First Step

The hazards occur during the operating process, thus the focus of the analysis origins here. From analyzing the process, it is possible to divide it into seven different, superior control actions that determines the outcome of whether a hazardous situation will occur or not. These seven control actions are evaluated by the four different hazard originators described in 3.2. The results are shown in table 5.1

The nature of the maintenance process is highly consecutive, making the hazardous situations mostly related to not following this sequence properly. This gives us five different safety constraints to work with:

1. The system must be properly isolated before pressure is being released
2. Pressure release must be properly done before drainage
3. Drainage must be properly done before the system is opened for maintenance
4. Pressure and leakage testing must be done after the system is properly closed and connected
5. Start-up must be done after the system is properly closed and connected

5.4 The Second Step

Performing the first step and achieving a set of safety constraints could suffice for some less complex systems (Leveson, 2011). If not, the safety constraints is viable in the execution of the

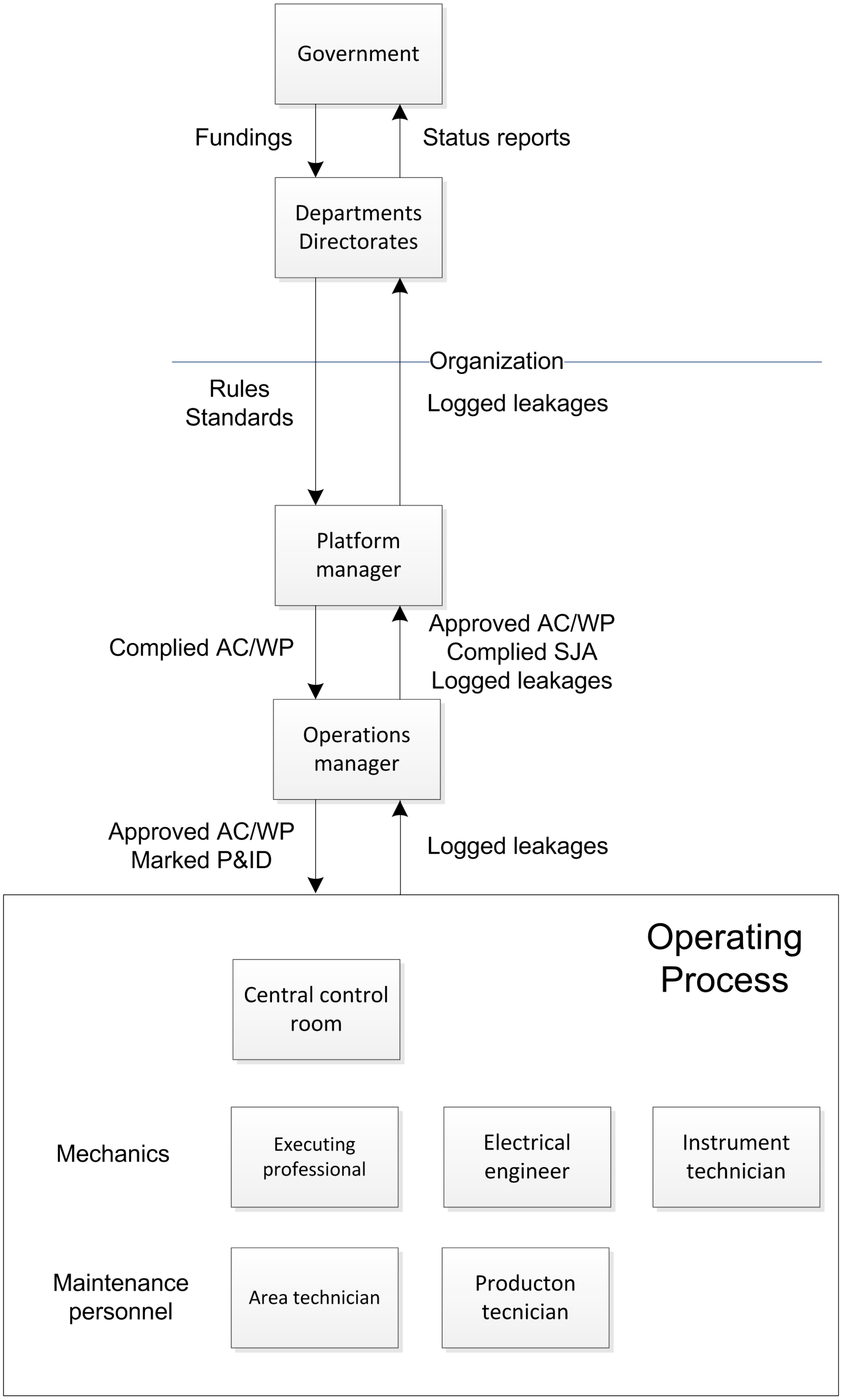


Figure 5.1: The hierarchical structure for maintenance of pressurized equipment containing hydrocarbons

Table 5.1: STPA: Step one

Control Action	**Not provided or followed**	**Is unsafe**	**Is provided at the wrong time or sequence**	**Stopped too soon or too late**
Isolating	System is open		Must be done before opening the system	Must not be stopped before closing the system
Pressure release	High system pressure	Must be done assured	Must be done before opening the system and after isolating	Too high pressure in the system
Drainage	System is filled with hydrocarbons	Must be done assured	Must be done before opening the system and after pressure release	Too much fluid in the system
Maintenance		If previous steps is not done correctly	Must be done after previous steps	
Closing and reconnecting	System is disconnected			
Pressure and leakage testing		Must be done assured	Must be done after closing and connecting	
Start-up		Must be done after the system is closed and connected		

second step, where they are used as a baseline for examining the control loops. This maintenance procedure is special in the way that the procedure is following a sequence and most of the tasks are directly done by humans. The sequential procedure makes the analysis easier to follow, but the emphasis on human operation is shown by the heavy contribution to the sensors and controllers in the control loops. The analysis can be seen in appendix B

The control loops are determined by the control actions from step one (see table 5.1), except for the start-up which is not a loop per se, but still a process necessary to the analysis. Every process' have some important input from previous step, like a clearance to begin, and likewise send some similar output to the next step visualized by the connecting arrows from the different processes. The first and last arrow represent the input/output from/to the operations manager in the hierarchical structure, creating a complete loop in the hierarchy (see figure 5.1).

At three of the processes, drainage, maintenance, and pressure and leakage testing, there is a possibility of leakage. Leakage is pictured as a dead end, because from here on the process stops and special precautions are necessary that reaches outside the scope of this thesis.

The control loops consist of four boxes: process, sensors, controllers and actuators. These boxes represent what is supposed to be done as a part of the process. In the sensors box there are listed the different sensors that are supposed to detect any abnormalities of the process, either technical sensors like pressure transmitters, or humans that supervise or check the process. The actuator box lists the different actions that "does" the process, like closing the valves to isolate the system. The controller are the persons performing the process, mainly because the processes are done by humans.

Connecting the boxes and creating the visual loops are the way things can go "bad" between the boxes, like a defective AC/WP or P&ID being used between the controller and the actuator. An exception is the arrow from the sensor that circulates back to the previous controllers, illustrating that a mishap from previous processes can be detected during later processes, and reported back to be corrected.

Above the different controller boxes are external disturbances and errors that affect the controller in a negative manner. In some cases this could be enough to fully assess the risk in the system, and further improvement could be made. Although, if the newly created control loops does not suffice in the search for plausible improvements, these disturbances appear as the greatest potential of further exploration.

5.5 Further Elaboration

From the current STPA risk model, there are three potential stages of the process that may cause leakage, during drainage, maintenance, and pressure and leakage testing. Considering what is stated in section 4.1, it is the leakages that involve more than 1 kg/s that is of main concern. That is why the main challenge is believed to be the leakages that happen during maintenance, primarily because of the unexpectedness and the potential amount of the leakage compared to the drainage, and the pressure and leakage testing during normal procedures. Interestingly, the maintenance procedure causes leakage mainly because of lack of completion of previous steps. Hence, to continue with the STPA, the previous steps of drainage and isolation process are chosen to further elaborate. Drainage because this is an area that directly could cause leakage, thus might leave some interesting results, and isolation is the most diverse process with the highest amount of external disturbances. Besides, the isolation process have a lot of common external disturbances with the other processes, making it easier to further elaborate those as well if necessary.

Among the external disturbances affecting the drainage process, errors/defects in AC/WP is the only one concrete enough to work with. Lacking co-ordination and variable concentration distractions are still relevant, although it is seen as far too ambiguous and ambitious to continue with. To proceed with the errors/defects in AC/WP, a new control loop is created, creating AC/WP. The result can be seen in appendix B.10.

Concerning the isolation process, there are three disturbances worth considering: Errors/defects in P&ID, system not shut off, and errors/defects in AC/WP. The last is identical to the control loop in the drainage process, and the other two are assessed as the processes creating P&ID and shutting off system. The result can be seen in appendix B.

5.6 Assessing the Maintenance Procedure

The very characteristic top-down approach of the STAMP/STPA is easily recognizable during this analysis. The hierarchical structure gives initially little information except from illustrating the overall process flow.

Continuing with the STPA of the operating process affords a greater extent of information regarding the process flow and the basic nature of hazards. Showing that the process is highly consecutive, step one emphasizes the need to perform the procedure properly in correct order. Step two further expands the depth by introducing the control loops, and finally a more complete understanding of the system unveils possible improvements of the procedure.

At first, the amount of human intervention is striking. The maintenance procedure is at core a manual procedure, and the majority of sensors are directly or indirectly affiliated with humans (like marking of valves or flanges). Thus, precise performance by the humans is of great importance. Another interesting discovery is the fact that all of the human sensors plays additional roles in the procedure, and most of them conduct actions on the system. As stated in section 2.1.1, the most common omission is pre-mature exits happening when people get preoccupied with the next task. Further section 2.1.3 argues that switching attention is an interval that provokes the appearance of accidents. Combining these thoughts implicate that humans determined to perform the work as sensors have a high probability to let mistakes pass by, because they are already preoccupied to do their additional work to make the maintenance procedure moving, and they need to switch attention from this work to act as a sensor. Adding the pressure to perform their work fast, because the total processing plant is shut off for the maintenance work, probably makes this an area of considerable improvement.

With the further elaboration of the drainage process (appendix B.10), nothing new arrives to advance the assessment. The operations manager is used as a sensor, while he likely have a lot of other work that could stress him to do a less thorough look on the AC/WP before it is proceeded.

The main concern comes with the further elaboration of the isolation process. The creating P&ID process have no sensor that gives feedback. This means that if the operations manager makes an error with the P&ID, it probably will not get noticed unless a sharp mind accidentally notices it. The P&ID is a highly critical documentation during the maintenance procedure, so introducing a sensor that provides feedback to verify the integrity of the document seems like a potential for major improvement in risk reduction.

How much further the STPA is supposed to go is up to the individual analyst, but the data necessary to further elaborate this particular case would reach beyond the scope of this thesis. However, two major concerns are revealed, and a suggestion would in any case be to examine the potential of these concerns before further elaboration.

5.7 Accommodating the New Paradigm

As a result of the analysis made of the maintenance procedure of pressurized equipment containing hydrocarbons, the STAMP/STPA proves to be a tidy and thorough analysis method. By continuously increasing the level of detail, the method forces the analyst to understand the system before coming to any conclusions. This might be the result of the selected case being unexpectedly well suited for analysis with STAMP/STPA. The system is complex concerning the high rate of manual human labor involved and multitude of possibilities to make errors. With that said, it is also a complete sequential procedure, thus maintaining a tidy progression of the control loops.

5.7.1 Support of a Safety Culture

STPA deals with failures in a more non-physical manner by focusing on constraints and interactions rather than physical components and their specific failure. By doing this, it manages to accommodate a risk perspective closer to a real life situation, especially concerning human error. There is no given order of how the different controllers make errors or how the sensors fail to notice errors, and since they are both to “blame” the actions leading to a hazard is more a team issue rather than a component failure issue.

This introduces one of the more important aspects of the STPA approach, the support of a safety culture. If an accident occurs, this is seen as a failure of the total system, because of poor variability monitoring, unfavorable activity, or not having the necessary constrains, rather than the specific component. On a human level, it is much easier to build a team spirit on a foundation that does not directly blame individuals, but the team as a whole. The resilience and STAMP mentality matches this healthy combination of the three “Cs” and four “Ps” that helps creating a safety culture (section 2.1.4). For example with the operations manager that creates a P&ID without any sensors: A constraint should keep him from performing the process wrong, so the questions is not whether he fails or succeeds, but why nobody helps him (or why there are no constraints, to use STAMP terminology). This is probably one of the strongest aspect of the STPA, doubled by the natural implementation of human errors as a part of the standard structure for identifying risks.

