FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study program/specialization: Industrial Economics / Risk Management & Project Management	Spring Semester, 2017 Open
Author: Ola Grav Skjåstad	…… (signature author)
Program coordinator: David Häger	
Title of master's thesis: On Operational Safety Compliance for More Reliable Risk Safety Functions in Offshore Installations	
Credits: 30	
Keywords: Risk Assessment Risk Analysis Dynamic Risk Assessment Bayesian Networks Compliance Safety Operations Personnel	Number of pages: 60 + supplemental material/other: 7 Stavanger, 15. June 2017

Title page for Master's Thesis

Faculty of Science and Technology

THIS PAGE HAS INTENTIONALLY BEEN LEFT BLANK

On Operational Safety Compliance for More Reliable Risk Safety Functions in Offshore Installations

THIS PAGE HAS INTENTIONALLY BEEN LEFT BLANK

Preface

This is a Master's Thesis that has been prepared during the spring semester of 2017 at the Department for Industrial Economics, Risk Management and Planning as part of my Master's Degree in Industrial Economics. This thesis is a discussion and exploration on operational safety compliance for more reliable risk safety functions. The thesis statement was arrived at after extensive research into state-of-the art risk management methods and technologies. Through discussions with my supervisor, David Häger, we saw an opportunity to use alternative risk analysis tools to provide operations personnel with the means to consider the consequences of their decisions and actions. The continual support from David has been invaluable throughout the thesis work.

The presumed background for the readers of this thesis is a higher technical education, preferably with knowledge of risk management.

Department of Industrial Economics, Risk Management and Planning

University of Stavanger

Ola Grav Skjåstad

Spring 2017

THIS PAGE HAS INTENTIONALLY BEEN LEFT BLANK

Abstract

Due to a recent increase in major accident risk, efforts are being made to improve the robustness of the safety functions of offshore installations. Based on how the safety functions are defined and structured, their reliability is heavily dependent on the performance of the operations personnel. The robustness of the safety functions is based on the assumption that the personnel will behave according to policies and procedures and not commit errors or make mistakes accidentally or intentionally. Since risk assessment is the support for decisions made during the planning phase of an operation, it is likely that it can also be utilized to provide similar decision support to the safety functions during the actual operation.

This thesis explores how the risk assessment can be used to better ensure the operational compliance and safe behavior of personnel in order to implement and maintain the safety functions that make up robust design and barriers. This is done by evaluating underlying factors for major accidents and the risk assessment process to determine what causes non-compliance and unsafe behavior.

The aggregated effect of non-compliance and unsafe behavior is one of the leading causes of major accidents. This is most likely related to the lack of understanding and awareness as people have not been given sufficient information to consider and/or be made aware of potential consequences of their actions. Relevant information that is generated in the risk assessments is not easily accessible as it is stored within numerous static comprehensive reports and based on tools that cannot include new emergent information during the operation.

Dynamic Risk Assessment (DRA) using dynamic Bayesian Networks provide relevant and timely decision support by representing a live overview of cause & effect relationships with conditional probabilities. This could allow for detection of abnormalities caused by non-compliance and unsafe behavior and also increase awareness of consequences of non-compliance and unsafe behavior. This is likely to reduce the risk of major accidents. However, further research is required for more conclusive findings.

THIS PAGE HAS INTENTIONALLY BEEN LEFT BLANK

Table of Contents

1 Introduction

1.1 Background

The challenge of accidents and safety is ever-present across many industries. This challenge becomes more difficult to address as organizations attempt to solve more complex problems. This is especially true in the oil and gas industry where many of the less difficult prospects have already been developed. The oil companies are forced to exploit more challenging reserves in harsher and more remote areas. Oil and gas operations are considered high risk as major accidents such as a blowout can have major consequences. The Macondo accident, for instance, was a blowout resulting in an explosion killing and severely injuring several people and costing the operators several billion dollars in damages [1].

The basis for accident prevention and safety management is the risk assessment. The risk assessment results in the criteria for the safety system against hazards. The safety system has several redundant layers with different intended safety functions. The redundant nature of the safety system ensures that no single failures can result in catastrophic events. For each of these safety functions there are technical, organizational and operational elements. Technical elements are the equipment, such as the blowout preventer. The organizational elements are the personnel that are required for the safety system to function. The operational elements are the activities that must be completed for the safety system to function.

The safety functions are broken down into two categories: robust design and the barrier system [2, 3]. Robust design is also known as inherently safe design. The goal of robust design is to eliminate the chance for hazards to exist. Examples of robust design can be quality of materials or detailed operating procedures intended to help operational personnel to avoid mistakes. The barrier system are the safety functions against hazards when they occur. Barriers are introduced to regain control in case of abnormal events. The barriers can be preemptive by stopping a potential harmful chain of events from escalating into a major accident. They can also be reactive by mitigating potential consequences of the major event.

Based on how the safety functions are defined and structured, reliability is heavily dependent on the performance of the personnel. The safety is based on the assumption that personnel will behave according to policies and procedures and not commit errors or make mistakes accidentally or intentionally. In this thesis, this is referred to as safety compliance or safety compliant behavior. Breach of procedure or safety policies accidentally or intentionally is referred to safety non-compliance or non-compliant behavior.

As a result, the most common responsive measures to avoid future accidents are to improve design, documentation and procedures. These are important measures, but they do not address the fact that the safety still is dependent on the behavior of the personnel. This is often addressed through training, courses and cultivating a healthy safety culture. However, it seems that the current methods of ensuring safety compliance is not enough. According to the Petroleum Safety Authority (PSA), "*the indicator for major accidents is higher for 2015 and 2016 than for 2013 and 2014"* [4]. The PSA has as a result launched three main initiatives called "Reverse the Trend" where a focus on robustness is one of the three [5].

In light of this, the industry could benefit from novel methods that have the potential of increasing the reliability of the personnel performance. Since risk assessment is the support for decisions made during the planning phase of an operation, it is likely that it can also be utilized to provide similar decision support to the safety system during the actual operation. The following thesis statement can then be formulated:

Risk assessment findings, which is the basis for the safety system, can be used to better ensure operational compliance and safe behavior of personnel in order to better implement and maintain the risk safety functions.

This is statement is explored by evaluating:

- the underlying causes of major accidents, both from the perspective of the oil and gas industry and from a more general perspective to gain an understanding of what affects operational compliance and safe behavior
- the risk assessment process and its findings to determine if it provides the necessary information for operational support and what any potential short comings may be
- decisional situations that may cause a major risk in relation to decision theory and support for cognitive processes
- options for the potentially safer operation based on the findings of the evaluations above

1.2 Glossary

Operations personnel: The people who are responsible for initiating and executing activities during the day to day operations.

Major accident: According to the PSA a major accident is defined as an acute incident, such as a major discharge/emission or a fire/explosion, which immediately or subsequently causes several serious injuries and/or loss of human life, serious harm to the environment and/or loss of substantial material assists.

Robust design: according to the "Reverse the Trend" initiative, "*robust means rock solid, compact, strong and hard wearing – something physically and mentally resistant, durable and lasting. Robust is something which withstands wind, weather and the ravages of time, and which copes with change and the unforeseen. Robust is a suitable word to describe the requirements facing the Norwegian petroleum industry.*"

Safety system: Any and all technical, organizational and operational safety functions that prevent hazards from existing, hazardous events from occurring and mitigates consequences of major accidents. See Appendix A for a more detailed explanation.

Barrier system: The barrier system ensures that control is regained in the presence of abnormal events. See appendix A for more detailed explanation.

Latent conditions: Technical, organizational and operational underlying causes of triggering events. See Appendix B for more detailed explanation.

Triggering events: Events that immediately or subsequently causes failure.

Safety compliance: Implies that operations personnel will comply with safety policies and procedures.

2 Causes of major accidents

To be able to understand how information from the risk assessment can be used to better ensure safety compliance, it is necessary to evaluate which factors affect safety compliance and what the consequences of non-compliance are. This is approached by reviewing the cause of major accidents both in the offshore industry and from a more general perspective, with focus on what affects the behavior and decisions of the personnel.

2.1 Accident causes from a general perspective

Several authors agree that the cause of a major accidents cannot be attributed to a single cause. Major accidents are usually caused by a combination of failures. This can be seen through investigation of several major incidents across chemical and petroleum industry to financial and societal. Table 2.1 summarizes the historical examples of major accidents across multiple domains while Table 2.2 summarizes examples of the systemic causes that lead to these mistakes. This shows that most accidents are the result of aggregated decisional errors made at different stages from planning to execution.

Similar conclusions are drawn by Bell and Healey [6] who conducted a comprehensive review of existing literature concerning the causes of major hazard incidents and how to improve risk control and health and safety management. In their review, they consulted existing literature to find the probable causes and underlying factors of major hazard incidents in the nuclear, offshore oil and gas and onshore industries. They report that the Bhopal Toxic gas leak in 1984 was due to inadequate maintenance, failure to interpret the plant's status and inadequate training of operators. The David Besse Nuclear Power Station Incident in 2002 happened partly due to the failure to recognize and consider other secondary warning signals in a holistic fashion due to inadequate safety culture and awareness. The Paks Fuel Damage Incident in 2003 happened partly due to an unsafe safety system and inadequate sharing of safety information.

