University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization: Offshore Technology/ Industrial Asset Management	Spring semester, 2015 ~~Open~~ / Restricted access
Writer: Andika Rachman	…… (Writer's signature)
Faculty supervisor: R.M. Chandima Ratnayake External supervisor(s): Arnaud Barre	
Thesis title: On the Use of Historical Failures Patterns to Confront the Unforeseen	
Credits (ECTS): 30	
Key words: unforeseen failure black swan accident	Pages: 84 + enclosure: 16 Stavanger, 15th June 2015

On the Use of Historical Failures Patterns to Confront the Unforeseen

by

Andika Rachman

A Thesis Submitted to

Faculty of Science and Technology

University of Stavanger

As Partial Fulfilment of the Requirements for the Degree of

Master of Science

2015

Abstract

Deepwater Horizon blowout, Bhopal gas tragedy, and Fukushima nuclear accident are some examples of failures that are seemed to be unforeseen and surprising from ones perspectives. The future occurrence of similar events is not tolerable due to the nature of their consequences that are detrimental to the society, environment, and business. Therefore, there must be some approaches that are implemented to prevent and mitigate unforeseen failures. The aim of this thesis is to map the patterns (e.g. factors and conditions) underlying unforeseen failures. The notion comes from the belief that even though failures occurred in different places, different industries, different scenarios, and so on, they have similar patterns that trigger their occurrences. Based on the identified patterns, some methods are proposed as means to encounter unforeseen failures.

The work begins with systematic literature review of several historical unforeseen failures in order to investigate their underlying causes. The reviews will not be limited to the proximate events, i.e. human errors and technical failures, but also causal factors and symptoms that have existed long before the moment of the failures, i.e. social and organizational factors. The premise is that the combination of sound technical, human, and organizational perspective is required to understand the problems causing the failures. Similar factors and/or conditions that underlie each of the historical unforeseen failures are then identified.

Four common patterns that underlie unforeseen failures are identified: (1) dysfunctional and complex interactions between regulatory agencies, company's management, operators, physical equipment, and other component of the system; (2) ineffective control by regulatory agencies and management failure to uphold safety; (3) the tendency of the management to prioritize profitability over safety generates, creating decisions and actions that are detrimental to the safety of the system; and (4) unrecognized and/or neglected warning signals preceding the failures.

Two general recommendations that are drawn based on the identified patterns. The first one is to use hazard analysis based on systemic accident causation model. The conventional hazard analyses are no longer suitable to be used in highly complex socio-technical system as it overlooks the hazards that are developed from the interactions between components of the system, unsafe decisions and actions by the management and regulator, and organizational factors. Hazard analysis founded on systemic accident causation model should be used to consider the aspects that are overlooked by the traditional hazard analysis techniques. The second recommendation is to adopt proactive risk management approach by implementing leading indicators in the system. The implementation of leading indicators will enable the detection of hazardous operation (including unsafe decisions and actions) in the system and recognizing the important early warning signals that precede a failure.

Key words: unforeseen failure, black swan, accident.

Acknowledgments

I would like to express my gratitude to God almighty for giving me the opportunity to pursue a master degree in University of Stavanger. It was a roller coaster journey that gave me a lot to learn in the past two years.

A big thanks is given to my parents that have support me financially and emotionally. Their words of encouragement and prayers are the driving force that keep me resilient and gritty in any adverse conditions. My motivation is always to keep both of them proud and happy.

I would like to thank my soon-to-be-wife, Lovita Ghassini, for her endless support during my study in Norway. Her encouragement and patience gave me the energy to keep thriving during the hard time.

Special thanks is given to Prof. R.M. Chandima Ratnayake that has given me guidance since the start of my study. I really appreciate his help as well as ideas, inputs and propositions regarding academic and other aspects while I am a student in University of Stavanger.

Special thanks is given to my external supervisor, Arnaud Barre, for his time, idea, comments, and critical thinking, which are immensely beneficial for the development of my thesis.

To my fellow Indonesians, Faras, Dinda, Gilang, Ade, Jessica, and Hafiz, it has been a wonderful two years and I will never forget our time together in Stavanger. Thank you for the chatter and laughter that have brighten my days and kept my life colourful in the gloomy Stavanger.

Very special thanks to Dinda that taught me how to cook and kept me alive until today.

Table of Contents

List of Table

Table of Figures

List of Abbreviations

BP	British Petroleum
CCPS	Center for Chemical Process Safety
CSB	Chemical Safety Board
DyPASI	Dynamic Procedure for Atypical Scenarios Identification
ETA	Event-Tree Analysis
FAA	Federal Aviation Administration
FMEA	Failure Mode and Effect Analysis
FTA	Fault-Tree Analysis
HAZOP	Hazard and Operability Study
HCM	HIPPS control module
HIPPS	High-Integrity Pressure Protection System
HRO	High Reliability Organization
HSE	Health and Safety Executive
INES	International Nuclear Event Scale
MBO	Management by Objective
MBR	Management by Results
MCS	Master Control Station
MIC	Methyl Isocyanate
MMS	The Minerals Management Service
NASA	National Aeronautics and Space Administration
P&ID	Piping and Instrumentation Diagram
PST	Partial Stroke Testing
PT	Pressure Transmitter
SDV	Shutdown Valve
SIS	Safety Instrumented System
STAMP	Systems Theoretic Accident Modelling and Processes
STPA	System-Theoretic Process Analysis
TEPCO	Tokyo Electric Power Company

1 CHAPTER ONE – Introduction

1.1 Background

Failure of industrial systems is deemed to be a scourge for facility owners, especially in the era where the losses stemming failures is increasing due to creation of new or increased hazards, such as radiation due to nuclear accident or environmental damage due to oil spill (Leveson, 2004). Humans look as if they can no longer control the technologies that are made by themselves. These failures came as a surprise and were seemed to be unforeseen prospectively, but appear to be explainable and preventable retrospectively. Deepwater Horizon blowout, Bhopal gas tragedy, and Fukushima nuclear accident are some examples unforeseen failures among exhaustive list of major accidents that have occurred in man-made systems.

Unforeseen failure can be understood as a surprising extreme event relative to the present knowledge/belief (Aven, 2013a). They are not identified by the persons who conduct the risks analysis (or other stakeholders) because of either they do not have the knowledge regarding the failures or the events were presumed to have very low probability of occurrences. Aven believes that the key to the assessment and management of unforeseen failures lies on the knowledge dimension. Several approaches have been proposed to confront the occurrence of unforeseen failures, such as an extended risk and performance perspectives, utilization of signals and warnings, and improvement on transfer of knowledge (Aven, 2014).

This thesis will try to see from another perspective regarding on how unforeseen failures can be encountered. Several historical unforeseen failure cases will be reviewed to see if there are common patterns underlying their causation. The notion comes from the belief that even though failures occurred in different places, different industries, different scenarios, and so on, they have similar patterns that bring about their occurrences (Venkatasubramanian, 2011). The patterns could be conceived as common causes, factors, and conditions that might potentially initiate the occurrence of unforeseen failures. These patterns will be the foundation to propose methods to confront unforeseen failures.

1.2 Objectives

The main objective of this thesis is to map the patterns underlying unforeseen failures and propose, based on patterns finding and literature review, prospective methods to confront (e.g. prevention and mitigation) the future unforeseen failures. The methods can be in the form of a new type of hazard analysis to identify the scenarios underlying the unforeseen failures, a new approach in risk management strategy, utilization of early warning signals, etc.

1.3 Approach

Several unforeseen failure cases from various industries are selected and studied to find if there are some generalities, e.g. causes, factors, or conditions, that led to their occurrences. The selected cases should reflect the definition of unforeseen failures given in the thesis. In-depth literature review

will be carried out from various sources, such as accident investigations reports, scientific journals and papers, and books, to investigate the causal of the failures. The results of the literature review are then used to identify common patterns underlying the failures. Subsequently, based on patterns finding and understanding the general causes of where the failures are stemmed from, some methods will be proposed to enable preventing and mitigating unforeseen failures in the future.

1.4 Research Limitations

Several historical failures are selected as the case studies and they are assumed as the representative of the entire unforeseen failure cases that has happened in the past. The major limitation lies on the possibility that the other cases have different characteristics and patterns with the selected cases. Additionally, the selected case studies are limited to the oil and gas, nuclear, refinery, and other industries where the loss of containment becomes the major hazard. Failures in aviation, rail transport, and maritime industry are not included and they might have different patterns.

1.5 Report Structure

The thesis will be structured as follow:

- Chapter two will provide the basic knowledge about unforeseen failures. This chapter is mainly founded based on the book *Risk, Surprises, and Black Swans* written by Terje Aven. Clear definition of unforeseen failure will be given as one of the foundations of the thesis. Moreover, the current proposed approaches to confront unforeseen failures will also be discussed.
- Chapter three will discuss about how to appropriately learn from accidents. Various accident investigation reports are different in terms of their perspectives on the accident. The important question to be raised here is: what and which aspects should be incorporated to reveal the true underlying causes of a failure or accident? Several accident causation models underlying accident investigation report will be reviewed. The information from this chapter will become the building block for the unforeseen failure patterns identification in the following chapter.
- Chapter four will be mainly about the identification of unforeseen failure patterns. The methodology, research limitations, as well as the summary of the studies for each of the case will be provided here. At the end of the chapter, the findings and observations from the studies will be given.
- Chapter five is constructed based on the findings and observations results in the previous chapter. The discussion will revolve on how to confront unforeseen failures based on the identified patterns. Some methods are proposed to identify unforeseen failures and prevent their occurrence in the future.
- The suggested methods identified in the fifth chapter will be demonstrated in chapter six. An industrial system will be taken as a case study.
- The last chapter is the conclusions and recommendations for further work.

2 CHAPTER TWO – Defining and Confronting Unforeseen Failures

2.1 Introduction

This chapter is intended to give brief explanations regarding basics of unforeseen failures. The clear definition as well as the current approach to manage and assess unforeseen failures are provided. A brief explanations about the concept of black swans is also given in relation to the notion of unforeseen failures.

2.2 Defining Unforeseen Failures

2.2.1 Unforeseen failures

Based on Oxford Dictionaries, the word 'unforeseen' can be interpreted as "not anticipated or predicted" while the word 'failure' literally means the "action or state of not functioning". Hence, unforeseen failure can be defined literally as unanticipated/unpredicted state/condition at which a system, equipment, or component is not able to function properly. In this thesis, the term 'unforeseen failure' and 'unforeseen event' will be considered as equivalent with no distinction made, thus will be used interchangeably.

There are not so many scholars that provide a comprehensive definition regarding unforeseen failure. England et al. (2008) defines it as any possible action which was not previously identified, or identified but dismissed because its probability of occurrence was too small. A more comprehensive description is formed by Aven and Krohn (2014), who include knowledge/beliefs dimension to the definition of unforeseen failure. They argues that the consideration whether an event is unforeseen or not is relative to the person's knowledge and beliefs. Aven and Krohn divide unforeseen events into three main categories:

1. Events that were utterly unthinkable and unknown to the scientific community, i.e. *unknown unknowns*.
2. Events that were not known and thus unidentified by ones point of views, but might have been identified from the others perspectives i.e. *unknown knowns*.
3. Events on the list of known events but deemed to have extremely low probability of occurrence.

The first type of unforeseen events is the *unknown unknowns*, which according to Aven (2014) must involve new phenomena or process that is unknown to the scientific community. This type of events will definitely be unanticipated and unpredicted as we do not know what we do not know. An example of *unknown unknowns* is a new type of disease caused by a new virus and a new degradation mechanism that causes failure in oil and gas pipeline. The second type is the *unknown knowns*, which are events that were unknown to the persons who did the risk assessment, but could have been identified by the others. This might happen because of the risk assessors' lack of

knowledge. The third one is events that were known, but presumed to have a very low probability and thus overlooked in the risk assessment.

The second and the third type of unforeseen failures will be surprising given their occurrence, but not necessarily for *unknown unknowns*. Gross (2010) argues that an event is regarded as surprising if its occurrence is against or deviated from ones belief and knowledge. As belief and knowledge create ones' expectation, we can say that there will be no surprise without expectation. In the case of *unknown unknowns*, we do not know what we do not know, i.e. we are free from any beliefs and expectations, and thus there will no surprise involved.

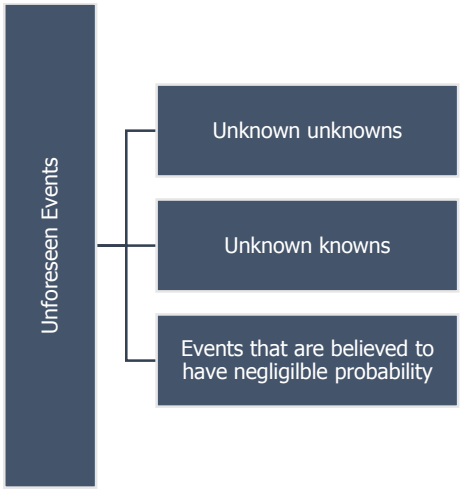

Figure 2.1 Aven and Krohn's definition of unforeseen events

2.2.2 Relation between black swans and unforeseen failures

Aven and Krohn relate their definition of unforeseen events with the concept of black swans. They argue that the three type of events described in section 2.2.1 can be expressed as black swans if their occurrence has extreme consequences.

The 'black swan' metaphor is firstly derived from a Latin quote written by Juvenal. He wrote "*rara avis in terris nigroque simillima cycno*", which in English means "a bird rarely seen on the lands, and very much like a black swan". At that time, the existence of black swans was considered implausible, thus this phrase was used to express impossibility. However, after the discovery of Australia, black swans were sighted at the first time in the Western Australia by Dutch explorer, Willem de Vlamingh in 1697. The observation of a single black swan tore down the Old World presumption regarding the existence of black swan. The truth is that if one has not observed or experienced a particular thing, it does not mean that thing is non-existent. This is in-line with the principle of falsifiability that expresses ones inability to prove the validity of a statement/hypothesis/theory if it cannot be experimentally tested, but only its falsity. Three centuries later, Taleb (2007) uses the black swan phrase to describe an event that comes as surprise and cause major consequences.

Taleb's definition regarding black swans is different with Aven and Krohn's. Aven and Krohn (2014) describes black swans with three categories of unforeseen failures (see section 2.2.1) while Taleb (2007) exclusively defines black swans as *unknown unknowns*. Taleb states, "What we call here a black swan is an event with the following three attributes. First, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme impact. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable". The *unknown unknowns* definition by Taleb is not as strict as Aven and Krohn's definition as it does not require the event to be a completely new phenomena or process.

While Aven and Krohn (2014) categorize events with very low probability of occurrence and extreme consequences as black swans, Taleb (2007) uses 'grey swans' metaphor is to express this type of events. According to Taleb, the main difference of grey swans with black swans is the expectation; black swans are not expected at all while grey swans are expected regardless of their rarity. Hole (2013) argues that statistical assessment of grey swan events is possible, but can be problematic as grey swans reside in the edge tail of a distribution (see Figure 2.2). There will be too many uncertainties in the estimation of grey swans probability of occurrences due to lack of pertinent data (2013). Therefore, there may still chance for people to overlook grey swan events, especially for those who have no proper tools to prepare. It is tempting to ignore grey swans given their scarcity. However, having 'ignoring the swans' policy can be dangerous due to their high impact.

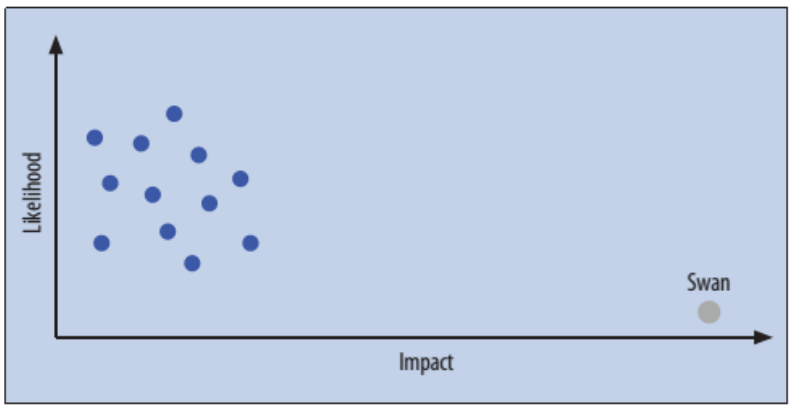

Figure 2.2 Illustration of a grey swan in likelihood versus impact graph (Hole, 2013)

Unlike Taleb and Aven and Krohn, Feduzi and Runde (2014) put distinction between the definition of black swans and *unknown unknowns*. Feduzi and Runde (2014) view an *unknown* as a hypothetical event, i.e. its real occurrence in the future is not known; it may either happen or not happen. They specify two distinct unknown based on the perspective of particular persons: *known unknown* which is imaginable from ones perspective and regarded as likely to occur in the future, and *unknown unknown* which is considered from ones viewpoint as unthinkable and unimaginable

to occur in the future. Meanwhile, they defines black swans as *unknown unknowns* that have become reality and been occurred.

2.3 Confronting Unforeseen Failures

Some approaches have been suggested by Aven (2014) to encounter the future occurrence of unforeseen failures. Some of them are concepts and ways of thinking that can be the foundations for further development in preventing unforeseen failures and surprises while some others are the newly developed or existing methods that might identify and prevent black swan type of events. Each of them will be briefly explained in the next sections.

2.3.1 Skepticism on the utilization of probability

An event might not be considered as a credible scenario in the risk analysis if it is deemed to have negligible probability of occurrence. Nonetheless, this could not be true as events with very low probability can still possibly occur. Aven (2014) argues that in order to prevent the occurrence of this type of unforeseen failures, probability alone shall not be used to determine whether an event or failure scenario is credible or not, especially in the case where uncertainties are extremely large and the knowledge strength is low. Similarly, Nafday (2009) argues that black swan type events cannot be predicted by the normal statistics of correlation, regression, or variance.

2.3.2 An extended risk and performance perspective

Based on the argument given in section 2.3.1, there is a need to see beyond probability to manage and assess black swan type of events. The new risk perspectives (Figure 2.3) as formulated by Aven (2013b) is proposed to enable seeing risk from broader viewpoint and to conceptualize unforeseen events and surprises.

Figure 2.3 The features of the new risk perspectives (adapted from (Aven, 2013b))

The new risk perspectives basically underline the importance knowledge dimension to reflect the strength of knowledge in the probabilistic analysis. From the new risk perspectives, Aven and Krohn (2014) proposes a fundamental idea to assess and manage unforeseen events and surprises that is constructed based on four basic elements:

1. A suitable risk conceptualization for the understanding, assessment and management of risk. This is based on the premise that probability-based approach alone will not be able to encounter unforeseen events and thus broader risk perspective is required.

2. Basic theory, principles and methods for risk assessment and management in line with this conceptualization, covering for example methods for quantifying risk and principles for the treatment of uncertainties, such as the precautionary principle.
3. Concepts and ideas from the quality management, relating to various types of variation and highlighting the importance of continuous improvement.
4. The concept of mindfulness as interpreted in the studies of High Reliability Organizations (HRO), capturing the five characteristics: preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience and deference to expertise

Each of these element will be discussed briefly in the following sections.

2.3.2.1 The proposed risk conceptualization

Aven (2014) suggests risk to be defined as (*C, U*) or (*A, C, U)*, where *A* is the activity considered, *C* is the consequence of the activity, and *U* is the uncertainty regarding the consequences of the corresponding activity. Based on that, risk can be described as (*C', Q, K*), where *C'* is the specified consequences, *Q* is the uncertainty measure, and *K* is the background knowledge of which *Q* and *K* are based on.

2.3.2.2 The methods for risk assessment and management conforming with the risk conceptualization

One of the idea proposed by Aven (2014), which is based on the risk conceptualization discussed in section 2.3.2.1, is to include the strength of knowledge dimension in addition to probability and consequence dimensions in the risk assessment process. The assignment of probability and consequence is based on several assumptions and using the probability criteria alone will hide the underlying assumptions, which are the essential aspects of risks and uncertainties (Aven, 2014). Additionally, the estimation of risk also may contain personal biases, especially when expert judgment is involved in the assessment of risk, thus deterring our ability to reveal and foresee black swans (Nafday, 2009).

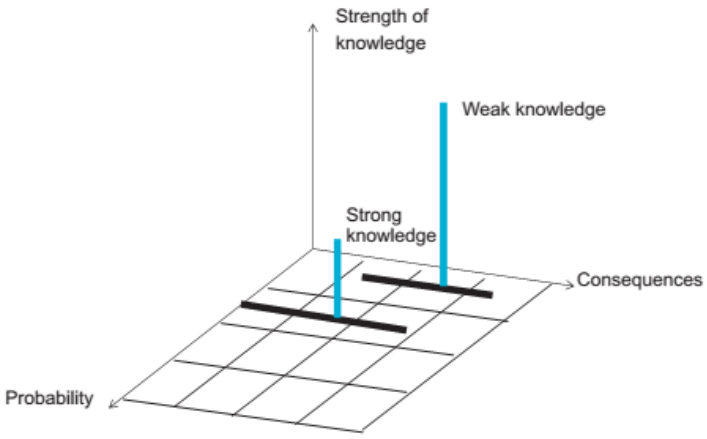

Figure 2.4 Aven's suggestion on how to include strength of knowledge and consequence value interval dimension in the risk assessment (Aven, 2013b)

The inclusion of the strength of knowledge will aid risk assessment by providing the reflection regarding the knowledge where the probability and consequence assessment are based on (Aven, 2014). Strength of knowledge may indicate the degree of uncertainty, for instance poor knowledge points out high level of uncertainty and vice versa. However, the assessment can still contain biases as the estimation of strength of knowledge requires judgement from the risk assessors. One can estimate that the knowledge are strong from ones perspective, but it might turn out to be weak from the other people's point of view.

The other idea is by inserting consequence value interval instead of just one fix value of expected consequence to reflect the uncertainty of the consequence in the risk assessment (Aven, 2013b). The problem with using the expected consequence is that the actual consequence might extremely deviate from the expected value, thus there is a need to see beyond the expected value.

2.3.2.3 Quality discourse

The notions of quality discourse basically relate to the concepts of common-cause and special-cause variation and underline the significance of learning and improvement (Aven, 2014). Some of the ideas will be addressed here.

One of the important notion in quality discourse is the utilization of management by objective (MBO) or management by results (MBR). MBO mainly involves the assessment of performance by monitoring and comparing the progress toward the initially defined objectives. Risk is then determined by the presence of gaps or deviations of the actual performance from the objectives (Aven, 2014). Every gaps found is analyzed and assessed to identify the sources of the differences, thus appropriate corrective actions can be carried out thereafter.

The next notion is on the importance of not focusing only on numerical goals. Deming (1986) analogizes numerical goals as the "fortresses against improvement of quality and productivity". Numerical goals will make us to focus only on the outcomes while overlooking the importance of the underlying processes. Understanding and improvement of the process is the focal point, especially in managing and encountering deviations, abnormalities, and failures (Aven, 2014).

The third idea is on the subject of common-cause variation and special-cause variation. As stated by Roebuck (2012), common-cause variation relates to stable phenomena and processes that are continually utilized and active in the system, thus the variation can be predicted accurately, for instance by probabilistic approach. Meanwhile, special-cause variation is associated with newly emergent phenomena that stands outside the realm of historical experiences that makes the performance unpredictable (Roebuck, 2012). Common-cause variation is a routine while special-cause variation can be viewed as surprises and unforeseen events (Aven, 2014). The concept of common-cause and special-cause variation is somehow related to the basic concept of risk assessment and management. The concept underlines the importance of highlighting special-cause variation to put more focus on surprising events.

The last notion from the quality discourse is that knowledge is built on theory (Lewis, 1929, cited in (Aven & Krohn, 2014)). Rational prediction needs theory and the systematic and extension of

theory are achieved by comparing the prediction with the actual observation (Deming, 2000, cited in (Aven & Krohn, 2014)).

2.3.2.4 The concept of mindfulness

The concept of mindfulness, as construed in the studies of High Reliability Organization (HRO), emphasizes on five primary elements: (1) preoccupation with failure, (2) reluctance to simplify, (3) sensitivity to operations, (4) commitment to resilience, and (5) deference to expertise.

'Preoccupation with failure' means the ability to learn from past failures and the aspiration to look for early warning signs of failure. Meanwhile, 'sensitivity to operations' is the ability to identify abnormality, deviations, and any other signs that may indicate possess threats to the integrity of the facility during the operations and to take immediate actions to remediate the conditions (Aven & Krohn, 2014).

'Reluctance to simplify' means that the decision regarding risk shall not be based on merely quantitative expression of risk, such as risk matrix (Aven & Krohn, 2014). This is closely related to what has been discussed in section 2.3.1. Risk must be perceived beyond than probabilities and expected consequences and should be viewed from broader perspective in order for us to prevent the occurrence of unforeseen failures (Aven & Krohn, 2014).

'Commitment to resilience' implies the ability of a system to tolerate surprises and unforeseen failures. Clear distinction should be made between resilience and robustness. Robustness is the ability of the system to encounter deviations from normal operating conditions (Aven, 2008). An example of robustness is by implementing safety factors in the design of structural components. In robustness, the potential hazards or threats are known in advance while in resilience, the hazards or threats are unknown. Aven (2008) argues that one of the way to achieve resilience is by implementing the system with an adaptation mechanism that can acclimatize with the changing environmental conditions.

Figure 2.5 Five elements of mindfulness concept

'Deference to expertise' refers to the commitment to only authorize the personnel with suitable qualifications and competences to make important decisions in critical operational circumstances (Aven & Krohn, 2014). For instance, it would be better to allow an experience operator to make decisions regarding daily operational conditions than give the responsibility to facility manager, who is lack of practical experience and only indirectly involves in the operation.

However, the concept of HRO is not without critic. Leveson, et al. (2009) state, "[…], an important problem with HRO theory is that the practices were observed in systems with low levels of uncertainty and stable technical processes". They argue that the features in HRO will not be applicable in most of the systems in this era of rapid technological advances, where the dynamicity of the technical processes is high with high level of uncertainty. In addition, Leveson, et al. (2009) also argue that HRO practices were observed in the organizations where safety was the primary goals. Examples of these organizations are firefighting teams and aircraft carrier operation for military purposes during peacetime. However, in the modern industrial environment, safety goals will be challenged and conflicted by the other objectives, such as profits and productivity goals, which make it difficult to prioritize and achieve safety. It is if often that safety must be sacrificed in order to achieve the other objectives. Hence, the applicability of HRO can be questioned, especially for organizations that operate in modern context.

Similar with Leveson, et al., Lekka (2011) questions the applicability of HRO in typical existing organizations. She mentions several limitations of HRO research as follow:

- Lack of a comprehensive theoretical framework that would help explain why HROs succeed where other organizations fail with a particular focus on understanding the factors that facilitate the successful development of HRO processes,
- Limited understanding of the effects of HRO work environments on individuals and the implications of such potential effects for more 'traditional', mainstream organizations,
- Limited evidence regarding the predictive validity of HRO-based quantitative measures in terms of safety performance or other relevant indicators.

2.3.3 Cautionary and precautionary principle

Aven (2014) argues that cautionary and precautionary principle can be the strategies to deal with events that are judged to have extremely low probability, i.e. *known unknowns*. The cautionary principle states that in the event of uncertainty regarding the consequences of a particular activity, caution, such as not initiating the activity or applying measures to reduce the uncertainty, should be the ruling principle (Aven, 2008). Aven argues that the level of caution adopted should be considered together with the other aspects, such as costs. Meanwhile, precautionary principle is a special case of cautionary principle, which is used when a particular action has scientific uncertainties regarding its outcomes. Precautionary principle suggests to not to carry out the action if it has scientific uncertainties, which may possibly cause highly negative consequences (Aven, 2008).