5.7.2 A Different View for Decision Making Support

It is exactly the nature of the STAMP/STPA that gives a new edge to decision making support as well. Whereas for example FTA focuses on failures of specific components, or HAZOP on system flow, STAMP/STPA directs attention on the surroundings and affiliations between components and actors within the process. This may shift the focus from a strictly result oriented view to a more functional perspective, that everything should work well together to create a synergistic effect rather than that each single component must perform adequately by themselves. By comparison, a HAZOP is rarely useful in the development of risk management strategies, and the results usually mitigate towards implementation of different technology or additional protective devices (Clarke, P. and Young, S. , 2006). STAMP/STPA on the other hand focuses on the constraints surrounding troublesome areas, and by that introduces a greater capability to affect the surroundings to manage the issues. Sure, constraints are added, but constraints represent an entity that is more than just addition of new technology, maybe by using the available resources in different manner, or adding new rules and regulations. Perhaps adding constraints to stimulate positive development instead of just failures is possible, like for example a constrain that ensures proper coaching of employees before they perform work on the system, and an indicator could be number of trained employees at work. As stated in section 2.3, even if failures happens seldom, it does not mean the safety integrity of the system is strong, so safety indicator numbers that increase with a more safe system is preferable.

Knowing that the human free will is limited by local circumstances (section 2.1.2), a thought is that STPA is more able to predict the possibility of human action because it analyses the situations surrounding the processes to a greater degree than existing methods. As mentioned, while conventional analysis methods focuses on a binomial success/failure approach, the constraints used in the STAMP/STPA takes account for a more composed situation of connections and affinities. It is still a matter of failure/success of the constraints, but unlike in existing methods where the components are the main focus, it is the constraints are not supposed to be main part of the process, but have more of a supervising effect. If human behavior is predictable to a certain level, adding constraints or visible boundaries to inhibit a risk enhancing variability in performance should be possible. In other words, STPA could in theory be a helpful tool in assisting the creation of a safety space similar to the one by Rasmussen (see figure 2.1).

5.7.3 A Demanding Analysis Method

Regardless of the advantages, STAMP/STPA is a demanding analysis method to use. Firstly, while creating the STAMP/STPA of the maintenance procedure, it was obvious how difficult it would be to direct the analysis to reasonable areas unless a specific hazard is sought to solve, which in this case was leakage. If the analyst were to begin without any structure, the extent of possibilities is overwhelming, as well as the amount of work ahead. A strong side of the STAMP/STPA is the possibility to dig deeper and deeper into the system depending on how detailed the analysis should be. But if there is no specific goal (other than general risk analysis of a system or procedure) or the hazard is not easily discovered, when do you stop adding control loops? When does the analysis reach a deep enough level of detail to be usable in risk reduction? Detailing the control loops from a general overview into concrete, usable solutions on a detailed level could turn out to be a tiresome, unnecessary and deluding process if the analysts do not know when a usable level of the analysis is reached. This means that a pre-analysis of the system could be necessary to perform before the STAMP/STPA to acquire some basic structure to work with.

The STPA does not point out directly areas of improvement, but gives the analyst the necessary information to figure it out. For example an event tree accompanies the analyst from an initiating event, through several barriers that alter the course of the event until the last barrier is crossed, and the inevitable consequence is more or less obvious. The STPA gives a more thorough situational understanding, but the analyst needs to carefully scan the created control loops to search for potential improvements. STAMP/STPA is like a topography map, where it shows the information about the terrain, but never tells you which trail that are easy or impossible to traverse. In that sense, even if the STPA is done correctly, it might be tough to extract any useful results from it if the analyst is inexperienced.

Giving all the different levels of depth possible to examine and combine it with the uncertainty and perhaps a non-consecutive procedure, the potential for a disorderly STPA is certainly there. The analyst may have an impressive control, but unless the control loops and connections are carefully managed, it will become difficult for anyone else to utilize the STPA, in contrary to the likes of FTAs and ETAs, thus making it rather unavailable for implementation in decision making. It is possible to make the control loops understandable, but the necessary effort could involve a lot of extra work. This is an area STPA resembles HAZOP, the greater need of qualified and experienced experts compared to other methods. Not only to perform the actual analysis, but to make it usable to everyone that has interest in a risk analysis. Since the method is looser in its own performance, the need for having a grasp on the concept and its use is more crucial than ever.

5.7.4 Following a High Pace of Change

A criterion for the new paradigm is to establish a method that manages to model a complex and more dynamic sociotechnical system (section 2.1.4). As stated, it is believed that the STPA could help in attaining a safety space, but is it adaptable to a dynamic system in constant change? It is difficult to conclude within this aspect with the procedure modulated in this thesis, although slight errors and slips were easy to change. Since the loops are modeled after fixed boxes (process, controller, actuator and sensor), updating the system with new devices and human positions is a matter of adding them to (or subtracting from) their respective box. Adding a completely new control loop may involve a lot of work, mainly because its addition creates a lot of new interactions, and thus challenges the overall view and control of the system by the analyst. But the physical work of adding a new control loop is just a matter of coordinating the connections and drawing lines. If it turns out that STPA is easily updatable, it really gives the method an edge heading towards a new paradigm.

The potential of the STAMP/STPA is present, although a few issues need to be fixed before a widespread implementation in the corporate world is to be made. Some other further improvements could still be made, like developing a way to quantify risk.

Chapter 6

Quantification of Risk Using STPA

6.1 Challenges Concerning Quantification

In the new paradigm, the emphasis on dynamic adaptability and fast pace of change, combined with human error, seems to make the system states far too varied to be presented in definite numbers. With that said, quantitative risk analysis is deeply rooted in the way risk analysis is practiced today, that even if a new paradigm without quantification emerge, it is bound to still be a major part of general analysis procedures for years to come.

By already performing a thorough analysis of a system using STPA, it would be a great advantage to utilize the depth and insight from the STPA analysis to form quantitative results. The challenge would be to fully integrate a method to streamline the quantification process as if it were a natural accomplice with the STPA.

6.1.1 The Event Trees

The attempted solution of implementing quantitative risk analysis into STPA involves event trees. In event trees, consequences and probabilities come forth from an initiating event traversing through a series of barriers in a binary fashion. The thought is to use failure of the actuators as initiating events and the different sensors as barriers. Using the isolation process as an example, the initiating event could be fail to choose right isolation method, while barriers could be marking of valves/flanges and executing professional. In this particular example, the process is accompanied by several external disturbances. They have an explicit influence over the initiating event, so to implement these they are inserted as barriers in the event tree. See appendix C for suggestions of event trees related to the isolating and drainage process of the maintenance procedure.

By following the branches of the event tree, specific consequences can be assumed. A lot of the consequences relate to the aspect of time consumption. If the last barrier "catches" the failure, it is assumed the time to fix it will be longer due to the progression of the maintenance procedure than if the first barrier detects the issue (hence the "extra time consuming", "extra time consuming +", and ++ as consequences in the event trees in appendix C). To accommodate the probability rates of the consequences, different methods could be used. A lot of mechanical equipment, like pressure transmitters, have failure rates from the specific manufacturer. If not, the use of fault tree analysis, maybe combined with a Bayesian belief network (BBN), to calculate a probability is a possibility. Considering human errors, human reliability analysis methods, like the human error assessment and reduction technique (HEART) and the technique for human error prediction (THERP) is possible solutions. The most interesting barriers are the ones that originate from external disturbances, like the "errors/defects in AC/WP" (see appendix C.1). Since they might be modeled as a control loop in the STPA, it is possible to create event trees from their actuators and sensors as well, thus generating probabilistic data for the other event tree barriers.

6.1.2 Reliability Block Diagrams

By creating event trees and successfully assign probabilistic data, it is possible to quantify the influence and risks of the external disturbances and the processes. Considering the different influence each process may have on the total system, the next step would be to assess the system as a whole. To do this, a suggestion is to utilize a reliability block diagram (RBD), where each process represents a "block". The event trees should be able to propose a reliability for each process, thus making it possible to use simple RBD calculations to figure the reliability of the total system. If RBD's are not preferred, they are usually easily converted into fault trees, making this method more adjustable to the analyst's preferences (Rausand and Høyland, 2004).

Looking at the maintenance procedure regarding pressurized hydrocarbon processing equipment, an RBD is particularly easy considering its sequential nature. The operating process begins with isolating, ends with pressure and leakage testing, and every step must be completed in order for the procedure to be successful. This pattern implies a purely series structure of the RBD, thus the reliability could be calculated by multiplying the reliability rates belonging to the specific processes obtained from the event trees (see figure 6.1).

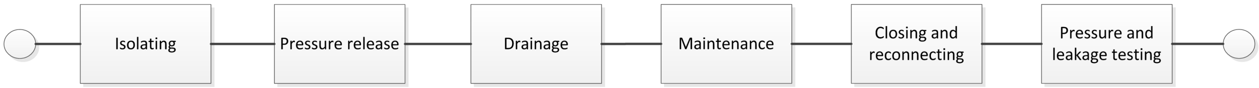


Figure 6.1: RBD of the operating process regarding maintenance procedure on pressurized hydrocarbon processing equipment

6.2 Data Requirements and Other Challenges

To summarize the quantification process step by step:

1. Perform a STPA analysis of necessary processes and appurtenant external disturbances.

2. From the control loops of the external disturbances, create representative initiating events from the actuators, and develop an event tree with the sensors as barriers. At least one of the consequences at the end of the event tree should be the actual external disturbance.

   - Calculate the frequency of the consequences by using probability data from the barriers.

3. From the control loops of the main process, create representative initiating events from the actuators, and develop an event tree with the external disturbances and sensors as barriers.

   - Calculate the frequency of the consequences by using probability data from the barriers.

If the event tree/RBD combination creates a quantification solution to STPA analysis, there is always the challenge of finding suitable data. The immediate advantage by quantifying risk with this method is the accessibility of existing data, or at least existing challenges in collecting data. Each sensor needs a reliable number if the fault trees should be quantitative, so the main concern is to acquire these. Regarding technical components this is usually obtainable from the manufacturer as a PFD, given SIL, or something similar. Human and organizational errors are quite the opposite. As stated, human and organizational errors are usually difficult to give concrete enough probabilities to use in quantification due to the complex and diverse nature.

There exists methods to calculate human errors, like HEART and THERP, that utilizes different factors and conditions to create a set of human error probabilities (HEP). In general, these methods do create possibilities for quantification, however the integrity of the methods are questionable and they tend to demand highly experienced analytical skills to achieve reasonable results (Rausand and Utne, 2009). Seljelid et al (2007) and Vinnem et al (2011) are examples of people who have tried to quantify a similar system to the one used in this thesis. Basically the methods used are advanced BBN models combined with risk influencing factors (RIF), where extensive studies of HEP was performed to help with gaining reliable calculations (Vinnem et al , 2011). However, even these data are somewhat lacking for their purpose, and they are fairly limited in use with other systems as well. This gives just an example of how difficult it is to acquire usable data. A lot of work has been, and is being, done regarding this particular area of human error, but if quantification of complex sociotechnical systems are to be used on a regular basis, further development must be done.

However, the thought behind introducing event trees and RBDs with the STPA is that it is an introduction into a well-known territory, and does not create entirely new needs. The highest concentration of reliable data is probably in areas already familiar with the challenge, hence event trees and RBDs that are well known and used methods. Besides, it makes it easier to learn a new method if something is recognizable, assuming that the STAMP/STPA is not a highly used method in the industry today.

Comparing the work scope of the STPA and event tree combination to regular ETA, it is obvious that the new method is far more resource demanding. Although, comparing regular ETA with the new combination, by using the actuators and sensors from the STPA as initiating events and barriers greatly reduces the amount of work needed to create the actual event tree. Which method that delivers the usable events and barriers first relies probably a lot on what kind of system is being dealt with. With a high level of complexity it is difficult to obtain usable and correct barriers and events with ETA. The STPA works especially well for finding usable data in complex systems, therefore a thought is that the thorough analysis ultimately accumulates less work the more complex the system is.

Event trees are one of the most common of the existing methods, including all their advantages and disadvantages. As stated, dynamic adaptability and fast pace of change makes it difficult to assign valid data to the different barriers of the event tree, especially human barriers. Not only that, but the sequential and binary barrier nature of the event tree makes it difficult to describe systems with co-existing states during the process. This is of course the core of the new paradigm that the resilience engineering philosophy attempts to address.

Although, a hope is that the combination of STPA and event trees will fix some of the major issues in the new paradigm. The STPA should manage to capture the essence of a dynamic system, by being the main contributor of risk analysis procedures, while the event trees are strictly used in quantification where it is needed. The sole reason for including a quantification process is the fact that numbers are a huge part of existing rules and regulations . By being strictly qualitative, the usefulness of the method is greatly limited. So if it is desired that the use of STAMP/STPA should increase, quantification may be a reasonable and necessary solution, at least for now.