The typical underlying causes presented here are similar and can be recognized when reviewing the underlying causes of well control incidents discussed earlier. The bottom line is that in some way or another, the culmination of different systemic errors is caused by human error and the poor decision-making of individuals. This is pointed out in the work by Reason [7] in the area of human and organizational risk. Among numerous sources of literature consulted in the report, Simpson, Tunley [8], identified five human factors that were influencing the accidents in the chemical industry: procedures, availability of information, communications, emergency planning and accident investigation. Bell and Healey [6] concludes that specific factors contributing to major accidents include:

- Poor management e.g. inadequate supervision
- Pressure to meet production targets
- Inadequate safety management systems
- Failure to learn lessons from previous incidents
- Communication issues e.g. between shifts, between personnel, and management etc.
- Inadequate reporting systems
- Complacency
- Violations/non-compliance behavior
- Inadequate training e.g. emergency response, fire and safety
- Lack of competency
- Excessive working hours resulting in mental fatigue
- Inadequate procedures
- Modification/updates to equipment without operator knowledge and/or revised risk assessment
- Inadequate/insufficient maintenance
- Maintenance errors

Table 2.1 Examples of Systemic Failures in Various Domains Source: [9]

Chemical	*BP Oil Spill* (*2010*): Off-shore oil platform explosion leading to a large oil spill: 11 people killed; > $20 billion losses; incalculable damage to the environment *BP Texas City* (*2005*): Explosion in the isomerization unit; 15 people killed; ~180 people injured; $10 billion law suit pending *Exxon Valdez* (*1989*): Oil tanker accident; ~$1 billion in losses in law suits/fines *Piper Alpha Disaster* (*1988*): Occidental Petroleum's off-shore oil platform explosion; 167 killed; ~2 billion in losses *Bhopal Gas Tragedy* (*1984*): Methyl isocyanate leak at Union Carbide's pesticide plant; 5000-15,000 killed; ~120,000 injured; ~1 billion in losses; Worst ever industrial disaster
Electrical	*North East Power Blackout* (*2003*): Massive power outage that affected an estimated 10 million people in Ontario and 45 million people in eight states in the U.S. ~$6 billion in losses

Mining	*Massey Energy* (*2010*): W. Virginia mine explosion; 29 killed; worst mine disaster in four decades; ~$130 million in losses
Pharmaceutical	*Schering Plough Inhalers Recall* (*2002*); 59 million inhalers for treating asthma were recalled; $500 million in fines; largest in FDA history
Financial	*Madoff Scandal* (*2008–09*): Outright fraud; Ponzi scheme; estimated $65 billion in losses; thousands of investors defrauded *Subprime mortgage* (*2007–08*): Caused by the end of the real estate bubble; precipitated a global financial crisis; trillions of dollars in losses; required governmental rescues in several countries *Lehman Bros* (*2008–09*): Collapse of a 158-year-old tony Wall Street firm; one of the largest bankruptcies in the US, triggered by excessive risk taking and the collapse of the subprime mortgage market; ~26,000 employees lost their jobs *WorldCom* (*2002*): Accounting fraud; ~$180 billion in market value lost; 57,000 employees lost their jobs; billions of dollars lost in retirement savings *Enron* (*2001*): Outright fraud – overstatement of profits through off-the-books partnerships aided by its auditor Arthur Andersen; one of the largest bankruptcies in the US; ~$60 billion in market value destroyed; 20,000 employees lost their jobs; billions of dollars lost in retirement savings
Societal	*Collapse of Mayan Civilization* (*~800–900 AD*): Several theories have been offered; most notable is environmental/ecological collapse *Easter Island Civilization* (*~1500 AD*): Several theories have been offered; most notable is environmental/ecological collapse

Table 2.2 Some Typical Examples of Failures at Various Levels in a Systemic failure Source: [9]

Individuals	• Poor operator training or inexperienced operators leading to human errors • Not enough personnel due to downsizing
Equipment	• Poor maintenance and wear and tear leading to equipment failure • Wrong material, capacity, or equipment

Procedures	• Standard operating procedures not followed, workers make up their own or perform short cuts • Past mini-accidents and warning ignored • Process hazard analyses not conducted thoroughly • Poor emergency planning and training
Safety Systems	• Safety systems not tested and maintained properly • Back-up and/or emergency systems not on automatic but on manual
Management	• Failure in communication between ranks • Safety is not first priority, cost cutting is • Senior management lacking the background to appreciate the risks inherent in complex process plants – too much emphasis on financial spreadsheets and not enough on process flow sheets • "Performance at all costs" culture encouraging excessive risk taking and unethical behavior among its employees
Corporate Board	• Rewarding short term performance instead of long term • Setting up perverse incentives that are detrimental to the long-term survival of the company
Government: Policies and regulators	• Laissez-faire regulatory bodies, reliance on self-policing • Policies not strictly enforced due to limited resources or inherent conflict of interests of the regulatory bodies
National: Political	• Anti-government or anti-regulations sentiment dominant • Sustainability warnings ignored

2.2 Examples from the Norwegian offshore industry

2.2.1 Drilling operations and well control

Drilling and well operations are characterized by a high degree of complexity as the system is depending on several individual interacting parts. The technological development is driven quickly by the need to develop deeper and more complex reservoirs. A high level of activity combined with frequent changes in management and organizational structure introduces challenges regarding the expertise required for critical safety systems such as well control systems. Critical operational decisions are often made under pressure and high degree of uncertainty. Decisions must balance

between efficiency and safety. The cost of non-productive time (NPT) is high and can be detrimental to the entire operation. The interaction between personnel, technology and organization is critical to maintain the safety of drilling and well operations.

A well control incident is defined as the influx of formation fluid into the well that results in pressure build up after the blowout preventer (BOP) is closed or during a positive flow check and a well kill operation is implemented. In terms of the safety system, introduced in Section 1 and described in more detail in Appendix A, a well control incident is an abnormal event that should not occur due to the mud column, i.e. robust design. The barrier system is activated and restores normal operation by closing the BOP and performing the relevant kill procedures. The BOP constitutes the technical barrier, the drill team the organizational barrier and the kill procedures the operational barrier.

2.2.2 Primary and underlying causes

SINTEF conducted a study in 2011 on the behalf of the PSA to better understand what the main contributions to well control incidents are and what main challenges the industry faces regarding safety [10]. The results of the study are shown in Figure 2.2. The causes are categorized as human, organizational or technical. The nature of the causes is separated into primary and underlying. The primary causes are considered as triggering events whereas the underlying causes are issues present before the incident takes place.

Several well control incidents were surveyed and the triggering causes are represented by the blue bars. These are failures at the "sharp end" implying a direct cause & effect relationship. The underlying causes are represented by the red bars. The underlying causes influence the triggering causes. The green bar represents the type of responsive measure that was taken. For example, a responsive measure such as improving the procedure would fall in the procedure category in the figure.

The most common triggering causes are technical. This is expected as the technical equipment is in directly related to the risk. The underlying causes are largely organizational and human with the following main contributors:

- planning and preparation
- risk assessment and analysis
- wrong actions related to ignorance of prevailing practice and procedure
- cognitive error and misconception

It is also clear from the study that few corrective actions have been taken for these contributors.

Based on the results from the study SINTEF and PSA have pointed out that the perceived causes of incidents are primarily [10]:

- Lack of communication and cooperation within the operator-contractor-service company hierarchy
- Technical failures and/or weaknesses in the systems and barriers and the lacking focus on responsive measures
- Lack of barrier management and risk assessments

Carlsen, Hauge [10] states that drilling and well operations are characterized by a dynamic risk picture that varies with changes in drilling plans, changing well parameters and the operational timeline. It is therefore important that the risk picture that is established takes all temporal changes into account and identifies the new performance requirements of the barrier system. The results from the initial risk assessment may thus not be relevant for a new risk situation. This is considered as significant underlying causal factors of major accidents in the industry.

Inadequate risk assessments and the lack of competence and knowledge are the most recurring reported underlying causes for accidents according to the involved companies. According to drilling contractors the main underlying cause is lack of understanding the failure mechanisms and the underlying phenomena that lead to failure. They blame this on the use of consultants and inexperienced personnel in central positions. Several informants in the study by Carlsen, Hauge [10] express that more thorough risk assessments will not reduce the risk. The informants suggest that measures to increase the competency and knowledge of the involved personnel will have a larger effect. They also suggest more detailed procedures and instructions as measures to ensure compliance and subsequently reduce risk.

In summary, safety non-compliance such as complacency, cognitive errors and violations are often the direct cause of accidents. The underlying causes are usually pointed out to be related to safety systems, procedures and risk assessments, lack of training and competency. This implies that the main underlying cause is a lack of knowledge. However, a lack of knowledge and understanding of the system or plant is does not reveal what the deeper underlying causes are; i.e. the underlying factors that affect the behavior and decision making that governs a person's ability to comply with safety policies and procedures. Further investigation into behavioral psychology and decision theory is needed.