However, the precautionary principle receives many critics upon their implementation and practicality. Marchant (2003) argues that the precautionary principle is lack of rule to decide when to apply the principle. The question to be raised here is: how much scientific uncertainties are required to apply the principle, or how much certainties are needed to allow carrying out the activity? No clear guidance is provided regarding the uncertainties acceptability to conduct certain action, causing ambiguity in the application of precautionary principle. This vagueness may result in arbitrary and dubious decisions and is prone to abuse by the decision-makers for personal or particular group interest (Graham, 2004; Marchant, 2003). In addition, the nature of precautionary principle will halt the development of new products and services, hamper technology advancement, and discourage innovation (Graham, 2004).

2.3.4 Using signals and warnings

Aven (2014) mentions signals and warnings as a way to manage unforeseen failures, particularly the *unknown unknown* type. There is a belief that signals and warnings are always present before the occurrence of major accidents (Leveson, 2015). Warning signs can be conceived as traces left by catastrophes prior to their occurrences. They may indicate the existence of defects or threats in the system or deviation of the operation from safe operating envelope (Dokas, et al., 2013). Prospectively, they might provide clues that can prevent failures to occur in the future. However, in many cases, most of them are not recognized or deliberately disregarded.

The ability of organizations to foresee failures depends on their capability to detect the presence of warning signs preceding accidents as well as interpret them into valuable information. However, detecting critical signals and warnings is a challenging task, especially in a complex system. There are thousands of signals and warnings during the operational phase and amongst them, there are 'innocent' signals and warnings, which can be considered as noises and might become a distraction in identifying the meaningful precursors that lay on the causal path of the accidents (Sonnemans & Körvers, 2006). From retrospective viewpoint, accidents may seem to be foreseeable, but from prospective point of view, accidents may not still be foreseeable even though critical warnings and signals exist.

2.3.5 Improvement on knowledge transfer

Aven (2014) argues that the improvement on the knowledge transfer and risk assessment methods are the two ways to encounter *unknown known* type of events. The main idea of knowledge transfer is to make the initially inexistence knowledge in a particular risk analysis and decision-making team to be available by implementing effective communication of experience and knowledge. Haugen and Vinnem (2015) add that it is necessary to only involve qualified people in the risk analysis process. These people should have considerable knowledge and experiences regarding the system to be analyzed, including the technical, management, and regulatory aspects.

2.3.6 Improvement on the risk assessment methods

Several methods that may improve the existing risk assessment methods are proposed by Aven, such as Anticipatory Failure Determination (AFD), *red teaming*, and the insertion of strength of knowledge dimensions and consequences interval in the risk assessment (see section 2.3.2.2). AFD

is basically hazard/threat identification methods, which is believed to be able to reveal the possible black swan events scenarios. The methodology of AFD is based on the so-called reverse thinking process to generate failure scenarios (Adesanya, 2014). The aim of the AFD is to invent the failure events and scenarios, thus the focus is not only to identify events or scenarios that have been occurred in the past, but also to reveal new events and scenarios that may occur in the future.

Meanwhile. *Red teaming* is a method which involves assignment of independent group to defy the existing ideas, assumptions, established thinking, etc. in an organization. The objective is to generate alternative options and as a basis for more robust decision making (UK Ministry of Defence, 2013). The implementation of *red teaming* in risk assessment process will possibly reveal the unforeseen events and surprises by challenging the assumptions used in the judgment of risks and to generate more scenarios that might lead to the occurrence of *unknown known* type of events in the future.

3 CHAPTER THREE – Learning from Failures

3.1 Introduction

In this thesis, the identification of patterns underlying unforeseen failures involves learning from the historical failure reports and other literatures concerning the failures. Different reports or literatures may discuss different aspects underlying the failures, from human errors, technological failures, until management and organizational factors. This chapter will review the theoretical background that underlies various accident investigations how it affects our understanding about the occurrence of unforeseen failures.

3.2 Accident and unforeseen failure

When unexpected event happens, it is more common to acknowledge the examination and analysis following the event as 'accident investigation' rather than 'failure investigation'. Therefore, there is a need to clarify the term 'accident' and 'unforeseen failure' here.

Oxford dictionary defines accident as "an unfortunate incident that happens unexpectedly and unintentionally, typically resulting in damage or injury". A broader definition is provided by Leveson (2014), who describes accident as an undesired and unplanned event that causes injuries/fatalities, environmental damage, asset destruction, and other type of losses.

If we use unforeseen failures definition by Aven and Krohn (2014), unforeseen failures can be considered as accidents, but not vice versa. As stated in the previous chapter, categorizing an event as an unforeseen failure requires the consideration of knowledge and belief of the people who see the event. In addition, unforeseen failure is limited to event that has extreme consequences. For instance, Fukushima nuclear disaster can be regarded as both accident and unforeseen failure considering its enormous impact and most people do not foresee it coming. However a car crash can only be considered as accident as it has relatively smaller consequence and most people can imagine its occurrences. Based on the discussion above, unforeseen failure can be seen as a special case of an accident.

3.3 Perspective on accident and accident investigation

Accident investigation normally relies on some models to facilitate the analysis of the event and make it easier in understanding its causal. This model, known as accident causation model, influences our assumption regarding how accidents happen (Cedergren & Petersen, 2011). Accident causation models present the conceptualization of an accident by showing its natures, which are typically shown by cause-effect relationship (Qureshi, 2007). Moreover, accident causation models are also the foundation of the existing hazard analysis and risk assessment methods (Leveson, 2004).

The development of accident causation model is largely dependent on the human perspective on accident, which has changed and evolved in the last 40 years as can be seen in Figure 3.1. There are primarily four periods that changes the way humans see accident: (1) the technical period, (2) the

human error period, (3) the socio-technical period, and (4) the inter-organization period (ESReDA, 2009). Each of them will be discussed briefly in the following sections.

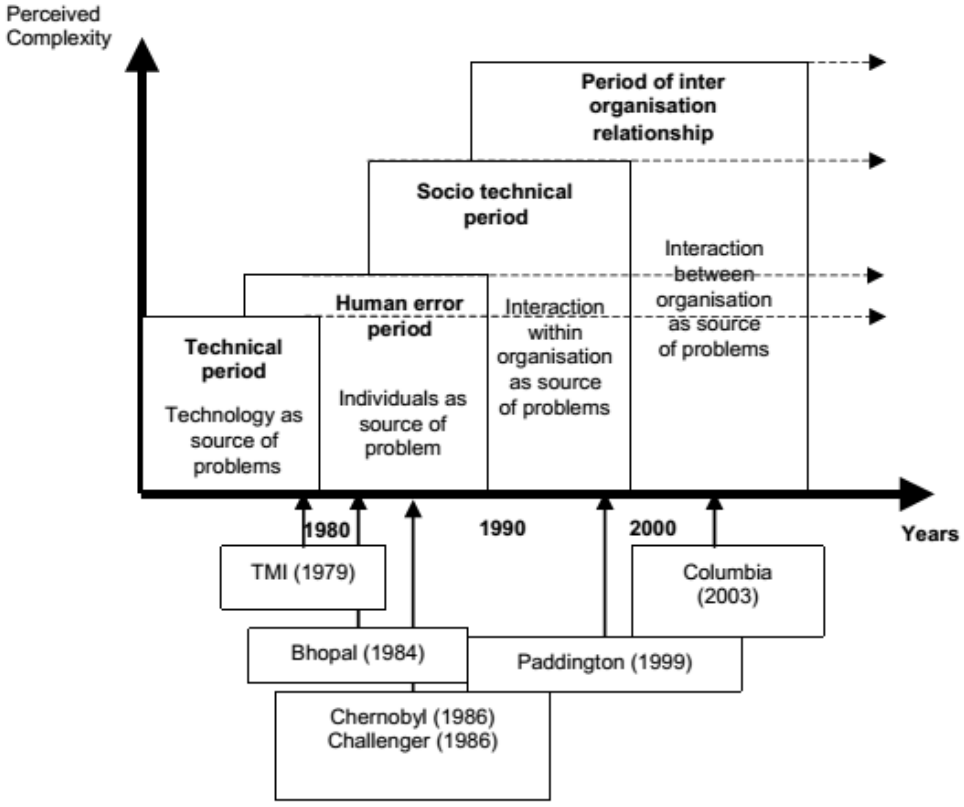

Figure 3.1 Research trend in safety for the last 40 years (ESReDA, 2009)

3.3.1 The technical period

The technical period is the first age in safety science, where technology was deemed to be the main source of problems and the root causes of accidents (ESReDA, 2009; Herrera, 2012). The concept of linearity about an accident was prominent in this era, where accident was simply described as a chain of distinct events that happen in a particular order (Hollnagel, 2004; Qureshi, 2007). The accident models that are adopted this linear thinking are called sequential accident model, which can be considered as the simplest type of accident models that are existed at the present. This accident model causes the tendency of the accident investigator to emphasize on technological breakdown (Leveson, 2011b). An initiating unexpected event will generate another event, and this occurrence happen continuously, creating a sequence of events until the last one causes a major consequence.

One version of this model is the domino theory developed by H.W. Heinrich in 1932. This theory mentions five factors that play a role in an accident sequence: (1) social environment, (2) fault of personnel, (3) unsafe act, (4) accident, and (5) injury. These factors are aligned in fixed linear order and form a chain of events that illustrate causes and effects (Qureshi, 2007). The falling of one of the dominoes will perpetuate to the next one until the last one falls and eventual consequences

occur. This model implies that an accident is caused by a single event, i.e. root cause, and if the root cause can be identified and eliminated or mitigated, the recurrence of accident can be prevented (Qureshi, 2007).

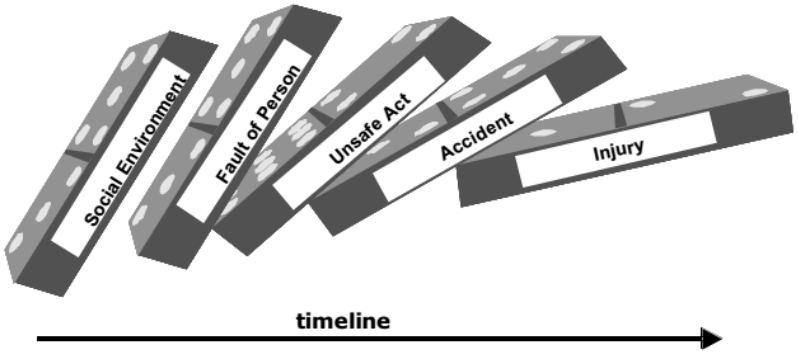

Figure 3.2 Domino model by Heinrich (Qureshi, 2007)

Sequential accident models explain accidents as a chain of events. Accidents are fathomed as linear sequence of events that have direct relationship (Leveson & Stephanopoulos, 2014). The premise is that there is a symmetry between cause and effect, i.e. the root cause of the catastrophe can be identified by tracking backward the chain of events preceding the loss (Dekker, 2011; Leveson & Stephanopoulos, 2014). They work based on the assumption that cause and effect must be directly correlated, thus the considerations are only made on proximate events while omitting non-linear causes and interactions (Leveson, 2011a). Consequently, sequential accident model tends to consider only technological failures, which are the most visible aspects in the occurrence of accidents while concealing more important factors that trigger the accident, such as organization aspects (Leveson, 2011b).

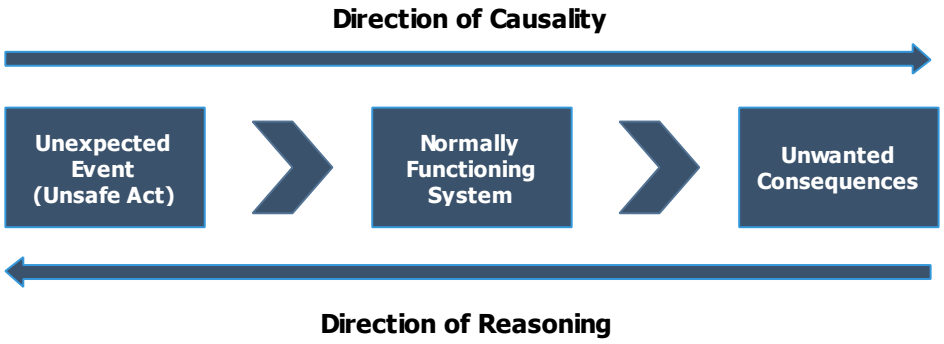

Figure 3.3 The sequential accident model (Hollnagel, 2004)

Additionally, this conception brings the belief that an accident can be prevented by creating safety barriers that could stop the propagation of events leading to an accident. The linear interpretation of events is found necessary to identify these barriers and to avoid the occurrence of accidents in the future (Dekker, 2011).

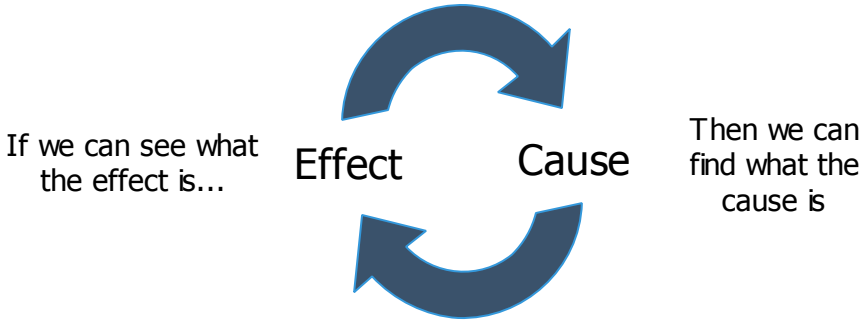

Figure 3.4 Reverse causation illustration (Hollnagel, 2004)

Sequential accident models are also based on the so-called *analytic reductionist approach*. It means that it possible to separate a system into components or subsystems and analyze them independently without distorting the analysis results (Leveson & Stephanopoulos, 2014). Dekker (2011) calls this as the principle of reductionism, which is rooted from the legacy of Newton and Descartes to comprehend a complex phenomenon. This approach works, in fact, on the premise that the behavior or properties of the system is the summation of its individual components or subsystems. The component behavior will be the same when observed individually as well as altogether with the other system's components.

Failure Mode and Effect Analysis (FMEA), Fault-Tree Analysis (FTA), Event-Tree Analysis (ETA), Cause-Consequence Analysis, and Hazard and Operability study (HAZOP) are some examples of hazard analyses that are derived from the sequential model (Leveson, 1995, cited in Qureshi, 2007).

3.3.2 The human error period

After the occurrence of Three-Mile Island accident in 1979, the accident causes was broaden by including human error besides merely technological context (Herrera, 2012). The safety research was focused on the search for the mechanism of human errors and the prevention of human errors by the consideration of ergonomics in the design of a system (Herrera, 2012). The most prominent accident model in this period is called epidemiological model, which explain accident by making analogy of spreading a disease, i.e. accident happens because of combination of factors, some manifest and some latent, that happen to exist together in space and time (Hollnagel, 2004).

Swiss Cheese Model by Reason (1997) is an example of epidemiological models that explains an accident as the product of cause-effect chain, i.e. one event leads to another event until major accident occurs. The occurrence of these events can be prevented by applying safety barriers to breakdown the cause-effect chain. Safety barriers functions as defenses that stops an event from happening, thus the subsequent events will not take place and manifestation of serious consequences will be halted. Ideally, the barriers will totally prevent any accidents, but in reality they are not perfect. These barriers have holes that represent weaknesses of the safeguard systems due to the combination of latent condition, active failures, and local triggering events. Poor safety cultures, false decision-making criteria, human errors, and technical failure are some of the latent

conditions that create holes in the barrier. If all of the holes existed on the barriers form a line and a certain hazard exists, this situation can escalate into an accident (Körvers & Sonnemans, 2008).

Epidemiological model extends sequential model by providing broader accident causation, but the influence of sequential accident models can still be felt as it still represents accident as alignment of linear events (Qureshi, 2007). Swiss Cheese Model represents a system as a static entity while in fact the system is dynamic in nature (Qureshi, 2007).

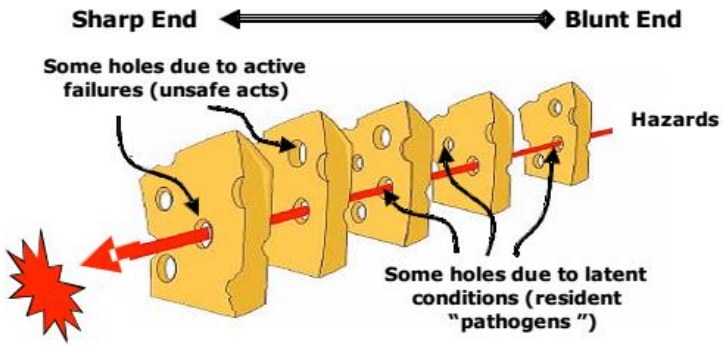

Figure 3.5 Reason's Swiss Cheese Model (Reason, 1997)

3.3.3 The socio-technical and inter-organization period

The Bhopal (1984) and Chernobyl (1986) tragedy opened the eyes of the safety scientists even larger by making them realized that organizational aspect could not be omitted as one of the problem sources in the occurrence of an accident. The Columbia Space Shuttle disaster in 2003 and Texas City Refinery Explosion and Fire in 2005 took safety science further by underlining the significance of institutional and organizational context (ESReDA, 2009). The focus in these periods are shifted to the inclusion of organizational aspect and the complexity of interaction between the components of a system in the occurrence of an accident (Herrera, 2012).

The significant notion in this period is the development of systemic accident causation model, which is rooted from the system theory (Herrera, 2012). Unlike sequential and epidemiological accident models, which assume accident simply as cause-effect chain of events, systemic accident models define accident as highly complex interrelated network of events (Qureshi, 2007). These network events are generated as the results of interaction of the components within the system. In a socio-technical system, the system can comprise of technological component, human, and organization.

Different with sequential model that assesses the components of the system separately, systemic accident models view the system as an entirety (Leveson, 2004). As Leveson & Stephanopoulos (2014) states that some phenomena/properties of the system can only be examined adequately by considering all aspects of the system altogether. These phenomena/properties emerge from the interaction and interconnectedness between technical, human, social and organizational aspects of

the system (Leveson, 2004). Accident is one of this emergent phenomena that can only be understood by taking into account all aspects of the system.

Furthermore, systemic accident causation model considers a system as a dynamic entity that constantly interacts with the environment and is continually adapting as reactions to changes in the environment or the system internal itself in order to serve its purposes and to achieve its goals (Leveson, 2004). The system is bounded by several constraints, e.g. financial, resource, and safety constraints to reach the goals. And to ensure the system is operated within the specified boundary, feedback loops mechanism are presence within the system to maintain the system's equilibrium (Leveson, 2004).

Adopting systems theory in accident model enables us to view the system as entirety. It allows us to not only identify the proximate events but also systemic factors behind the accident. This information is valuable to implement design controls that prevent the system to migrate to states of higher risks and help in detecting high-risk situation before the occurrence of loss (Leveson & Stephanopoulos, 2014).

3.4 Summary and Discussion

There are three main accident causation models discussed in the previous sections: (1) sequential accident model, (2) epidemiological accident model, and (3) systemic accident model. They can be summarized as presented in Table 3.1.

Table 3.1 Main type of accident models (adapted from (Hollnagel, 2004))

	Sequential Models	**Epidemiological Models**	**Systemic Models**
Search Principle	Specific causes and well-defined links	Carriers, barriers, and latent conditions	Tight couplings and complex interactions
Analysis Goals	Eliminate or contain causes	Make defenses and barriers stronger	Performance monitoring and control

Kletz (2001) likens accident investigation with peeling an onion; there is another layer beneath one layer and so on. The exterior layer is the most visible one, which is the technical causes, such as physical equipment failures or human errors. The deeper layers comprise of causes that indirectly induce the events, such as management system deficiencies, but are oftentimes hidden behind the immediate causes. Kletz (2001) argues that the consideration of the entire layers of the "onion" is required in order to prevent future accidents. Similarly, Leveson (2011a) states that we will never fully learn from accidents if the focus of the investigation is merely on technical failures and human errors without considering the entire accident process. Emphasis on technical failures and human errors will create tendency to assign blame to the operators, technicians, or other personnel that

are directly involved in the operations, but it will not solve any problems and prevent future occurrence of accidents.

From the argumentation above, accident investigation based on sequential or epidemiological model are no longer be adequate the serve the main purpose of the investigation, which is to reveal the causes of the accident, to learn from the accident, and to prevent the future occurrences. The entire system, from technical, human, and organizational aspects, must be considered to disclose the true underlying causes of an accident.

4 CHAPTER FIVE – Unforeseen Failure Pattern Identification

4.1 Introduction

The argument about the existence of common pattern underlying failures has been suggested by Venkatasubramanian (2011). He believes that different failures and disasters that happened in different facilities and industries have commonalities. He also states that identifying these patterns requires broader perspective, which includes the system as a whole. In this chapter, several historical unforeseen failures will be reviewed with the purpose to identify if there are patterns that underlie their occurrences.

4.2 Methodology

4.2.1 Selection of case studies

The selection of the case studies will be mainly based on the definition of unforeseen failures discussed in chapter 2. An event can be categorized as unforeseen failure if it fulfil either of the following criteria:

1. Events that were utterly unthinkable and unknown to the scientific community, i.e. *unknown unknowns*.
2. Events that were not known and thus unidentified by ones point of views, but might have been identified from the others perspectives i.e. *unknown knowns*.
3. Events on the list of known events but deemed to have extremely low probability of occurrence.

Additionally, the selected case studies should be events that resulted in major negative impact to the societies, environment, and the business (e.g. damaged assets and loss of reputation).

Based on the that considerations, Bhopal, Deepwater Horizon, Texas City, and Fukushima accident are selected as the unforeseen failure case studies. The reasoning behind the selection of these events are provided as follow:

- The failure to identify the hazard possessed by methyl isocyanate (MIC) due to lack of knowledge and information was one of the causes underlying Bhopal accident (Shrivastava, 1994; Bowonder, 1987), thus it can be categorized in *unknown known* type of events. It was not identified by the Union Carbide (as the owner of the facility) and the local government, but it could have been identified by the other stakeholders given sufficient information and knowledge.
- Deepwater Horizon can be included in the *unknown knowns* category as it involves a sequence of events that was extremely improbable to occur, which was most likely to be unidentified by the risk assessment process (Aven, 2014).

- Overfilling of the raffinate tower, which is the initiating event of Texas City Refinery Explosion and Fire, was considered as an incredible scenario in the process hazard analysis, i.e. the event was deemed to have an extremely low probability of occurrence and hence overlooked. Based on this fact, Texas City Refinery accident can be categorized as the third category of unforeseen failures.
- The possibility of a tsunami reaching height beyond the plant design criteria was considered to be very low and the risk was believed to be acceptable, thus Fukushima accident can be categorized as the third category of unforeseen failures.

Furthermore, Bhopal, Deepwater Horizon, Texas City, and Fukushima accident are undoubtedly have significant impact to the societies, environment, and the business. Table 4.1 shows the general information regarding the case studies, including the consequences of their occurrence.

Table 4.1 General information about the selected case studies

	Bhopal	**Deepwater Horizon**	**Texas City**	**Fukushima**
Date	2-3 Dec 1984	20 Apr 2010	23 Mar 2005	11 Mar 2011
Facility Owner	Union Carbide	BP	BP	TEPCO
Location	Bhopal, India	Gulf of Mexico	Texas City, U.S.	Okuma, Japan
Plant typology	Chemical plant	Oil drilling rig	Oil refinery	Nuclear power plant
Causes	Runaway reaction	Failure of cement barrier and BOP	Overfilling of raffinate tower	Failure of reactor cooling system
Consequences	approximately 8000 fatalities and 100,000 injuries	11 fatalities; 17 injuries; fatal environmental damage	15 fatalities; 180 injuries; $1.5 billion financial losses	1,600 fatalities during the evacuations process; health impact and environmental damage from radioactive exposure

There is no selected case study for *unknown unknown* type of events. An event can be categorized as *unknown unknowns* if the entire scientific community cannot think or imagine it at all. This definition is the main issue in deciding whether an event is *unknown unknown* or not as we do not know the knowledge level of the scientific community at the time of the occurrence of the event. Even the September 11 attack, which is characterized as *unknown unknown* by Taleb (2007), cannot be considered entirely as *unknown unknown* because risk analysis carried out by Federal

Aviation Administration (FAA) had identified similar event prior to September 11, 2011 (Aven, 2015).

4.2.2 Data and information sources

Data and information regarding the selected unforeseen failures are obtained from accident investigation reports as well as related scientific journals, papers, and books. Accident investigation reports authored by independent agencies and investigation commissions are established as the primary source of data and information as they are considered as having the most objective results among the other literatures. Additional literatures are acquired from electronic databases, such as Sciencedirect and Taylor & Francis Online with the focus on safety and reliability journals. The search is limited to only peer-reviewed scientific papers and articles to ensure the quality of the content.

Table 4.2 Sources of data and information about the selected case studies

Event	Sources of data and information
Bhopal	(Eckerman, 2005), (Bowonder, 1987), (Chouhan, 2005), (Shrivastava, 1994), (Bowonder & Linstone, 1987)
Deepwater Horizon	(CSB, 2010a)*, (Reader & O'Connor, 2014), (The Bureau of Ocean Energy Management, Regulation, and Enforcement, 2011), (Norazahar, et al., 2014), (Hopkins, 2011), (Neill & Morris, 2012)
Texas City	(CSB, 2007)*, (Saleh, et al., 2014), (Baker, et al., 2007)*, (NASA, 2008)
Fukushima	(Saleh, et al., 2014), (Atsuji, et al., 2011), (Alvarenga & Melo, 2015), (Wang, et al., 2013), (Kaufmann & Penciakova, 2011), (Onishi & Belson, 2011), (NAIIC, 2012)*

* - Report by independent agencies and accident investigation commissions

4.2.3 The review approach

Based on the discussion in chapter 3, the review of selected unforeseen failure cases will not emphasize to merely technical perspective, i.e. physical component failures. All of the four selected case studies were happened in large complex socio-technical system, which consists of technological, human and organizational elements. Hence, the combination of sound technical, human, and organizational perspective is required to understand the underlying problems causing the catastrophes. Moreover, the reviews will not be restricted to merely proximate events, but also causal factors and symptoms that have existed long before the moment of the accident.

General event information, sequence of events, the underlying causes will be discussed in each of the selected case study. Three hierarchical levels will be used to categorize the attributed causes as shown in Table 4.3. The highest level is macrolevel, which represent inter-organizational factors, regulators, and government. The next level is mesolevel, which includes intra-organizational aspects. The last level is microlevel, which represents operators, technicians, and physical equipment.

Table 4.3 Three hierarchical levels used for categorizing the accident causes (Cedergren & Petersen, 2011)

Hierarchical Level	Description
Macrolevel	Regulators, associations, and government
Mesolevel	Company and management
Microlevel	Technical base and staff

4.3 Related Research

As stated earlier, Venkatasubramanian (2011) argues about the similarities among major accidents. He describes Bhopal, Deepwater Horizon, Texas City, Fukushima and other historical major accidents as systemic failures that have common patterns as follow:

1. They are rarely caused by a single component failure or human error. The failure occurs at not only in the lowest organization hierarchy level, but also in several organizational levels, such as management and regulator.
2. Degradation of safety in the system is caused by numerous safety violations.
3. Failure in identifying all of the relevant hazards that threaten the system. Venkatasubramanian argues that a comprehensive hazard analysis were not conducted.
4. The company did not equip the personnel with appropriate training regime to prepare in encountering emergency circumstances.
5. Regulatory ineffectiveness

The third statement, which is the failure to identify relevant hazards, is already evident in the discussion in section 4.2.1. The hazard that initiated the accident was failed to be recognized and/or identified because either the risk assessors completely did not know about the hazard or the risk assessors ignored it because it was presumed to have negligible probability.