Chapter 7

Conclusions and Discussions

7.1 The Literature Survey

It has become a paradigm shift in how to approach risk analysis from looking at specific component failure, to failure of the system as a whole. The new paradigm considers what is called a sociotechnical system, a rapidly evolving, and dynamic system with intricate interactions of humans and technical components. By introducing failure as a lack of constraints, rather than a result of events, the STAMP/STPA approach models systems with a combination of hierarchical structures and control loops to perform risk analysis.

To test the STAMP, leakage of hydrocarbons as a result of maintenance work related to pressurized process equipment is chosen as an appropriate hazard to analyze. This hazard has little to no improvement in number of occurrences over the past years, and is recognized as a complex procedure with a lot of human interactions.

7.2 The Qualitative Model

By utilizing presented, relevant, literature, a STAMP/STPA model is developed to analyze the vulnerable maintenance procedure on pressurized hydrocarbon processing equipment. The STAMP/STPA has been performed in four steps by:

1. Developing a hierarchical structure of the total process

2. Developing a table considering hazardous situations related to the maintenance procedure

3. Developing a set of control loops that represents the operating process

4. Performing a further elaboration of two selected processes, drainage and isolation

From the performed analysis, two suggestions for improvement were made:

1. Do not let the workers that perform the maintenance procedure have a secondary function as a primary inspector for errors.

2. Get an inspector that gives feedback to the operations manager to verify the integrity of the P&ID while preparing it for the maintenance procedure.

The result is seen in appendix B.2, and it has been used as a foundation to assess and evaluate STAMP/STPA as a risk analysis method.

7.3 Assessment of the Qualitative Model

During the development of the model, the STAMP/STPA proved to be a tidy and thorough analysis method, although the potential for being disorderly is certainly there. The focus on constraints probably manages to accommodate a risk perspective more resembling to a real life situation, and at the same time diverge blame from individuals to the system as a whole. An opinion is that this aspect of STAMP/STPA could lead to a stronger support for a safety culture.

By directing attention on the surroundings and affiliations of a system, a thought is that the STAMP/STPA may shift focus during decision making from a strictly result oriented view to a more functional perspective. That everything should work well together rather than an adequate isolated performance by itself.

Further, knowing that human free will is limited by local circumstances, it is possible that STPA is more able to establish usable safety measures to contain human behavior inside the limits of a safety space because of the focus on constraints rather than the strictly success/failure of components.

STAMP/STPA is a demanding analysis to perform compared with traditional methods of analysis. First of all it is probably useful to perform a pre-analysis of the system to acquire some basic structure to work with. The possibility to choose a level of depth wished to analyze show some positive flexibility to the analysis, but without a proper goal during the analysis it is easy to get lost. This concern is strengthened by the method not necessarily showing that a solution or a problem is found. Combine this with the potential a disorderly model, and the need for an experienced analyst to perform, utilize and present the model is high.

7.4 The Quantitative Model

To identify possible data requirements to an eventual quantification process, a way to perform quantitative risk analysis, with the developed STPA as a framework, is presented. The result is seen in appendix C.

The quantification method uses the actuators and sensors from the STPA as initiating events and barriers in an event tree to quantify each specific process. Hence, the data requirements needed is the failure frequency of the barriers in the event tree. Once the consequences in the event trees are calculated, they can be used to quantify the whole system by using a reliability block diagram, where each process represents the specific process.

7.5 Assessment of the Quantitative Model, Required Data, Availability of Data, and Necessary New Data

The immediate advantage with the presented method is that required data is known, collecting data is a well-known challenge, and some usable data is probably available for a lot of systems. By introducing a quantitative method together with STAMP/STPA does not necessarily give any new possibilities related to decision making, but it makes it easier to adapt STAMP/STPA to present decision making principles, rules and regulations. However, obtaining representative data concerning human error has always been, and still is, a major challenge.

Comparing the work scope of the STPA quantification method with regular event tree analysis, it is obvious that the STPA method is far more resource demanding in general. Although, a thought is that the more complex the system is, the STPA method will ultimately make the process easier to quantify, because the challenge of finding suitable barriers/events with regular event tree analysis will be increasingly more difficult comparing it with the STPA.

7.6 Recommendations for Further Work

The next step to achieve greater knowledge about the STAMP/STPA would be to perform an analysis of a specific system. The model developed in this thesis represent a general view on a concrete problem, it would be interesting to test the method on a similar system in real life. The major difference is the level of detail and specifics that would need to be modeled, and to see whether all the ideas and thoughts presented in the thesis is representative of real life situations. Further, if quantification is to be done, human error data would need to be collected and achieve an agreeable integrity.

Appendix A

Abbreviations and Acronyms

AC/WP Activity and Control Form/Work Permit

BBN Bayesian Belief Network

ETA Event Tree Analysis

FTA Fault Tree Analysis

HAZOP Hazard and Operability Analysis

HEART Human Error and Assessment Technique

HEP Human Error Probability

KB Knowledge-based

MIC Mechanical Isolation Certificate

NPD Norwegian Petroleum Directorate

PFD Probability of Failure on Demand

P&ID Piping and Instrumentation Diagram

PSA Petroleum Safety Authority of Norway

PSF Performance Shaping Factors

RB Rule-based

RBD Reliability Block Diagrams

RNNP Risk Level Project (Norwegian: Risikonivå i Norsk petroleumsvirksomhet)

SB Skill-based

SIL Safety Integrity Level

STAMP System- Theoretic Accident Model and Processes

STPA System- Theoretic Process Analysis

THERP Technique for Human Error Prediction

Appendix B

Complete STAMP and STPA charts

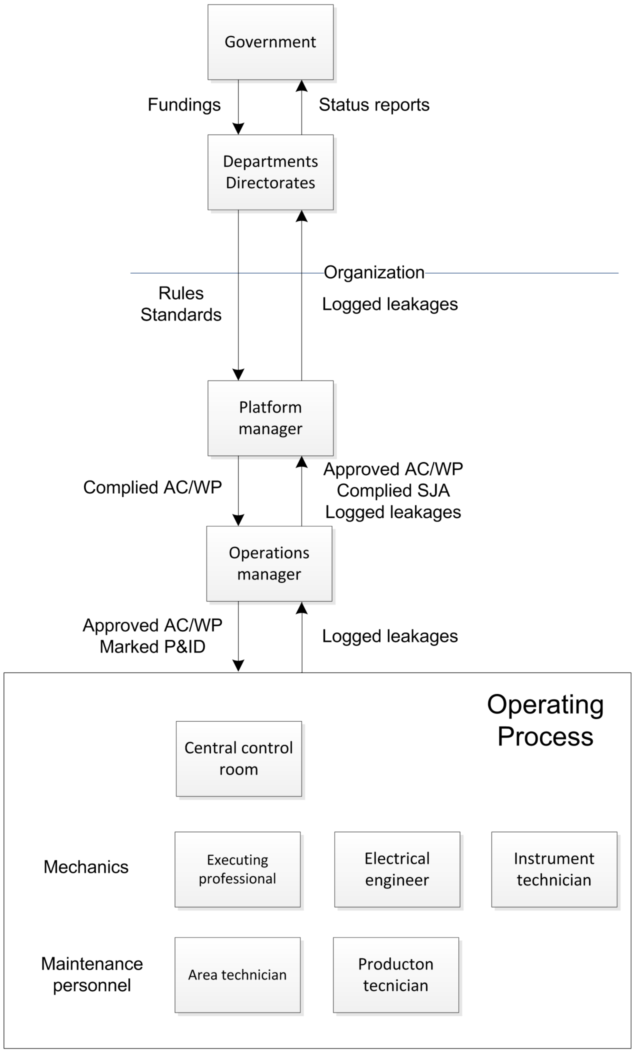


Figure B.1: Overall hierarchy of the maintenance procedure

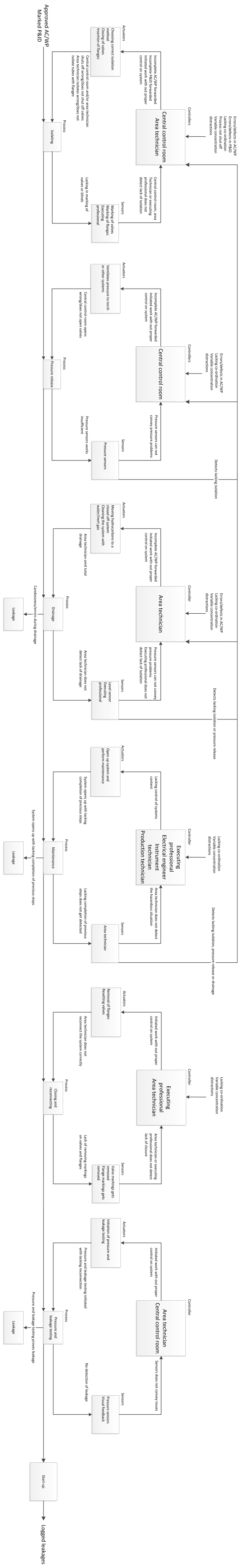


Figure B.2: STPA of the operating process

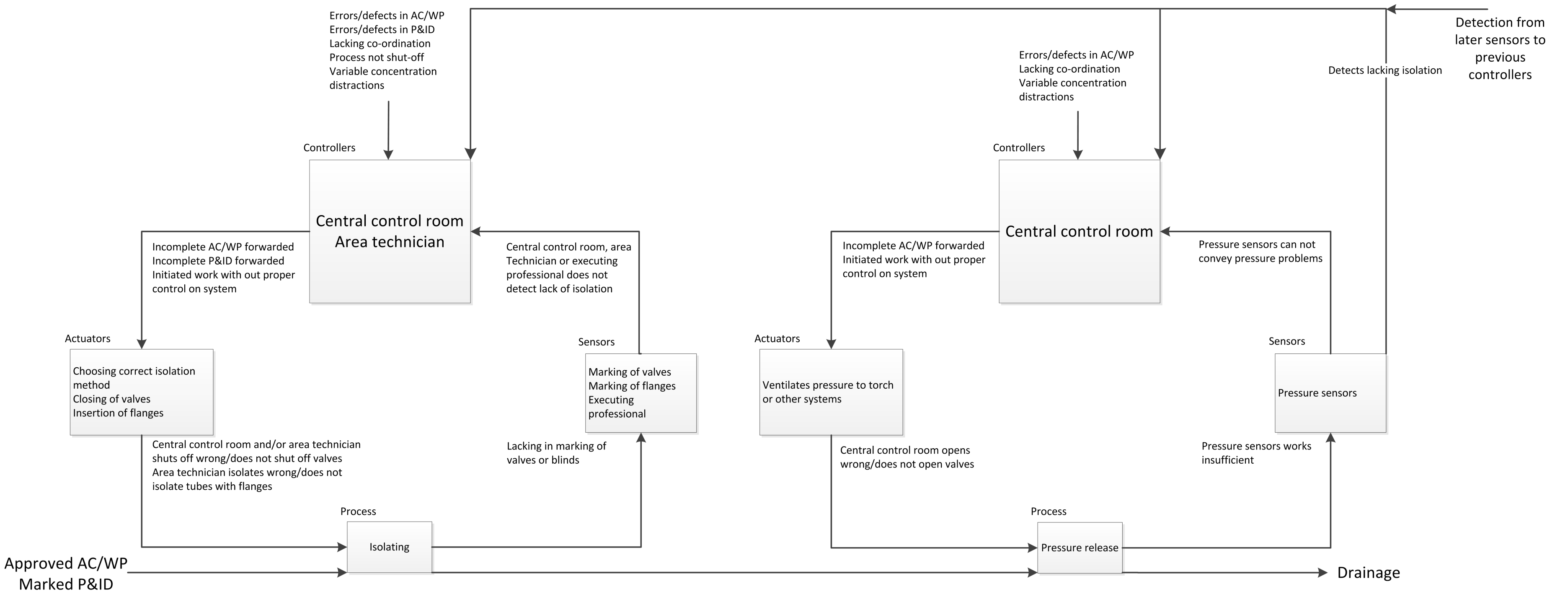


Figure B.3: The leftmost loops of the STPA of the operating process (figure B.2)