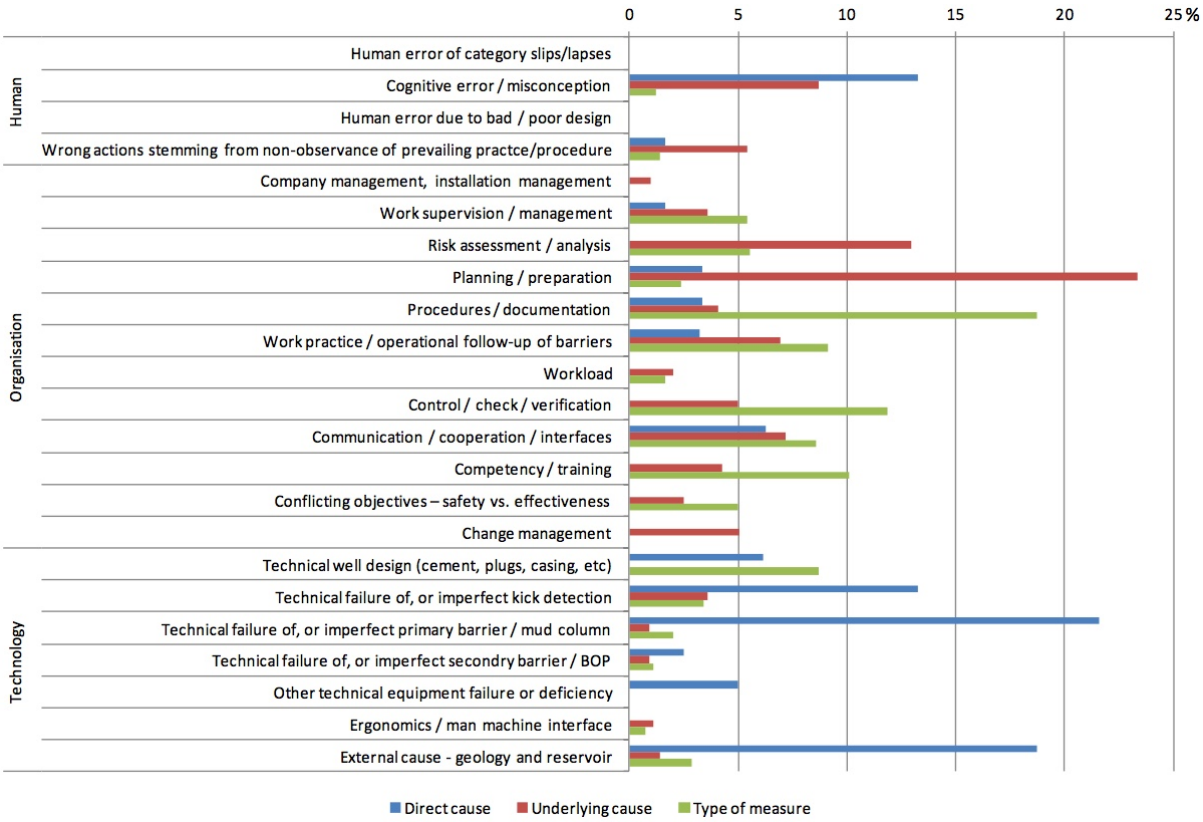

Figure 2.2 Comparison of identified causes (primary and underlying) and proposed measures following the well control incidents for the internal company investigations. [11]

2.3 Non-compliance and unsafe behavior

During an operation, it is important to consider the information that is available to the personnel. Assuming that the operation has been planned properly resulting in adequate procedures and policies to ensure both a robust system and a functional barrier system, the execution and performance of the personnel is required to ensure safety. It is up to the individuals in conjunction with automatic systems to recognize potential hazards and act accordingly. Immediate human causes such as

- operating without authority,
- failure to secure/warn,
- failure to recognize defective equipment,
- failing to use equipment properly,
- horseplay,
- failure to wear personal protection equipment,
- lack of attention and working on unsafe of live equipment

can still arise. Based on a study regarding the contribution of human factors to accidents in the offshore oil industry, Gordon [12] presents a list of individual factors that serve as underlying causes of accidents. These are, among others,

- competence,
- decision-making,
- lack of anticipation,
- risk perception/risk-taking behavior,
- distraction,
- insufficient thought
- and inattention.

These can also be viewed as underlying factors of many of the factors presented by Bell and Healey [6] in subsection 2.2.

Wagenaar, Hudson [13] concur with the discussion 2.1 and 2.2 that most accidents are caused by several coincidently coinciding unsafe acts by personnel. However, the personnel are usually unaware of their unsafe behavior and the potential consequences of their decisions and actions. Wagenaar, Hudson [13] also state that warnings, rules and procedures seldom work as an optimal solution to the issue. This is also analogous to the procedures that must be followed. The reason for this is the failure to perceive the meaning behind them. The failure to recognize the implication and reasoning behind the safety management systems, procedures, reporting systems and the like may explain many of the underlying individual factors presented by identified by Carlsen, Hauge [10], Gordon [12] and Bell and Healey [6].

A common responsive measure to reduce the likelihood of human errors is to raise risk awareness typically by cultivating a safety culture. However, this only helps if people are prepared to extrapolate the consequences of their actions [13]. A general raised awareness of risk provides little information necessary to make the subjective risk analyses to decide whether an action or activity is unsafe or not.

Wagenaar, Hudson [13] goes on to state that the reason why people are unable to recognize unsafe acts and fail to consider the consequences of their actions is the tendency to use backward reasoning instead of forward reasoning. Forward reasoning entails extrapolating from known action to an unknown accident. Backwards reasoning starts with known accidents and then the conditions for their occurrence is compared to the conditions of the operations personnel.

This implies that non-compliant safe behavior is caused by the failure to recognize the meaning or reasoning behind safety policies and procedures and because operations personnel are not applying forward reasoning to account for unknown accidents.

For example, one of the main issues is that people often take short cuts instead of following procedure. The procedure may be perceived as overly detailed and unnecessary. The operations personnel do not understand why the procedure is written as it is. Therefore, they are not able to consider what can go

wrong if a wrongly perceived unnecessary step is skipped. If they knew that skipping that step would result in a hazardous situation, they would be more likely to comply with the procedure.

Falck, Flage [14] suggest that *"the knowledge concerning how variables and uncertainty parameters that alone or in combinations have an impact on risk level and how they can be controlled and measured are of value during an operation."*

It is therefore likely that providing specific, relevant and meaningful information to the right person at the right time will assist them in making the necessary considerations to evaluate the consequences of their actions and decisions. This will make them more likely to follow procedure or realize that their actions may have drastic consequences down the line. It is likely that this information exists within the knowledge generated from the numerous risk assessments that are carried out.

3 Review and evaluation of conventional risk assessment

Previously it was determined that the cause of major accidents stem from the aggregated errors made by humans both during planning and operationally. Evidence suggests that the reason for this is the lack of relevant decision support and information that enables humans to adequately make the necessary considerations regarding their decisions and actions. This implies that the risk assessments fail to provide the necessary information to operations personnel. A review and evaluation of conventional risk assessments is required to understand how and why.

ISO31000 is the most widespread approach to risk assessment across many industries, including the oil and gas industry. NORSOK Z-013 uses the same approach as well as the petroleum regulatory body in Norway, Petroleum Safety Authority (PSA). The general risk management process, available tools and deliverables are prevalent in the oil and gas industry. An overview of the general process is illustrated in figure 3.1. The overall process is usually followed, but the content in each step varies based on the context of the risk assessment. Different tools are used to accomplish different goals. Qualitative assessments are usually used in the early phases of planning in order to establish design goals. Quantitative assessments are used for more detail oriented analyses of risk. The following discussion will be based on what can be considered as a typical operational risk assessment by Carlsen, Hauge [10]. This provides some context of what is available to the personnel during an operation and may help shed some light on the apparent issues outlined and discussed in chapter 2 as well as provide grounds for measures to mitigate these issues.

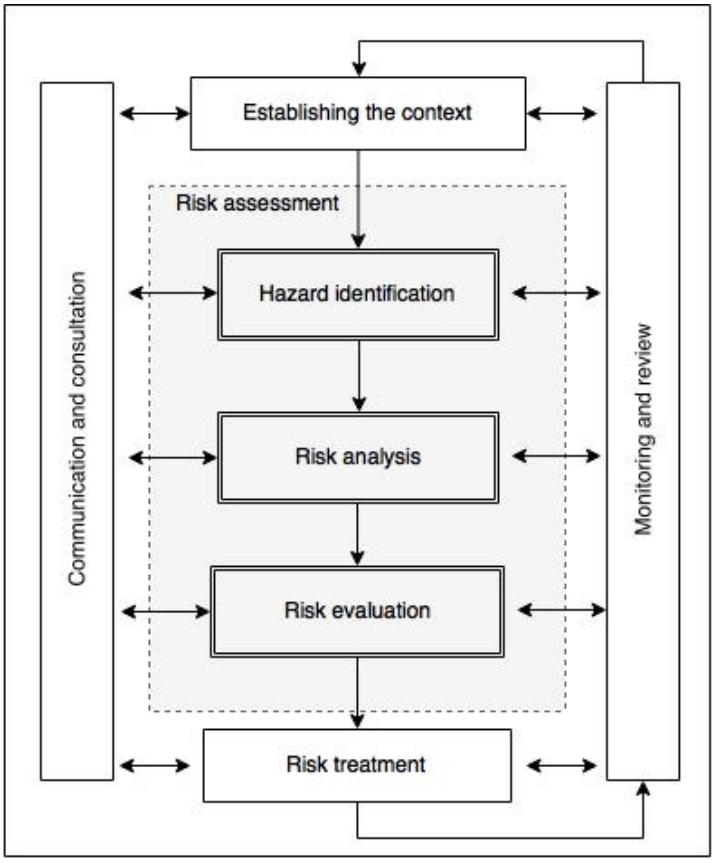

Figure 3.1 Risk management framework [15]

3.1 Example of a typical operational risk assessment

This description is adapted from Carlsen, Hauge [10].