The findings and observations from this thesis will be compared with the argument stated by Venkatasubramanian above.

4.4 Case Studies Review Summary

The review summary for each of the case study will be discussed individually before findings and observations are presented in the next section. The data and facts presented here is only a portion of the total information provided in the investigation reports and other literatures, but considered as the most essential and representative for depicting the entire events. At the end of this chapter, the common patterns underlying the unforeseen failures will be presented.

4.4.1 Bhopal chemical accident

4.4.1.1 General event information

Chemical accident at the Union Carbide Corporation pesticide production plant was happened on the night of 2-3 December 1984 in Bhopal, India. It was caused by the leakage of approximately 40 tons of MIC from the underground storage tanks. It was considered as the world's worst industrial

disaster. The plant was located nearby a highly populated area, enabling the MIC to spread rapidly over the neighborhoods and kill around 8000 people during the first weeks while injuring 100,000 others (Eckerman, 2005). The direct cause of the accident was the entrance of water into MIC unit storage that resulted in runaway reaction. This reaction led to rapid increase of storage pressure and temperature, causing severe corrosion to the vessel wall and eventually leakage of hazardous MIC to the atmosphere. The accident was said to be the result of technological catastrophe and its combination with legal, organizational, and human factors (Bowonder & Linstone, 1987; Bowonder, 1987; Chouhan, 2005).

4.4.1.2 Sequence of event

On December 2, 1984, the production superintendent of the plant asked the operator to clean the pipelines together with four filter pressure safety valves. When the operator started to clean the pipelines, some amount of water, together with the other catalytic materials such as iron and rust, entered the line main header, which was connected to the MIC storage tank, through some leaky valves. The leak happened because of badly choked valve due to salts accumulation. The contamination of the storage tank with water and the catalytic materials led to exothermic reactions, and within an hour turned into runaway reactions that resulted in high temperature and pressure in the tank. The high temperature caused the bursting of MIC tank casing, releasing the toxic compound to the atmosphere. The reactions products and unreacted MIC were also released through the vent line.

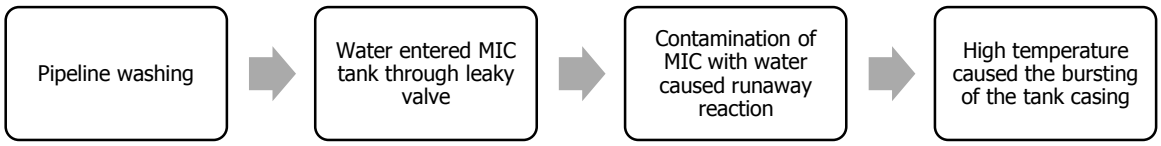

Figure 4.1 Bhopal tragedy chain of events

4.4.1.3 Underlying problems

Microlevel

Some technical failures and human errors contributed to the occurrence of accidents were mentioned by Bowonder (1987) and Shrivastava (1994) as follow:

- Some instrumentations were malfunctioned. For example, the pressure indicator showed 10 psi when the actual pressure had exceeded 40 psi.
- Wrong material selection.
- The plant design was defective. The arrangement of the instrumentation was poor. Some important parameters were not monitored, such as the level of MIC in the storage tank. Moreover, there was no redundancy in the monitoring system and no interlocking arrangement in the plant.
- The MIC storage was not designed according to the existing specifications. This made the MIC to be easier to react with water.

- The operator did not consider increasing pressure in the MIC tank as a threat.
- The operator was too late in recognizing the entrance of water into the MIC tank.
- The communication among operators was faulty. It was evident when the earlier shift operator failed to convey the information about the pressure increase in the MIC tank to the new operator during shift change.
- The decision of the operator to wash the pipelines at night and without slip blinds was erroneous and turned out to be the primary causes of the accident.

Mesolevel

There were clear evidences that the safety management was poor at the corporate level. It is indicated by inadequate operational procedure, defective plant design, poor inspection and maintenance practices, lack of management of change, inadequate training for staffs, unavailability of emergency management plan, etc. (Bowonder, 1987).

There were conflicting goals that exist between productivity and safety (Bowonder, 1987). The economic pressure to generate maximum profits requires high productivity. However, the efforts to produce higher productivity, such as increasing machine efficiency and production speed, improving utilization of production capacity, reducing "unnecessary" costs, and trimming personnel number, seemed to degrade the safety performance (Bowonder, 1987). This is clearly evident as these efforts led to overused of the machines and equipment, poor maintenance, ineffective employee training, incompetent staffs, and poor plant safety design (Shrivastava, 1994). Furthermore, the contradiction between productivity and safety made the safety culture of the organization to be poor, causing the system be more prone to failures and encouraging risky decisions and behaviors (Shrivastava, 1994). Chouhan (2005) states that, "The merciless cost-cutting severely affecting materials of construction, maintenance, training, manpower and morale resulted in the disaster that was waiting to happen".

Moreover, early warning signals, such as audit results and minor incidents, were ignored (Bowonder & Linstone, 1987). Safety audit conducted in 1984 indicated the risks of runaway reaction in the MIC storage tank, but no risk reducing measure or mitigation action was taken (Bowonder & Linstone, 1987). Two safety audits in 1979 and 1981 also indicated poor safety management in the plant (Bowonder, 1987), but no corrective action was taken by the management.

Macrolevel

The regulatory agency failed to identify the hazard possessed by MIC, e.g. its potential to cause uncontrolled chemical reaction and its consequences to the community in the course of leakage, leading to lack of preparedness in the case of leakage (Shrivastava, 1994). There were no evacuation plan in the event of crises and no information for the residents on the actions to be taken in the event of leakage (Eckerman, 2005; Bowonder, 1987). These are worsen by other factors such as poor zoning and industrial siting procedures and poor safety regulatory system (Bowonder, 1987). Moreover, the state government also failed to afford adequate essential daily infrastructures, e.g. water, electricity, transportation, and communication (Shrivastava, 1994).

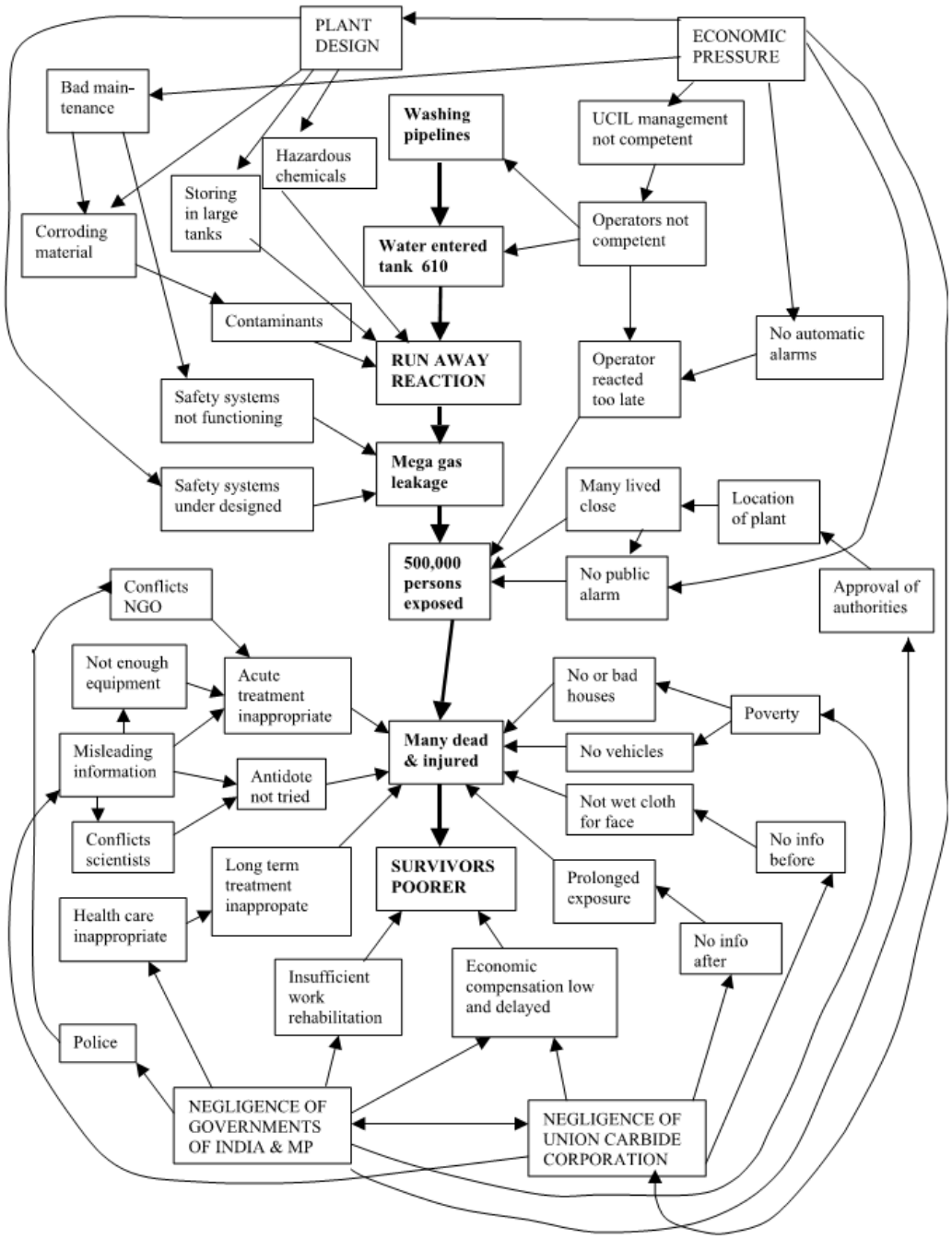

Figure 4.2 Cause and effect relationship of Bhopal chemical accident (Eckerman, 2005)

4.4.2 Deepwater Horizon oil spill

4.4.2.1 General event information

Deepwater Horizon oil spill, also known as Macondo blowout, happened on 20 April 2010 in the Gulf of Mexico. Macondo blowout impact was catastrophic and considered as one of the worst offshore oil spill and environmental disasters in the petroleum industry and U.S. history.

Approximately 5 million barrels of crude oil was discharged into the Gulf of Mexico. It claimed 11 lives while injuring 17 others.

4.4.2.2 Sequence of events

The accident occurred during temporary well-abandonment activities. Cement plug was intended to seal the hydrocarbon below the seafloor before the removal of the Blowout Preventer (BOP). However, the cement barrier was not installed appropriately, thus impairing the integrity of the cement job. The negative-pressure test to ensure the cement integrity was misinterpreted by the crew, causing them to believe that the well had been successfully closed. Subsequently, the drilling fluid column was removed, causing the pressure to decrease lower than the hydrocarbon reservoir, and eventually allowed the hydrocarbon from the reservoir to flow through the failed cement barrier up to the drilling rig. The failure of the personnel to recognize this condition was evident due to their actions to keep removing the drilling fluid column, resulting in increasing hydrocarbon flow toward the rig. This condition remained for approximately an hour without human supervision or automated controller until a blowout happened. The crew decided to activate the BOP in order to seal the well and stop the hydrocarbon the flow. However, this action was also failed to stop the flow because of the failure of the BOP. The hydrocarbon flooded the rig floor and eventually ignited.

4.4.2.3 Underlying problems

Technical failures might be the most apparent cause in the Macondo accident. Failure of the cement barrier and blowout preventer were deemed to be the main reason why the accident happened. However, deeper analyses by various parties show that the causes were not merely due to technological catastrophe. Deficiencies in some organization hierarchical levels were thought to have an important role in the occurrence of the blowout.

Microlevel

The failure of cement barrier and BOP was the most evident technical failure that contributed directly to the occurrence of blowout. The redundancy of the BOP design should have increased its reliability during its operation in normal and upset condition, but it was still failed in sealing the well and preventing the blowout. New failure mechanism was unidentified and compromised the redundancy of the BOP (CSB, 2010b).

The negative-pressure test was incorrectly performed (Reader & O'Connor, 2014). Furthermore, the misinterpretation made by the crew regarding the result of negative-pressure test was also contributed to the occurrence of blowout (CSB, 2010b; Reader & O'Connor, 2014). They believed that the well had been fully closed by the cement while in reality it had not. The unexpected readings observed during the test, which indicated problems with the integrity of the cement, were ignored. The crew were also failed in monitoring and interpreting the real-time data that showed the sign of a blowout (Reader & O'Connor, 2014).

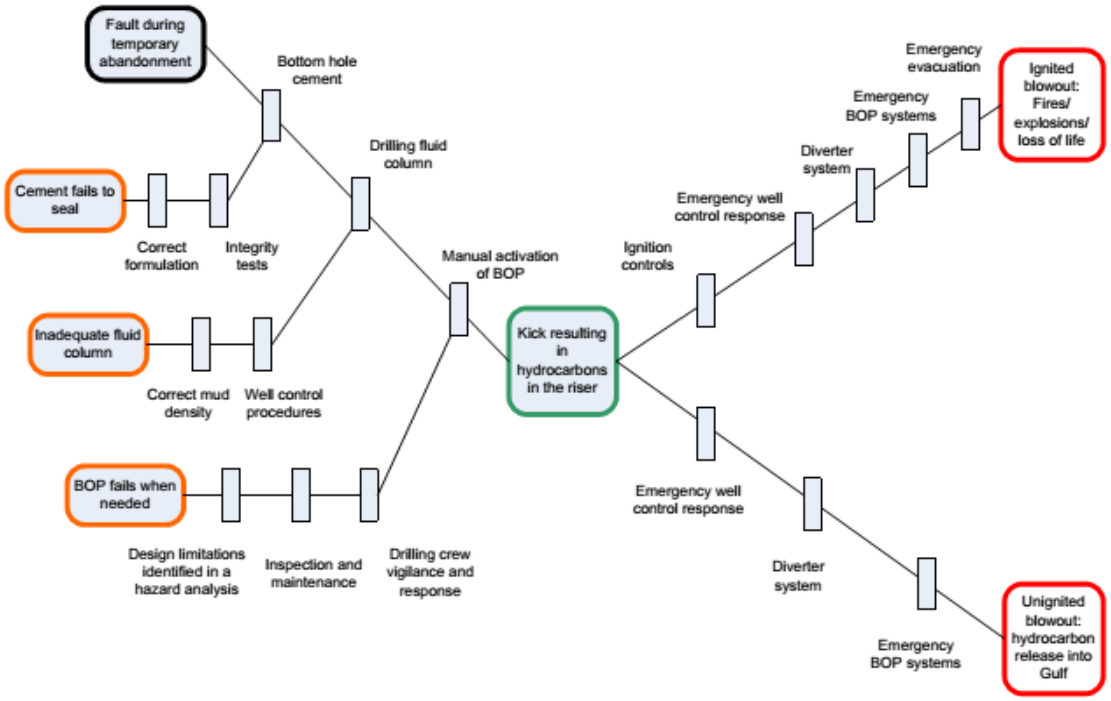

Figure 4.3 Bow-tie diagram illustrating of interconnection between hazards, barriers and the main accident events in Deepwater Horizon blowout (CSB, 2010b)

Mesolevel

CSB (2010a) states, "[…], the Macondo blowout resulted from a complex combination of deficiencies: process safety safeguards and inadequate management systems and processes meant to ensure safeguard effectiveness, human and organizational factors that created an environment ripe for error, organizational culture focused more on personal safety and behavioral observations than on major accident prevention, and a regulatory regime unable to deliver the necessary oversight for the high-risk activities involved in deepwater exploration, drilling, and production". The Bureau of Ocean Energy Management, Regulation, and Enforcement (2011) adds that the blowout was caused by a series of decisions that led to increasing operational risks and the failure to recognize and mitigate those risks.

Reader and O'Connor (2014) discuss the behavior and organizational factors that played parts in the accident. Safety culture, which reflects the organization ways of managing safety in the workplace, was poor. One of the factors that cause poor safety culture is the productivity pressure imposed by the management to the workers (Reader & O'Connor, 2014). Macondo well had not been in production phase yet, but deepwater drilling operation was an expensive process and the pressure to achieve high productivity was high in order to balance the cost. Consequently, the operational decisions and actions taken by the workers were focused on how to save time and reduce cost without considering the risks and their impact on safety (Reader & O'Connor, 2014; Størseth, et al., 2014). It was believed that the operation should keep going even though it

endangered the integrity of the well and the drilling operation itself (Hopkins, 2011, cited in Reader & O'Connor, 2014). This belief is evident in the failure of the operators to discontinue the work even after receiving several warnings and signs, such as sudden increase of the drill pipe pressure, which were later revealed as the major contributor in the causation of the blowout (The Bureau of Ocean Energy Management, Regulation, and Enforcement, 2011; Deepwater Horizon Study Group, 2011).

Poor human factors considerations, e.g. inadequate staff training, excessively complex safety manuals, poor work planning and scheduling (which led to fatigue), and poor human-machine interface, were deemed as one of the factors that caused the accident (Reader & O'Connor, 2014). BP management was aware of the possibility of blowout during drilling operation, but they failed to provide adequate training program to deal with emergency situations and evacuations operation to their workers (Norazahar, et al., 2014).

No appropriate maintenance and inspection program for emergency equipment was ever conducted by BP (CSB, 2010b; Norazahar, et al., 2014). Poor maintenance and inspection program caused impairment of the equipment reliability, especially the safety critical elements (e.g. BOP) in the case of emergency.

Macrolevel

Lack of control from both industrial standards and US regulations is deemed as one of the accident causes. The Mineral Management Service (MMS)[1] failed to impose effective control to the company due to corruption within the organization, lack of resources, lax in regulation, and conflict of interests (Neill & Morris, 2012). In addition, Reader and O'Connor (2014) state that the MMS was deficient in technically competent staffs and tend to give priority to maximize profits from leasing and production without considering the safety impact.

US regulations failed to impose regulations regarding the management of safety critical elements. Moreover, there was no requirement to demonstrate the effectiveness of safety barriers in handling risks associated in drilling operation (CSB, 2010b).

Figure 4.5 gives a clear picture the interconnection between the proximate events (technical failures) and indirect factors (regulator and management) that cause the accident.

4.4.3 Texas City Refinery Explosion and Fire

4.4.3.1 General event information

Texas City Refinery explosion and fire on 23 March 2005 was considered as one of the worst industrial accident in US history, killing 15 workers and injuring 180 others, and resulting in financial losses of roughly $1.5 billion. This catastrophe event occurred due to overfilling of raffinate splitter tower, which was located in isomerization unit, during the commencement of start-up process. The overfilling led to release of flammable compound through the blowdown stack, which was eventually ignited and caused fire and explosion.

[1] MMS is an organization that has the responsibility for mineral resource development, regulation, and management on the US outer continental shelf.

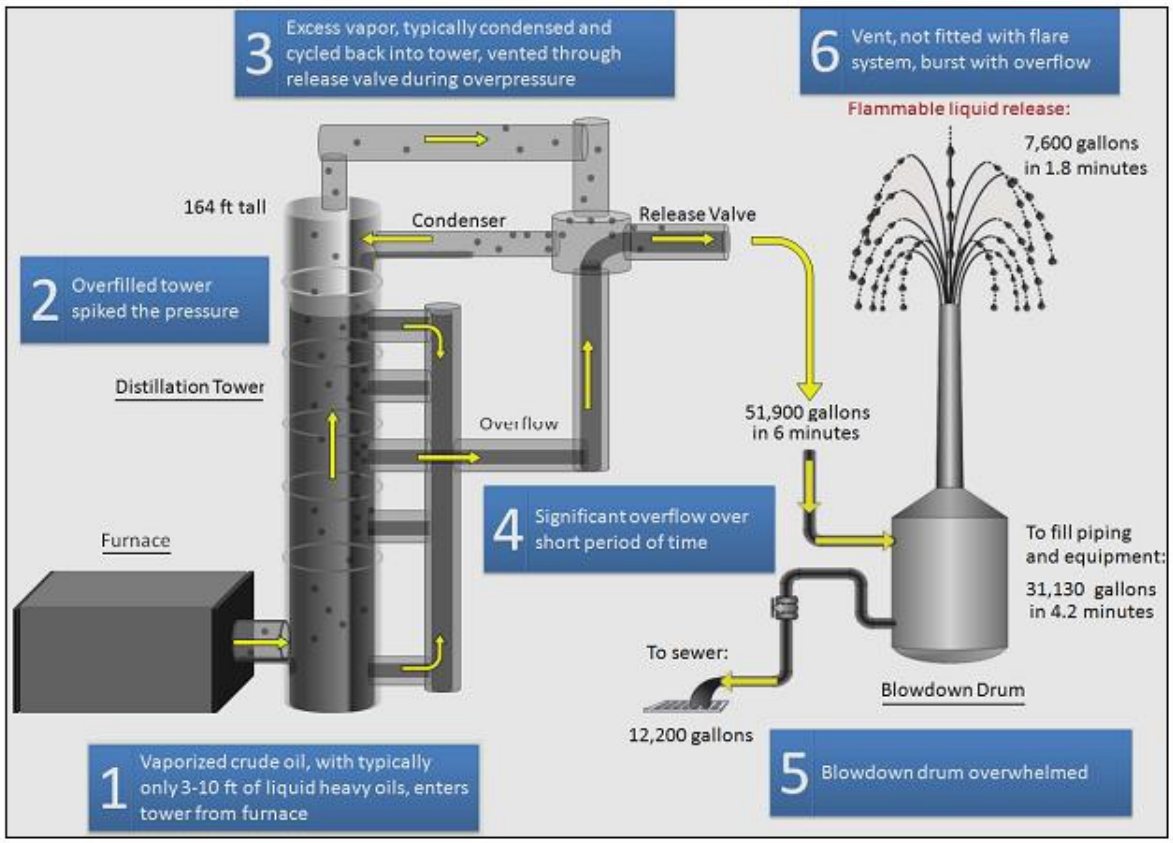

Figure 4.4 Chain of events of Texas City Refinery Explosion and Fire (NASA, 2008)

4.4.3.2 Sequence of events

On March 2015, the raffinate splitter tower was recommenced after maintenance shutdown. According to the official startup procedure, the tower shall be emptied before pumping in liquid hydrocarbons. However, the plant operators did not follow the instruction and pumped the hydrocarbon straightaway to the tower without emptying it beforehand. Moreover, the instrumentations and critical alarms on the tower were malfunctioned, providing false indication regarding the liquid level of the tower. The indicator showed that the liquid level was still in acceptable range despite the fact it had been overfilled and overflowed to the overhead pipe at the tower top. The liquid overfilling increased the pressure of the tower and the piping section connected to it, causing the pressure relief valve to open. The opening of relief valve caused liquid overflow to the adjacent blowdown unit, resulting in flammable liquid release from the blowdown stack. The released liquid created a vapor cloud that was eventually ignited, probably by a nearby running vehicle engine. The illustration of the sequence of events can be seen in Figure 4.4.

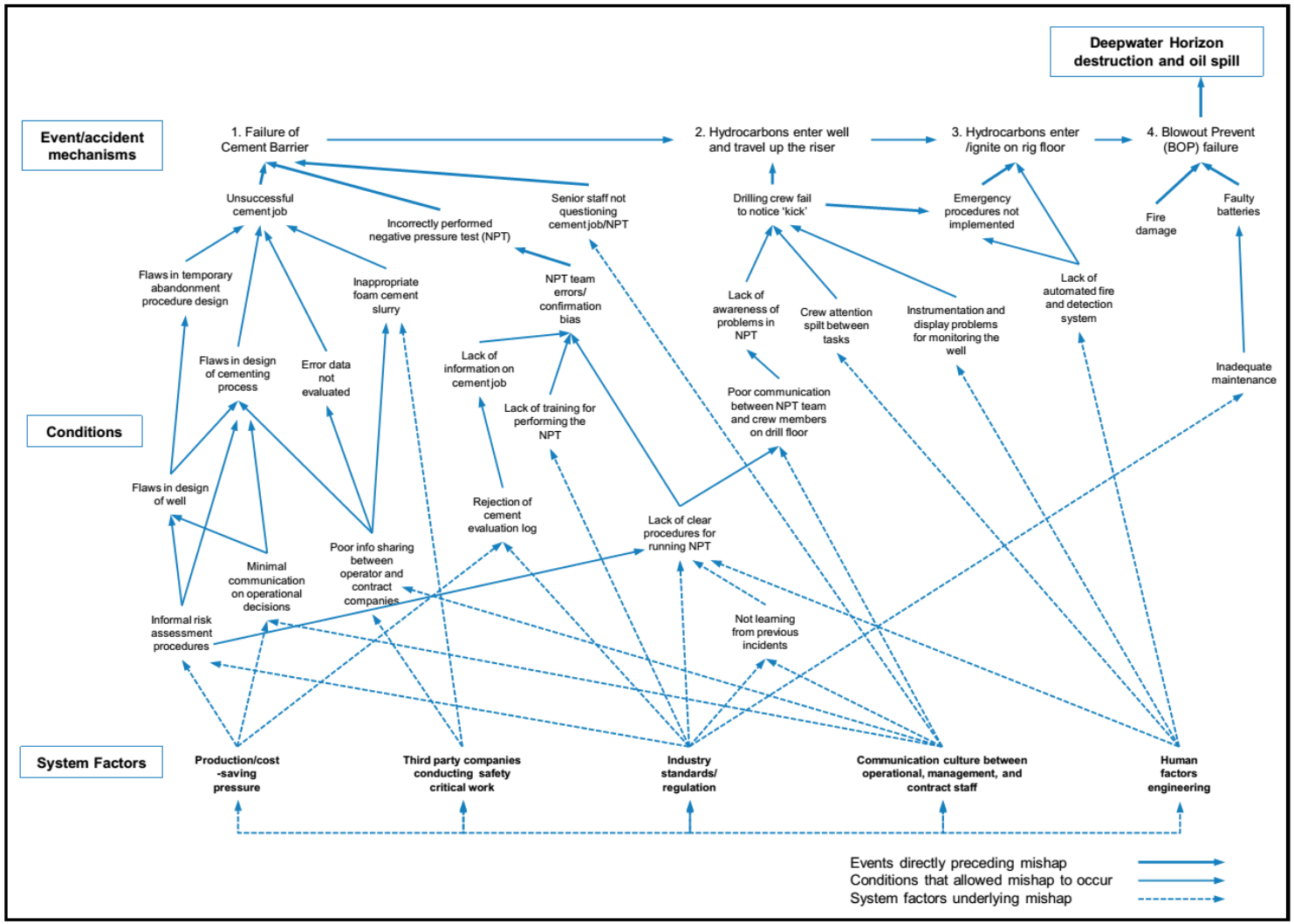

Figure 4.5 Events, conditions, factors, and their interactions leading to the Deepwater Horizon Oil Spill (Reader & O'Connor, 2014)

4.4.3.3 Underlying problems

Technical failures (e.g. malfunctioned liquid level indicator and faulty high level alarm) and human errors (e.g. operators overfilling the distillation tower) were the most visible causes of the accident. However, the cause of this accident was more than faulty technical elements or human errors. Defective management system created deficiencies in safety culture, process safety management, and plant design, which were found to have a share in the accident occurrence.