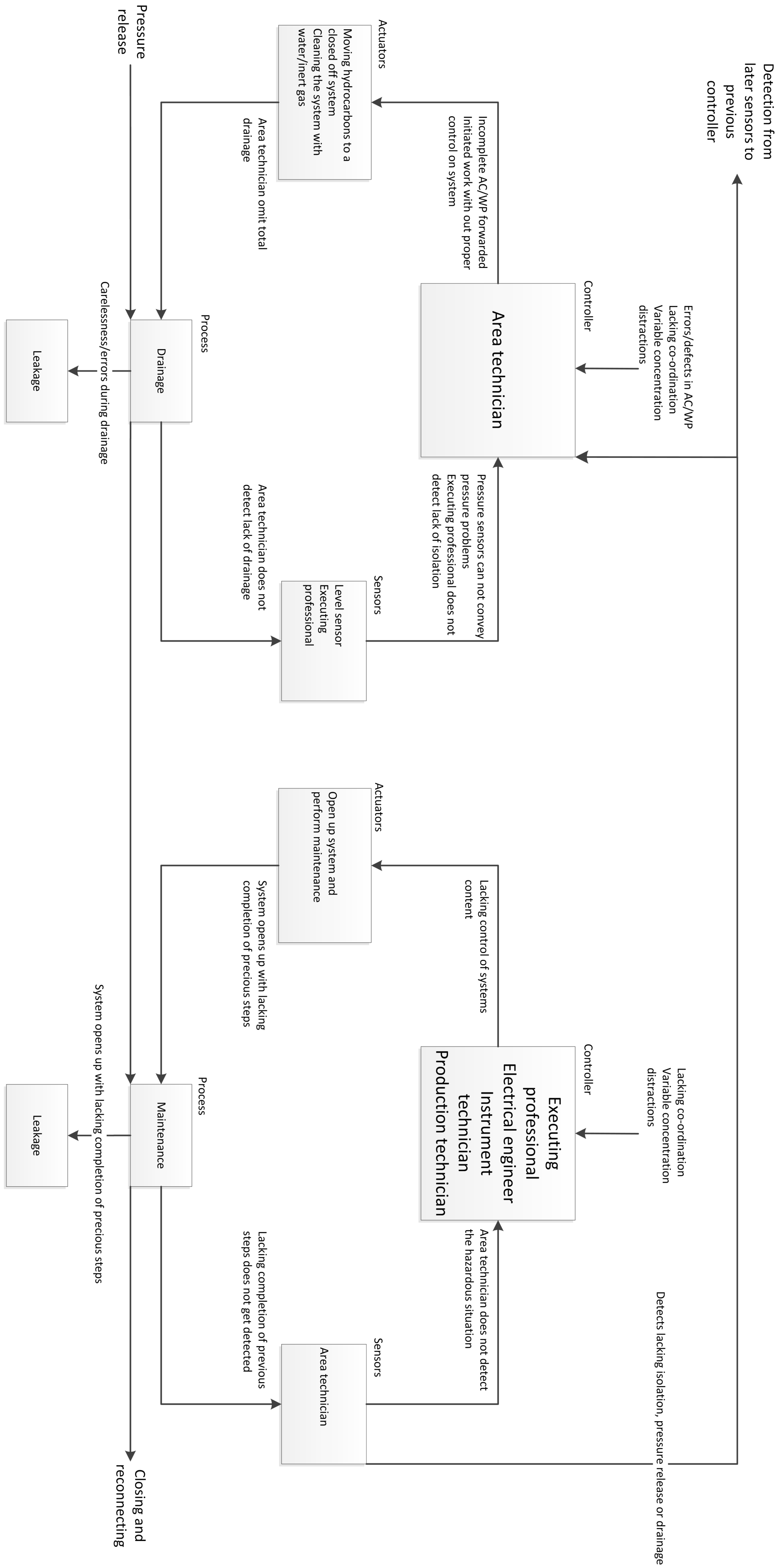

Detection from later sensors to previous controller
Errors/defects in AC/WP
Lacking co-ordination
Variable concentration
distractions
Controller
Area technician
Actuators
Moving hydrocarbons to a closed off system
Cleaning the system with water/inert gas
Incomplete AC/WP forwarded
Initiated work with out proper control on system
Area technician omit total drainage
Pressure release
Process
Drainage
Carelessness/errors during drainage
Leakage
Pressure sensors can not convey pressure problems
Executing professional does not detect lack of isolation
Sensors
Level sensor
Executing professional
Area technician does not detect lack of drainage
Lacking co-ordination
Variable concentration
distractions
Controller
Executing professional
Electrical engineer
Instrument technician
Production technician
Actuators
Open up system and perform maintenance
Lacking control of systems content
System opens up with lacking completion of precious steps
Process
Maintenance
System opens up with lacking completion of precious steps
Leakage
Area technician does not detect the hazardous situation
Sensors
Area technician
Lacking completion of previous steps does not get detected
Detects lacking isolation, pressure release or drainage
Closing and reconnecting

Figure B.4: The middle loops of the STPA of the operating process (figure B.2)

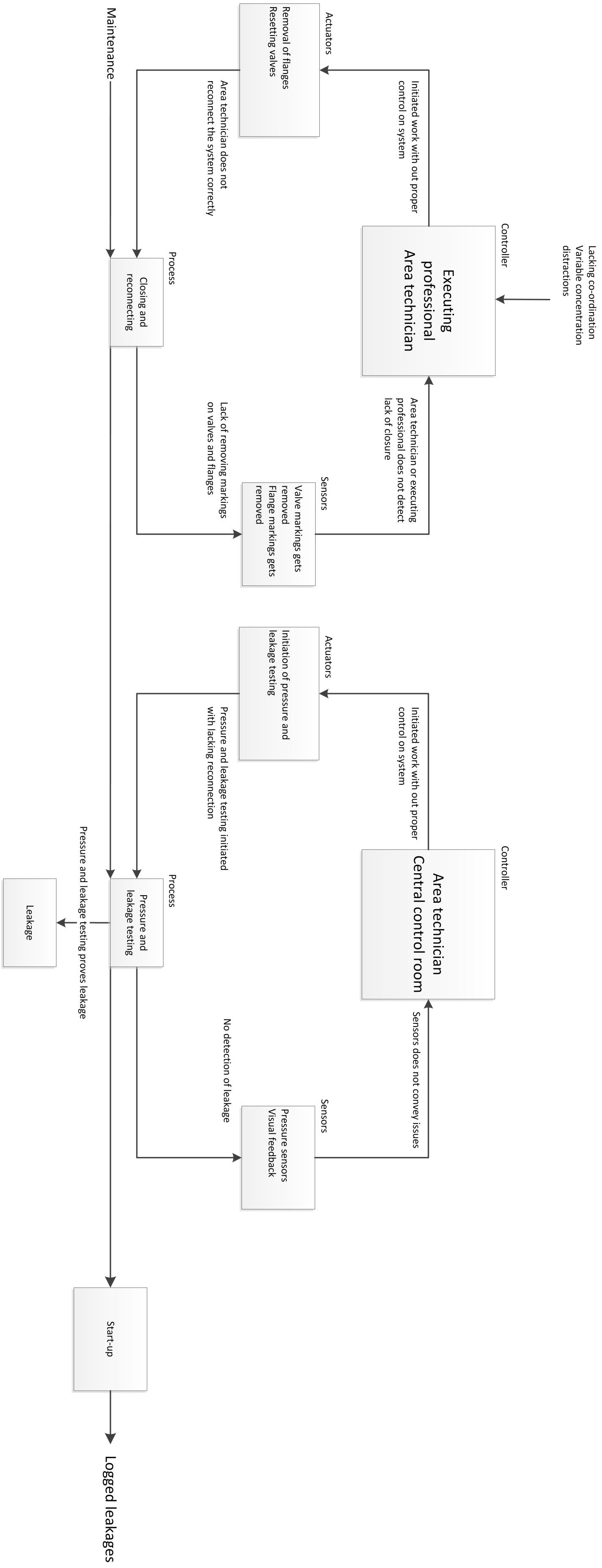

Lacking co-ordination
Variable concentration
distractions
Controller
Executing professional
Area technician
Initiated work with out proper control on system
Actuators
Removal of flanges
Resetting valves
Area technician or executing professional does not detect lack of closure
Sensors
Valve markings gets removed
Flange markings gets removed
Area technician does not reconnect the system correctly
Lack of removing markings on valves and flanges
Process
Closing and reconnecting
Maintenance
Controller
Area technician
Central control room
Initiated work with out proper control on system
Actuators
Initiation of pressure and leakage testing
Sensors does not convey issues
Sensors
Pressure sensors
Visual feedback
Pressure and leakage testing initiated with lacking reconnection
No detection of leakage
Process
Pressure and leakage testing
Pressure and leakage testing proves leakage
Leakage
Start-up
Logged leakages

Figure B.5: The rightmost loops of the STPA of the operating process (figure B.2)

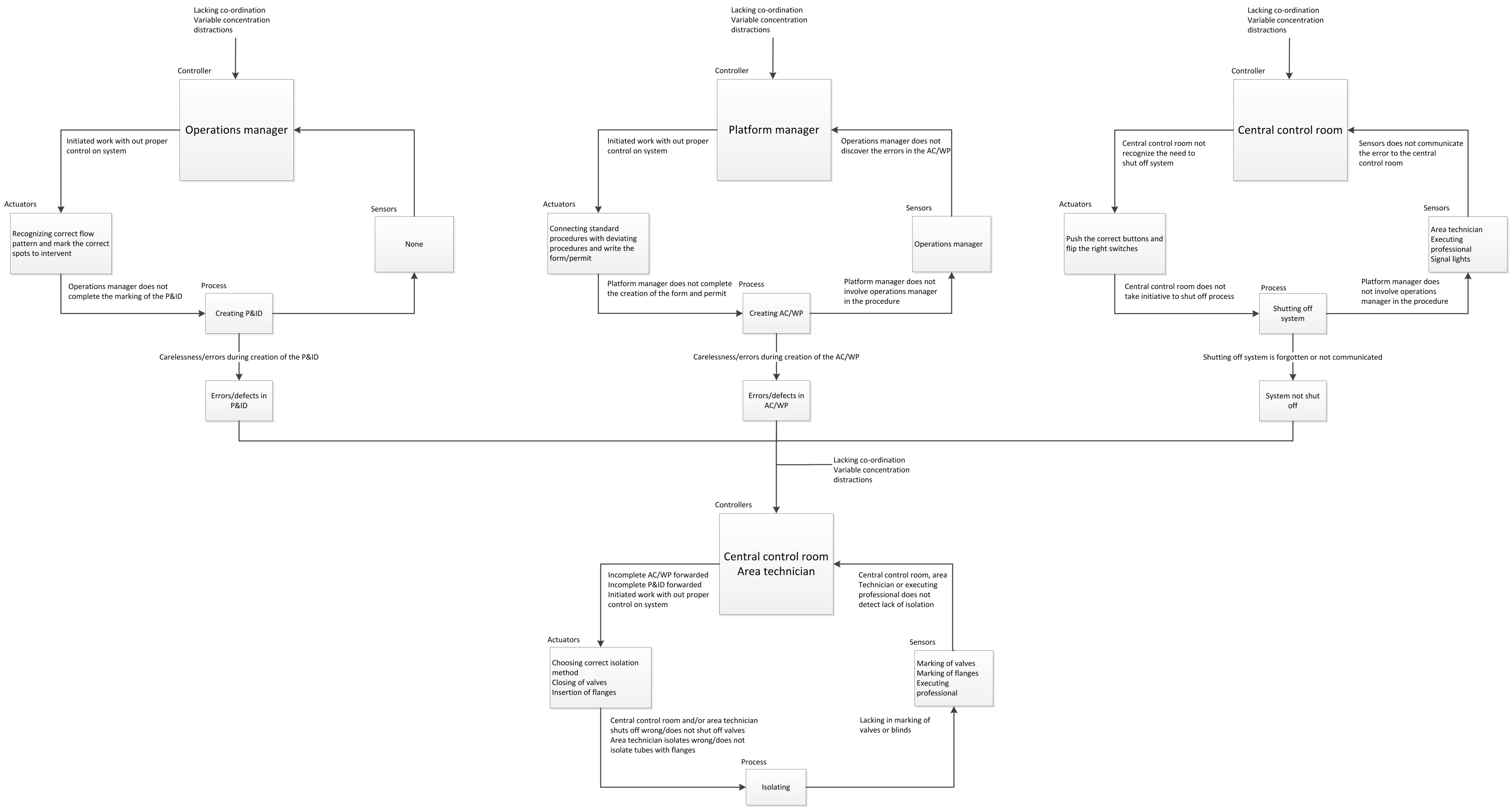

Lacking co-ordination
Variable concentration
distractions
Controller
Operations manager
Initiated work with out proper control on system
Actuators
Recognizing correct flow pattern and mark the correct spots to intervent
Operations manager does not complete the marking of the P&ID
Process
Creating P&ID
Sensors
None
Carelessness/errors during creation of the P&ID
Errors/defects in P&ID
Lacking co-ordination
Variable concentration
distractions
Controller
Platform manager
Initiated work with out proper control on system
Operations manager does not discover the errors in the AC/WP
Actuators
Connecting standard procedures with deviating procedures and write the form/permit
Sensors
Operations manager
Platform manager does not complete the creation of the form and permit
Process
Creating AC/WP
Platform manager does not involve operations manager in the procedure
Carelessness/errors during creation of the AC/WP
Errors/defects in AC/WP
Lacking co-ordination
Variable concentration
distractions
Controller
Central control room
Central control room not recognize the need to shut off system
Sensors does not communicate the error to the central control room
Actuators
Push the correct buttons and flip the right switches
Sensors
Area technician
Executing professional
Signal lights
Central control room does not take initiative to shut off process
Process
Shutting off system
Platform manager does not involve operations manager in the procedure
Shutting off system is forgotten or not communicated
System not shut off
Lacking co-ordination
Variable concentration
distractions
Controllers
Central control room
Area technician
Incomplete AC/WP forwarded
Incomplete P&ID forwarded
Initiated work with out proper control on system
Central control room, area Technician or executing professional does not detect lack of isolation
Actuators
Choosing correct isolation method
Closing of valves
Insertion of flanges
Sensors
Marking of valves
Marking of flanges
Executing professional
Central control room and/or area technician shuts off wrong/does not shut off valves
Area technician isolates wrong/does not isolate tubes with flanges
Lacking in marking of valves or blinds
Process
Isolating