The responsible drilling/well engineer from the operator company is in charge and responsible for preparing the well and to provide a plan for the entire operation. Inputs to this is among others geological surveys and experience from similar previously drilled wells. At the center of the risk analysis is the risk register. This is a matrix describing the different risk aspects tied to the well that includes frequencies and consequences that in combination result in the green, yellow and red classes. Common practice is for the drilling/well engineer to prepare a first draft of this register based on previous similar operations. This preliminary register is then reviewed in a formal risk meeting led by the operator company and involves representatives from the contractors and service companies. The well program is reviewed and evaluated section by section, and the risk register is updated and completed through focus on new and unique risks and on the most critical procedures with an assumed high level of risk. Relevant risk reducing measures are proposed in the process. The risks and the corresponding measures are then implemented in the increasingly more detailed drilling and operational procedures intended to be used by the crew during operation. The risk register is not

included in the procedures but kept separate as a potential attachment. Technical barrier diagrams are also prepared and included in the appropriate documentation. Preparation of the risk register can in some cases trigger the need for more in depth analyses where HAZOP is usually performed. In addition to the highly qualitative analyses done in preparation of the operational documentation, quantitative analyses are also completed, usually by a consultancy.

3.2 Hazard identification

3.2.1 Overview

The first step in the risk assessment outlined above is identifying potential hazards. Hazard identification (HAZID) is a comprehensive and thorough process of identifying any and every conceivable hazard present in the system or operation. The purpose for hazard identification is the [16]:

- Identification of hazards associated with the defined systems and of the sources of these hazards, as well as events or sets of circumstances that may cause the hazards and their potential consequences
- Generation of a comprehensive list of hazards based on those events and circumstances that might lead to possible unwanted consequences within the scope of the risk and emergency preparedness assessment process
- Identification of risk reducing measures

There is no formal method of performing a HAZID and it is often completed using one or more of several different tools such as:

- Check lists developed by experts to aid the review of planned operations
- Using historical and reference studies as starting points for new studies
- Using accident and failure statistics such as case studies of actual failures and accidents
- HAZOP, a detailed study to identify sequences of failures or conditions that can lead to accidents [17]
- SAFOP, a detailed review of sequences of failures and conditions that can lead to accidents [18]

Here it is important to consider the context of the risk assessment. More detailed HAZID studies such as HAZOP and SAFOP are only carried out if deemed necessary.

3.2.2 HAZOP

A hazard and operability study (HAZOP) is conducted by using detailed information concerning the design and operation of a process, analyzing consequences of deviations and identify possible consequences and causes of these deviations. The HAZOP is usually carried out during the detailed technical design phase.

The study is conducted by a team of experts that systematically apply certain guide words to individual processes of the system or operation. For example, for a valve, these guidewords can be no, less, more, reverse leading to certain states such as no flow, less pressure, more temperature, reverse flow or additional flow, respectively. The cause of a valve with no flow can be malfunction or blocked passage while the consequences can be burst pipe.

This is a thorough process completed by teams of typically 5 – 7 experts. British Standard [19], states that the success of the HAZOP study strongly depends on the alertness and concentration of the team members and it is therefore important that the sessions are of limited duration and that there are appropriate intervals between sessions.

3.3 Risk analysis

3.3.1 Overview

As seen in Figure 3.2, risk analysis concerns the analysis of both initiating events and potential consequences of said events. The ultimate objective of the risk analysis is to establish the risk picture. In short, this entails providing decision makers with meaningful support during the planning and operational phase in relation to the identified potential hazards during the HAZID. The risk picture is established by assessing the likelihood for hazardous events to occur and their respective consequence. The risk assessment can be carried out qualitatively, quantitatively or as a mix of both. Qualitative analyses can be considered as educated assumptions of experts based on extensive experience and historical information.

In quantitative risk analysis (QRA), the risk is calculated based on statistics and models resulting in a probability along with a consequence that can be expressed qualitatively, semi-quantitative or quantitative, depending on the context. According to Vinnem [16], the following are the objectives of consequence analyses:

- To analyze potential event sequences that may develop following the occurrence of an initiating event

- To determine the influence of the performance of barriers, the magnitude of the physical effects and the extent of damage to personnel, environment and assets, according to what is relevant given the context of the assessment.
- To assess the possible outcomes of identified and relevant initiating events that may contribute to the overall risk picture

Several methods and tools are available when conducting a risk analysis. The most widely used in the industry are fault tree analysis (FTA) [20], event tree analysis (ETA) [21], failure mode and effect analysis (FMEA) [22] and the bow-tie model [23].

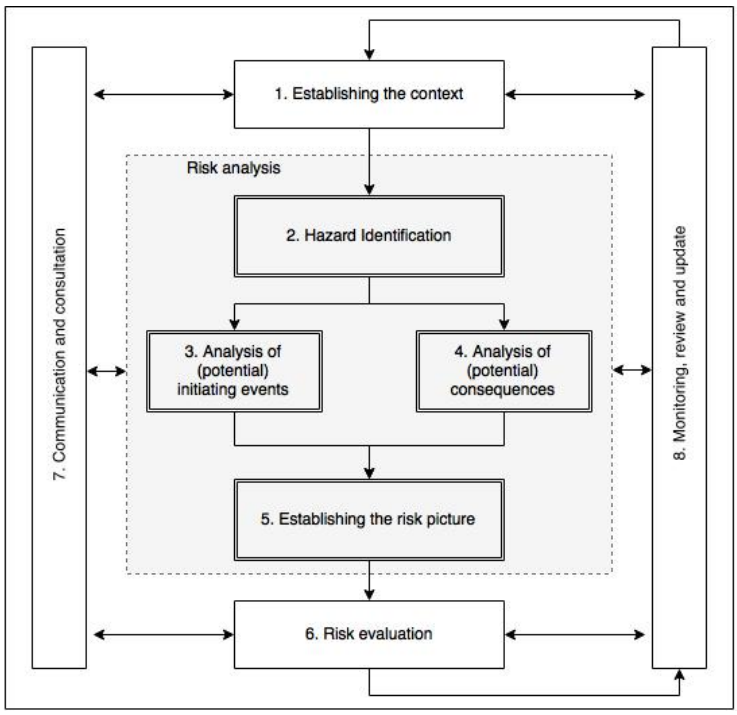

Figure 3.2 Risk analysis and risk evaluation process. Source: Vinnem [16]

3.3.2 Fault tree analysis

A fault tree analysis (FTA) is used to identify potential causes for system failure. It is based on Boolean logic to illustrate graphically the chain of events necessary to for a hazardous event to occur. An example of a simplified fault tree is illustrated in Figure 3.3. Email server failure, event D0, is the top-level event that is considered a system failure if it occurs. For D0 to occur, either D1 or D2 must occur as illustrated by the OR gate, G1. The diamond in D1 indicates that the causes are not developed any further. For D2 to occur, both D3 and D4 must occur in unison as indicated by the AND gate, G2. The circles of D3 and D4 represent basic or initiating events. FTA analysis illustrate the dependencies and conditions for critical chain of events that must occur for failure to occur and reveal system design or operational weaknesses for which safety features or barriers can be introduced.

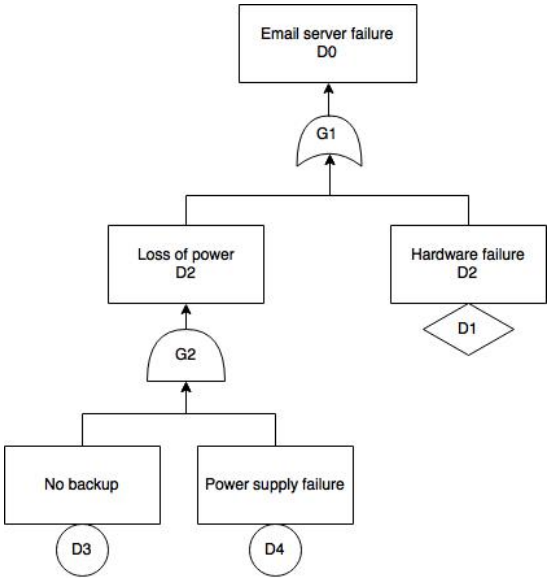

Figure 3.3 Simplified example of a fault tree

3.3.3 Event tree analysis

Event trees graphically illustrate the chain of events that will occur given a top event for example how a gas leak can lead to fire or explosion. The tree is built by starting with the top event such as a gas leak and then asking a list of yes or no questions such as "ignition?". The diagram in Figure 3.2 illustrates how the trees are built. The top event, gas leak, is assumed to occur. If ignition does not occur, there is no explosion. If ignition does occur, a fire or explosion will occur depending on how long gas has leaked before the ignition. The probabilities for the top event, the branching points (nodes) and the terminal events are calculated. The tree can also be used for the direct calculation of consequences such as the potential of loss of lives during and evacuation event. Fault trees can be combined with event trees where the fault tree describes the initiating events and the branching points.

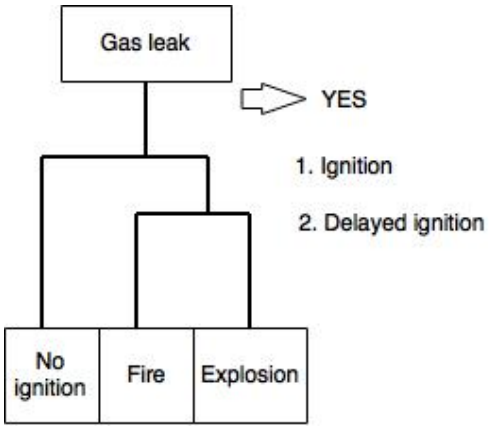

Figure 3.2 Simplified example of an event tree

3.3.4 Failure mode and effects analysis

Failure mode and effects analysis (FMEA), or failure mode, effects and criticality analysis (FMECA), is one of the earliest methods for evaluating the effects and risk of a potential hazard developed in the 1950s [22]. The method is a logical and structured method using inductive reasoning to describe the failure and its effect on the system with associated failure rate, severity ranking and risk reducing measures for a system function with a specific operational mode. A worksheet for a FMEA is shown in Figure 3.3.