Microlevel

Some of the notable technical failures and human errors based on CSB (2007) investigation are mentioned as follow:

- Faulty and malfunctioning instrumentation of the raffinate tower. The level indicator indicated declining liquid level despite the fact that the tower was overfilling.
- The plant operator deviated from the start-up procedure. The procedure stated that the level control valve shall be opened to send the remaining liquid in the tower to the storage during the restart. However, the operators kept this valve closed and filled the tower without prior draining.
- The communication between operators and supervisors were poor during shift change.

Mesolevel

In depth analysis by CSB (2007) shows that the decision of the BP executive managers to trim costs resulted in the impairment of process safety performance in the Texas City Refinery. Significant budget cut in 1999 and 2005 led to staffs downsizing. Consequently, Texas City refinery were understaffed for years, resulting in excessive working hours to the remaining personnel (CSB, 2007). The excessive working hours was believed to cause fatigue and compromise the safety performance, which led to hazardous actions, e.g. deviations from existing procedures and work instructions (Baker, et al., 2007).

Independent Safety Review Panel (2007) states that "BP has not provided effective leadership on or established appropriate operational expectations regarding process safety performance at its five U.S. refineries". Interviews conducted by Independent Safety Review Panel (2007) to some workers and management personnel confirmed that production goals, operational pressures, and budget limitations had eroded the process safety performance in the refinery. Moreover, substantial percentage of the U.S. refinery workforces disbelieved in process safety as one of core values at BP (Baker, et al., 2007).

The panel also indicates that BP dwelled on personal safety over process safety (Baker, et al., 2007). Texas City refinery relied on personal injury rate as safety indicator, which is considered as inappropriate for depicting the true process safety performance (CSB, 2007). The reliance on wrong safety performance metrics created false sense of assurance that increased the process safety risks in the refinery (Baker, et al., 2007).

Saleh, et al. (2014) adds that the safety culture in the plant was poor. Recurrent safety violation, inadequate safety procedures, and poor safety practices were some indications of the weaknesses in the Texas City refinery safety culture. (Saleh, et al., 2014) Some of the evidences of the poor safety practices in the refinery are presented as follow:

- The blowdown drum design had been outdated and should have been replaced (Saleh, et al., 2014). Some incidents years prior to the explosion had indicated that the blowdown drum was not safe, but BP's management took no refurbishment or replacement actions (CSB, 2007).
- The operators were not given adequate training to face hazardous situations, such as during plant restart and shutdown (CSB, 2007).
- Malfunctions and faulty instrumentations on most of the raffinate tower indicated improper maintenance management in Texas City refinery. The sight glass was dirty, which impaired its visibility. The level transmitter also wrongly calibrated, thus providing wrong information to the operators (Saleh, et al., 2014).

Lack of management of change was also believed as one of the factors. The impact of changes of personnel, policies, and/or organization structure were not evaluated carefully by the Texas City (CSB, 2007). For example, Texas City did not assess and evaluate the impact of cost-cutting strategy to the safety performance.

Independent Safety Review Panel (2007) shows that the inadequacy of the process management system to identify and to provide proper analysis of relevant process hazards as one of the contributors in the accident occurrence. The inadequacy was related to process hazard analyses that only considered threats in normal operation. The analyses did not have conservative approach and was not robust enough to analyze upset conditions (Baker, et al., 2007). The weakness in the process hazard analyses practice was apparent when the raffinate tower overfill was not considered as a credible scenario, thus it was overlooked and no mitigation was prepared to anticipate its occurrence. Additionally, the lessons from previous accidents, incidents, and near misses were hardly incorporated in the hazard assessments (CSB, 2007).

Multiples warnings and signs that indicated the possibility of major accident in Texas City refinery were existed. The management was clearly aware of them, but there was no action taken to respond and to intervene them to prevent their development into major problems (CSB, 2007). In addition, the management of the refinery did not encourage its workforces to report incidents, near misses, and other concerns related to safety, which might indicate problems in the refinery and early symptoms of a major accident (Baker, et al., 2007). The positive and trusting environment for that purpose had never been established in the Texas City refinery (Baker, et al., 2007). Interviews conducted by Independent Safety Review Panel (2007) indicate that some of the workers did not report safety-related concerns because of fear of punishments or retaliations from the management.

Figure 4.6 illustrates the connection between the direct accident sequences of events with non-direct factors, such weak safety culture and design flaws.

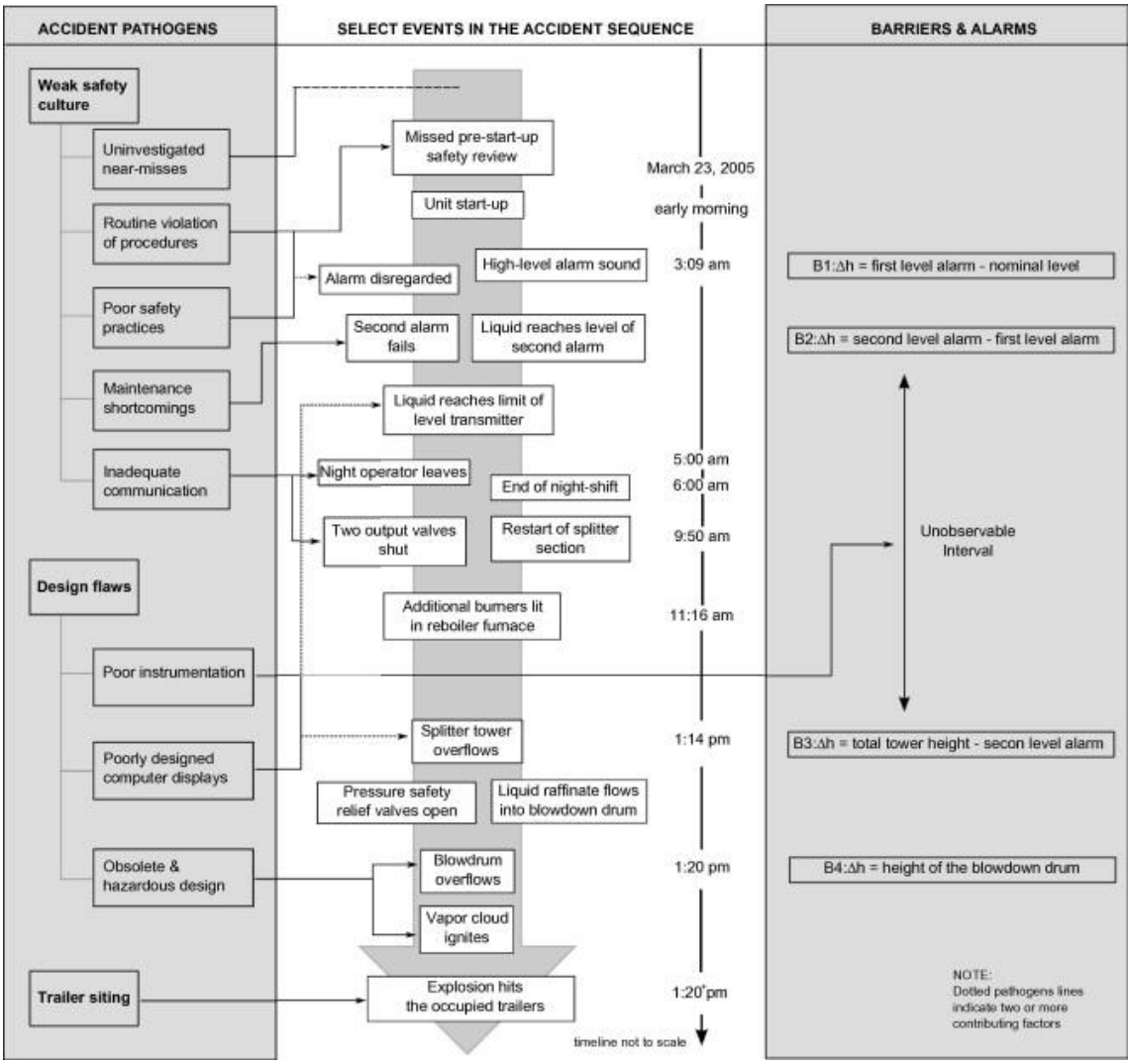

Figure 4.6 Illustration of interconnections between accident proximate events and indirect factors in Texas City Refinery accident (Saleh, et al., 2014)

4.4.4 The Fukushima Nuclear Accident

4.4.4.1 General event information

On March 11, 2011, the Fukushima nuclear power plant, owned and operated by the Tokyo Electric Power Company (TEPCO), was meltdown, causing the release of significant amount of radioactive material. It was affirmed as Level 7 by the International Nuclear Event Scale (INES) and was considered as one of the largest nuclear disasters after Chernobyl and Three Mile Island. There was no fatalities as the result of short term radiation exposure, but about 1,600 people died during the evacuation process. Furthermore, it also had substantial impact on the local communities due to radioactive contamination that threatened their health after long exposure.

4.4.4.2 Sequence of events

The meltdown was initiated by 9.0 Richter-scale earthquake that led to 14 meters high tsunami, overwhelming the seawall that had only 5.7 meters height. The tsunami flooded the nuclear plant and devastated power-related equipment, such as emergency diesel generators, the seawater cooling pumps, the electric wiring system, and the DC power supply, causing total power outage in the plant. The loss of power was directly contributed to the failure of reactor cooling system, and eventually the three cores meltdown.

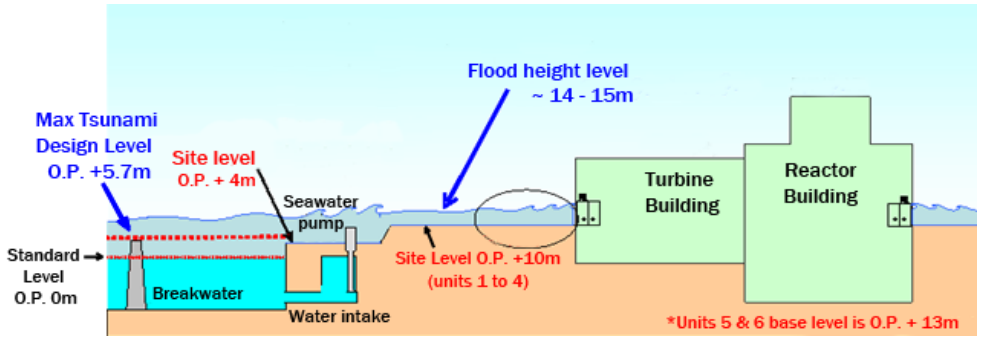

Figure 4.7 A schematic diagram showing the tsunami impact to the nuclear power plant (Anon., 2011)

4.4.4.3 Underlying problems

The direct cause of the accident was natural disaster. The earthquake was anticipated, but the magnitude on the accident was not expected due to its very rare occurrences. In-depth analysis by various parties shows that the issues were not only due to natural catastrophe; regulatory and organizational faults were said to be the root causes of the tragedy (NAIIC, 2012). Some information from several investigation reports and research papers are presented below to give illustrations of the deeper underlying problems causing the disaster.

Microlevel

Total power outage caused by the failure of emergency diesel generators, the seawater cooling pumps, the electric wiring system, and the DC power supply was the technical failure contributed in the accident. The tsunami flooded the power-related equipment, causing them to be non-functional.

Mesolevel

The management of TEPCO had propensity to prioritize profits over safety. It is apparent in the management policy to initiate trimming the “unnecessary” costs as their reaction towards the decreasing profits in the nuclear power industry in the recent years (NAIIC, 2012). This effort was also done to maintain Japan’s reliance of nuclear power (NAIIC, 2012). In addition, TEPCO’s tendency to prioritize the company’s financial growth over the community safety is also evident in the way they addressed technical problems. Most of damages, such as reactor cracks and loosening bolts, were not handled appropriately (Atsuji, et al., 2011). The measures to confront accidents were not planned and prepared adequately by TEPCO (Alvarenga & Melo, 2015; Kurokawa, et al., 2012). They

did not provide their workforces with adequate training program to prepare them in encountering accidents and emergency situations.

Both the decisions and actions taken by the regulator and the operator tend to prioritize their organization interest over public safety. One of the evidences was the opportunities to put prevention measures prior the occurrence of accident, which were not taken by both the regulator and the operator (NAIIC, 2012).

Macrolevel

The regulator failed to update the existing regulations to respond with the evolving technology (Kaufmann & Penciakova, 2011; Alvarenga & Melo, 2015; Wang & Chen, 2012). TEPCO was reluctant to accept and follow the updated nuclear safety regulations because they were afraid the new regulations would disrupt the stability of their operation and weaken their position in potential lawsuits (NAIIC, 2012). NISA, which should have enforced the new regulations, was committed to the mutually beneficial relationship with TEPCO and kept the old regulations to maintain the TEPCO's interests. Both of them has compromised the enforcement of the new regulations that would hinder effective control in the nuclear power plant (NAIIC, 2012).

Similarly, Kurokawa, et al. (2012) and Wang & Chen (2013) convinced that the collusion of interests between the government, Nuclear and Industrial Safety Agency (NISA), and TEPCO was one the causes leading to the disaster. They formed a mutually beneficial relationship, which harmed the governance of the nuclear industry. As discussed previously, the NISA received some incentives from TEPCO in return for giving them favorable policies (Wang & Chen, 2011; Wang & Chen, 2012a; Wang & Chen, 2012b; Onishi & Belson, 2011, cited in (Wang, et al., 2013)). This condition caused the decisions and actions to be directed towards both the regulator and operators interests, thus resulting in lack of control on the operation of the nuclear power plant. Wang, et al. (2013) argue the accident could have been prevented if effective nuclear safety rules and regulations had been in place prior to the catastrophe.

Moreover, NISA failed to plan an appropriate crisis management system to prevent emergency situation further developed into more critical situation. The system was judged to have failed in giving public health and safety protection (NAIIC, 2012).

Macro- and Mesolevel

NISA as the regulator and TEPCO as the operator were aware of the danger of total power loss as one of the hazards that threaten the integrity of the plant, but there was no serious consideration to prepare measures to reduce and mitigate the risks (NAIIC, 2012). Independent Investigation Commission also found evidence that NISA had informed TEPCO regarding the total power outage scenario, but they suggested to neglect it due to its low probability and assurance to the existing measures (NAIIC, 2012).

TEPCO and NISA were also completely aware regarding the possibility of the tsunami level exceeding their assumptions and the risks as the result of that. However, neither of them took actions to plan risks reducing measures (NAIIC, 2012). TEPCO and NISA disregarded five tsunamis

warnings after the year of 2000; no meaningful actions were taken to prepare for the possibility of tsunamis (Wang, et al., 2013).

4.5 Observations and Findings from Case Studies

This section will discuss the results of observations from the preceding case studies. The results will also be compared with Venkatasubramanian (2011) viewpoints regarding the patterns underlying systemic failures (see section 4.3).

Four key findings are identified: (1) unforeseen failures develop from non-linear and complex interactions of the system components, (2) ineffective control by regulatory agencies and management failure to uphold safety, (3) conflict between productivity/profitability and safety, and (4) unrecognized or neglected early warnings. They will be discussed individually in the following sections.

4.5.1 Unforeseen failures develop from non-linear and complex interactions of the system components

This first finding is the confirmation of what Venkatasubramanian (2011) has stated in section 4.3. All of the four case studies show that physical component failures and human errors have contribution in the unforeseen failure occurrence, but deeper analysis indicates more than that. It is obvious in the case studies that several failures in the management and regulator level also contribute in the occurrence of the catastrophes. Failure to provide adequate training to the workers, lack of management of change, and failure to provide adequate safety procedures are some examples of failures that happened in the management level while collusion, corruption, and poor regulatory system are some examples of failures found in regulatory level.

Venkatasubramanian (2011) argues that failures are developed from the dysfunctional interactions between regulatory agencies, company management, engineers, operators, physical equipment, etc., and his argument is evident in all of the case studies. Some factors directly contributes to the occurrence of the failure, such as the failure of cement barrier and BOP in the Deepwater Horizon blowout and the failure of liquid level indicator in Texas City accident. They are the direct causes and clearly visible at the moment of the accident. However, some factors do not have any immediate impact, such as lack of human factor consideration in the plant design, poor procedure design, or poor safety cultures. These are the factors that indirectly contribute to the occurrence of the failure and already exist long before the moment of the accident. The indirect factors are normally sourced from the unsafe decisions and actions made by upper organization level. Because of the interactions and interrelationship between hierarchical levels in the organization, these unsafe decisions and actions will bring impact to the other organizational layers and influence the system as a whole, causing the system to be fragile (Venkatasubramanian, 2011). For instance, in the Deepwater Horizon case, lack of human factors consideration in the design of the drilling rig control room causes difficulty for the drilling crew to monitor the well. Consequently, the drilling crew failed to notice ‘kick’ event just before the blowout occurrence. Figure 4.2, Figure 4.5, and Figure 4.4 clearly illustrate the complex interactions and the factors (both direct and indirect) involved in the occurrences of Bhopal, Deepwater Horizon, and Texas City case studies.

Because of complex interactions and indirect factors involved in the occurrence of failure, the complete picture of failure cannot be fathomed by merely looking at linear sequence of proximate events (Leveson & Stephanopoulos, 2014). Investigating only the proximate events will merely reveal the direct causes. Indirect factors will be hidden and missed and the underlying cause of the failure will never be truly revealed. For example, in Bhopal accident, if we only look at the chain of events at the moment of the catastrophe (see Figure 4.1), we will lean toward blaming the personnel as the main cause of the accident, which was not the true underlying causes. Furthermore, a particular outcome is not influenced by merely a single variable. For instance, in the case of human error, inadequate training program is not the only factor that increases the likelihood of human errors as poor safety culture, pressure to produce high productivity, and poor work planning and scheduling will also influence human reliability. Because a set of interacting variables will affect one particular variable, there is no clear linear relationship between cause and effect.

4.5.2 Ineffective control by regulatory agencies and company management failure to uphold safety

Regulatory agencies responsibilities are to impose regulations and govern the activities of companies in the industry, i.e. they are the controller of the companies. In the case studies, it is apparent that ineffective control by regulatory agencies is one of the unforeseen failures common causes. Poor regulatory system, corruption, collusion, conflict of interests, inability to identify hazards, etc. are the factors that lead to lack of control by the agencies. Similar argument is also given by Venkatasubramanian (2011) who states that ineffectiveness of regulatory agencies as the cause of systemic failures.

The danger of lack of control lies on the propensity of the companies to prioritize profits over safety. When there is lax in safety regulations or there is no safety restriction on certain activities, the companies have the opportunities to cut the corner to improve their productivity and maximize the profits while overlooking the importance of safety. This is clearly obvious in Deepwater Horizon case; the failure of the MMS to enforce regulation regarding safety critical element affected the quality of maintenance practice of the BOP. Because of no strict regulations on the maintenance and testing of BOP, BP might choose to cut the expenditure on maintenance. CSB (2010b) and Reader and O'Connor (2014) report that maintenance was inadequate, which contributed to the occurrence of blowout.

In Fukushima nuclear disaster case, the collusion between the NISA and TEPCO was the main issue. The mutual relationship created between them tends to weaken the control imposed by the regulator to the company. TEPCO had the opportunity to bargain any policies released by NICA, such as new safety regulations. The danger becomes bigger if the bargaining power possessed by the company is bigger, as if the company has taken over the regulatory agency as the controller of the activity.

Meanwhile in Bhopal disaster, ineffective control is related to the failure of the government and agencies to prepare the community in the event of leakage and the poor location of the plant. The summary of findings for each of the case study is presented in Table 4.4.

Table 4.4 Summary of findings that show ineffective control by regulatory agencies

Event	Ineffective control by regulatory agencies	Sources
Bhopal	Failure of the regulatory agencies to identify the hazard possessed by MIC, leading to lack of preparedness in the case of leakage and poor regulatory system to control the risks	(Shrivastava, 1994)
Deepwater Horizon	The failure of the regulatory agency to regulate effectively, caused by lack of resources, corrupt organizational culture, poorly written legislation, and the interaction between oil interests and politics	(Neill & Morris, 2012)
	Failure to impose regulations to manage safety critical elements	(CSB, 2010b)
	Regulatory agency was deficient in technically competent staffs and tend to give priority to maximize profits from leasing and production without considering the safety impact	(Reader & O'Connor, 2014)
Texas City	None is found	
Fukushima	Collusion of interests between the government, NISA, and TEPCO, which endangered the governance of the nuclear industry	(Kurokawa, et al., 2012; Wang, et al., 2013).
	Failure of the regulatory agency to update the existing regulations to respond with the evolving technology	(Kaufmann & Penciakova, 2011; Alvarenga & Melo, 2015; Wang & Chen, 2012a).

Management failure to uphold safety has similar meaning with ineffective control by regulatory agency. While the regulatory agency controls the company, the management of the company controls the hierarchical level below it, such as department managers, engineers, operation supervisors, operators, and physical equipment. Deficient safety management is clearly visible in all case studies. HSE UK (1997) defines five main elements required to achieve effective safety management:

1. **Policy** – effective policies are the key for the organization to achieve adequate safety.
2. **Organizing** – the organization should be able to engage all staffs to sustain safety in the organization by means of effective communication, promotion of competence, and leadership.
3. **Planning** – this element concerns about minimizing risks through planned and systematic approach. Risks shall be reduced as low as reasonably possible by implementing appropriate facility design, maintenance, inspection, or physical safety barriers.
4. **Measuring performance** – performance monitoring is required to identify any system deficiencies during operation and to enable immediate actions to remediate the situation.
5. **Auditing and reviewing performance** – auditing and review activities are functioned to give feedback to the entire system components.

If we compare these five elements with the findings shown in Table 4.5, the safety management of Union Carbide, BP, and TEPCO could be said as far from effective. For instance, defective plant design, poor maintenance practices, inadequate staff training, and failure to prepare measures to reduce the risks are violating of the third element in effective safety management while inappropriate definition of safety indicator as in the Texas City Refinery case does not conform to what states in the fourth element of effective safety management.

Poor safety culture is another evident of management failure to uphold safety. Safety culture can be defined as the company's way in managing safety in the workplace. The studies indicate that the decisions and actions taken by company's management would significantly influence the safety culture, which shapes the employees belief, attitudes, and perception to safety. For instance, repeated safety violations and unsafe acts from the workers are rooted from poor operational procedure developed by the management.

Table 4.5 Summary of findings that show deficient safety management in the case studies

Event	Deficient safety management system	Source
Bhopal	Inadequate operational procedure, defective plant design, poor inspection and maintenance practices, lack of management of change, inadequate provision of training, unavailability of emergency management plan	(Bowonder, 1987)
Deepwater Horizon	Poor safety culture, caused by productivity pressure imposed on the employees	(Reader & O'Connor, 2014; Størseth, et al., 2014)
	Inadequate staff training, excessively complex safety manuals, poor work planning and scheduling (which led to fatigue), and poor human-machine interfaces	(Reader & O'Connor, 2014)
	Poor maintenance and inspection program for emergency equipment	(CSB, 2010b; Norazahar, et al., 2014).
Texas City	Recurrent safety violation, inadequate safety procedures, and poor safety practices indicated poor safety culture	(Saleh, et al., 2014).
	Reliance on personal injury rate as the safety indicator to reflect the plant's safety performance	(CSB, 2007)
	Improper maintenance management that was shown by malfunctions and faulty instrumentations	(Saleh, et al., 2014).
Fukushima	TEPCO was aware of the danger of total power loss as one of the hazards that threaten the integrity of the plant, but there was no serious consideration to prepare measures to mitigate the risks.	(NAIIC, 2012)
	Decisions and actions taken tend to prioritize their organization interest over public safety.	(NAIIC, 2012).
	Unplanned and unpreparedness to encounter accident occurrences	(Alvarenga & Melo, 2015; Kurokawa, et al., 2012).

Ineffective control by regulatory agencies and company management failure to uphold safety can be explained by using the concept of *hierarchy*. In this concept, a particular system is depicted as having a hierarchical structure with several levels, where the top level establishes constraints for the level below it and it goes like that further down continuously until the lowest hierarchical level (Checkland, 1999, cited in (Leveson, 2011b)). Constraints can be conceived as the acceptable ways for the system to accomplish its common objectives (Leveson, 2011b). In other words, the higher level acts as the controller of the lower level, ensuring its behavior to be kept inside the constraints envelope. The problem emerges when a particular level does not impose adequate control to the

level beneath it, which could cause the behavior of the controlled level to be out of the defined constraints. Moreover, the uncontrolled behavior may percolate until the lowest hierarchical level, like a domino effect.

Regulators create regulations, standards, laws, and penalties as the constraints for the companies to operate and run the business safely. Nonetheless, if the constraints are too lax or there is no available constraint to control certain activities, safety can be compromised, especially if we recall companies' tendency to prioritize profits over safety. Similarly, the company management imposes control to the hierarchical levels below it, e.g. technicians, engineers, operators, etc. in the form of safety management and safety culture. Flawed safety management and poor safety culture can induce hazardous behaviors in the microlevel and lead the system to be out of safety constraints and eventually, the emergence of catastrophic events.

4.5.3 Conflict between productivity/profitability and safety

It is clearly evident that the conflict between productivity/profitability and safety at organization level is one of the factors that plays significant role in the occurrence of unforeseen failures in all of four case studies. It is also obvious that Bhopal, Deepwater Horizon, Texas City, and Fukushima disaster were caused by the management's higher emphasis on maximizing profits than on improvement of safety. The efforts were directed toward saving time and reducing "unnecessary" cost, such as maintenance cost reduction and staffs downsizing. The company suppressed the workers to achieve production goals without underlining the importance of safety. The summary of findings regarding the conflict between productivity/profitability and safety is shown in Table 4.6.

Table 4.6 Several findings that show the decisions of the company to save time and cost and their impact

Event	Decision	Effect	Source
Bhopal	Increasing machine efficiency and production speed and improving utilization of production capacity	Overused machines and equipment, higher equipment breakdown, less opportunity for preventive maintenance	(Bowonder, 1987)
	Limiting training on MIC operation	Ineffective employee training, incompetent staffs	(Joseph, et al., 2005)
	Reducing personnel number	Fatigue of the workers, higher probability of human error	(Shrivastava, 1994)
	Shutting down the MIC storage refrigeration system[2] to save power	The storage is more likely to undergo overheating and expansion in the event of MIC contamination	(Chouhan, 2005)
Deepwater Horizon	Anomalies were found during the execution of negative-pressure test, but no further investigation was conducted to assess the anomalies	Problems in the cement job were not known	(Reader & O'Connor, 2014)
	Not installing additional physical barriers to stop the flow of	The cement job at the bottom of the well was the only physical barrier	(Reader & O'Connor, 2014)

[2] The function of the refrigeration system in MIC storage is to lower the probability overheating and expansion in the event of storage contamination.

	hydrocarbons up the production casing, and displacement of mud from the riser before setting cement plug	stopping the flow of hydrocarbons up the production casing	
	Rejection of the full suite of tests for evaluating cement job	The evaluation of the cement job was reliant on a far more limited set of data	(Reader & O'Connor, 2014)
Texas City	Significant budget cuts and staffs downsizing	Excessive working hours that compromised the workers safety performance	(CSB, 2007)
	Reducing maintenance expenditure	Increasing problems related to equipment integrity	(CSB, 2007)
Fukushima	Improper treatment of technical problems	Most of damages, such as reactor cracks and loosening bolts, were not handled appropriately	(Atsuji, et al., 2011)

Rasmussen and Svedung (2000) believe that the management's focus on short-term financial goals while having less concern to safety is caused by a highly aggressive and competitive environment where the companies lived. This is fairly true in all of the study cases as shown in Table 4.7. What creates this type of environment is resources scarcity (e.g. budget, time, and manpower) and the pressure to keep achieving maximum profits (Rasmussen & Svedung, 2000). In this kind of situation, the decision-makers have tendency to make decisions and actions that lean toward the fulfillment of financial objectives without adequate assessment of how these decisions and actions impact on the safety performance (Dekker, 2011). In the study cases, it is clear that these decisions and actions compromised the safety of the system. The management did not realize the consequences of their decisions and actions until catastrophic event occurred at some point.