Figure B.6: Further elaboration of the isolation process

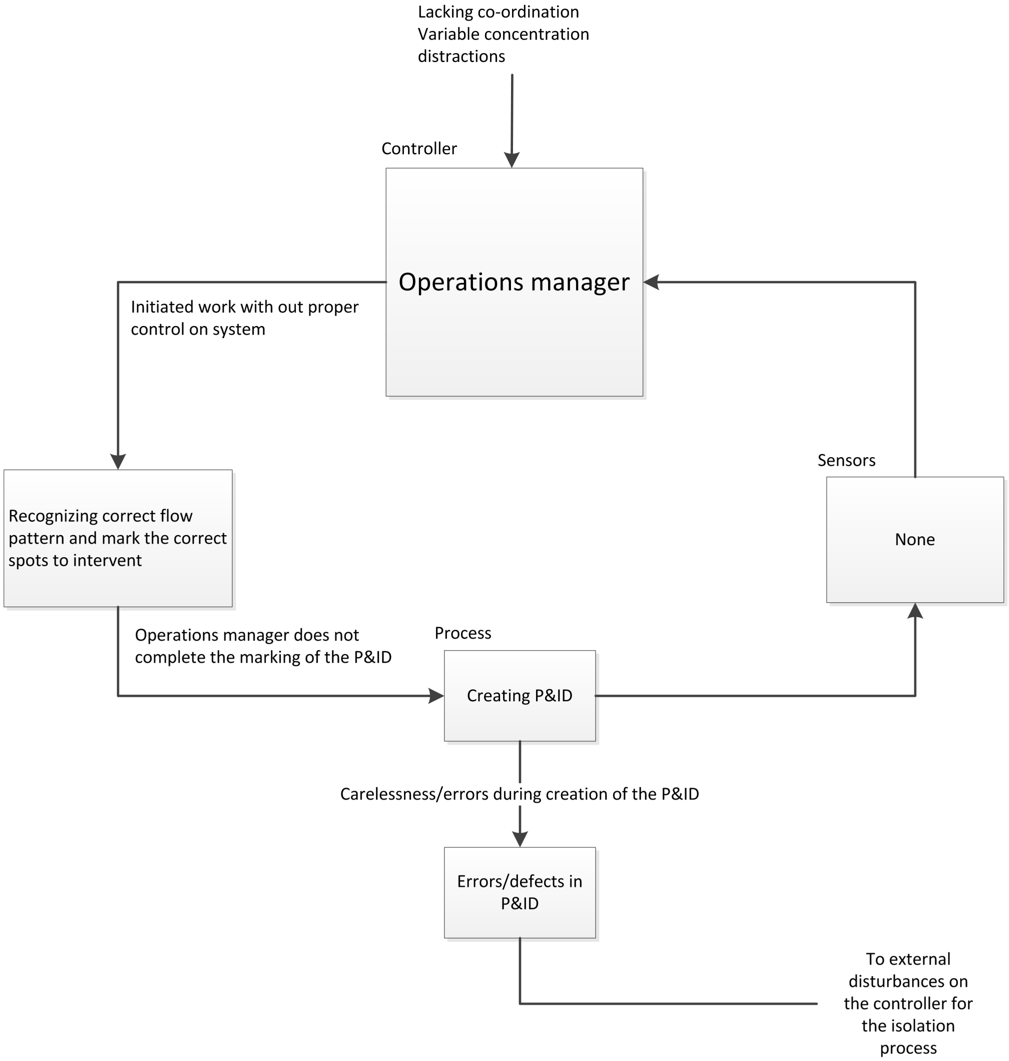

Lacking co-ordination
Variable concentration
distractions
Controller
Operations manager
Initiated work with out proper control on system
Recognizing correct flow pattern and mark the correct spots to intervent
Sensors
None
Operations manager does not complete the marking of the P&ID
Process
Creating P&ID
Carelessness/errors during creation of the P&ID
Errors/defects in P&ID
To external disturbances on the controller for the isolation process

Figure B.7: Left part of the further elaboration of the isolation process (figure B.6)

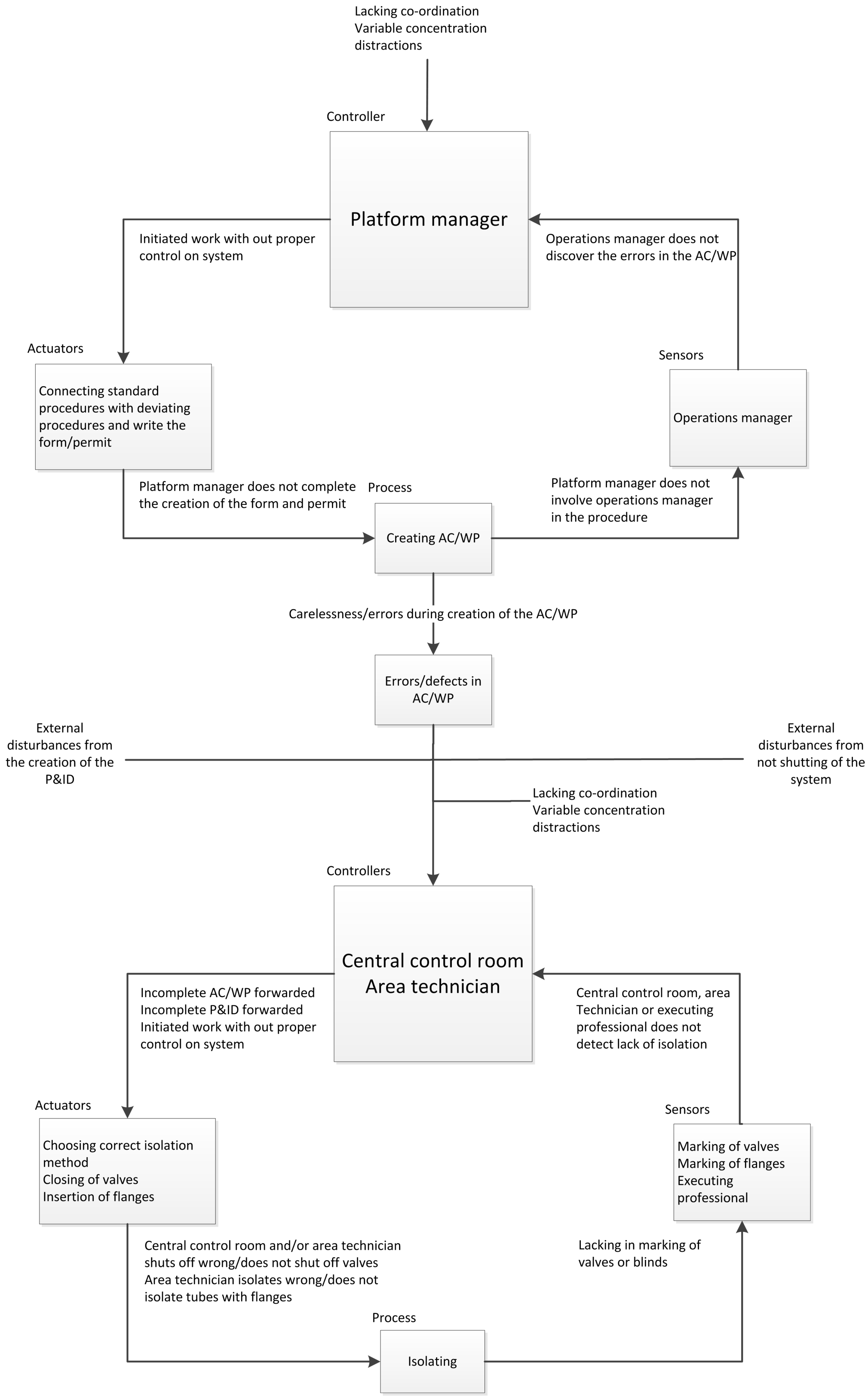

Lacking co-ordination
Variable concentration
distractions
Controller
Platform manager
Initiated work with out proper control on system
Operations manager does not discover the errors in the AC/WP
Actuators
Connecting standard procedures with deviating procedures and write the form/permit
Sensors
Operations manager
Platform manager does not complete the creation of the form and permit
Process
Creating AC/WP
Platform manager does not involve operations manager in the procedure
Carelessness/errors during creation of the AC/WP
Errors/defects in AC/WP
External disturbances from the creation of the P&ID
External disturbances from not shutting of the system
Lacking co-ordination
Variable concentration
distractions
Controllers
Central control room
Area technician
Incomplete AC/WP forwarded
Incomplete P&ID forwarded
Initiated work with out proper control on system
Central control room, area Technician or executing professional does not detect lack of isolation
Actuators
Choosing correct isolation method
Closing of valves
Insertion of flanges
Sensors
Marking of valves
Marking of flanges
Executing professional
Central control room and/or area technician shuts off wrong/does not shut off valves
Area technician isolates wrong/does not isolate tubes with flanges
Lacking in marking of valves or blinds
Process
Isolating

Figure B.8: Middle part of the further elaboration of the isolation process (figure B.6)

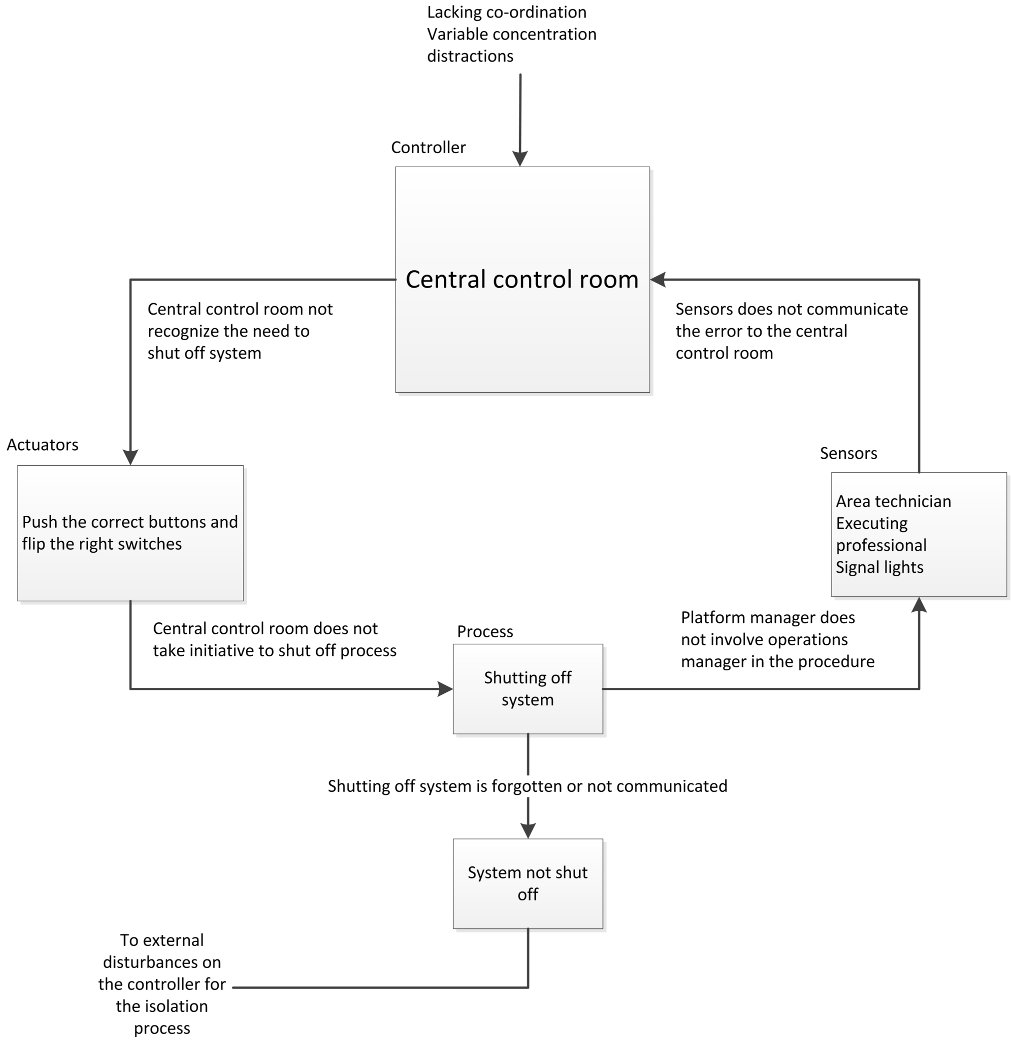

Lacking co-ordination
Variable concentration
distractions
Controller
Central control room
Central control room not recognize the need to shut off system
Sensors does not communicate the error to the central control room
Actuators
Push the correct buttons and flip the right switches
Sensors
Area technician
Executing professional
Signal lights
Central control room does not take initiative to shut off process
Process
Shutting off system
Platform manager does not involve operations manager in the procedure
Shutting off system is forgotten or not communicated
System not shut off
To external disturbances on the controller for the isolation process