System: Performed by:

Ref. drawing no.: Date: Page: of

Description of unit			Description of failure			Effect of failure		Failure rate	Severity ranking	Risk reducing measures	Comments
Ref. no	Function	Opera-tional mode	Failure mode	Failure cause or mechanism	Detection of failure	On the subsystem	On the system function				
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)

Figure 3.3 FMEA worksheet. Source: [22]

3.4 Risk evaluation

3.4.1 Overview

Risk evaluation is where the established risk picture is incorporated in the decision-making process. The risk for hazards and events are evaluated and taken into consideration for the design of systems and processes based on a risk tolerance in relation to the context. Decisions are made regarding which risks should be treated in relation to priorities.

3.4.2 The Bow Tie model

The Bow Tie model can be used as a tool to evaluate risk by effectively illustrating the risk picture. It is essentially a combination of a traditional fault tree and event tree. The fault tree makes up the left-hand side leading to the initiating top event in the middle. The event tree illustrates the chain of events that occur if the top event occurs on the right side. See Figure 3.4. It provides an easily communicable view of the root causes for an initiating event along with potential consequences. Active and reactive barriers that can work as risk reducing measures can also be added to the diagram.

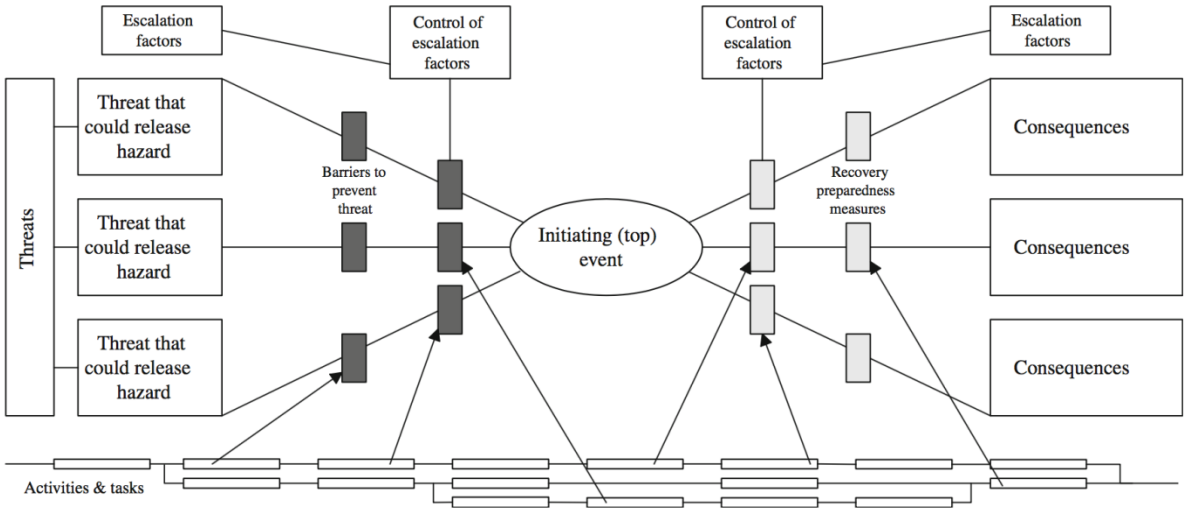

Figure 3.4 A typical bow-tie display. Source: [16]

3.5 Risk treatment

The selection of barriers and their respective effect is carried out during risk treatment. The risk picture is reevaluated including the effect of the risk treatment. This is a cyclical process until an acceptable level of risk is achieved. In classical risk treatment the following options exist [16]:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Seeking an opportunity by deciding to start or continue with an activity likely to create or maintain the risk
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including insurance)
- Retaining the risk, either by choice or by default

3.6 The Quantitative Risk Assessment

Quantitative risk assessment (QRA) is a frequently used term that describes the thorough analyses and evaluations used to form the basis for design and risk reducing measures, respectively. The QRA can also be referred to as:

- Probabilistic Risk Assessment (PRA)
- Probabilistic Safety Assessment (PSA)
- Concept Safety Evaluation (CSE)
- Total Risk Analysis (TRA)

Although QRA is a quantitative analysis, the qualitative techniques outlined in the previous sections can be used in a semi-quantitative fashion. Before a quantitative analysis can be conducted, the risks and hazards must be identified, evaluated and prioritized usually in the early concept phase of the project. This is done by coarse cause and consequence analyses followed by increasingly detailed quantitative consequence analyses. The risk is then calculated and often presented as a combination of the probability of occurrence and the consequence. Fatal accident rates (FAR) are popular representations of risk. The risk must be lower than a predetermined threshold. Risk reducing measures are often implemented according to ALARP principle to make sure the risk stays below the threshold. The ALARP principle stands for as low as reasonably practicable and states that the cost risk reducing measures cannot be grossly disproportional to the consequences.

According to Vinnem [16], when an offshore or marine structure is considered, the consequence loads are mainly related to the following:

- Fire loads from ignited hydrocarbon releases
- Explosion loads from ignition of hydrocarbon gas clouds
- Structural impact from collisions, falling objects, etc.
- Environmental loads

The consequence analyses are an extensive effort involving many different disciplines, third party consultant agencies, people from all levels of the organization, suppliers and contractors. They cover a series of steps including [16]:

- Accident scenario analysis of possible event sequences
- Analysis of accidental loads, related to fire explosion and impact
- Analysis of the response systems and equipment to accidental loads
- Analysis of final consequence to personnel, environment, and assets
- Escalation analysis, relating to how accidents may spread from the initial equipment to other equipment

HAZOPs, FMEAs, FTAs and ETAs are among others popular techniques for the semi-qualitative cause and consequence analyses. The FTAs and ETAs are used in combination with synthesis models, Monte Carlo simulation, human error quantification techniques and statistical models based on historical frequency for quantitative analyses. For a total detailed QRA, the sheer amount of knowledge and documentation that is produced is incredible. Vinnem [16] presents the following lists of steps required for a complete QRA evaluating personnel risk:

1. Hazard identification
    a. Systematic hazard review
    b. Top event spectrum
2. Hazard analysis
    a. Blow out hazard study
    b. Riser/pipeline hazard study
    c. Process hazard study
    d. Fire and smoke analysis
    e. Explosion analysis
    f. Dropped object hazard study
    g. Collision hazard study
    h. Structural failure study
    i. Overall event tree study
3. Analysis of critical risks
    a. Barrier study
    b. Detailed probability study
    c. Detailed consequence study
    d. Revised event tree study
4. Impairment analysis
    a. Escape ways impairment study
    b. Shelter area impairment study
    c. Evacuation impairment study
    d. Impairment study of command and control safety function
5. Fatality risk analysis
    a. Immediate fatality risk study
    b. Escape ways risk study
    c. Shelter area risk study
    d. Evacuation means availability study
    e. Evacuation risk study
    f. Pick up and rescue risk study
    g. Overall fatality risk summation

The presentation of the risk picture is often done in comprehensive reports. The NORSOK Standard Z-013 2001 [24] has a dedicated subsection for the presentation of the risk picture obtained in the QRA. See Appendix C for an excerpt from the standard. There is an immense amount of information that is contained within these reports. However most of the knowledge is retained by the risk consultant agencies that conduct the QRA on behalf of for example the operator company. Examples of these agencies are DNV GL and Lilleaker AS.

3.7 Risk assessment latent conditions

3.7.1 Unavailability

The comprehensive risk assessment reports and risk registers that are used to provide decisional support for designing the safety system could have value in the operational phase. Somewhere within the vast amounts of knowledge that is generated there exists valuable information that can assist personnel during operation to understand the reasoning behind the organizational and operational safety functions. The fault trees, event trees and bow ties that are used in the risk analyses explain the mechanisms behind potential hazards and accidents. The challenge is that this information is unavailable to the personnel. The bottom line is that based on the scope of a QRA as presented in

subsection 3.6, the information needed to provide personnel with the means necessary to perform forward reasoning exists somewhere within the collective knowledge generated during the QRA.

All of the risk assessment documentation can be considered as a segmented collective database. In Figure 3.5 the squares represent different individual analyses and assessments. The shaded squares represent the information within the database that is relevant to a person performing some activity. They represent the information that was used to plan and develop the procedures that must be followed to ensure the integrity of the safety system.

Maintenance personnel cannot easily consult fault trees that are relevant to the technical equipment they are performing maintenance on. A fault tree could show what the consequences might be if the procedure is not followed as it is wrongly perceived as needlessly complicated. The reasoning behind the procedure is available through reviewing the risk assessment.

The collective knowledge gathered over the years by operators and consultants such as DNV GL is enormous. However, as this information exists within individual reports it is difficult to allocate specific relevant information on request to relevant personnel in a timely manner. Most of the knowledge generated during the risk assessments in the planning phase is underutilized and largely unavailable to operational personnel.