Table 4.7 The condition that created highly aggressive and competitive environment in the case studies

Event	Condition(s) that created highly aggressive and competitive environment	Source
Bhopal	The profitability of the Bhopal plant was reducing as the result of low demand of pesticides	(Joseph, et al., 2005)
Deepwater Horizon	The pressure to achieve high productivity was high because the operational expenditure of deepwater drilling is enormously high and there was a tight time constraint to finish the project	(Reader & O'Connor, 2014)
Texas City	The Texas City refinery management was pushed to reduce the amount of expenditure due to imbalance between profit contributions to capital consumption	(CSB, 2007)
Fukushima	Management of TEPCO was under pressure to keep profitable in the condition of declining substantial profit in the nuclear power industry	(NAIIC, 2012)

The discussion about the conflict between profitability and safety and company management failure to uphold safety (section 4.5.2) is in fact related to each other. The management tendency to prioritize profits over safety is one of the causes of deficiencies in safety management. This tendency will percolate to the entire system and affect the decisions and actions taken by the lower

hierarchical structure, such as engineers and operators. The consequence is that the layers of defense designed in the system to prevent accident (e.g. procedures, training, inspection and maintenance, physical barriers, emergency response, etc.) were degraded as shown in Table 4.6. For instance, in Deepwater Horizon case, anomalies in the results of negative pressure test to ensure the integrity of the cement job was neglected by the drilling crew. No further investigation was taken in order to save time and money. Consequently, the cement job was failed to withstand the 'kick' pressure from the well. The crew did not realize the danger of their actions and focused on the goal set by the management to complete the project within the set budget and time. In other words, following the strict written instructions may not help, thus getting shortcuts by neglecting some steps and procedures are found to be rational for them as long as they can fulfil what the management wants (Rasmussen & Svedung, 2000). The actors in the system did not realize the impact of their decisions toward the safety of the system. Economic pressure will shape their behavior, making their decisions appear to be safe and rational within their own local context, but not necessarily when looking into the entire system (Leveson, 2004).

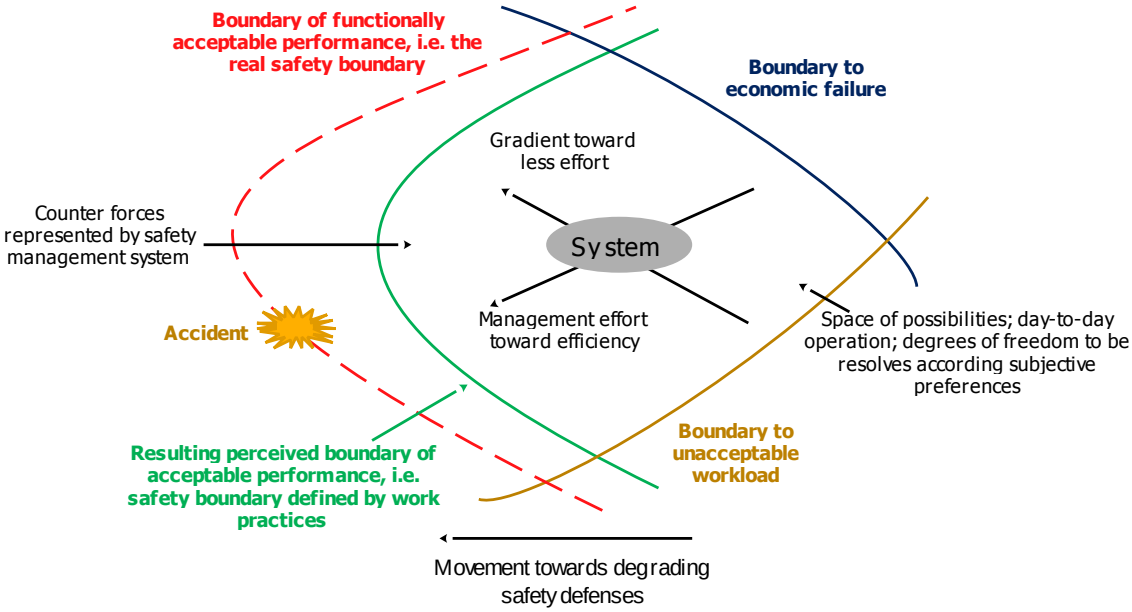

Figure 4.8 'Migration toward the boundary' model (adapted from (Rasmussen, 1997))

From the discussion above, we can say that the behavior of the entire organization is influenced by the environment surrounding it. This has been discussed and modelled by Rasmussen (1997). He views a system as a dynamic entity that always undergoes adaptations whenever there are disturbances from the environment or within the system. He defines three boundaries that constrain the system: financial, individual workload, and safety boundary (see Figure 4.8). The three boundaries create an envelope where the system can navigate freely. The pressure from one of the boundaries can create disturbance within the system. For instance, economic pressures and emphasis on high productivity will push the system closer to either individual workload or safety

boundary and similarly, pressure from individuals to ease up workload will create movement toward either economic or safety boundary as the system's adaptation mechanism against disturbances. In the case studies, what happen is that the economic pressure causes the system to migrate closer to the safety boundary. Rasmussen and Svedung (2000) call this as "systematic migration of organizational behavior under the influence of pressure toward accident under the influence of pressure toward cost-effectiveness in an aggressive, competitive environment".

Similar argument is expressed by Dekker (2011). He calls it "decrementalism", i.e. the groundwork of an accident is built in such small steps years before. Pressures from the internal as well as from the environment (e.g. competitiveness and resource scarcity) bring the system the requirement to adapt. Decisions made in every hierarchical level are one of the system ways to adapt with changing environment. Because of the complexity of the system and its interaction with environment, the system often does not realize the impact of decisions toward the safety of the system. A series of decisions may cause the system to deviate from the predetermined acceptable norm, which may results in drift of the system gradually toward hazardous state (Dekker, 2011; Leveson, 2004). In addition, the migration of the system toward the boundary will cause the designated system's defenses to deteriorate through time (Rasmussen, 1997).

4.5.4 Unrecognized or neglected early warnings

Leveson (2015) argues that there are always early warnings before major accidents. Her argument can be proven in the case studies. It is evident that several early warnings were existed prior to the occurrence of the catastrophe given in the case studies, but they were either neglected or unrecognized. As a result, no appropriate action was taken to respond to the warnings. The summary of the observed early warnings in each case studies is shown in Table 4.8.

Table 4.8 Several early warnings prior to the occurrence of the catastrophe given in the case studies

Event	Early Warnings	Source
Bhopal	Safety audit conducted prior accident occurrence in 1984 indicated the risks of runaway reaction in the MIC storage tank, but no risk reducing measure or mitigation action was taken	(Bowonder, 1987)
	Two safety audits prior year 1984 indicated poor safety management in the plant, but no follow up was taken to address the problem	(Bowonder, 1987)
Deepwater Horizon	Increasing drill pipe pressures and pump flow-out exceeded flow-in shown in the real-time data indicated that something was wrong and the well should have been closed, but the operators decided to continue the work	(Deepwater Horizon Study Group, 2011)
	Anomalies was found during the execution of negative-pressure test, but no further investigation was conducted to assess the anomalies	(Reader & O'Connor, 2014)
Texas City	Lack of encouragement from the plant management to report incidents, near misses, and other concerns related to safety, causing early warnings to be missed	(CSB, 2007)
	Multiples warnings and signs that indicated the possibility of major accident, but no action was taken to respond and to intervene them to prevent their development into more major problem	(CSB, 2007).

Fukushima	TEPCO and NISA disregarded five tsunamis warnings after 2000; no meaningful actions were taken to prepare for the possibility of tsunamis	(Wang, et al., 2013)

Dokas, et al. (2013) defines early warning signs as perceivable sets of data that pinpoint the existence of defects or threats or deviation of the operation from safe operating envelope in the system. The term 'accident precursor' has resemblance meaning with early warning signs. NASA (2011) apprehends an accident precursor as an anomaly that potentially indicates the occurrence of more severe event in the future. Based on these understandings, warning signs can be conceived as traces left by catastrophes prior to their occurrences. If properly identified and acted upon, early warnings or accident precursors can be used as tools to prevent the occurrence of major accident in a prospective manner.

Warning signs in industrial systems can be analogized to pain reaction in the human body. If the body feels pain, it indicates that there is something wrong with the body. Ignoring the pain will not solve the problem, but can even worsen it as the underlying causes of pain is unknown. For example, headache that has been ignored for a long time turn out to be a brain cancer, which could have been treated and cured if the action was made immediately once the headache was felt.

There are no fact or information regarding why Union Carbide, TEPCO, and BP did not take action to response the warning signs. There are two possibilities: whether they deliberately ignored the warning signs or they did not recognize them entirely. The attitude to actively ignore the warning signs is dangerous as proved in the case studies. The culture of the organization may affect the response to the warning signs. This is clearly evident in the case of Texas City, where poor safety culture causes lack of encouragement of the management to the workers to report concerns related to safety. In Deepwater Horizon accident, the decision to ignore increasing drill-pipe pressure might be caused by the pressure to achieve high productivity during the operation.

Additionally, the tendency to ignore early warning signs might be caused by the belief that the emerging signs are merely noises and considered to be insignificant to the integrity of the operation (Leveson, 2015). For instance, the warning signs have repeatedly occurred without any significant consequences, which caused common perception among the workers to consider them as unimportant. Another possibility is that the warning signs are deemed to be ambiguous, i.e. the signals may or may not possess real threat in the future, thus the managers, engineers, or operators choose to see and wait what will happen rather than take preventive actions (Roberto, et al., 2006).

4.6 Summary of the Findings and Observations

The findings and observations from the selected case studies are similar with Venkatasubramanian (2011) statement in section 4.3. Addition is made by mentioning conflict between productivity/profitability and safety and unrecognized or neglected early warnings. So, to summarize this chapter, the following points are given:

- Unforeseen failures are developed from the dysfunctional interactions between regulatory agencies, company's management, operators, physical equipment, etc., and the

involvement of indirect factors (e.g. unsafe decisions and actions by the management and regulator and organizational factors), which are virtually impossible to be completely captured by merely linear sequence of events.

- Technical failures and operator errors were the direct causes, but we cannot overlook the contribution from regulatory agencies, corporate board, and company management. Their failure to impose adequate safety control to the level beneath them is one of the factors that lead to the occurrence of unforeseen failure.
- The conflict between financial and safety objectives is deemed as one of the causes of unforeseen failure. The companies' decisions and actions tend to lean towards the fulfillment of financial goals without assessing their impact towards the safety of the system, thus making them unaware about the harmful effect of their decisions and actions to the safety of the system,
- Early warning signs were existed prior to failure, but no action was taken by the companies to respond to them. The warning signs might be considered as non-threatening to the system or had ambiguous characteristic, thus repelled the management desire to take meaningful actions.

5 CHAPTER FIVE – Discussion and Recommendations

5.1 Discussions

Based on observations and findings made in the previous section, three prerequisites are drawn to encounter future occurrence of unforeseen failures as follow:

1. The needs for new hazard analysis technique
2. The needs to address the dynamics of the system
3. The requirement to implement a method to differentiate between the important early warning signs and noises

Each of them will be discussed in the following sections.

5.1.1 The needs for new hazard analysis technique

There is no information regarding the type of hazard analysis used in Bhopal chemical plant, Deepwater Horizon drilling rig, Texas City refinery, and Fukushima nuclear plant. The conventional hazard analysis techniques, such as FTA, FMEA, and HAZOP were most probably used as they are the most widely used techniques and have been used in the various industries many years ago. However, these techniques are no longer adequate to be used in a highly dynamic and complex socio-technical system due to their underlying assumptions and approaches. As stated previously in section 3.3.1, they are based on sequential accident model, which focuses only on proximate events that have direct causality with the failure event, i.e. linear chain of events. They are constructed based on the assumption is that there must be direct causality between events prior to the occurrence of failure (Leveson, 2011a). In fact, based on the observations and findings in the section 4.5.1, unforeseen failures are developed from complex interactions between system components that are virtually impossible to be entirely explained and understood by merely a linear chain of events. Additionally, the occurrence of unforeseen failures involves both direct and indirect factors, thus the utilization of traditional hazard analysis techniques will hide the contribution from these factors.

Furthermore, as the conventional hazard analysis techniques are founded on linear chain of events model, their focus is merely on failure of electrical and mechanical components (Leveson, 2011b). Nonetheless, based on the findings in section 4.5.2, management and regulatory agencies are also responsible to the occurrence of unforeseen failures. Their unsafe actions and decisions will affect the lower level and contribute to the development of the failures. Organizational factors, such as management deficiencies and flaws in the company's safety culture will not be able to be identified (Leveson, 2004). Their contribution to failures cannot be captured and remain hidden and unknown if conventional hazard identification methods are used.

Based on this notion, a new approach in hazard analysis is required to reveal some factors that are omitted in the conventional hazard analysis techniques, such as interactions between components,

unsafe decisions and actions by the management and regulator, and organizational factors (Leveson, 2011b).

Table 5.1 The summary of assumptions used in conventional hazard analysis techniques, unforeseen failure characteristics, and the effects if conventional hazard analysis techniques are used

Assumptions of conventional hazard analysis techniques	Unforeseen failure characteristics	The effects if conventional hazard analysis techniques are still used in highly complex and dynamic system
The occurrence of failures involve only direct factors.	The occurrence of failures involve both direct and indirect factors.	Indirect factors will be omitted.
The occurrence of failures can be explained by linear chain of events.	The occurrence of failures involve complex interactions between system components.	The risks emerged from components interactions will be ignored.
Focus only on failure of physical equipment.	Regulatory agencies, management, and human factors have contribution in the failure occurrence.	Contribution of regulatory agencies, management, and human factors will be overlooked.

5.1.2 The needs to address the dynamics of the system

The finding addressed in section 4.5.3 brings the understanding that a system is not a static entity. A system always tries to adapt with the surrounding environment. The decisions and actions that tend to lean towards the fulfillment of financial objectives can be conceived as the adaptation mechanisms owned by the system to respond to the increasing competitiveness and aggressiveness in the industrial environment. However, the pressure towards cost-effectiveness will potentially produce system behavior that will lead to degradation of system's defenses over time (Dekker, 2011; Rasmussen, 1997). The impact of decisions and actions of high level management cannot be directly felt, but they will possibly propagate throughout the organization, affect the lower hierarchical level behavior, and incrementally drift the system into failure. The system will get closer and closer to the safety boundary without being recognized.

In addition, the designated risk controls or risk reducing measures may become ineffective because of changes in the surrounding environment. Relying only on the hazard analysis techniques will not be sufficient as the system's adaptation mechanisms will potentially create new hazards during the operation of the system, such as hazards that are emerged from the deterioration of system's defenses without being recognized and enforced.

Therefore, there is a need to define a technique that can be used to notify the decision-makers regarding the current state of the system, thus early actions can be carried out to prevent further system safety degradation that can lead to system failure.

5.1.3 The requirement to implement a method to differentiate between the important early warning signs and noises

From the findings in the section 4.5.4, it is clear that all of the unforeseen failures in the given case studies left early warnings before their occurrence, but nobody recognizes them or someone notice them but deliberately ignore them, thus no corrective action was taken. The latter is prominent in the case study because of the influence of poor safety culture and pressure toward achieving high productivity, which have been addressed in section 5.1.2.

The other causes are the presumption of people that the warning signs are not threatening to the system or the signals are ambiguous. Additionally, there must be enormous number of early warning signs existed during the operation phase and it is difficult to distinguish between the important ones and the noises. Therefore, it can be argued that a method to differentiate between the important warning signs and the non-significant ones are required to be applied in the system. The purpose is to ensure that necessary actions are conducted on the potentially threatening warning signs to prevent their development into more serious problems.

5.2 Recommendations

In order to fulfill the prerequisites stated in the previous sections, two recommended techniques are given:

1. The utilization of system-based hazard analysis
2. The implementation of leading indicators

They will be discussed in the following sections.

5.2.1 The utilization of system-based hazard analysis

Instead of constructing hazard analysis based on sequential or epidemiological accident models, systemic accident model shall be the basis of the hazard analysis (Leveson, 2011b). The purpose is to cover the whole accident process by taking into account of factors that are neglected by traditional accident hazard analysis techniques, such as component interactions, human decision-making, social and organizational factors (Leveson, 2011b).

Several novel hazard analysis techniques were introduced in the recent years. Some of them that are worthy to mention are Blended Hazard Identification (BLHAZID), System-Theoretic Process Analysis (STPA), and Dynamic Procedure for Atypical Scenarios Identification (DyPASI). BLHAZID is constructed based system theory (Seligmann, et al., 2012) while STPA is a hazard analysis based on systemic accident model (Leveson, 2011b). DyPASI is claimed to be able identify *unknown unknown* and *unknown known* type of events (Paltrinieri, et al., 2013). However, BLHAZID and DyPASI are still founded on conventional hazard analysis, such as FTA, ETA, FMAE, and HAZOP. The complete review of DyPASI and BLHAZID is provided in Appendix A

The only hazard analysis that is based on systemic accident model is STPA. STPA is a new hazard analysis method, developed by Leveson (2011b), that has the same function as the conventional hazard analysis techniques, but with different approach; while conventional hazard analysis

techniques are still based on sequential or epidemiological accident models, STPA is based on Systems Theoretic Accident Modeling and Processes (STAMP), a systemic accident causation model (Leveson, 2011b). STAMP is constructed based on the premise that every organizational layers have roles and contributions in the occurrence of major failures. Three principal elements that underlie STAMP are safety constraints, hierarchical control structures, and process models (Leveson, 2011b).

1. **Safety constraints** – In STAMP, safety is seen as an emergent property that is created by the components interactions and interrelationship. Safety has its own constraints and the violation of these constraints may lead to accident. For example, in Texas City Refinery, the safety constraint is that the flammable compounds must be contained in the pressure vessel or piping and the violation of this constraint has caused major loss as described in section 4.4.3. In other words, accident happens if the safety constraints are not enforced (Leveson, 2004). Constraints can in the form of safety policies, procedures, work instructions, safe operating limitations, etc.
2. **Hierarchical control structure** – STAMP is based on the premise that a system is comprised of hierarchical structures, where the upper levels control the lower levels by inflicting constraints. For instance, regulatory agencies impose regulations and laws to the company, or the operator set operating limit to the equipment. Besides the imposition of constraints from a certain level to the level beneath it, the controlled level will also provide feedback to its controller as a mean to provide adaptive control to the system (Leveson, 2004). The exchange of constraints and feedbacks between two control levels create a communication channel between control levels as illustrated in Figure 5.1. An example of generic hierarchical control structure is presented in Figure 5.3.

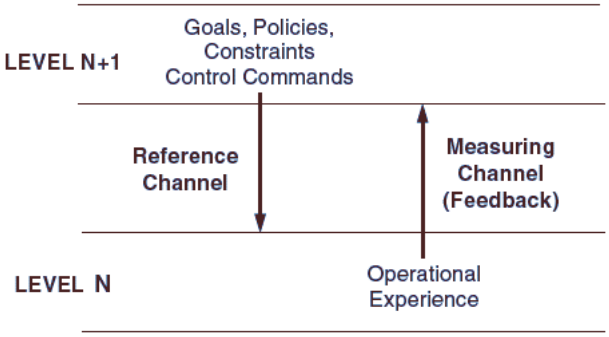

Figure 5.1 Establishment of communication channel between control levels by exchanging of constraints and feedbacks (Leveson, 2011b)

3. **Process models** – Process model can be described as the logic embedded in the level that acts as the controller. The process model helps the controller in making decisions regarding what appropriate control actions to issue. It uses feedbacks provided by the controlled level to generate control actions and keep the controlled level within the specified safety constraints. A process model can be explained simply by taking thermostat as an example. A thermostat is set to always keep the temperature of a particular room below 25 °C and

above 15 °C. In this case, the controller is the thermostat, the controlled level is the room, and the safety constraint is the temperature between 25 °C and 35 °C. The process model is the logic inside the thermostat that keeps the temperature between 25 and 35 °C. The room give feedback by informing the current temperature to the thermostat. The control action taken by the thermostat will depend on the feedback, i.e. the current temperature. If the temperature is still within the constraint, then no control action is required. However, if the temperature violates the constraints, control action will be issued to remediate the temperature back into the defined constraint.

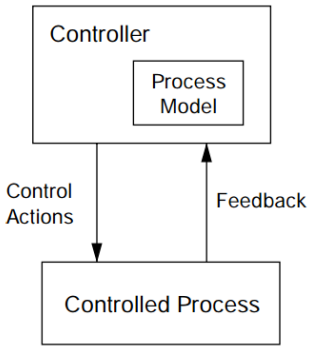

Figure 5.2 The process model embedded in the controller (Leveson, 2011b)

Based on the three elements above, Leveson (2011b) classifies two general causes of accident. She believes that the occurrence of accident must involve the following:

1. Lack of enforcement of safety constraints by the controller.
    a. No control actions is provided by the controller.
    b. The control actions are provided at the wrong sequence/time.
    c. The control actions result in violation of the safety constraints, i.e. unsafe control actions are issued.
2. Controller has sent control actions, but they are not executed/followed by the controlled level.

STPA uses “guidewords” resembling with HAZOP. However, unlike HAZOP which develops the guidewords based on Piping and Instrumentation Diagram (P&ID), STPA uses functional control diagram as the basis for constructing the guidewords (Leveson, 2011b). Moreover, the guidewords in STPA express unsafe control actions in the system rather than deviations in the process parameters.

Several experimental comparisons between STPA and conventional hazard analysis techniques have been carried out and the results indicate STPA superiority compared to its counterparts. Leveson (2011b) mentions some of them as follow:

- The application of STPA in the U.S. missile defense system has successfully identified failure scenarios that could not be revealed by using other hazard analyses.
- Comparison between STPA and FTA was carried out on unmanned spacecraft owned by JAXA (the Japanese Space Agency). The result shows that STPA were successfully identified all of the failure scenarios that were identified by FTA. Moreover, additional failure scenarios beyond technical component failures that were not identified by FTA were successfully identified by STPA.

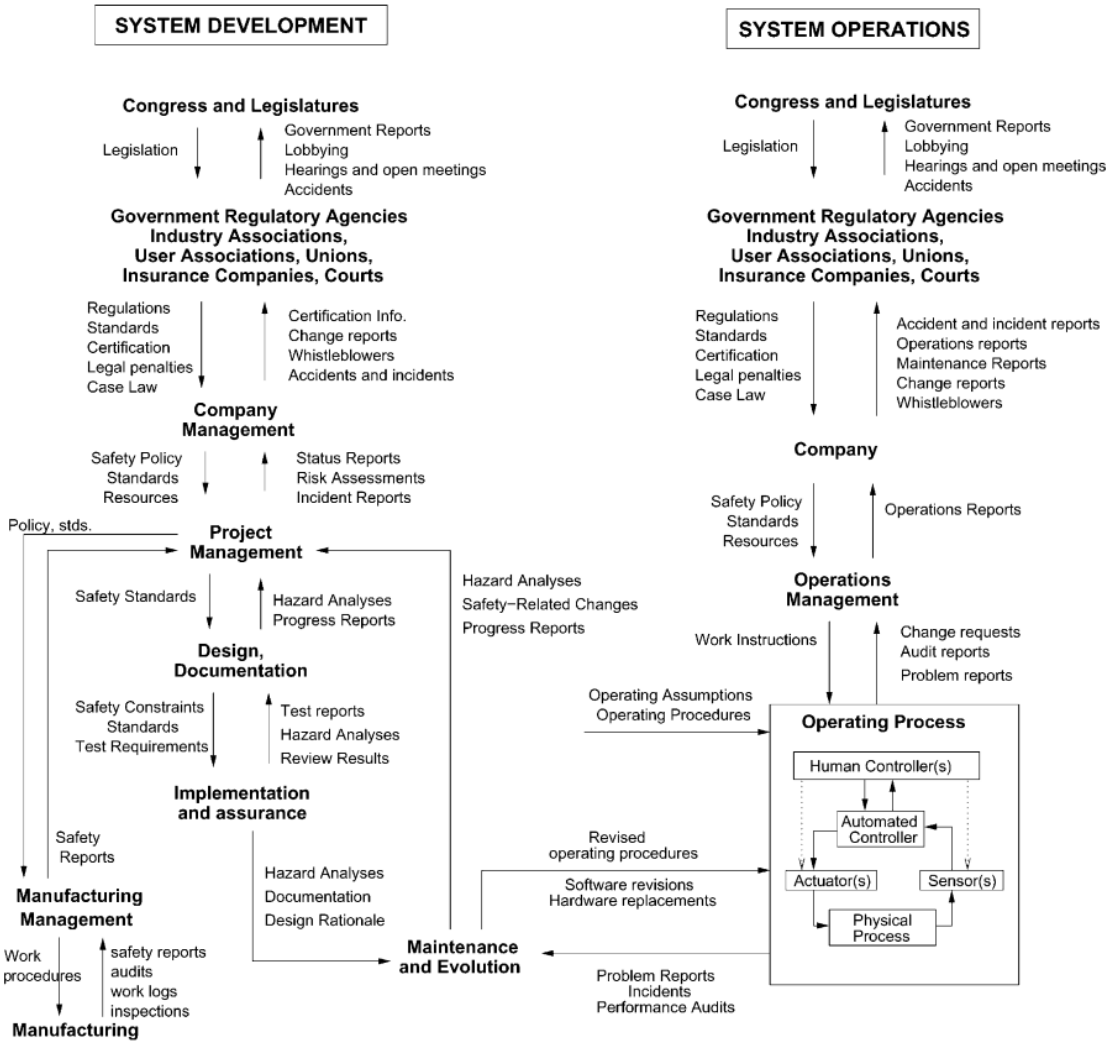

Figure 5.3 Typical organization hierarchical control structure (Leveson, 2004)

5.2.2 Implementation of leading indicators into the risk management process

To address the dynamicity of a system, Rasmussen and Svedung (2000) suggest a proactive risk management, which is aimed to counteract pressures that drive decision-makers to make unsafe decisions and actions that move the system towards the safety boundaries. In proactive approach, risk management is viewed as a control problem (Rasmussen & Svedung, 2000). The control relies on continuous monitoring of the actual safety level. To do this, the comparison and measurement

of margin between the present system conditions and predetermined system safe operation is required. The margin is kept within certain distance to keep the system safe by utilizing a closed loop feedback control strategy. Control action shall be carried out by the decision-makers when the margin is deviated from the predetermined safe conditions.