Figure B.9: Right part of the further elaboration of the isolation process (figure B.6)

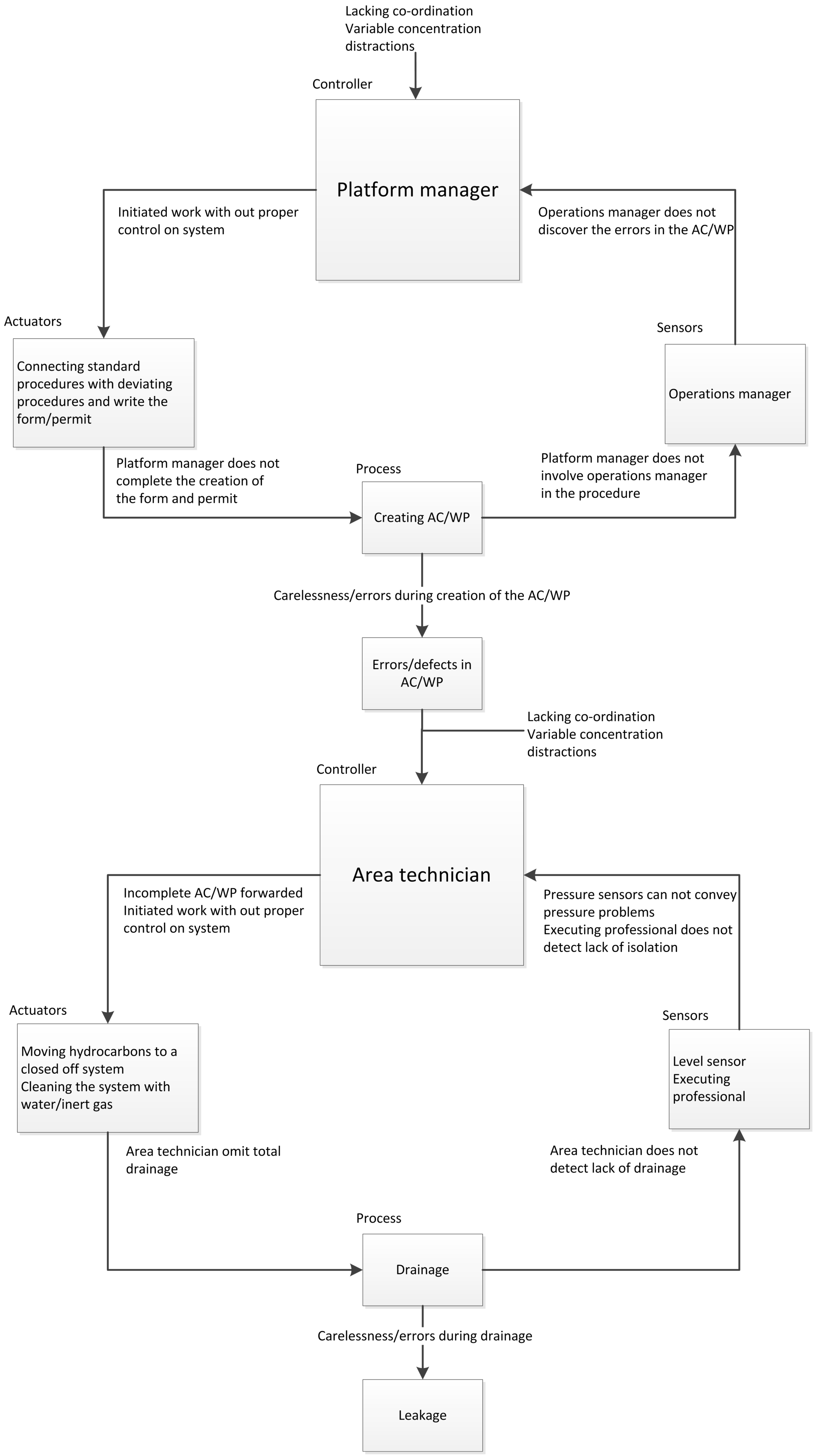

Lacking co-ordination
Variable concentration
distractions
Controller
Platform manager
Initiated work with out proper control on system
Operations manager does not discover the errors in the AC/WP
Actuators
Connecting standard procedures with deviating procedures and write the form/permit
Sensors
Operations manager
Platform manager does not complete the creation of the form and permit
Process
Creating AC/WP
Platform manager does not involve operations manager in the procedure
Carelessness/errors during creation of the AC/WP
Errors/defects in AC/WP
Lacking co-ordination
Variable concentration
distractions
Controller
Area technician
Incomplete AC/WP forwarded
Initiated work with out proper control on system
Pressure sensors can not convey pressure problems
Executing professional does not detect lack of isolation
Actuators
Moving hydrocarbons to a closed off system
Cleaning the system with water/inert gas
Sensors
Level sensor
Executing professional
Area technician omit total drainage
Area technician does not detect lack of drainage
Process
Drainage
Carelessness/errors during drainage
Leakage

Figure B.10: Further elaboration of the drainage process

Appendix C

Complete Event Trees

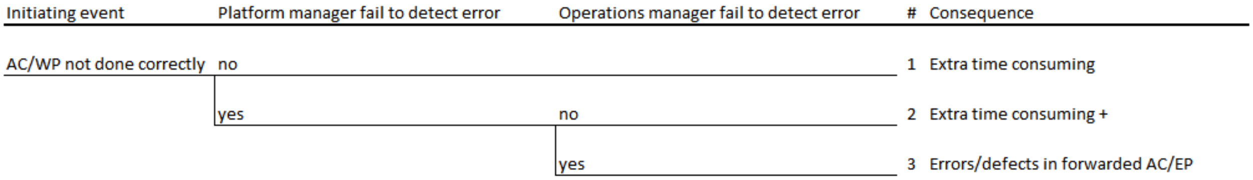

Initiating event
Platform manager fail to detect error
Operations manager fail to detect error
#
Consequence
AC/WP not done correctly
no
1
Extra time consuming
yes
no
2
Extra time consuming +
yes
3
Errors/defects in forwarded AC/EP

Figure C.1: Event tree of the “creating AC/WP” process

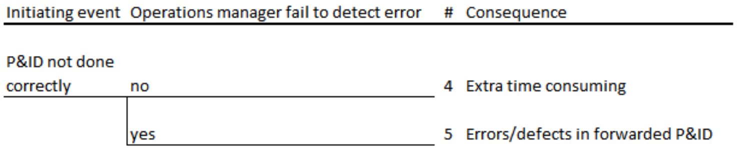


Figure C.2: Event tree of the “creating P&ID” process

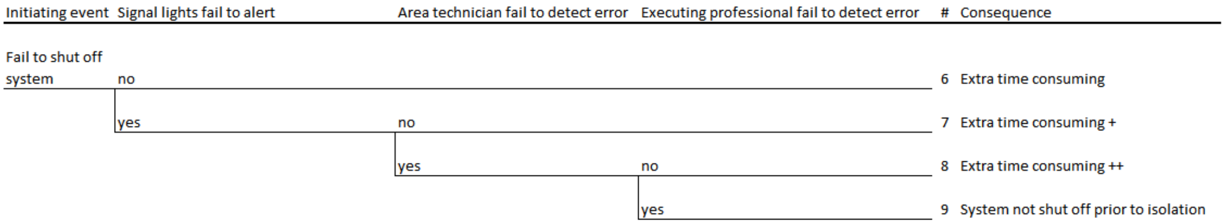

Initiating event
Signal lights fail to alert
Area technician fail to detect error
Executing professional fail to detect error
#
Consequence
Fail to shut off system
no
6
Extra time consuming
yes
no
7
Extra time consuming +
yes
no
8
Extra time consuming ++
yes
9
System not shut off prior to isolation

Figure C.3: Event tree of the “shutting off system” process

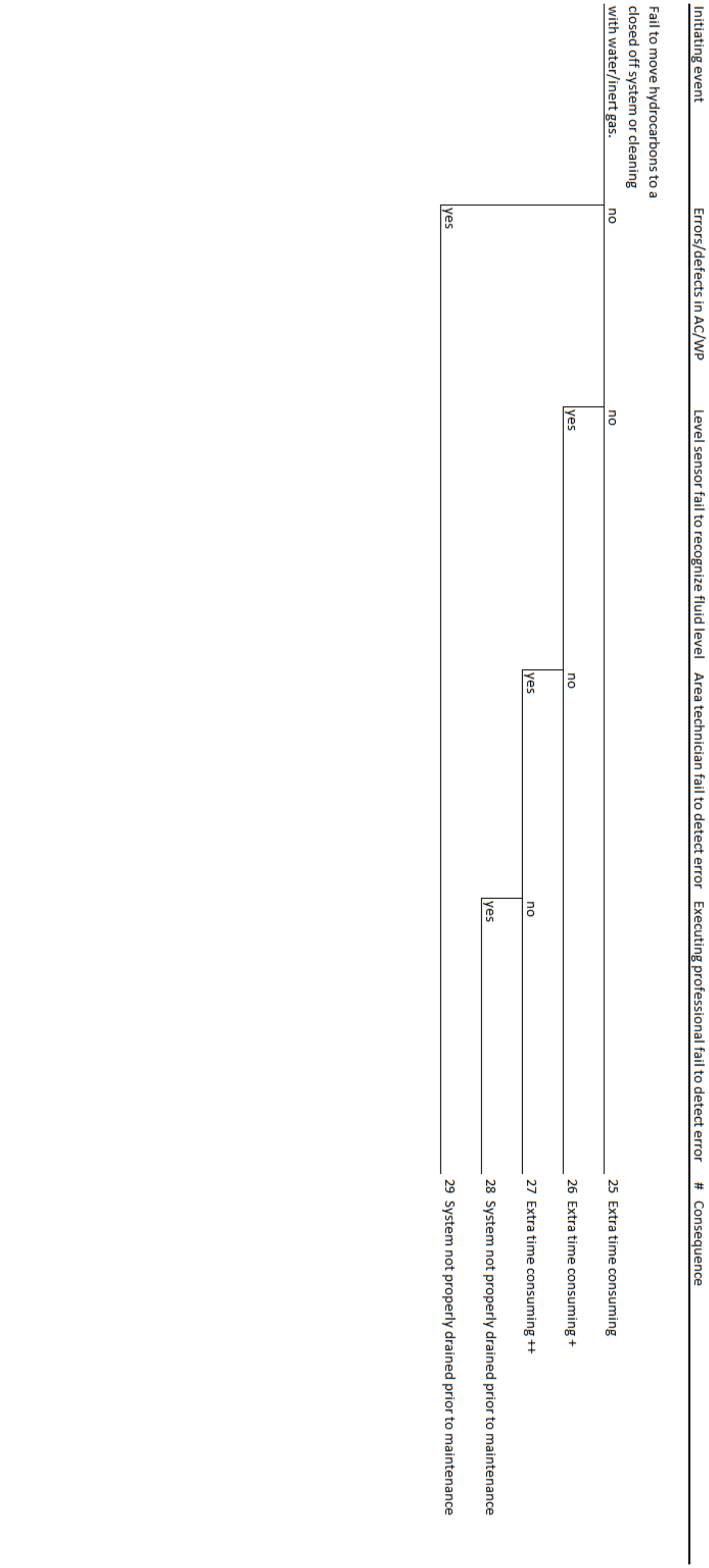

Initiating event
Errors/defects in AC/WP
Level sensor fail to recognize fluid level
Area technician fail to detect error
Executing professional fail to detect error
#
Consequence
Fail to move hydrocarbons to a closed off system or cleaning with water/inert gas.
no
yes
no
yes
no
yes
no
yes
25 Extra time consuming
26 Extra time consuming +
27 Extra time consuming ++
28 System not properly drained prior to maintenance
29 System not properly drained prior to maintenance