The assumption that this knowledge is largely unavailable is supported by a workshop conducted by SINTEF [25] that was aimed at proving that the collective knowledge of individuals would be more effective at building an understanding of risk than single individuals. They did this by exploring the cause and effect of a hazardous incident. The findings of the workshop were that none of the individuals had a comprehensive understanding of all aspects of the incident on the outset. Furthermore, the participants were surprised by the number of possible hazardous outcomes of decisions related to the incident that they did not consider. As SINTEF already had all the necessary information before conduction the workshop implies that if this was provided to the participants during the operation, they would immediately have been aware of the mechanisms and consequences of their decisions and of the incident. Hence, effective communication of relevant information gained during risk assessment will have a positive impact on the compliance and behavior of personnel. Accident and scenario models are particularly helpful.

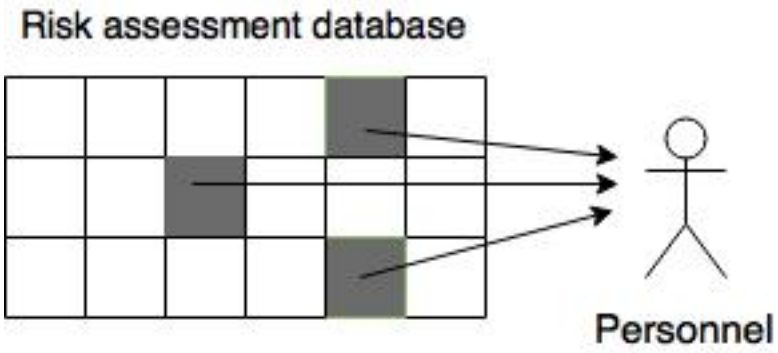

Figure 3.5 Representation of the collective knowledge gained from the risk assessment and how different parts of that knowledge might be relevant to operational personnel

3.7.2 Dynamics and complexity

Consider the basis on which decisions are made regarding robust design, the barrier system and during operations. Both robust design and the barrier system arise from a long history of thorough risk assessments. The risk is managed based on the recommendations made by the risk assessment. This puts a lot of faith in the tools used to identify, analyze and prioritize potential hazards, failures and accidents that ultimately make up the risk. Of these tools, FTs, ETs and Bowties are much used within the field of risk analysis of process systems and fault diagnosis [26-33].

However, these tools are inherently flawed when considering highly complex and dynamic systems such as an offshore drilling rig. In this system, the state of safety is never static and the different system components are always to some degree interconnected. Frank Børre Pedersen, Group Technology and Innovation, DNV GL, states [34]:

"Conditions change over time, new knowledge becomes available, and changes in context may affect our risk tolerability. Risk models are just approximations of real life. In order to provide relevant and timely decision support, models need to keep track with current conditions and context. Managing the safety of complex dynamic systems requires dynamic risk assessment."

For example, there is always a threat for a kick occurring as the bottom hole conditions necessary to facilitate a kick is highly unpredictable. The state of the primary barrier, mud column, will for the same reasons always be uncertain. The barrier can be in rough terms be modified preventatively, but the fine tuning necessary to sustain a safe operation will be mostly reactive based on new information. Furthermore, the different activities and decisions made on a day to day basis will affect the risk of accidents on a more overarching level. Hot work such as welding on one part of the rig happening simultaneously with engine maintenance and a heavy lifting operation will have a potential effect on the emergency preparedness and increase the risk of mistakes and thereby the risk of an explosion should a kick occur at the wrong time. The dynamics and interdependency between seemingly

irrelevant and insignificant parts of the system and operation cannot be captured by FTs, ETs and Bow Ties. According to Khakzad, Khan [35] and Abimbola, Khan [36], standard FTs are not suitable for analyzing large systems, particularly if the system presents redundant failures, common cause failures, or mutually exclusive initiating events. They assume that events are mutually exclusive, are not easily updated given a change in environmental and operational conditions. This limits them from incorporating multi-state variables, dependent failures, functional uncertainty and expert opinions [35].

The major uncertainty due to the limitations of the fundamental tools used in conventional risk assessment is considered a major latent condition that can be considered a contributor to major accidents. Furthermore, it fails to incorporate the vast amounts of new information generated during the operational phase. This reduces the validity of the original assessment and fails to provide operators with up to date information. Acting on outdated and incomplete information makes it even more difficult to make the correct decisions, act safely and recognize possible hazards that may emerge during the operation.

A more relevant and updated picture of risk would more specifically beneficial in terms of people being able to identify otherwise undiscovered errors or mistakes. A dynamic picture of risk can allow operators to observe how their own performance relates to the overall safety during the operations. Depending on the performance of the dynamic risk assessment operators could in theory observe the effects of certain decisions or unexpected changes and thereby act accordingly.

4 Safety compliance in relation to decision making

Two apparent challenges or latent conditions concerning the risk assessment have been established in subsection 3.7:

1. Vast amounts of detailed information concerning the chain of events that may lead to accidents and their respective influencing factors is available in underutilized databases, reports and expert opinions.
2. The risk information is based on assumptions and approximation prior to operations where new information that can provide a more updated and accurate picture of risk is not considered due to the prevalent use of tools that require unjustifiable amounts of resources to update.

Even though a likely cause for safety non-compliance has become apparent, specific measures to overcome the aforementioned challenges while providing the means for forward reasoning is not apparent. Deeper insight into decisional situations of relevance for major risk in relation to decision making and situational awareness (SA) is needed.

4.1 Decisional situations of relevance for major risk

Yang and Haugen [37] proposed a typology that describes the different types of decisions made in hazardous processes. Planning decisions and execution decisions are the two main categories. They are both divided into two sub-categories. Planning decisions consist of strategic and operational decisions while execution decisions consist of instantaneous decisions and emergency decisions. Strategic decisions are long term (years) where risk and benefits of alternatives are considered carefully. Operational decisions have a shorter planning horizon but long enough to carry out risk assessment. Instantaneous decisions are spontaneous to follow or violate procedure or decisions triggered by external deviations. Emergency decisions are related to how to avoid or adapt to hazardous situations. They are fundamentally impacted by experience and judgements.

This topology was used partly as a basis for a study carried out by Kongsvik, Almklov [38]. They investigated the available decision support for different decisional situations of relevance for major accident risk. The study reveals what information that is available and used when making strategic, operational and instantaneous decisions.

Strategic decisions are made in relation to main plans that can span several years and operational plans spanning months. Activities that involve risks are considered in the plans where data from the overall plan is exported to a risk tool. Fatal accident rates are calculated and shown based on the QRA. Revisions to the plan are made if the FAR values are above the risk acceptance level. At this level, plans and risk evaluations do not benefit the operations personnel.

At the operational level, decisions are made regarding the planned activities. The most important decisions made regarding risk are made when coordination work orders and work permits are established. According to the study by Kongsvik, Almklov [38], the prioritizing of work orders is not based on major accident risk. The decisions are made based on available resources, timing and necessity. Permits are issued based on short term FAR-values obtained from a risk tool. The FAR values are estimated based on the plant QRA, the number of people involved and the number of adjacent hazardous activities such as hot work. A comment by the authors is that "*an improvement would be if the major hazard risk could be reflected more explicitly, including also the effect on major hazard risk during the execution of the work itself*".

On a more instantaneous level, the final decision to carry out work orders is up to the responsible operator. It is at this level safety compliance becomes relevant. The operator must decide whether or not to execute the activity based on the surrounding conditions. As pointed out earlier, operators seldom have the necessary information at hand to consider failure scenarios and chain of events. At the activity level, operations personnel are expected to comply with procedures and safety policies, but they are in the same predicament as the operator. According to the study, common practice is to evaluate the safety of the activity in relation to spatial and temporal considerations without any decision support systems. The evaluations are made based on the operators own reasoning abilities. However, as pointed out earlier, people are inclined to apply backwards reasoning resulting in undiscovered mistakes.

Kongsvik, Almklov [38] suggests that as decisions approach the operations and activity level decision support should be increasingly more factual than probabilistic. It is suggested that decisions should be supported by visualizing hazardous interdependencies between activities, such as how a spark appearing from one activity can ignite a leakage caused by another. As decision support assists in people's ability to reason, it is highly likely that the same suggestions also apply to safety compliance. The difference between decision making and safety compliance is that decision making forces people to do some form of explicit reasoning. Whereas for safety compliance, explicit reasoning is not enforced. Explicit forward reasoning should be both encouraged at critical times and supported by some tool or method that provides necessary grounds for evaluating ostensibly unknown or irrelevant factors.

4.2 Naturalistic decision making and situational awareness

Naturalistic decision making (NDM) explains more accurately how decisions are made in real-life situations. According to Klein [39], the features of naturalistic decision making are:

1. Ill-defined goals and ill-structured tasks
2. Uncertainty ambiguity, and missing data
3. Shifting and competing goals
4. Dynamic and continually changing conditions
5. Action-feedback loops (real-time reactions to changed conditions)
6. Time stress
7. High stakes
8. Multiple players
9. Organizational goals and norms
10. Experienced decision makers

The goal of NDM is to understand the cognitive work of decision making, especially when performed in complex sociotechnical contexts. Considering the features above, the context for naturalistic decision making is similar to the operational conditions experienced by operations personnel. Operations personnel must conduct a similar form of reasoning to extrapolate potential consequences of their behavior. According to Endsley [40], the key to supporting cognitive processes of an operator is to support situation awareness (SA). This is also the key to support NDM and forward reasoning. SA is defined as being aware of what is happening around you and understanding what that information means to you now and in the future. This definition can be broken down into three separate levels: (i) perception of the elements in the environment, (ii) comprehension of the situation, and (iii) projection of future status.