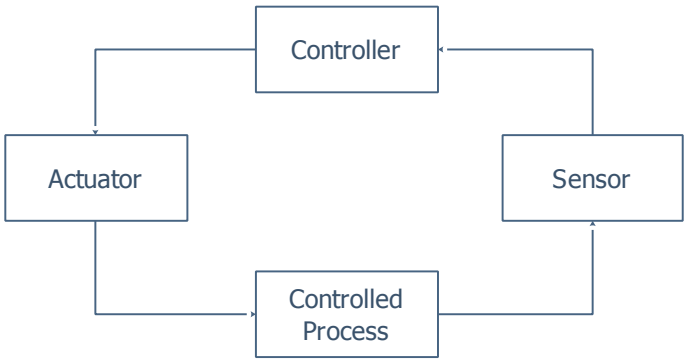

Figure 5.4 A general closed loop feedback process

One way to adopt proactive risk management approach is by implementing leading indicators to the system. Leading indicator is a type of proactive monitoring that provides feedback before occurrence of an accident (HSE UK, 2006). Leading indicator main function is to monitor the safety level in the system (Dokas, et al., 2013), or in other words to measure the system position toward the safety boundary if we refer to 'migration towards boundary' model by Rasmussen (1997). The implementation of leading indicators will enable the detection of hazardous operation of the system, thus violation of safety boundary can be identified early in the operation. This information can be used to notify decision-makers regarding the state of the system, thus early actions can be carried out to prevent further system safety degradation that can lead to system failure. Moreover, it can also be used to identify hazards that is unidentified during the design phase as well as new hazards that emerge as the result of changes in the environmental conditions (Khawaji, 2012).

In addition, leading indicator can act as early warning as it looks further back to measure and monitor the conditions and factors that contribute to the occurrence of accident (Øien, et al., 2011). The identification of leading indicators will be valuable as a systematic collection of early warnings and to enable recognizing the important early warnings, thus differentiation between noises (or insignificant warning signs) and threatening signals can be made. The implementation of leading indicator will increase the ability of the system to adapt with the environment without degrading safety, i.e. the system will be more resilient and able to cope with both expected and unexpected events.

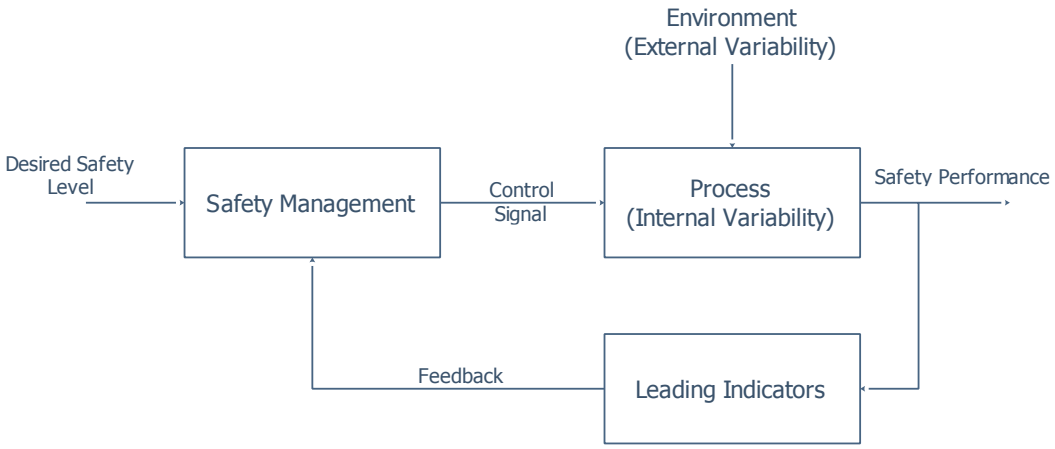

Figure 5.5 Closed loop feedback process in the implementation of leading indicators (adapted from (Hollnagel, 2008))

Figure 5.5 shows a simple illustration of how leading indicators work in a system. The performance of the process is affected by the variability that is sourced from system internal and external. External variability can be in the form of changing market trend, increasing competitiveness, economic recession, and other aspects from the environment that potentially affect the system in some ways. The system's adjustment and adaptation with external variability will create internal variability. The adjustment can be in the form of cost cutting, reduction of employees, and other decisions and actions that often harm the safety of the system. Some examples of internal variability are employees' safety performance and behavior, equipment functionality, maintenance and inspection effectiveness, etc. The leading indicators act as the sensor to monitor the safety performance of the system and to identify hazards that are sourced from the internal and external variability. The monitoring results are sent to the safety management system as feedbacks regarding the actual safety performance of the system. The safety management compares the actual safety performance with the desired safety level (or safety constraint). The identified gap between actual and desired safety will trigger control action to close the gap of performance.

Another performance measurement that is commonly used in the industry is lagging indicator. Unlike leading indicator, it provides retrospective view and reflect the performance of the system in the past or the occurrence of historical events, e.g. incidents, near misses, and accidents (Herrera, 2012). Some examples of prevalent lagging indicators are the number of equipment/instrumentation failure, the number of fire incident, and the number of injured worker during worktime. Lagging indicator cannot be used as early warning. For instance, in Texas City refinery accident, the management of the plant used personal injury rate as the safety indicator. However, low number of injury could not reflect the safety performance in the system. This is evident after the occurrence of the disaster that the safety performance and safety culture of the Texas City refinery was poor despite the attainment of low personnel injury number.

Leading indicator can be applied to measure the performance of every hierarchical level, from equipment level, operator, until management and regulator (see Table 5.2).

Table 5.2 Different hierarchical levels and their related leading indicators

Hierarchy Level	Related Leading Indicators
Technical Equipment	Process parameters (e.g. pressure, temperature, flow, etc.) and condition-related parameters (e.g. vibrations, level of contaminant, wall thickness, efficiency, etc.)
Operator, Technician	Level of competences, physical and psychological conditions.
Management	Evaluation of safety culture, audits of safety management, maintenance and inspection program adequacy study, assessment of existing procedures

Leading indicators can be beneficial to achieve acceptable safety level in a system. However, the indicators can cause false sense of system condition/performance if they are not implemented correctly, as happened in Texas City Refinery accident (CSB, 2007). Complete knowledge about the concept of leading indicators must be acquired in order to appropriately select the indicators that can reflect the actual condition/performance of the system. Herrera (2012) mentions some properties that must be possessed by leading indicators as follow:

- **Meaningful** – the indicators must be able to point out hazardous actions that happen in the system.
- **Sensitive** – the indicators must be sensitive to detect and inform any changes that are potentially can threaten the system.
- **Measurable** – the indicators must be able to be measured either quantitatively or qualitatively.
- **Unbiased** – an indicator is unbiased of all people conceives it in similar way without the needs of personal judgement or subjectivity.
- **Verifiable** – the indicators must be able to be verified to confirm the validity of their measurement.
- **Affordable** – the benefits obtained by the applying the indicators should outmatch the costs of their implementation.

There is no one agreed guidance to develop leading indicators. Several guidelines for developing safety leading indicators have already been existed in the industry, provided by organizations and associations, such as API, CCPS, and HSE UK. API (2010) provides guideline that focuses on the identification of lagging and leading indicators in refinery and petrochemical industries and other industries where the release of process containment is the primary hazard. API mentions the following alternatives to identify lagging and leading indicators:

- Utilize hazard analysis and risk assessment results
- Use the result of accident investigation to identify indicators related to the accidents
- Use past experiences of the successful application of particular indicators

API (2010) also mentions the importance of involving employees, engineers, and process safety professionals during the selection process indicators to produce a more comprehensive picture of process safety performance.

Similar with API, CCPS (2010) proposes the utilization of hazard analysis, incident investigation report, past experiences as the basis to develop leading indicators. In addition, CCPS (2011) also proposes several prescriptive leading indicators that can potentially inform the safety level in a certain system. The identification of these indicators are based on industrial experiences on barrier management and some reviews of CCSP Risk-Based Process Safety book and limited to the area of mechanical integrity, safety culture, training and competency, operation and maintenance, and fatigue risk management (CCPS, 2011).

However, both API and CCPS do not provide a clear step-by-step guidance to identify critical leading indicators. CCPS refers to the methodology developed by HSE UK as the step-by-step guidance to identify leading indicators (see section 0). HSE UK (2006) uses hazard analysis as the basis to identify leading indicators, but put more emphasis on the identification of leading indicators based on the defined risk control or risk reducing measure to control the identified hazards. An interesting notion from HSE UK is the concept of “dual assurance”, i.e. the leading and lagging indicators are implemented together to provide double protection of the system safety and to ensure the risk control effectiveness in enforcing the safety constraints.

The recommendation of API and CCPS to use the result of accident investigation and past experiences have major weaknesses. By using accident investigation, the leading indicators will only be affiliated to the events that occurred in the accident while overlooking the other events outside the accident that will possibly occur in the future. Using past experiences can be an alternative, but leading indicators that have been used in the past might not be suitable anymore in the current system condition, given that the system is always evolving any time.

The suggestion to use hazard analysis can be argued as a better option compared to using accident investigation and past experiences. The coverage of hazard analysis is relatively larger as it does not only rely on past events. However, the quality of the leading indicators will be largely dependent on the result of the hazard analysis. As the main purpose of the leading indicators is to monitor the safety level in the system or to measure the system position toward the safety boundary, the leading indicators shall cover the entirety of the system, from the technical issues until the management aspects. This argument is proponent by the fact that the safety level/the migration of system position towards the safety boundary are not only dependant on technological and human factors, but also interactions between components, unsafe decisions and actions by the management and regulator, and organizational factors (Dekker, 2011). Hazard analysis based on systemic accident causation model (e.g. STPA) is suggested to be used instead of using the more conventional hazard analyses in order to enable the monitoring of the entire socio-technical system.

5.3 Summary

The following points are summarized based on the discussion and recommendation made in this chapter:

- The occurrence of unforeseen failure always involves the dysfunctional interactions between components, unsafe decisions and actions by the management and regulator, and organizational factors. These aspects cannot be well captured by the conventional hazard analysis techniques that are still constructed based on sequential accident model. Hazard analysis founded on systemic accident causation model should be used to consider the aspects that are omitted by the traditional hazard analysis techniques. One of the suggested approach is to use STPA, a hazard analysis technique that are based on STAMP, a systemic accident causation model.
- A socio-technical system is highly dynamic and complex entity that constantly adapts with its surrounding environment. The adaptation mechanism emerges in the form of decisions and actions taken by the management to respond to highly aggressive and competitive environment. The danger arises when these decisions and actions bring the entire system to state of higher risk. The system will migrate towards the safety boundary and eventually violate it without the actors inside the system realizing it. The failure will be unforeseen for most the personnel inside the system. Adopting proactive risk management by implementing leading indicators is suggested as an approach to notify decision-makers regarding the state of the system, thus early actions can be carried out to prevent further system safety degradation that can lead to system failure. In addition, implementation of leading indicators will also be beneficial as a systematic collection of early warnings and to enable recognizing the important early failure warnings.

6 Chapter Six - Case Study

6.1 Introduction

The purpose of this chapter is to demonstrate the suggested approach from chapter 5, which is STPA and leading indicator, to a real industrial system. High-Integrity Pressure Protection System (HIPPS) in a subsea installation is selected as the case study. The case study will be focused only on the execution Partial Stroke Testing (PST) of HIPPS. Detail information about the case study will be provided in the following sections.

The selection of HIPPS as the case study is motivated by the Deepwater Horizon accident. One of the causes of the Deepwater Horizon catastrophe is the failure of BOP, one of the physical barriers to stop uncontrolled flow of hydrocarbons towards the rig. Maintenance and testing program as means to maintain the functionality of the BOP were deemed as inadequate (CSB, 2010b; Reader & O'Connor, 2014). Lack of regulation and requirement from the regulatory agency to manage safety critical element (e.g. BOP) was believed to be the cause of the inadequacy of maintenance and testing program (CSB, 2010b; Reader & O'Connor, 2014). BP management that tends to prioritize profits over safety would not create and execute proper maintenance and testing by itself without any regulation imposement from the regulator. The combination of these factors deteriorate the ability of the BOP to function on demand.

Similar occurrence might happen with HIPPS. HIPPS is one the physical barrier in a subsea installation that has function to prevent overpessure in a subsea production system. HIPPS is deeemed to have high reliability with its redundancy and fail-safe design. However, it is not impossible for a HIPPS to undergo failure even with the design that is considered as highly safe. From the technological perspective, HIPPS might be very unlikely to be failed. But, learning from Deepwater Horizon and other unforeseen failure cases, the influence from dysfunctional interactions between system components, unsafe decisions and actions by the management and regulator, and social and organizational factors can degrade the ability of HIPPS to function and cause subsequent catastrophe.

6.2 General Description of HIPPS

6.2.1 HIPPS in subsea production system

HIPPS is basically a safety instrumented system (SIS) that is designed to protect flowlines/pipelines/equipment downstream of the subsea production tree(s)/manifold from hazardous overpressure scenarios. Overpressure can be initiated by failure of choke valve, blockage of the flowlines caused by hydrate formation, inadvertent shutting of downstream valve, and operator error (Frafjord, et al., 1995). HIPPS module is normally installed downstream of the subsea production tree(s) and subsea production manifold.

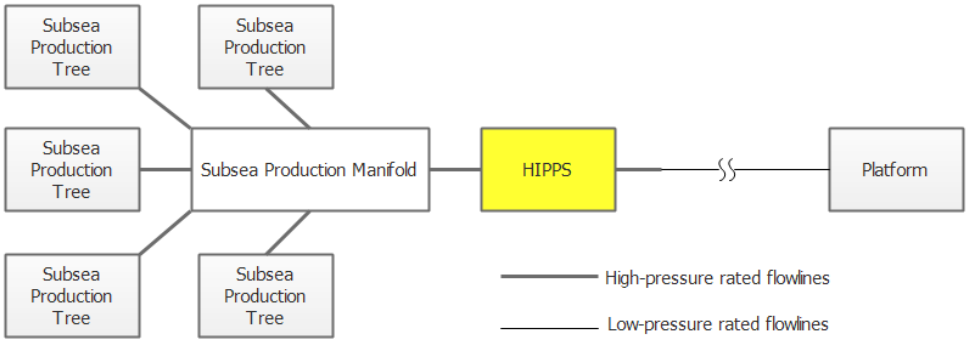

Figure 6.1 An example of simplified schematic diagram of subsea production system with five subsea trees, commingled in a subsea production manifold

Flowlines, pipelines, risers, and other subsea equipment in a subsea production system shall be designed to have full shut-in pressure rating of the wells (Gall, et al., 2002). This is a cautionary design to anticipate possible wellhead choke failure and flowline blockage due to hydrate formation that can cause overpressure. The installation of HIPPS will allow the reduction of the pressure-rating of downstream flowlines, pipelines, risers, and topside equipment, thus the system can be constructed in lower capital expenditure. In addition, HIPPS will provide higher integrity and safety to the production system.

6.2.2 HIPPS basic components: features and functions

HIPPS has three main components: the HIPPS control module (HCM), pressure transmitter (PT), and shutdown valve (SDV). HIPPS is commonly designed to have more than one PT and SDV in order to provide redundancy and higher fault tolerance. The functions and features for each of them will be explained as follow.

- PT measures the pressure of the flowlines and sends the information signal to the HCM. Redundancy is provided by installing more than one transmitters. Three PTs with 2-out-of-3 (2oo3) voting logic is typically used as it provides good balance between safety and production availability (Phillips & Roberts, 2005).
- HCM is basically the controller of the HIPPS. It contains a logic solver that processes the signal sent by PT by comparing the signal pressure information with the HIPPS setpoint limit. Setpoint is the pressure value at which the SDV initiates to close. When the setpoint is reached, HCM sends signal to the solenoid valve to de-energize, causing the SDV to close. Solenoid valve is the valve that supply power to the SDV to keep it open during normal operation. It is normally located inside the HCM. In the event of overpressure, the HCM will send signal to the solenoid to de-energize, i.e. to stop supplying power to SDV, which causes the SDV to close.
- HCM also contains secondary controller that allows communication with the Master Control Station (MCS) located at the topside to enable testing, maintenance, and monitoring of HIPPS (Phillips & Roberts, 2005).

- The SDV main function is to close the valve in the event of overpressure with the command from the HCM. During normal operation, SDV will be kept opened by energizing it with air pressure (pneumatic power supply), hydraulic fluid (hydraulic power supply, or electric power supply. The SDV has fail-close design, i.e. the valve will close automatically in the event of loss of power.

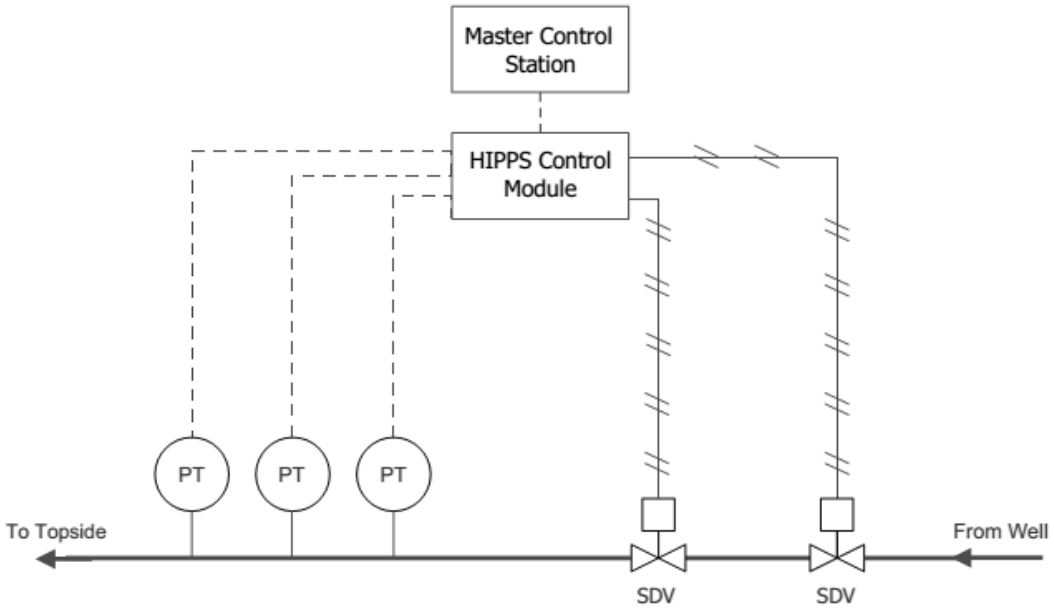

Figure 6.2 Simplistic schematic diagram of generic HIPPS in subsea production system

Subsea HIPPS module is connected to the MCS to enable the operator to carry out testing and maintenance as well as to monitor the current state of HIPPS from the topside. MCS receives the monitoring signal from the HCM and presents the information to the operator regarding the HIPPS state, thus enabling the operator to act immediately when required (Phillips & Roberts, 2005). Some of the information required to monitor HIPPS includes alarm when the flowlines pressure exceeds the setpoint, alarm in the event of fault or malfunctioning of individual component (e.g. pressure reading deviation, logic solver error, and stuck open valve), pressure trends, and valve status (close or open).

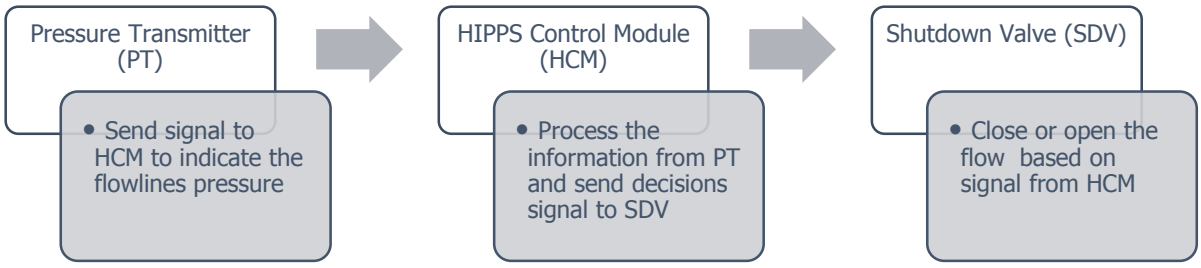

Figure 6.3 Function description of main HIPPS components

6.2.3 Partial stroke testing

HIPPS shall be routinely tested to ensure its functionality upon demand. Partial Stroke Testing (PST) is a type of test that can be implemented for this purpose. Unlike the conventional full stroke test, PST can be carried out online, i.e. without shutting down the production process. PST will also not cause disturbances to the process as the valve movement is too small to disrupt process flow or pressure (Lundteigen & Rausand, 2008). The execution of PST can be supervised from the MCS.

The main purpose of PST is to ensure that the valve is able to open on demand, i.e. the valve is not stuck open. In PST, the valve is instructed to close partially. The assumption used in PST is that partial movement can indicate valve ability to fully close in real demand situation. One of the options to enable carrying out PST in HIPPS is by integrating PST capability with logic solver contained in HCM (Lundteigen & Rausand, 2007).

The command to conduct PST comes from the MCS. The initiation signal is sent to the HCM, which will subsequently deactivate the solenoid valve. The solenoid valve is then de-energized, causing the SDV to close. Before the SDV is fully closed, the HCM will re-energize the solenoid valve, returning the SDV to its initial position (Lundteigen & Rausand, 2007).

Although PST has some advantages over the more conventional test, it also has some major drawbacks. Some of the disadvantages of PST are given below:

1. It cannot reveal all of the dangerous failure modes that threaten the functionality of HIPPS. For example, PST could not indicate leakage on valve in fully close position.
2. PST causes higher risk of spurious valve closure (Mostia_Jr., 2003). Although spurious trip is considered as a safe failure mode, it can cause water hammer effect, which will potentially damage the associated flowlines and adjacent equipment (Langeron, et al., 2007, cited in (Lundteigen & Rausand, 2007)).
3. Frequent execution of PST will increase wear on the valve components, which induces valve leakage (Lundteigen & Rausand, 2007).

6.3 The Implementation of STPA

6.3.1 Methodology

As discussed in section 5.2.1, STPA is a hazard analysis that is based systemic accident model. STPA basically has two main steps: (1) identification of unsafe control actions that can bring hazards to the system and (2) identification of scenarios that could lead to unsafe control actions (Leveson, 2011b). However, these steps can be divided into five smaller steps as given below:

1. **Define the hierarchical control structure of the analyzed system**
   The development of the control structure requires the determination of the system's boundaries, the hierarchical levels existed in the system, and the information exchanges between adjacent hierarchical levels.
2. **Identify the relevant hazards that may threaten the system and cause severe impact**

For instance, in chemical processing plant, one of the major hazards is the release of explosive and flammable process fluid from its containment.

3. **Determine the safety constraint, which reflect the limitation of safe and unsafe operation**
   For example, in chemical processing plant, the safety constraints can be the operating parameters (e.g. pressure, temperature, flow velocity, vibration) and organizational parameters (e.g. limit value of process safety performance indicators).

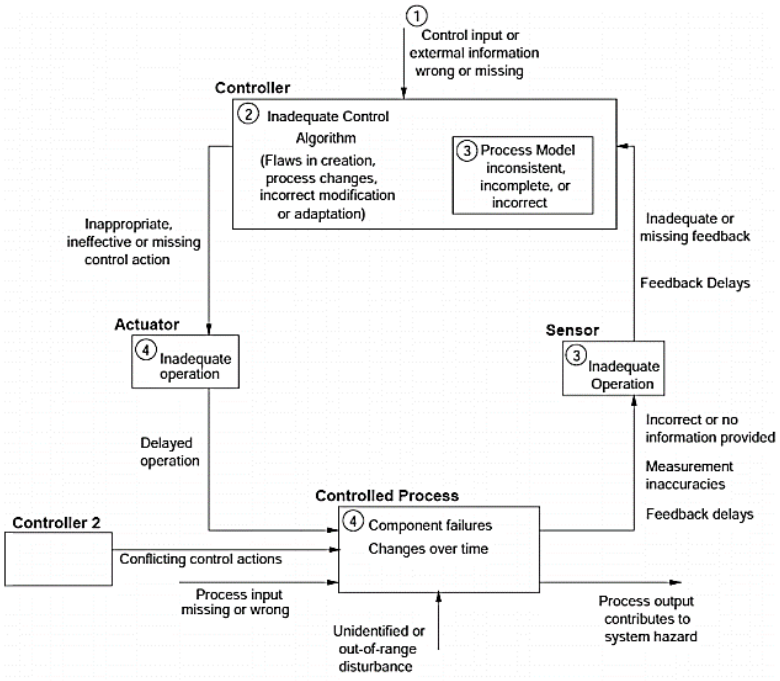

Figure 6.4 Causal factor loop used in the unsafe control actions scenarios identification (Leveson, 2011b)

4. **Determine the unsafe control actions that may lead to the identified hazards and subsequently, identify the causes of the unsafe control actions**
   Causal factor loop (Figure 6.4) can be used as the reference for revealing the causes underlying unsafe control actions.
5. **Identify the risk controls or risk reducing measures to control the hazards**
   Based on the identified causes of unsafe control actions, risk control of risk reducing measures are determined, if necessary, to enforce the safety constraints.

These steps will be elaborated in detail in the following sections.

6.3.2 Case study scope and limitations

The scope and limitations of the case study are given as follow:

- The case study will only be limited to the implementation of STPA in the execution PST in HIPPS module.

- The probability for each identified failure scenarios will not be assigned. All of the scenarios are assumed as credible.

6.3.3 Step-by-Step Work

6.3.3.1 Construction of hierarchical control structure

STPA is started with determining the system to be analyzed. The system is then modelled as a hierarchical control structure with control loops between each of the components. Figure 6.5 presents the hierarchical control structure of the entire system.

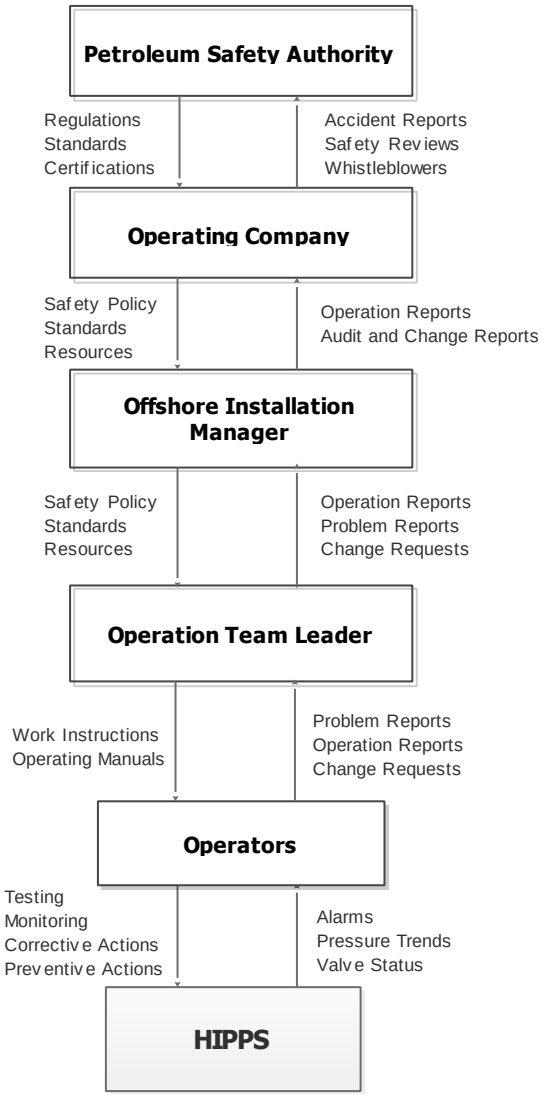

Figure 6.5 Hierarchical control structure for the HIPPS module

The downward arrow is the safety constraint imposed by the upper hierarchical level to the level beneath it while the upward arrow is the feedback given by the lower hierarchical level to its controller. For instance, operator imposes control to HIPPS by carrying out testing to ensure its

ability to function on demand. HIPPS then gives feedback regarding the test results in form of alarms and valve status.

While Figure 6.5 shows the entire system hierarchical control structure, Figure 6.6 is the magnification of Figure 6.5, which presents the hierarchical control structure during the execution of PST. The operator and MCS act as the controller of the activity, which is the PST. The HCM play two roles in this structure: as the actuator and the sensor. The SDV is the component to be controlled and monitored during the PST.