Figure C.4: Event tree of the “drainage” process

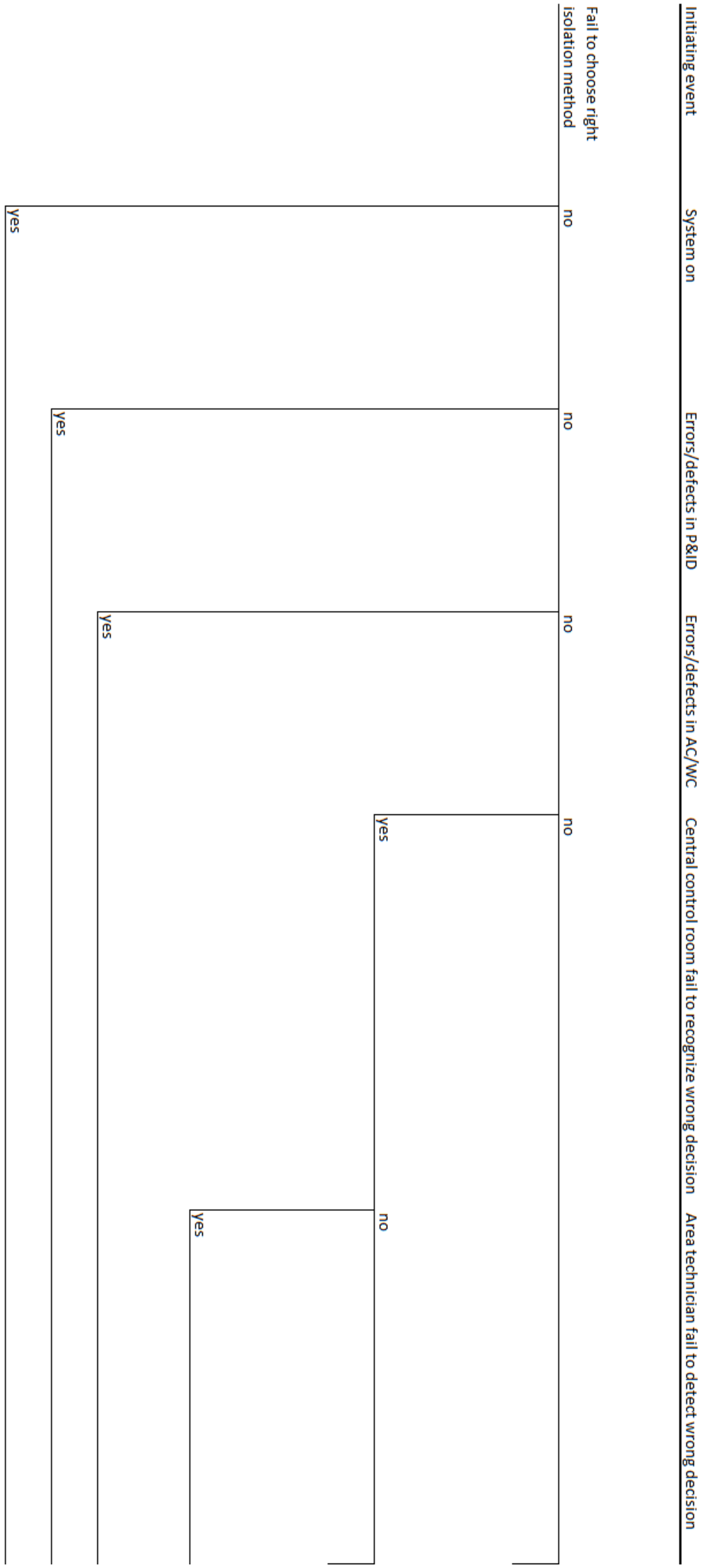

Initiating event
Fail to choose right isolation method
System on
Errors/defects in P&ID
Errors/defects in AC/WC
Central control room fail to recognize wrong decision
Area technician fail to detect wrong decision
no
yes
no
yes
no
yes
no
yes
no
yes

Figure C.5: Event tree of the “isolating” process. Continue on next page

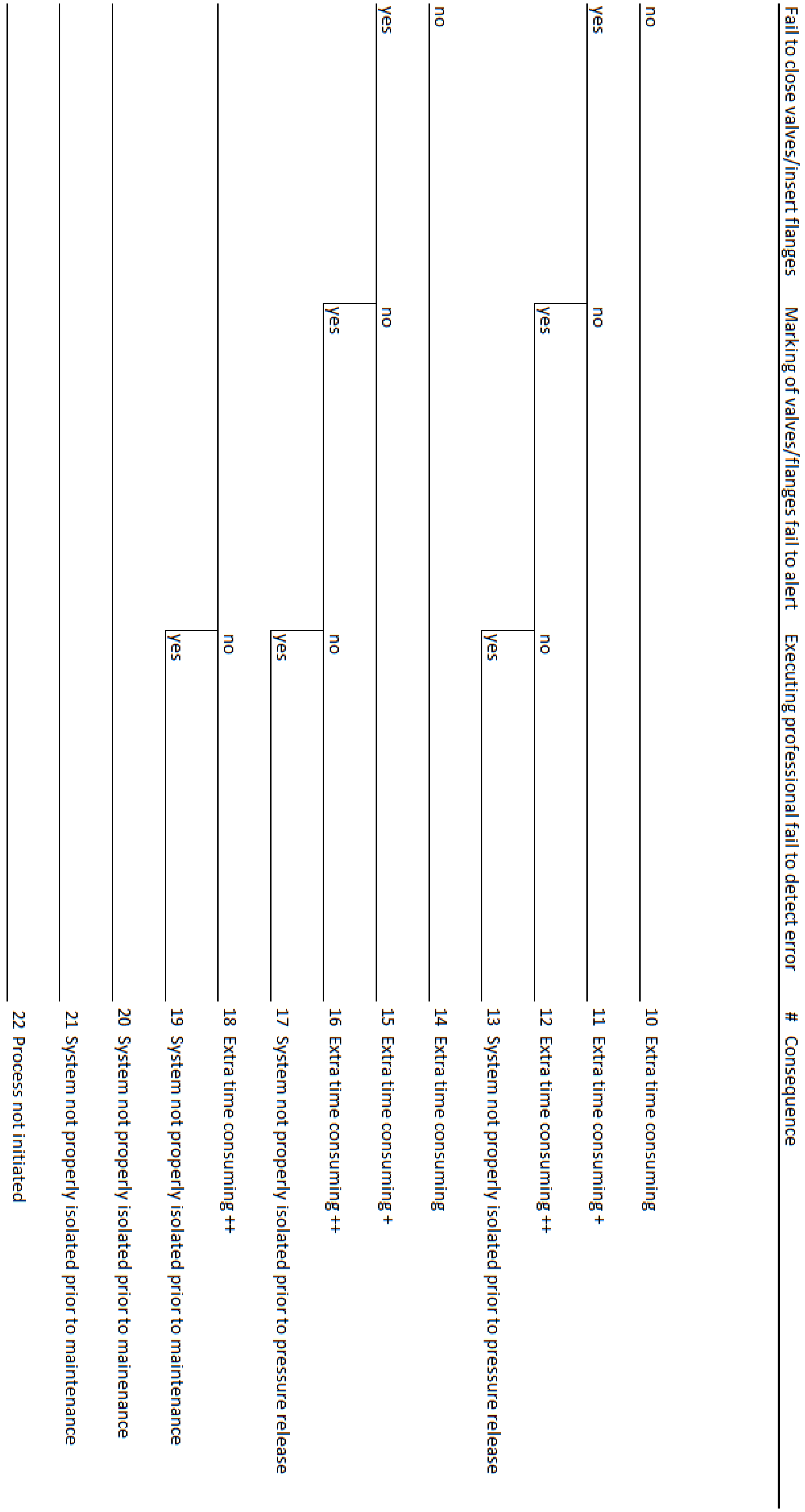

Fail to close valves/insert flanges
Marking of valves/flanges fail to alert
Executing professional fail to detect error
# Consequence
no
yes
no
yes
no
yes
no
yes
no
yes
no
yes
no
yes
10 Extra time consuming
11 Extra time consuming +
12 Extra time consuming ++
13 System not properly isolated prior to pressure release
14 Extra time consuming
15 Extra time consuming +
16 Extra time consuming ++
17 System not properly isolated prior to pressure release
18 Extra time consuming ++
19 System not properly isolated prior to maintenance
20 System not properly isolated prior to mainenance
21 System not properly isolated prior to maintenance
22 Process not initiated

Figure C.6: Event tree of the “isolating” process

Appendix D

Pre-study Report

D.1 Introduction

This pre-study report is developed as an assistance to the early stages of the master thesis, regarding a quick analysis of the objectives at hand and setting an approximately time schedule to secure a steady progress. The main objective is to test the STAMP and the corresponding STPA on a definite problem concerning process leaks on an offshore installation, thus a set of subtasks is defined to accommodate this objective:

1. Literature Study - review and summary of relevant literature about STAMP and STPA, and address the challenges.
2. Establish a model for leakage, based on the STAMP/STPA. The model should be qualitative, but the goal is to form a basis for quantitative assessment.
3. Identify data requirements for such a model and assess the availability of data necessary to quantify risk.
4. Consider the developed model and the performed work in terms of:
    - (a) Work scope, compared with traditional methods of analysis
    - (b) New possibilities related to decision making support, compared with traditional methods of analysis

(c) Whether quantification is possible with such a model, an if so, which new types of data must be provided to quantify the results.

5. Summarize and make recommendations for further work.

The pre-study report commence by describing the project into more detail, including personal, current, thoughts about the subject. In the end the report will include a simple WBS and GANTT. Obviously, this report is a result of early assumptions and unexperienced thoughts, so subjects is certain to change.

D.2 Project Description

D.2.1 Analysis of the Project Objectives

Task One

Literature Study - review and summary of relevant literature about STAMP and STPA, and address the challenges.

Using previously written assignments and utilizing accumulated knowledge regarding this field, task number one should be easy to overcome in a quick manner. Sectioning up task one in human reliability, the emerging new paradigm, resilience and STAMP seems like a good idea, probably adding a part about the hydrocarbon leakage issue. The major challenge is to draw in enough knowledge about the methods to actually apply the method, but this concerns task two.

Task Two

Establish a model for leakage, based on the STAMP/STPA. The model should be qualitative, but the goal is to form a basis for quantitative assessment.

This is, at the moment, the most crucial task and the core of the thesis. Obviously this should be the main concern at the beginning, and probably the task that needs the most attention and time throughout the thesis. Getting enough data to perform this part is necessary, but how much data needed is uncertain. The strategy is to attack this part of the thesis after quickly performing task one, and see where it goes. Performing task two well is needed for the thesis to be of any relevance, but even so it is important not to get lost and have enough time to perform rest of the thesis.

Task Three

Identify data requirements for such a model and assess the availability of data necessary to quantify risk.

Hopefully this task will solve itself naturally while performing task two, or at least be more obvious, because right now this is a challenging task to solve. It is the second part that receives most concern, because it is not necessary that such possibility exist. As stated, this should become clearer with the time, thus postponing this task seems logical.

Task Four

Consider the developed model and the performed work in terms of:

1. *Work scope, compared with traditional methods of analysis*

2. *New possibilities related to decision making support, compared with traditional methods of analysis*

3. *Whether quantification is possible with such a model, an if so, which new types of data must be provided to quantify the results.*

Just like task three, this is highly affected by the work in task two. Likewise the last subtask resembles task three, and probably have some correlations. Although besides task two, this is probably the task that takes the most time to work through, and the second subtask could prove some interesting results.

Task Five

Summarize and make recommendations for further work.

This comes natural at the end of the thesis. This is a part of the thesis that probably is useful to work on together with the conclusions and summary.

D.2.2 Course of Action

Workload

The workload of the thesis should resemble 48 hours of work per week, and 20 weeks worth of work, meaning approximately nine hours and 36 minutes per day by excluding weekends. Hope this includes lunch..!