4.3 Suggested method for better ensuring safety compliance

There is a clear connection between the causes of non-compliant safety behavior outlined by Wagenaar, Hudson [13] in chapter 2 and the current state of the risk assessment. Operations personnel are not receiving the necessary information in a timely manner in order to apply forward reasoning to their situation or circumstances. Measures need to be taken to ensure better timely communication of relevant information that allows for risk informed reasoning and decision making.

Based on the previous discussions on the cause of major accidents and the risk assessment paradigm, there is a clear disconnect between the data produced and the information needed. The data exists within the risk assessments, but it is not communicated sufficiently to operations personnel. The

information that is stored in the risk assessment reports does little to create SA and it does not account for emergent new information.

A lack of SA directly impacts the ability for a person to make effective decisions and conduct forward reasoning [40].

SA can be increased by:

(i) increasing the perception of the elements in the environment by providing a graphical real time representation of the interdependency between hazardous elements

(ii) increasing the comprehension of the situation by highlighting only the most relevant information to the task at hand

(iii) allow operations personnel to project future status by updating the interdependency between hazardous events according to intent

(iv) implemented decisions and actions should be used to update the situation such that unintentional deviations can be discovered

This is likely to provide the necessary SA to support the cognitive processes required for adequate NDM and forward reasoning which affects safety compliance.

5 Dynamic risk assessment

Dynamic risk assessment (DRA) can achieve the suggested methods for better ensuring safety compliance by enhancing SA.

DRA involves overcoming the challenge of dynamics and complexity and the detection of emergent system behavior and is currently gaining traction in the risk community. DNV GL, SINTEF, the PSA and several experts are all in agreement that methods of achieving real time updating risk based on operational information is highly valuable [3, 10, 32, 34, 41-43].

This chapter describes the recent developments and innovations that have the potential of realizing a real-time DRA tool and discusses how they can be modified to include SA.

5.1 System condition monitoring

The first step to DRA is system conditioning monitoring. Monitoring variables in the technical system can allow the computation of reliability and maintenance intervals. Condition monitoring is how new information is attained during the operation. Usually condition monitoring only applies to the technical system, but for DRA organizational and operational variables must also be monitored. The specific variables that must be monitored depends on the scope of the DRA.

There are three levels of condition monitoring that must be considered: anomaly detection, diagnosis and prognosis [41]. Diagnosis and prognosis can be considered as a part of the logic, inference or reasoning achieved through DRA.

Anomaly detection is detection of defects, faults or deviations that can be considered precursors of failures or accidents. Anomalies are observed by recognizing unexpected deviations and trends. Deviation only indicates that something might be wrong, but cannot determine what is wrong. This is the second level of conditioning monitoring. Diagnosis implies inference from collected data to determine actual system/component states. Prognosis is the third level and implies inference from collected data to predict future behavior.

The ideal solution to the abovementioned challenges is a fully integrated condition monitoring system where every single conditional dependency is known such that the interdependency between fault and event mechanisms and cause and effect relationships can be observed. For example, the degradation of a certain valve may increase the risk of dangerous pressure buildup in another part of the system. The most probable connected path would be highlighted and easily observed to pinpoint where responsive measures need to be taken. Backtraceability is also preferred, where an observed increase in risk can be traced back to the most likely source(s) by analyzing the cause and effect interdependent relationships.

5.2 Dynamic risk assessment methodology

Dynamic risk assessment (DRA) can be described in three ways. First, the dynamics of the operation can be modelled before the operation providing the operator with a view of how the risk will fluctuate based on pre-emptive approximations and assumptions. Essentially the development of risk is predicted. Second, the dynamics of risk is at first based on the conventional static picture which in Bayesian terms is the prior probability function and new information attained from real time monitoring of precursors and risk influencing factors is the bases for the posterior function. In theory, implications of decisions and activities are reflected in a real-time updated risk picture. Third, the dynamics are captured through the search for and continuous discovery of new hazards that were not accounted for in the initial risk assessment.

One suggested framework is presented by Paltrinieri, Khan [44], see Table 5.1. This framework is built around the established risk management/governance frameworks such as the iNTeg-Risk Emerging Risk Management Framework, CAN/CSA-Q850 Framework for Risk management and the International Risk Governance Council Risk Governance Model [44]. This framework is reminiscent of the ISO31000 risk management framework, but puts more emphasis on the continuous activities. Monitoring, review and continuous improvement is in under this framework taken more literally. The framework centers around discovery of new hazards that emerge over time which cannot be planned for before commencing operation. Through monitoring and increased vigilance, precursors of new hazards can be discovered, assessed and mitigated in a timely fashion.

The first complete methodology for continuous temporal update of the risk picture based new operational information was developed by Meel, Seider et al. [45-47]. The overall methodologies developed are summarized and illustrated in Figure 5.1 by Kalantarnia, Khan [42]. This methodology takes advantage of the results of the risk assessment from the planning phase as a starting point. The dynamic failure assessment in the shaded box focuses on monitoring real time data to automatically update the probability assessment. Thereby it results in a living risk picture that can be monitored and tracked. This allows operators to correlate their decisions and actions with the fluctuations in the risk picture. The viability of this method has been shown in several case studies [46-49]. One drawback of this methodology is the lack of consequence assessment [43].

A combination of the two methodologies would be the optimal solution; a DRA that both continually updates the probabilities based on incoming new emergent information while incorporating new unaccounted for hazards.

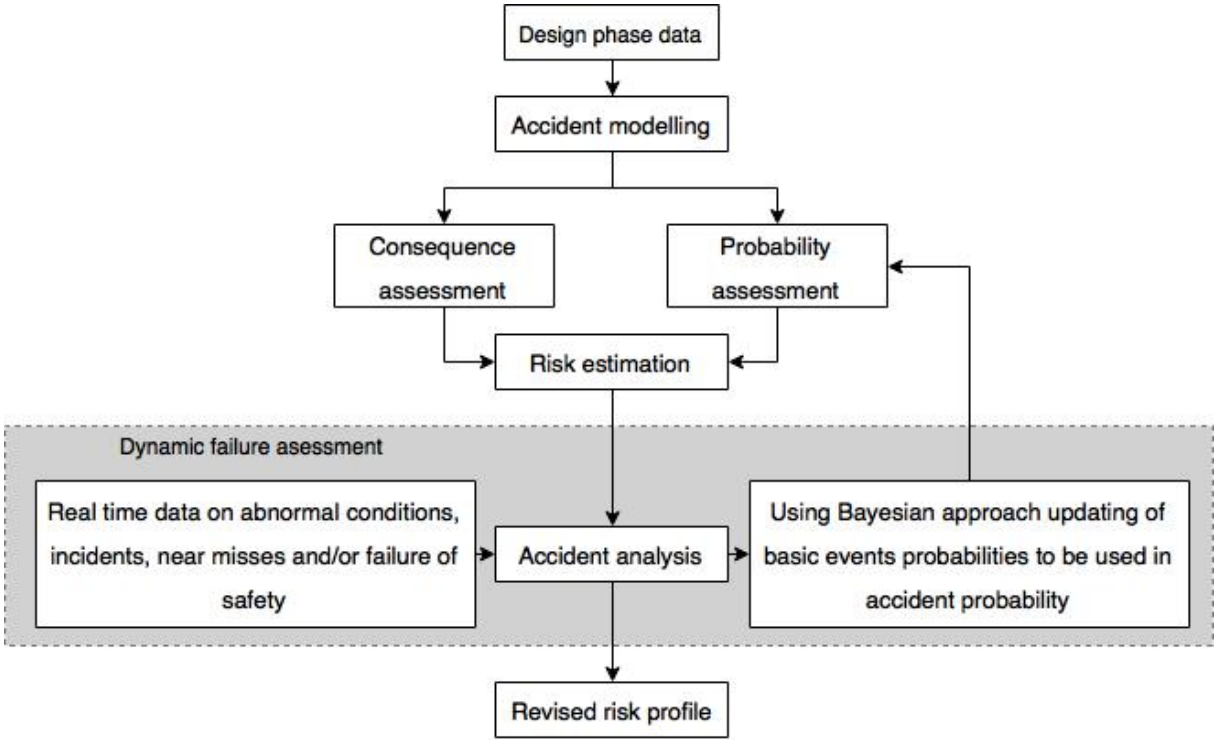

Figure 5.1 Dynamic risk assessment methodology [42]

Table 5.1 Dynamic Risk Management Framework [44]

<table>
<tr><th>Phases</th><th>Stages</th><th colspan="2">Continuous activities</th></tr>
<tr><td>Horizon screening: This phase aims to frame the risk issues, define the limits of the system to be studied, consider early warning systems. Context and organizational structure under which specific a risk management problem will be resolved, are defined in this phase. Risks need to be detected as early as possible and their evolution needs to be constantly monitored, also with respect to different spheres.</td><td rowspan="2">Understanding: It refers to the process of knowledge and information management</td><td rowspan="4">Monitoring, review and continuous improvement.</td><td rowspan="4">Communication and consultation</td></tr>
<tr><td>Identification: This phase aims to identify hazards related to the process considered, the equipment and the substance handled. The result is a set of potential accident scenarios, whose risk will be assessed in the next phase.</td></tr>
<tr><td>Assessment: The quantitative assessment of risk related to the scenarios previously identified addresses both their frequency and severity to have a numerical estimation. The combination of the two components gives an indicator of risk, whose tolerability or acceptability is evaluated according to specific risk criteria.</td><td rowspan="2">Deciding: It refers to the process of elaboration and judgement of information subsequent intervention.</td></tr>
<tr><td>Decisions and actions: This final step includes the decision-making process and consequent implementation of regulatory and voluntary actions for non-acceptable risks.</td></tr>
<tr><td colspan="4">Reference risk management governance frameworks
iNTeg-Risk Emerging Risk Management Framework
CAN/CSA-Q850 Framework for Risk management
International Risk Governance Council Risk Governance Mode</td></tr>
</table>

5.3 Bayesian dynamic risk assessment

When it comes to implementing DRA to monitor the behavior of the risk picture over time, a Bayesian approach have been proven successful on numerous occasions [31, 35, 36, 42, 47, 49-56]. This approach is called Bayesian Dynamic Risk Assessment (BDRA) and utilized Bayesian Networks to create models of systems, hazards and accidents.