The operator performs the PST by sending the command through MCS. MCS continues the command by sending the signal to HCM. Subsequently, HCM sends signals to deactivate the solenoid valve, causing the SDV to gradually close. Before the SDV is fully closed, HCM reactivate the solenoid valve and the SDV is re-opened again. The SDV gives feedback regarding its status (open/close) by sending signal through HCM and MCS until it is finally shown in MCS display to be shown to the operator.

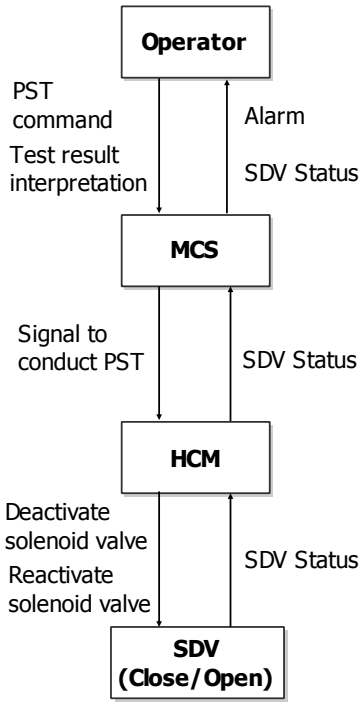

Figure 6.6 Hierarchical control in the execution of PST

6.3.3.2 Identification of system hazard and safety constraint

In STPA, hazard is defined as a set of conditions that together with the presence of set of environmental conditions will lead to major losses (An STPA Primer, 2014).

Two hazards can arise during the execution of PST:

1. The PST execution causes damage to the adjacent flowlines and equipment.
2. PST fails to reveal the failure modes existed in HIPPS

The former is related to the unexpected closure of SDV during PST. Because PST is executed during normal operation, instantaneous closure of SDV will induce water hammer effect that will impact proximate flowlines and equipment. Meanwhile, the latter can happen if the test result does not reflect the actual condition of the SDV. For instance, the SDV is judged as "operating as intended" while in reality the SDV fails during the test. Hence, the failure mode as well as it causes will still be hidden and unknown. Based on these arguments, two safety constraints are defined:

1. SDV shall only be partially closed during partial stroke test.
2. The test result must reflect the actual condition of HIPPS.

This can be summarized as presented in Table 6.1.

Table 6.1 Identified hazards and their associated safety constraints

Hazard	Associated Safety Constraint
Damage of associated flowlines and adjacent equipment	SDV shall only be partially closed during partial stroke test
Failure in revealing the existing failure mode	The test result must reflect the actual condition of HIPPS

6.3.3.3 Identification of unsafe control actions

The next step is the assessment of system safety control by identifying the potential unsafe control actions that might lead to violation of safety constraints and subsequent hazardous conditions. Leveson (2011b) mentions four generic forms of unsafe control as follow:

1. The control action necessary for achieving safety is not provided or followed.
2. The control action is provided, but creates hazardous circumstances.
3. The control action is provided, but not in the right sequence and timing (too early or too late).
4. The control actions is applied too long, or stopped too early.

Based on the identified hazards and safety constraints in the previous section, two control actions are identified: (1) closing of SDV and (2) approval of the test result. Both of them can potentially bring hazardous situation to the considered system.

The first control action, "closing of SDV" is provided after the PST initiation signal from MCS is sent. The safe control action is provided if the SDV closes partially and reverts to its initial position before it is entirely closed. The second control action, "approval of the test result" can be understood as the verdict regarding the test results (either "accepted" or "not accepted"). In this case study, the ruling about the test result is simplified: accept the test result if the SDV is successfully closed and reject it if the SDV fails to close during PS execution. The summary of the identified unsafe control actions are presented in Table 6.2.

Table 6.2 Identified unsafe control actions

Control Action	Not providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long
Closing of SDV	**CA-1**: SDV is not closed during PST **[Not hazardous]**	**CA-2**: SDV is closed, but cannot revert back to the open position, i.e. SDV is fully closed **[Hazardous]**	Not applicable	Not applicable
Approval of the test result	**CA-3:** The testing result is not approved as acceptable when it is actually acceptable **[Not hazardous]**	**CA-4:** The testing result is approved as acceptable when it is actually not **[Hazardous]**	Not applicable	Not applicable

The explanation for each control action in Table 6.2 is provided below:

- **CA-1**: This control action can be simply referred as "fail-to-close" and is considered as non-hazardous given its occurrence during PST. This statement is made under the assumption that corrective action will be performed immediately after the failure is discovered. Different consideration will obviously be given if this unsafe control action occur in the event of overpressure during normal operation.
- **CA-2**: The control action "closing of SDV" brings hazard if the initiation of PST causes the SDV to be fully closed without being able to revert back to the open condition. During PST, the SDV is supposed to close partially and re-open before the valve reach fully closed state. As stated in section 6.3.3.2, full closure of the valve can potentially damage the adjacent flowlines and equipment.
- **CA-3:** This control action will not possess any hazard event though misinterpretation of test result is made. The assumption is that the decision to reject the test result will drive the operator find the underlying problem.
- **CA-4:** This control action is clearly hazardous as the operator presumes that the SDV is in acceptable condition to operate while in actuality it is fail-to-close. There will be no measures to fix the failure and thus the failure remains hidden.
- The third and the fourth unsafe control action are considered as irrelevant for this case study.

6.3.3.4 Determination of the unsafe control actions scenarios and identification of risk control

This step is basically identifying the scenarios that can lead to the unsafe control actions identified in the previous section. Figure 6.4 is used as the reference to identify the scenarios. The identification of causal scenarios requires the inclusion of process models for each component in

the control structure diagram. The control structure diagram and process model for each of the controller are shown in Figure 6.7.

In this case, two unsafe control actions are identified and analyzed: “SDV is fully closed” and “the testing result is judged as acceptable when it is actually not”. Their results are shown graphically in Figure 6.8 and Figure 6.9.

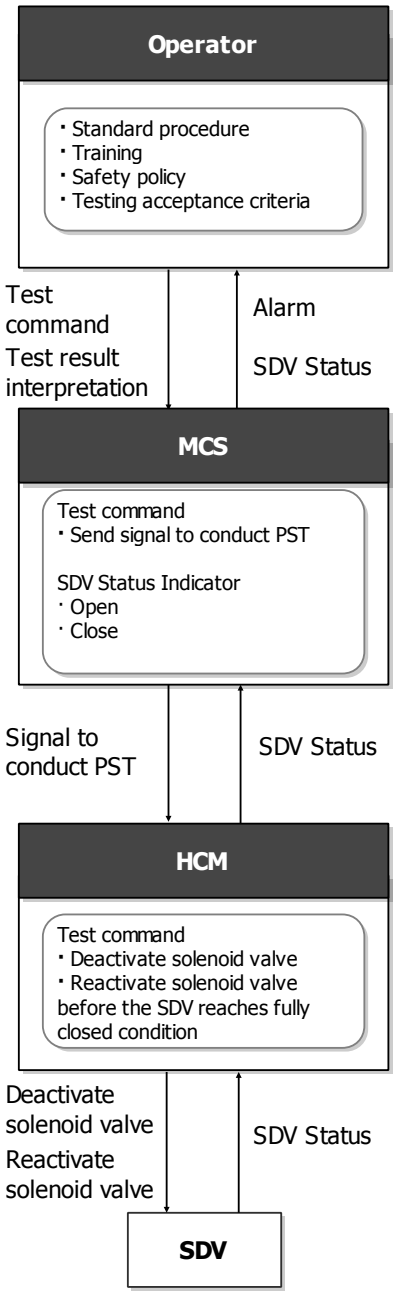

Figure 6.7 The control structure and process model in PST

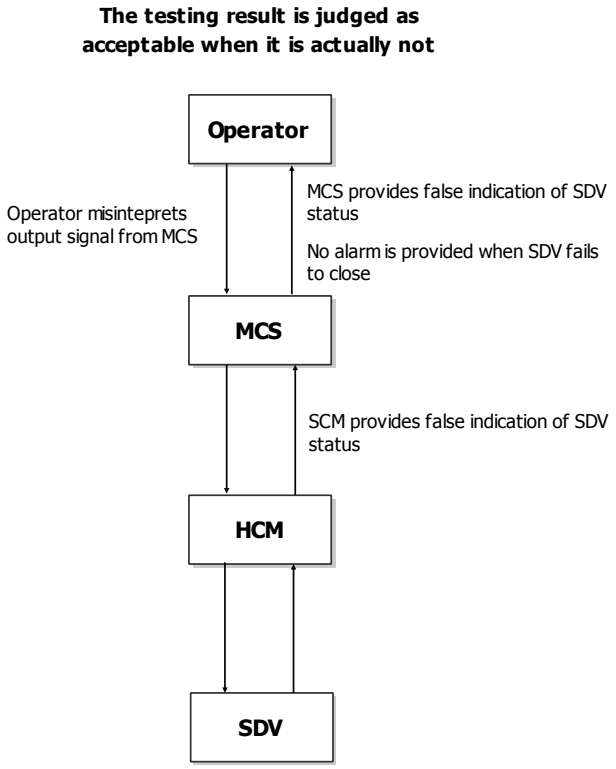

Figure 6.8 Scenarios for "The testing result is judged as acceptable when it is actually not"

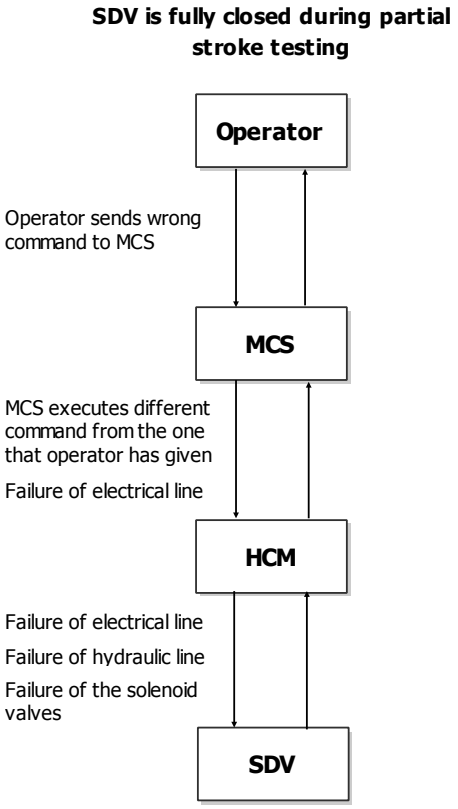

Figure 6.9 Scenarios for "SDV is fully closed during partial stroke testing"

These results can be still refined until appropriate measures and/or mitigations can be identified and designed (An STPA Primer, 2014). The identified scenarios, causal factors, as well as the allocated measures/mitigations are summarized in Table 6.3. Failure of electrical line, failure of hydraulic line, and failure of solenoid valve are scenarios that do not specifically happen during the execution of PST. They could happen during the normal operation and normally due to inadequate design. Therefore, they are not included in the assessment.

Table 6.3 Refinement of scenarios identified for unsafe control action "The testing result is judged as acceptable when it is actually not"

Unsafe Control Action: The testing result is judged as acceptable when it is actually not		
Scenario	**Associated Causal Factors**	**Measures/Mitigations**
Operator misinterprets output signal from MCS	Operator lack of knowledge and incompetency	Providing training for the operator and carrying out examination after the completion of the training
	Poorly designed human-machine interface, causing confusion of the operator in interpreting data	Carrying out testing and design evaluation after the completion of the design phase by involving the operators
MCS provides false indication of SDV status	The algorithm and requirements are not implemented correctly in the software	• Conducting routine functional test for the MCS • Installing diagnostic tool as part of the MCS
	Hardware/software issues (e.g. bugs, viruses, etc.)	
No alarm is provided by MCS when SDV fails to close	Incorrect alarm trip point setting	Conducting routine functional test for the alarm system
	Failed alarm connection	
	Failed alarm system	
HCM provides false indication of SDV status	The algorithm and requirement are not implemented correctly in the software	• Conducting routine functional test for the HCM • Installing diagnostic tool as part of the HCM
	Hardware/software issues (e.g. bugs, viruses, etc.)	

Table 6.4 Refinement of scenarios identified for unsafe control action "SDV is fully closed during partial stroke testing"

Unsafe Control Action: SDV is fully closed during partial stroke testing		
Scenario	**Associated Causal Factors**	**Required Measures/Mitigation**
Operator sends wrong PST command to MCS	Operator lack of knowledge and incompetency	Providing training for the operator and carrying out examination after the completion of the training
	Defective test procedure (e.g. inaccurate and highly complex procedure)	Conducting usability test for the procedure
	Poorly designed human-machine interface	Carrying out testing and design evaluation after the completion of the design phase by involving the potential users, i.e. the operators
MCS executes different command from the one that operator has given	The algorithm and requirement for execution of PST are not implemented correctly in the software	• Conducting routine functional test for the MCS • Installing diagnostic tool as part of the MCS
	Hardware and/or software issues (e.g. bugs, viruses, etc.)	

6.4 Identification of Leading Indicators

In this case study, the identification of leading indicators by using the approach given by HSE UK (2006) will be demonstrated. The six main steps to identify leading indicators suggested by HSE UK are given as follow:

1. **Set up a team** - the first step is related to the establishment of a group of people that will contribute to the development leading indicators.
2. **Determine the scope and carry out hazard analysis** - the second step is mainly about setting the scope to determine for which part or hierarchical level of the system the indicators will be applied. Subsequently, hazard analysis is carried out to identify the hazards and their corresponding scenarios in the considered system parts/levels.
3. **Identify risk control to prevent the identified hazards to develop into major accidents** - the prevention and mitigation actions, i.e. risk control system, for each of the identified hazards and hazard scenarios are identified. HSE UK does not specifically suggest the hazard analysis to be used in this step. The desired safety outcome is defined to express the outcome expectation of the risk control system.
4. **Identify the leading indicators based on the risk control** - The fourth step is the identification of the leading indicators based on the defined risk control.
5. **Establish data collection and reporting system** – this step is related to the definition and arrangement of how to do the measurement and collect the data and how to represent the result and make it understandable to the stakeholders.
6. **Review** - the review step is carried out to check if the actual safety performance (indicated by leading indicators) complies with the desired safety outcome (as defined in step three). Any detected deviations may indicate violation of safety constraints that can lead to bigger problems. The review results will become the basis for deciding the necessary actions to bring the performance back on track.

In this case study, only step 2, 3, and 4 are carried out. The hazard analysis and the identification of risk control (i.e. prevention and mitigation actions) have been done in the previous section by utilizing STPA. The identified leading indicators are shown in Table 6.5 and Table 6.6

Table 6.5 The identified leading indicators for unsafe control action "The testing result is judged as acceptable when it is actually not"

Unsafe Control Action: The testing result is judged as acceptable when it is actually not				
Scenario	**Associated Causal Factors**	**Measures/Mitigations**	**Desired Safety Outcomes**	**Potential Leading Indicators**
Operator misinterprets output signal from MCS	Operator lack of knowledge and incompetency	• Providing training for the operator and carrying out examination after the completion of the training	The operators shall be able to correctly interpret the signal from MCS	The percentage of operators that passes examination on the first try
	Poorly designed human-machine interface	• Carrying out testing and design evaluation after the completion of the design phase by involving the operators		The percentage of operators that believe the interface provided by MCS is ergonomists and able to provide clear information
MCS provides false indication of SDV status	The algorithm and requirements for execution of PST are not implemented correctly in the software	• Conducting routine functional test for the MCS	MCS shall be able to indicate the actual status of the SDV	• The percentage of functional tests that are conducted within the specified schedule • The percentage of functional test that are conducted in accordance with the test specification • The percentage of corrective actions to rectify problems with MCS that are in accordance with the specification
	Hardware/software issues (e.g. bugs, viruses, etc.)	• Installing diagnostic tool as part of the MCS		• The percentage of diagnostic program that is run within the specified schedule • The percentage of hardware/software issues that are solved in accordance with the specification
No alarm is provided by MCS when SDV fails to close	Incorrect alarm trip point setting	• Conducting routine functional test for the alarm system	Alarm shall be able to activate correctly when SDV fails to close	• The percentage of functional test that are conducted within the specified schedule • The percentage of functional test that are conducted in accordance with the test specification • The percentage of corrective actions to rectify problems with alarms that are in accordance with the specification
	Failed alarm connection			
	Failed alarm system			

HCM provides false indication of SDV status	The algorithm and requirement are not implemented correctly in the software	• Conducting routine functional test for the HCM	HCM provides the actual status of the SDV	• The percentage of functional tests that are conducted within the specified schedule • The percentage of functional test that are conducted in accordance with the test specification • The percentage of corrective actions that are in accordance with the specification
	Hardware/software issues (e.g. bugs, viruses, etc.)	• Installing diagnostic tool as part of the HCM		• The percentage of diagnostic program that is run within the specified schedule • The percentage of hardware/software issues that are solved in accordance with the specification

Table 6.6 Identified leading indicators for unsafe control action "SDV is fully closed during partial stroke testing"

Unsafe Control Action: SDV is fully closed during partial stroke testing				
Scenario	**Associated Causal Factors**	**Required Measures/Mitigation**	**Desired Safety Outcome**	**Potential Leading Indicator**
Operator sends wrong PST command to MCS	Operator lack of knowledge and incompetency	• Providing training for the operator and carrying out examination after the completion of the training	The operators shall be able to send the right PST command to MCS	The percentage of operators that passes examination on the first try
	Defective test procedure (e.g. inaccurate and highly complex procedure)	• Conducting usability test for the procedure		The percentage of operators that believe the test procedure has been clearly written and easy to understand
	Poorly designed human-machine interface	• Carrying out testing and design evaluation after the completion of the design phase by involving the operators		The percentage of operators that believe the interface provided by MCS is ergonomists and able to provide clear information
MCS executes different command from the one that operator has given	The algorithm and requirement for execution of PST are not implemented correctly in the software	• Conducting routine functional test for the MCS	MCS shall execute the command as per operator instruction	• The percentage of functional tests that are conducted within the specified schedule • The percentage of functional test that are conducted in accordance with the test specification

				• The percentage of corrective actions to rectify problems with MCS that are in accordance with the specification
	Hardware and/or software issues (e.g. bugs, viruses, etc.)	• Installing diagnostic tool as part of the MCS		• The percentage of diagnostic program that is run within the specified schedule • The percentage of hardware/software issues that are solved in accordance with the specification

6.5 Discussion

6.5.1 On the utilization of STPA

STPA can be considered as the extension of the conventional hazard analyses. The results shown in Table 6.3 and Table 6.4 prove that STPA is not only able to identify the scenarios related to HIPPS component failures, but also other aspects, such as poorly designed human-machine interface, defective test procedure, and operator incompetency and lack knowledge, which are possibly rooted from management and organizational factors. Moreover, in the study case, the utilization of hierarchical control structure in STPA helps in acknowledging the interactions between components in the system (e.g. operators, MCS, HCM, and SDV) as well as identifying the hazards that develop because of those interactions.

The case study only considers the operator as the highest hierarchical level (see Figure 6.5). The analysis can be extended by including several higher hierarchical levels (e.g. Petroleum Safety Authority and company management) or even the entire system as shown in Figure 6.6. The addition of more hierarchical levels will be beneficial as more scenarios can be generated, including those which are related to the regulatory agencies and management. However, covering the entire system in STPA will be very demanding as it requires enormous efforts and time. In addition, it will require the participation of representatives from each of the hierarchical level to provide the complete knowledge regarding the system. An operator knows in detail about the operation and very technical matter, but the management only knows about planning, staffing, and other management related stuffs. Hence, the combination of their knowledge is important to cover the entire picture of the system.

However, despite the advantages that are offered by STPA, it still has weaknesses. Similar with the other hazard analysis techniques, STPA is carried out by humans and humans have limitations in knowledge and information processing capacity. The quality analysis will considerably depend on the knowledge and experience of the assessors about the considered system. The persons who will involve in the STPA process should have the complete knowledge of system, covering technical level to the management level.

In addition, the STPA methodology have not been clearly defined and still in development process. The methodology provided by Leveson (2011a) is very general, allowing the STPA practitioners to do improvisation by themselves. Consequently, there is a possibility that the purpose of the analysis is not achieved because of improper STPA practices due to lack of guidance in implementation.

STPA is suitable to be implemented in complex socio-technical systems, but would be unnecessary for relatively simple systems. In a system where the interaction between components is low, traditional hazard analysis techniques might be sufficient.

6.5.2 On the utilization of leading indicators

As stated in section 5.2.2 HSE UK (2006) uses hazard analysis as the basis to identify leading indicators, but put more emphasis on the identification of leading indicators based on the defined risk control or risk reducing measure to control the identified hazards. The defined risk control or

risk reducing measure can be considered as the defense owned by the system to encounter threatening hazards. As stated in section 4.5.3, the system's layers of defense are gradually degraded because of various factors, such as management tendency to prioritize profit gain over safety. The HSE UK approach to assign leading indicators based on risk control or risk reducing measure can be beneficial as a mean to monitor the degradation of defense occurred during the operation phase, thus preventive and corrective actions can be taken immediately once the risk control or risk reducing measure is ineffective anymore in controlling the hazards.

For instance, as shown in Table 6.5, training and examination are provided as the measure to prevent operator lack of knowledge and incompetency. However, the training might become inadequate or ineffective because of various factors, such as the decision of the management to cut the training budget or the reduction of the training duration to save time. By assigning "the percentage of operators that passes examination on the first try" as the leading indicator, the effectiveness and adequacy of the training will be known. A large number of failures during the examination might indicate something wrong with the adequacy of the training. In other words, the leading indicators can also act as early warning signs.

For this purpose, a constraint must be assigned. For example, if the percentage of the operators who pass the examination on the first try is below 60%, the training package must be reviewed and reassessed. The leading indicator will allow the immediate actions to prevent further deterioration of layer of defense and enforce it. The tricky part in the implementation of the leading indicator is the determination of the constraint value. There must be a justification why the 60% value is selected. There are two possibilities that can happen if inappropriate value of constraint (e.g. too high or too low) are set: (1) it might be too late to carry out actions and accident might already happen and (2) too many unnecessary review and reassessment are conducted, making the implementation of leading indicator to be costly. However, HSE UK, API, and CCPS do not address this issue in their guidelines. There shall be a systematic methodology to determine the leading indicator value constraint, thus appropriate actions can be conducted in timely and cost-optimal manner.

7 Conclusions and Recommendation for Further Research

7.1 Conclusions

The main objective of this thesis is to map the patterns underlying unforeseen failures and propose, based on patterns finding and literature review, prospective methods to encounter the future occurrence of unforeseen failures. The following sections will briefly summarize the result of the thesis.

7.1.1 Unforeseen Failure Patterns

There are four shared characteristics found in all of the unforeseen failure cases, which can be considered as the common patterns underlying unforeseen failure as shown below:

- Unforeseen failures are developed from the dysfunctional interactions between regulatory agencies, company's management, operators, physical equipment, etc., and the involvement of indirect factors (e.g. unsafe decisions and actions by the management and regulator, and organizational factors), which are virtually impossible to be completely captured by merely linear sequence of events.
- Unforeseen failures are not only caused by technical failures or human errors. Regulatory agencies, corporate board, and company management also have significant contribution in their occurrence. Their failure to impose adequate safety control to the hierarchical level beneath them is one of the factors that lead to the occurrence of unforeseen failure.
- The conflict between financial and safety objectives is deemed as one of the causes of unforeseen failure. The companies' decisions and actions tend to lean towards the fulfillment of financial goals without assessing their impact towards the safety of the system, thus making them unaware about the harmful effect of their decisions and actions to the safety of the system,
- Early warning signs were existed prior to failure, but no action was taken by the companies to respond to them. The warning signs might be considered as non-threatening to the system or had ambiguous characteristic, thus repelled the management desire to take meaningful actions.

7.1.2 Suggested Approach to Prevent the Future Occurrence of Unforeseen Failure

Unforeseen failures were happened not simply because of failure of technological components or individuals. The occurrence of unforeseen failure develops from the complex interactions between components and involves risky decisions and actions by the management and regulator and organizational factors. These aspects cannot be well captured by the conventional hazard analysis techniques, which are still constructed based on sequential accident model. Hazard analysis founded on systemic accident causation model should be used to consider the aspects that are

omitted by the traditional hazard analysis techniques. One of the suggested approach is to use STPA, a hazard analysis technique that are based on STAMP, a systemic accident causation model.

In addition, a socio-technical system is highly dynamic and complex entity that constantly adapts with its surrounding environment. The adaptation mechanism emerges in the form of decisions and actions taken by the management to respond to highly aggressive and competitive environment. The danger arises when these decisions and actions bring the entire system to state of higher risk. The system will migrate towards the safety boundary and eventually violate it without the actors inside the system realizing it. The failure will be unforeseen for most the personnel inside the system. Adopting proactive risk management by implementing leading indicators is suggested as an approach to notify decision-makers regarding the state of the system, thus early actions can be carried out to prevent further system safety degradation that can lead to system failure. Moreover, implementation of leading indicators will also be beneficial as a systematic collection of early warnings and to enable recognizing of important early failure warning

7.2 Recommendation for Further Work

This thesis is far from complete and requires further work in the future. Some points are identified that can be the improvement of this thesis and the foundation of the further study in the future as follow:

- **Adding more historical cases and cases from other industries**
  Due to time and resource constraint, only four case studies are selected in this thesis. More case studies should be selected in the future to clarify if the underlying patterns found in this thesis can be applied to the other unforeseen failure cases. Moreover, adding more cases might potentially lead to identification of additional patterns that enhances understanding about how the unforeseen failure happens.
- **Exploring cases from other industries**
  The unforeseen failure cases selected in this thesis is limited only to the industries where the loss of containment is the major hazard. Exploring historical cases from other industries should be done in the future to if there is a difference of unforeseen failure characteristic between them. Aviation industry can be a good example as there are still a number of plane crashes occurring in the recent years despite rapid advancement in the aviation technology.

8 References

Adesanya, A. O., 2014. *Master Thesis: Strengths and Weaknesses of Anticipatory Failure Determination in Identifying Black Swan Type of Events,* Stavanger: University of Stavanger.

Alvarenga, M. & Melo, P. F. e., 2015. Including severe accidents in the design basis of nuclear power plants: An organizational factors perspective after the Fukushima accident. *Annals of Nuclear Energy,* Volume 79, pp. 68-77.

An STPA Primer, V. 1., 2014. [Online]
Available at: http://sunnyday.mit.edu/STPA-Primer-v0.pdf
[Accessed 6 March 2015].

Anon., 2011. *SeekerBlog.* [Online]
Available at: http://seekerblog.com/2011/04/17/fukushima-earthquake-tsunami-impacts/
[Accessed 27 April 2015].

API, 2010. *ANSI/API Recommended Practice 754 - Process Safety Performance Indicators for the Refining and Petrochemical Industries.* 1st ed. Washington D.C.: American Petroleum Institute.

Atsuji, S. et al., 2011. Systems Pathology of Social Organizations: Fukushima Nuclear Catastrophe 3.11. *Information Research,* Volume 35, pp. 1-15.

Aven, T., 2008. *Risk Analysis - Assessing Uncertainties Beyond Expected Values and Probabilities.* 1st ed. Chichester; Hoboken: John Wiley & Sons Ltd..

Aven, T., 2013a. On the meaning of a black swan in a risk context. *Safety Science,* Volume 57, pp. 44-51.