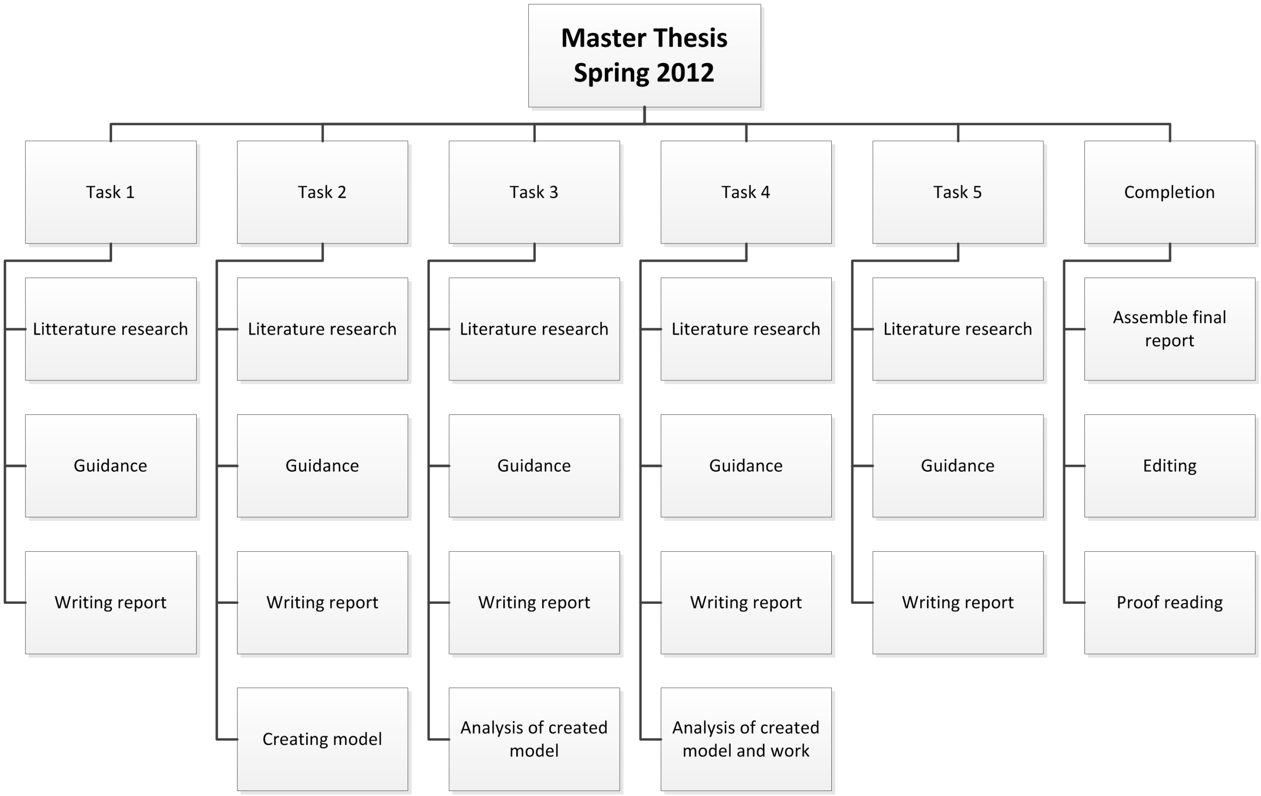
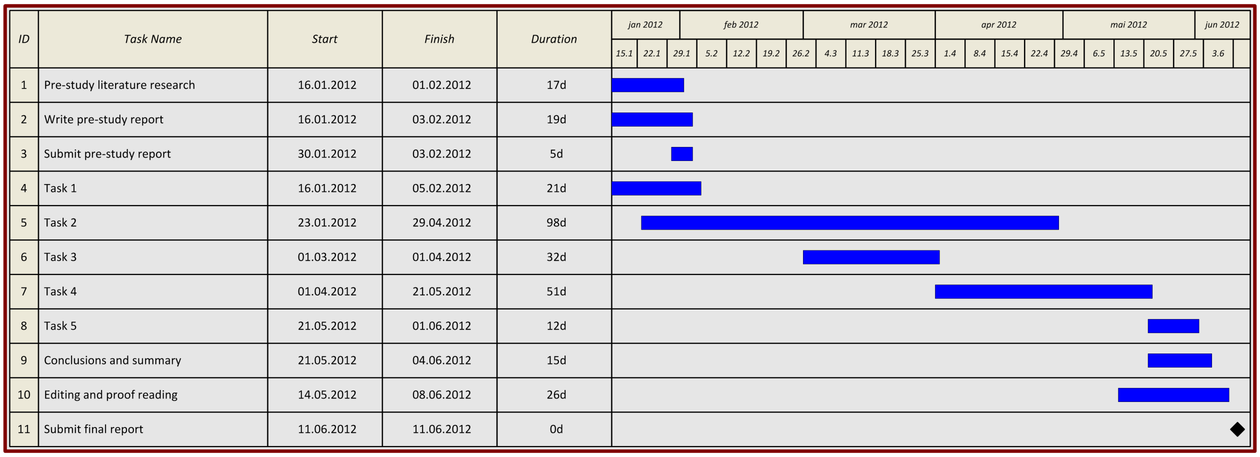


Figure D.1: A work breakdown structure of the master thesis



ID	Task Name	Start	Finish	Duration
1	Pre-study literature research	16.01.2012	01.02.2012	17d
2	Write pre-study report	16.01.2012	03.02.2012	19d
3	Submit pre-study report	30.01.2012	03.02.2012	5d
4	Task 1	16.01.2012	05.02.2012	21d
5	Task 2	23.01.2012	29.04.2012	98d
6	Task 3	01.03.2012	01.04.2012	32d
7	Task 4	01.04.2012	21.05.2012	51d
8	Task 5	21.05.2012	01.06.2012	12d
9	Conclusions and summary	21.05.2012	04.06.2012	15d
10	Editing and proof reading	14.05.2012	08.06.2012	26d
11	Submit final report	11.06.2012	11.06.2012	0d

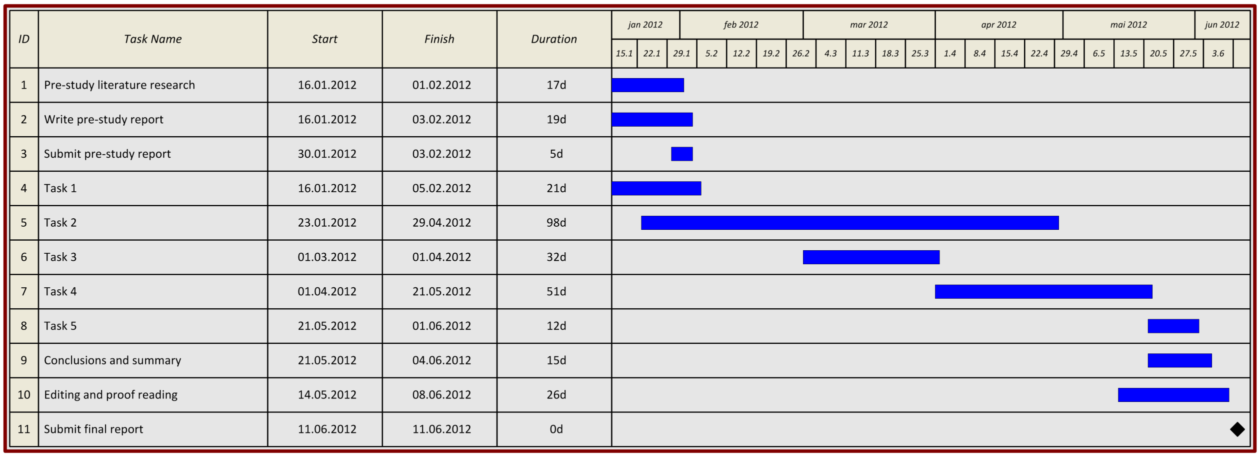
Figure D.2: A Gantt chart of the master thesis

Appendix E

Progress Report, End of March

This progress report is used as an opportunity to take a look in the rear-mirror and reflect upon the work that has actually been done, and at the same time do some adjustments to further progress.

E.1 Expected Progress and Deviations



ID	Task Name	Start	Finish	Duration
1	Pre-study literature research	16.01.2012	01.02.2012	17d
2	Write pre-study report	16.01.2012	03.02.2012	19d
3	Submit pre-study report	30.01.2012	03.02.2012	5d
4	Task 1	16.01.2012	05.02.2012	21d
5	Task 2	23.01.2012	29.04.2012	98d
6	Task 3	01.03.2012	01.04.2012	32d
7	Task 4	01.04.2012	21.05.2012	51d
8	Task 5	21.05.2012	01.06.2012	12d
9	Conclusions and summary	21.05.2012	04.06.2012	15d
10	Editing and proof reading	14.05.2012	08.06.2012	26d
11	Submit final report	11.06.2012	11.06.2012	0d

Figure E.1: GANTT featured in the pre-study report

According to my expected progress (see figure E.1), task 1 and 3 were supposed to be finished, task 2 two thirds finished and task 4 is about to be started. As it stands now, task 1 is roughly finished together with task two, but task 3 has yet to be started.

There was a lot more work involved in task 1 than first anticipated, especially for getting to know the maintenance procedure. Thus, getting started on the STPA took more time than expected. On the contrary, it took less time to finish the STPA than expected. This means that even though the work on task 3 is lagging, it is more time to perform it now than expected.

E.2 Future Progress

Task 4 is mostly thought out by performing the STPA, and a lot of notes are made for use in this task. Some initial thoughts and possible solution have been explored about task 3 as well, but right now this is the most crucial part. Overall, the progress looks good and the work with the thesis seems to be ahead of schedule. The major work input will obviously be directed towards task 3 and 4 from now on.

Bibliography

Clarke, P and Young, S. (2006) *Reliability-centered Maintenance and HAZOP - Is there a need for both?*. Available from: http://www.assetpartnership.com/downloads/RCMvsHazop.pdf (Acquired: 28.05.2010).

Degani, A. and Wiener, E. L. (1994) 'The four "P"s of flight deck operation." In N. Johnston, N. McDonald and R. Fuller (eds) *Aviation Psychology in Practice.* Aldershot: Avebury Technical.

Haugen, S. et al. (2011) *Analysis of Causes of Hydrocarbon Leaks from Process Plants* SPE European Health, Safety and Environmental Conference in Oil and Gas Exploration and Production. Vienna.

Hoel, F. (2011) *Investigation of Alternative Framework for Risk Assessment.* Project Thesis. Norwegian University of Science and Technology, Trondheim.

Hollnagel, E. et al. (2008) *Resilience Engineering Perspectives, Volume 1: Remaining Sensitive to the Possibility of Failure.* Aldershot: Ashgate Publishing Limited.

Hollnagel, E. et al. (2008) *Resilience Engineering Perspectives, Volume 2: Preparation and Restoration.* Aldershot: Ashgate Publishing Limited.

Ishimatsu, T. et al. (2010) *Modeling and Hazard Analysis using STPA.* NASA 2010 IV&V Annual Workshop. Available from: http://www.nasa.gov/centers/ivv/pdf/482479main_3500_-_2010_IV%26V_Modeling_and_Hazard_Analysis_Using_STPA.pdf (Acquired: 27.02.2012).

Leveson, N. (2003) *A New Accident Model for Engineering Safer Systems.* Available from: http://sunnyday.mit.edu/accidents/safetyscience-single.pdf (Acquired: 05.09.2011).

Leveson, N. et al. (2006) *Engineering Resilience into Safety-Critical Systems*, in Hollnagel, E. et al. (ed.) *Resilience Engineering Concepts and Precepts*. Aldershot: Ashgate Publishing Limited.

Leveson, N. (2010) *A New Approach to Safety in Software-Intensive Systems*. Available from: http://www.azimuth-corp.com/conference/S52010/papers/presentations/Day_1/A%20 New%20Approach%20to%20Safety%20in%20Software-Intensive%20Systems%20%5BLeveson %5D.pdf (Acquired: 05.09.2011).

Leveson, N. (2011) *Engineering a Safer World - Systems Thinking Applied to Safety*. Massachusetts: MIT Press.

Nakao, H. et al. (2011) *Safety Guided Design of Crew Return Vehicle in Concept Design Phase Using STAMP/STPA*. Available from: http://sunnyday.mit.edu/safer-world/CRV.pdf (Acquired: 27.02.2012).

Qureshi, Z. H. (2008) *"A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems"*. Edinburgh: Command, Control, Communications and Intelligence Division DSTO.

Rasmussen, J. (1997) "Risk Management in a Dynamic Society: A Modelling Problem", *Safety Science*, 27 (2/3), p.183-213.

Rausand, M (2011) *Risk Assessment Theory, Methods, and Applications*. Hoboken: John Wiley & Sons, inc.

Rausand, M and Høyland, A. (2004) *System Reliability Theory - Models, Statistical Methods, and Applications*. Hoboken: John Wiley & Sons, Inc.

Rausand, M. and Utne, B. (2009) *Risikoanalyse - teori og metoder*. Trondheim: Tapir akademisk forlag.

Reason, J. (1990) *Human Error*. Cambridge: Cambridge University Press.

Reason, J. (1997) *Managing the Risk of Organizational Accidents*. Aldershot: Ashgate Publishing Limited.

Reason, J. (2008) *The Human Contribution - Unsafe Acts, Accidents and Heroic Recoveries*. Farnham: Ashgate Publishing Limited.

Vinnem, J. E. et al. (2007) *Operational Risk Analysis - Total Analysis of Physical and Non-physical Barriers*. Available from: http://www.preventor.no/bora/BORA%20Handbook%20Rev%2000.pdf (Acquired: 17.11.2011).

Vinnem, J. E. et al. (2011) *Risk modelling of maintenance work on major process equipment on offshore petroleum installations*. Draft edition: Elsevier Editorial System for Journal of Loss Prevention in the Process Industries.

Zio, E. (2009) "Reliability engineering: Old problems and new challenges", *Reliability Engineering and System Safety*, 94, p.125-141.