Aven, T., 2013b. Practical implications of the new risk perspectives. *Reliability Engineering and System Safety,* Volume 115, pp. 136-145.

Aven, T., 2014. *Risk, Surprises and Black Swans.* 1st ed. Abingdon: Routledge.

Aven, T., 2015. Comments to the short communication by Jan Erik Vinnem and Stein Haugen titled “Perspectives on risk and the unforeseen”. *Reliability Engineering & System Safety,* Volume 137, pp. 69-75.

Aven, T. & Krohn, B. S., 2014. A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering and System Safety,* Volume 121, pp. 1-10.

Baker, J. A. et al., 2007. *The Report of the BP U.S. Refineries Independent Safety Review Panel,* s.l.: BP U.S. Refineries Independent Safety Review Panel.

Bertalanffy, L. v., 1968. *General System Theory.* Edmonton: George Braziller.

Bowonder, B., 1987. The Bhopal Accident. *Technological Forecasting and Social Change,* Volume 32, pp. 169-182.

Bowonder, B. & Linstone, H., 1987. Notes on the Bhopal Accident: Risk Analysis and Multiple Perspectives. *Technological Forecasting and Social Change,* Volume 32, pp. 183-202.

CCPS, 2010. *Guidelines for process safety metrics.* 1st ed. Hoboken: Wiley Center for Chemical Process Safety.

CCPS, 2011. *Process Safety Leading and Lagging Metrics.* New York: American Institute of Chemical Engineers.

Cedergren, A. & Petersen, K., 2011. Prerequisites for learning from accident investigations – A cross-country comparison of national accident investigation boards. *Safety Science,* Volume 49, pp. 1238-1245.

Checkland, P., 1999. *Systems Thinking, Systems Practice: Includes a 30-year of retrospective.* 1st ed. Chichester: John Wiley and Sons Ltd.

Chouhan, T., 2005. The unfolding of Bhopal disaster. *Journal of Loss Prevention in the Process Industries,* Volume 18, pp. 205-208.

CSB, 2007. *Investigation Report: BP Texas City Refinery Explosion and Fire,* Texas: U.S. Chemical Safety and Hazard Investigation Board.

CSB, 2010a. *Investigation Report Overview: Explosion and Fire at the Macondo Well,* Washington, DC: US Chemical Safety and Hazard Investigation Board.

CSB, 2010b. *Investigation Report Volume 2: Explosion and Fire at the Macondo Well,* Washington, D.C.: U.S. Chemical Safety and Hazard Investigation Board.

Deepwater Horizon Study Group, 2011. *Final Report on the Investigation of the Macondo Well Blowout,* Berkeley: Deepwater Horizon Study Group.

Dekker, S., 2011. *Drift into Failure: From Hunting Broken Components to Understanding Complex Systems.* 1st ed. Farnham: Ashgate Publishing Ltd..

Deming, W., 1986. *Out of the Crisis.* 1st ed. Cambridge: Massachusetts Institute of Technology, Center for Advanced Engineering Study.

Deming, W., 2000. *The new economics.* 1st ed. Cambridge: MIT CAES.

Dokas, I. M., Feehan, J. & Imran, S., 2013. EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. *Safety Science,* Volume 58, pp. 11-26.

Eckerman, I., 2005. The Bhopal gas leak: Analyses of causes and consequences by three different models. *Journal of Loss Prevention in the Process Industries,* Volume 18, pp. 213-217.

England, J., Agarwal, J. & Blockley, D., 2008. The vulnerability of structures to unforeseen events. *Computers & Structures,* 86(10), pp. 1042-1051.

ESReDA, 2009. *Guidelines for Safety Investigations of Accidents.* 1st ed. Oslo: ESReDA (European Safety Reliability and Data Association).

Feduzi, A. & Runde, J., 2014. Uncovering unknown unknowns: Toward a Baconian approach to management decision-making. *Organizational Behavior and Human Decision Process,* Volume 124, pp. 268-283.

Frafjord, P., Corneliussen, S. & Adriaansen, L., 1995. *The development of subsea High Integrity Pipeline Protection System (HIPPS).* Houston: Offshore Technology Conference.

Gall, G., Turner, P. & Seaton, R., 2002. *Reliability of Subsea Control Systems: HIPPS a case Study.* Paris, Society of Underwater Technology.

Graham, J. D., 2004. *The Heritage Foundation.* [Online]
Available at: http://www.heritage.org/Research/Lecture/The-Perils-of-the-Precautionary-Principle-Lessons-from-the-American-and-European-Experience
[Accessed 5 May 2015].

Gross, M., 2010. *Ignorance and Surprise - Science, Society, and Ecological Design.* 1st ed. Massachusetts: The MIT Press.

Haugen, S. & Vinnem, J. E., 2015. Perspectives on risk and the unforeseen. *Reliability Engineering & System Safety,* Volume 137, pp. 1-5.

Herrera, I. A., 2012. *Proactive safety performance indicators: Resilience engineering perspective on safety management,* Trondheim: Norwegian University of Science and Technology.

Hole, K. J., 2013. Management of Hidden Risks. *Computer,* 46(1), pp. 65-70.

Hollnagel, E., 2004. *Barriers and Accident Prevention.* 1st ed. Aldershot : Ashgate.

Hollnagel, E., 2008. Safety management, looking back or looking forward. In: E. Hollnagel, C. Nemeth & S. Dekker, eds. *Resilient Engineering Perspectives, vol. 1, Remaining Sensitive to the Possibility of Failure.* Aldershot: Ashgate.

Hollnagel, E., 2012. *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems.* 1st ed. Farnham: Ashgate Publishing Ltd..

Hopkins, A., 2011. Management Walk-arounds: Lessons from the Gulf of Mexico Oil Well Blowout. *Safety Science,* Volume 49, pp. 1421-1425.

HSE UK, 1997. *Successful health and safety management.* 1st ed. London: Health and Safety Executive.

HSE UK, 2006. *Developing Process Safety Indicators - A step-by-step guide for chemical and major hazard industries.* 1st ed. Richmond: UK Health and Safety Executive.

Joseph, G., Kaszniak, M. & Long, L., 2005. Lessons after Bhopal. *Journal of Loss Prevention in the Process Industries,* Volume 18, pp. 537-548.

Kaufmann, D. & Penciakova, V., 2011. *Brookings.* [Online]
Available at: http://www.brookings.edu/research/opinions/2011/04/01-nuclear-meltdown-kaufmann
[Accessed 9 March 2015].

Khawaji, I. A., 2012. *Developing System-Based Leading Indicators for Proactive Risk Management in the Chemical Processing Industry,* Massachusetts: Massachusetts Institute of Technology.

Kletz, T., 2001. *Learning from Accidents.* 3rd ed. Oxford: Gulf Professional Publishing.

Körvers, P. & Sonnemans, P., 2008. Accidents: A discrepancy between indicators and facts!. *Safety Science,* Volume 46, pp. 1067-1077.

Langeron, Y., Barros, A., Grall, A. & Berenguer, C., 2007. Safe failures impact on safety instumented systems. In: T. Aven & J. Vinnem, eds. *Risk, reliability, and societal safety: proceedings of the European Safety and Reliability Conference 2007 (ESREL 2007), Stavanger, Norway, 25-27 June 2007 : Vol. 2 : Thematic topics.* London: Taylor & Francis, pp. 641-648.

Lekka, C., 2011. *High reliability organisations: A review of the literature,* Buxton: UK Health and Safety Executive.

Leveson, N., 1995. *Safeware: System Safety and Computers.* 1st ed. Reading: Addison-Wesley.

Leveson, N., 2004. A new accident model for engineering safer system. *Safety Science,* Volume 42, pp. 237-270.

Leveson, N., 2011a. Applying systems thinking to analyze and learn from events. *Safety Science,* Volume 49, pp. 55-64.

Leveson, N., 2011b. *Engineering a Safer World.* 1st ed. Cambridge: MIT Press.

Leveson, N., 2015. A systems approach to risk management through leading safety indicators. *Reliability Engineering and System Safety,* Volume 136, pp. 17-34.

Leveson, N., Dulac, N., Marais, K. & Carroll, J., 2009. Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems. *Organization Studies,* 30(2-3), pp. 227-249.

Leveson, N. & Stephanopoulos, G., 2014. A System-Theoretic, Control-Inspired View and Approach to Process Safety. *Journal of American Institute of Chemical Engineers,* 60(1), pp. 2-14.

Lewis, C., 1929. *Mind and the world order: outline of a theory of knowledge.* 1st ed. New York: Dover Publications.

Lundteigen, M. A. & Rausand, M., 2007. *The effect of partial stroke testing on the reliability of safety valves.* Stavanger, European Safety and Reliability Conference 2007.

Lundteigen, M. & Rausand, M., 2008. Partial stroke testing of process shutdown valves: How to determine the test coverage. *Journal of Loss Prevention in the Process Industries,* 21(6), pp. 579-588.

Marchant, G. E., 2003. From General Policy to Legal Rule: Aspirations and Limitations of the Precautionary Principle. *Ethics and Environmental Health,* 111(14), pp. 1799-1803.

Mostia_Jr., B., 2003. Partial stroke testing simple or not?. *Control (Chicago, Ill),* 16(11), pp. 63-69.

Nafday, A. M., 2009. Strategies for Managing the Consequences of Black Swan Events. *Leadership and Management in Engineering,* 9(4), pp. 191-197.

NAIIC, 2012. *The Official Report of The Fukushima Nuclear Accident Independent Investigation Commission,* s.l.: The National Diet of Japan.

NASA, 2008. *System Failure Case Studies: Refinery Ablaze - 15 Dead.* s.l.:NASA.

NASA, 2011. *NASA Accident Precursor Analysis Handbook.* 1st ed. Washington, D.C.: National Aeronautics and Space Administration.

Neill, K. A. & Morris, J. C., 2012. A Tangled Web of Principals and Agents: Examining the Deepwater Horizon Oil Spill through a Principal-Agent Lens. *Politics and Policy,* 40(4), pp. 629-656.

Norazahar, N., Khan, F., Veitch, B. & MacKinnon, S., 2014. Human and organizational factors assessment of the evacuation operation of BP Deepwater Horizon accident. *Safety Science,* Volume 70, pp. 41-49.

Øien, K., Utne, I. & Herrera, I., 2011. Building Safety indicators: Part 1 – Theoretical foundation. *Safety Science,* 49(2), pp. 148-161.

Onishi, N. & Belson, K., 2011. *Culture of complicity tied to stricken nuclear plant.* New York: The New York Times.

Paltrinieri, N. et al., 2013. Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool. *Journal of Loss Prevention in the Process Industries,* Volume 26, pp. 683-695.

Paltrinieri, N., Tugnoli, A. & Cozzani, V., 2015. Hazard identification for innovative LNG regasification technologies. *Reliability Engineering and System Safety,* Volume 137, pp. 18-28.

Phillips, R. & Roberts, P., 2005. *Delivering a HIPPS Safety Critical Control System.* Aberdeen, Society of Petroleum Engineers.

Qureshi, Z. H., 2007. *A Review of Accident Modelling Approaches for Complex Socio-Technical Systems.* Adelaide, 12th Autralian Workshop on Safety Related Programmable Systems.

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

Rasmussen, J. & Svedung, I., 2000. *Proactive Risk Management in a Dynamic Society.* 1st ed. Karlstad: Swedish Rescue Service Agency.

Reader, T. W. & O'Connor, P., 2014. The Deepwater Horizon explosion: non-technical skills, safety culture, and system complexity. *Journal of Risk Research,* 17(3), pp. 405-424.

Reason, J., 1997. *Managing the Risks of Organizational Accidents.* Aldershot: Ashgate .

Roberto, M. A., Bohmer, R. M. & Edmondson, A. C., 2006. Facing Ambiguous Threats. *Harvard Business Review,* November, 84(11), pp. 106-113.

Roebuck, K., 2012. *Predictive Analysis: High-impact Emerging Technology - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors.* 1st ed. s.l.:Emereo Publishing.

Saleh, J. H., Haga, R. A., Favarò, F. M. & Bakolas, E., 2014. Texas City refinery accident: Case study in breakdown of defense-in-depth and violation of the safety–diagnosability principle in design. *Engineering Failure Analysis,* Volume 36, pp. 121-133.

Seligmann, B. J., Németh, E., Hangos, K. M. & Cameron, I. T., 2012. A blended hazard identification methodology to support process diagnosis. *Journal of Loss Prevention in the Process Industries,* Volume 25, pp. 746-759.

Shrivastava, P., 1994. Technological and Organizational Roots of Industrial Crises: Lesson from Exxon Valdez and Bhopal. *Technological Forecasting and Social Change,* Volume 45, pp. 237-253.

Sonnemans, P. J. & Körvers, P. M., 2006. Accident in the chemical industry: are they foreseeable?. *Journal of Loss Prevention in the Process Industry,* Volume 19, pp. 1-12.

Størseth, F., Hauge, S. & Tinmannsvik, R. K., 2014. Safety barriers: Organizational potential and forces of psychology. *Journal of Loss Prevention in the Process Industries,* Volume 31, pp. 50-55.

Taleb, N. N., 2007. *The Black Swan - The Impact of the Highly Improbable.* 1st ed. London: Penguin.

The Bureau of Ocean Energy Management, Regulation, and Enforcement, 2011. *Report Regarding the Causes of the April 20, 2010 Macondo Well Blowout,* s.l.: U.S. Department of the Interior.

UK Ministry of Defence, 2013. *Red Teaming Guide,* Swindon: The Development, Concepts, and Doctrine Centre (DCDC).

Venkatasubramanian, V., 2011. Systemic Failure: Challanges and Opportunities in Risk Management in Complex Systems. *Journal of American Institute of Chemical Engineers,* 57(1), pp. 2-9.

Wang, Q. & Chen, X., 2011. Nuclear accident like Fukushima unlikely in the rest of the world?. *Environmental Science & Technology,* 45(23), pp. 9831-2.

Wang, Q. & Chen, X., 2012a. Regulatory failures for nuclear safety – the bad example of Japan – implication for the rest of world. *Renewable and Sustainable Energy Reviews,* 16(5), p. 2610–7.

Wang, Q. & Chen, X., 2012b. Regulatory transparency—How China can learn from Japan's nuclear regulatory failures?. *Renewable & Sustainable Energy Reviews,* 16(6), p. 3574–8.

Wang, Q., Chen, X. & Yi-chong, X., 2013. Accident like the Fukushima unlikely in a country with effective nuclear regulation: Literature review and proposed guidelines. *Renewable and Sustainable Energy Reviews* , Volume 17, pp. 126-146.

Appendix A Review of DyPASI and BLHAZID

A.1 DyPASI

DyPASI is new systematic hazard identification techniques that is emerged as the result of European Commission FP7 iNTegRisk project. It is based on bow-tie analysis and provide a continuous systematization of information from early warnings of risk related to past events, e.g. accidents, incidents, near-misses, etc. (Paltrinieri, et al., 2013). The main aim of DyPASI is to identify atypical accident scenarios in the complex industrial systems. Paltrinieri, et al. (2015) defines the term 'atypical scenario' as accident scenario that has occurred in the past and was failed to be identified by the hazard analysis, e.g. *unknown unknowns* and *unknown knowns*. DyPASI consists of these two basic steps:

1. **Development of bow-ties for the analyzed facility** - This step is basically carrying out the conventional FTA and ETA to identify the failure scenarios and the potential consequences of the failure. The results are then plotted into a bow-tie diagram.
2. **Identification of atypical scenarios** –This step is essentially about searching of all information regarding early warning signals and historical accident scenarios, and then incorporated them in the bow-tie diagram developed in the previous step (Paltrinieri, et al., 2013). The search of historical accident scenarios will not be limited only in the analyzed facility or system, but also in the other affiliated system/facility. For example, if the analyzed facility is an LNG plant, the past events can be the occurrences that happened in other LNG plants or other similar facilities related to LNG industry. In order to search and identify the historical accident scenarios, Information and Communication Technology (ICT) is used as the support tool.

The key idea of this technique is to incorporate and integrate the early warning signals preceding a major loss (e.g. incident and near-misses) and historical accident scenarios into the developed bow-tie analysis. For instance, a new oil refinery hazard analysis includes the accident scenario involved in the Texas City Refinery as one of the credible failure scenario and integrate it within the bow-tie diagram. An example of DyPASI result is shown in Figure 8.1. In the figure, the identified atypical scenarios are terrorist attack, cryogenic damages, cryogenic burns, rapid phase transition, and asphyxiation, while the rest (shown by the black line) are the scenarios identified by conventional FTA and ETA.

DyPASI extends the conventional techniques by incorporating the early warning signals and integrating failure scenarios that had happened in the past in the hazard analysis. The methodology used in DyPASI will provide a platform to learn from to failure scenarios that have occurred in the considered system/facility as well as in other related systems/facilities. It also provides a basis for systematic collection of early warning signs and enhancement of knowledge management (Paltrinieri, et al., 2013). The biggest challenge is to find the relevant and qualified information in the sea of data and information. This technique also relies heavily on the application of available knowledge and experience to identify early warning signals.

However, as DyPASI is basically the combination of FTA and ETA, it still embodies their inherent weaknesses. As stated previously in section 5.1.1, FTA and ETA are founded on the sequential accident model. The causal factors emerged from social and organization aspects, such as poor safety culture and risky decision-making will not be able to be identified by using this technique (Paltrinieri, et al., 2013). *Unknown unknown* type of events will not be able to be identified as this technique relies heavily on learning from the occurrence of historical accidents, which are clearly not *unknown unknowns*, but might be *unknown knowns*.

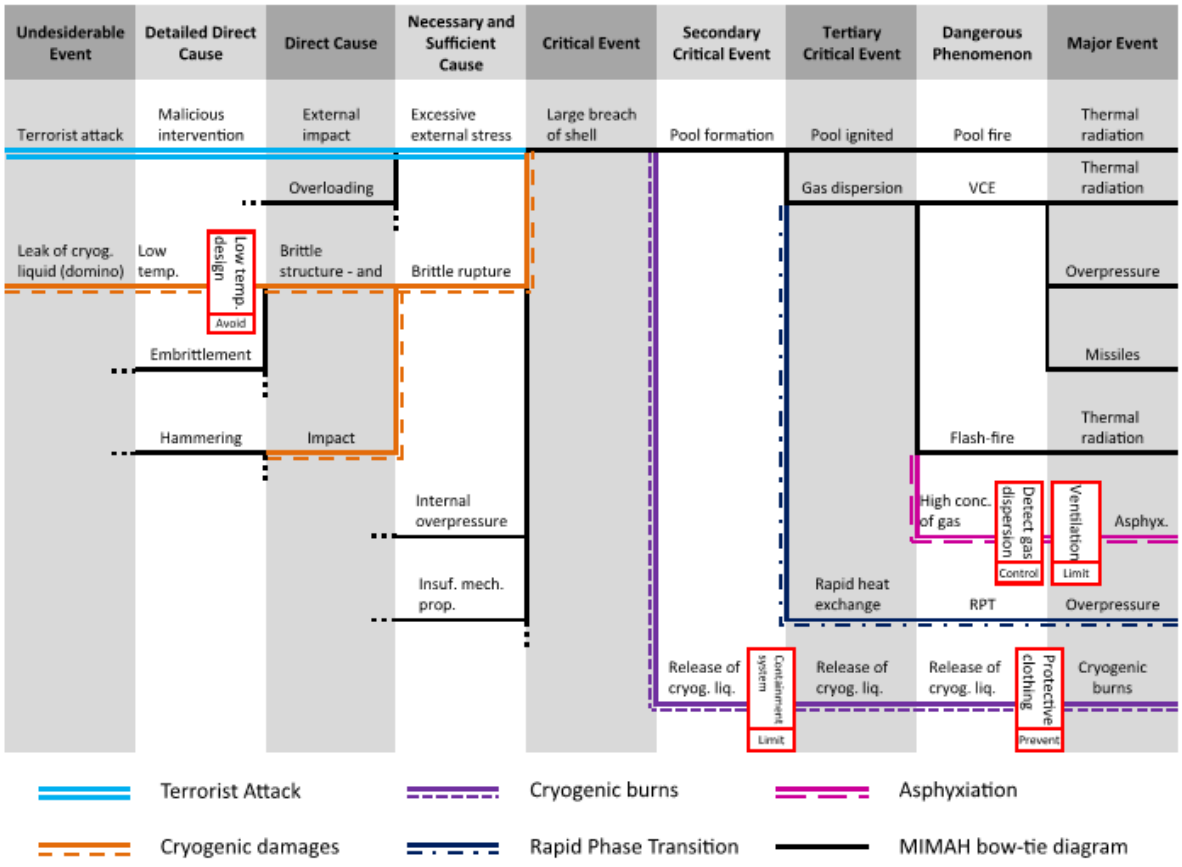

Figure 8.1 An example of bow-tie diagram integration with atypical scenarios. The typical scenarios are shown by the black lines (Paltrinieri, et al., 2015)

A.2 BLHAZID

BLHAZID is a new type of hazard identification technique that is basically the blending of two well-known hazard identification methods, which are HAZOP and FMEA (Seligmann, et al., 2012). This technique is founded on the so-called Functional Systems Framework (FSF). FSF is constructed on general system theory described by von Bertalanffy (1968). The FSF concept basically explains the connection and interrelationship between structure, function, and goal of a system. A system comprises of several components, such as physical equipment, working personnel, policies and procedures, etc. and they are linked to each other by a number of *streams*. These *streams* can be conceived as any entities that connect system components and create interdependency between

them. Some examples of *streams* are material streams during the production, signals sent between the equipment and operator, and communication between working personnel (Seligmann, et al., 2012).

Every individual components and *streams* in the system have their own capabilities and these capabilities have the capacity to impact and affect the state of the system. For example, a compressor can increase the pressure, a pump can increase the flow of the liquid, pipes allow the containment and flow of fluid, etc. If the capabilities of the components and *streams* are integrated, new capabilities that cannot be achieved by a single component or *stream* are actuated. For instance, the shell and tube heat exchanger is able to transfer heat between fluids, but heat transfer capability cannot be achieved by merely the tube or the shell itself. These capabilities can be fathomed as system's functions that can only be attained when all of the system's components working together. These functions are then used by the system to achieve the system's goals (Seligmann, et al., 2012). The illustration of FSF can be seen in Figure 8.2.

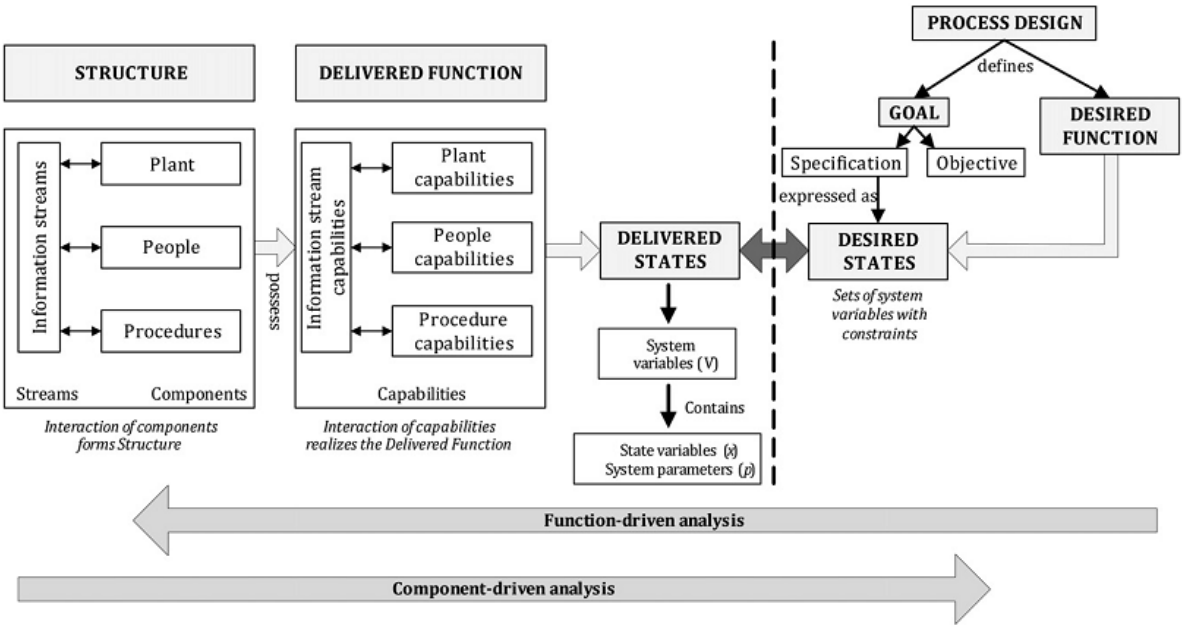

Figure 8.2 Functional Systems Framework (Seligmann, et al., 2012)

As stated previously, BLHAZID blends two different hazard identification techniques, i.e. FMEA and HAZOP. The term 'blending' should be differentiated with 'combining'. Combining two hazard analyses can mean the utilization of both techniques individually and merging their outcomes for further application. Meanwhile, blending two different techniques requires the unification of their basic elements and concepts to produce a new methodology (Seligmann, et al., 2012). Blending two different techniques has advantages of gaining the benefits of both techniques while eliminating or reducing their weaknesses. HAZOP has function-driven approach while FMEA has component-driven approach. Component-driven approach focuses on the component failures modes and causes identification (Seligmann, et al., 2012) while function-driven approach mainly

identifies the deviations that occur in the process variables, which could interrupt the functionality of the system. These variables are normally related to the process parameter, such pressure, temperature, and flow rate, or in BLHAZID is called *streams*. In other words, HAZOP does not identify component failures directly, but as the results of deviations that occur in the system, i.e. *streams* failure. Conversely, FMEA puts emphasizes on the identification of component failures. For instance, failure mode that occurs in the component, such as corrosion on the pipe, is more effective to be investigated by using FMEA since it focuses on the component failure mode and cause identification. However, the effect of the pipe leak to the entire system due to corrosion, e.g. variable deviations, is easier to be identified by utilizing HAZOP. By blending HAZOP and FMEA, both components and *streams* failure can be identified, thus generating a technique that has generate higher hazards coverage than individual hazard analysis (Seligmann, et al., 2012).

However, BLHAZID still emphasizes merely on the identification of physical component failures. It focuses on electric and mechanical components due to its reliance on HAZOP and FMEA, which are basically conventional hazard analysis techniques constructed on sequential accident models. Consequently, hazards arisen from risky decisions and actions by the management and organizational factors will be overlooked.

Appendix B Glossary for Selected Terms

Direct factors	The factors that contribute directly to the occurrence of an accident. These factors are typically associated to human errors and technical failures.
Emergent property/phenomena	The property/phenomena that can only be understood by taking into account the entire system components and their interactions within a particular system.
Hazard analysis	A tool to identify various hazards that are relevant to the considered system, thus prevention and mitigation can be designed to the system to avoid the hazards to develop into more serious problems.
Indirect factors	The factors that are indirectly related to the occurrence of an accident. These factors normally exist long before the accident occurrence, but still significantly contribute to the accident.
Organizational factors	The factors that influence the organization ways in achieving its objectives.
Proximate events	The events that are occurred just before the moment of an accident. For instance, in Fukushima nuclear accident, tsunami and the failure of reactor cooling system are the proximate events.
Safety barrier	Technical, operational, and organizational elements that are designated to prevent and/or mitigate hazards or accident to occur.
Socio-technical system	A system comprising humans and technologies that must work together to accomplish the common goals of the system.
System behavior	The behavior that emerges from the interactions between system components. System behavior is closely related to emergent property.
Social factors	The factors that affect individuals' attitude and behavior.