The first generation of DRA developed by Meel, Seider et al. was further developed by to integrate Bayesian failure mechanisms with consequence assessment [31, 32, 42, 57].

5.3.1 Brief introduction to Bayesian Networks

A Bayesian Network is a graphical model used to model phenomena or situations where uncertainty is present [58]. It is a tool that allows for quantitative reasoning of uncertainty given observations. The BN is built based on actual causal or influencing dependencies. In the literature, Bayesian Networks are also known as Causal Probabilistic Networks (CPN), Bayesian Belief Networks (BBN) or Belief Networks. BNs primarily consists of two main elements. A graphical structure where nodes and directed arcs define dependencies or independencies. The strength of these interdependencies is given by conditional probability.

For every node A, with parent nodes $B_1 \ldots B_n$ a local conditional probability distribution $P(A|B_1 \ldots B_n)$ is defined in a node probability table (NPT) for every node. For example, a node A can represent the probability of "cancer" and a node B can represent the probability of the patient smoking or not. The probability of A is conditionally dependent on node B. If evidence of is provided such that the probability of smoking equals 1, the probability that the patient has cancer will increase based on the Bayes rule of conditional probability. The properties of the net allow for predictions by testing different scenarios by providing evidence for certain nodes and observing the effect on the network. Furthermore, the behavior of the network will change and adapt based on the updated new variable input.

An example of a probability distribution provided by a Bayesian Network is given by Equation 5.1 and show in Figure 5.2

$$P(A_1, \ldots, A_4) = \prod_{i=1}^{4} P\big(A_i | pa(A_i)\big) = P(A_4|A_2, A_3) \times P(A_2|A_1) \times P(A_3) \times P(A_1) \quad \text{.....Eq. 5.1}$$

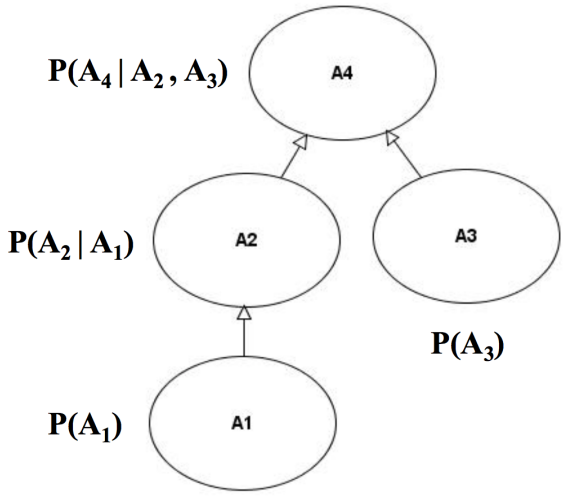

Figure 5.2 Example of a Bayesian Network

5.3.2 Bayesian dynamic risk assessment methodology

Kalantarnia, Khan [42] presents an algorithm that utilizes Bayesian approach for DRA, see Figure 5.3. This algorithm focuses on monitoring the apparent risk level of a specific process. Conventional risk assessment is carried out for a process where hazards, abnormal events are identified and safety system components are identified. An event tree, fault tree or bow tie is created. Prior probabilities for each safety system is obtained using a deterministic approach where deterministic values represent the probabilities, a probabilistic approach using the median point of probability distributions or a risk analysis approach using Monte Carlo simulation to obtain probabilities. The algorithm is adopted by Kaltarina, Khan from the work by Meel, Seider et al.

Khakzad, Khan [31], Khakzad, Khakzad [59], in fact, developed DRA models for quantitative risk analysis of blowout on offshore drilling rigs using Bayesian inference. They conclude that

"...Bayesian networks provides greater value than the traditionally used bow tie model since it can consider common cause failures and conditional dependencies along with performing probability updating and sequential learning using accident precursors." - Khakzad, Khan [31]

For instance, they used

"...event trees and hierarchical Bayesian analysis to establish informative distributions for offshore blowouts using data of near accidents, such as kicks, leaks, and failure of BOPs collected from a variety of offshore drilling rigs. These informative distributions could be used as predictive tools to estimate relevant failure probabilities in the future." - Khakzad, Khakzad [59]

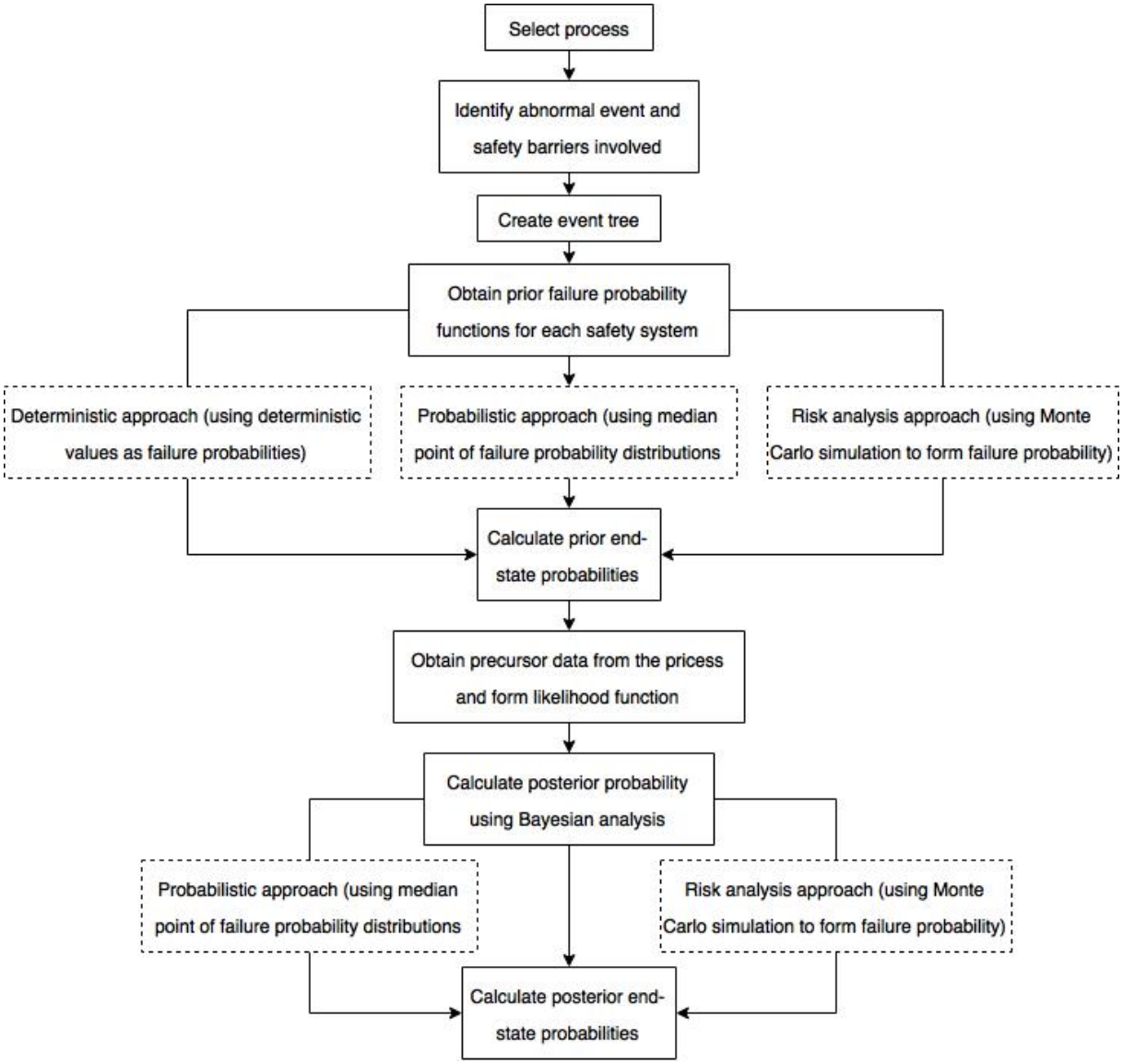

Figure 5.3 Algorithm for dynamic assessment of a process unit [42]

5.3.3 DNV GL MARV

MARV stands for Multi-Analytic Risk Visualization and facilitates risk informed decisions. This is a software risk monitoring platform developed by DNV GL. According to their own documentation the platform [41]:

"…analyses complex cause-effect relationships through failure models and expert inputs, and presents the risk information in a visual touch-screen interface that combines geographical maps, physical models, and risk outputs in one user friendly interface"

MARV has been successfully tested in the onshore pipeline industry for failure modelling of pipelines due to corrosion [50, 54]. The case studies conclude that the transparent nature of the networks can easily represent the interdependent connections such that continuous improvement of the

corresponding system can be made by the software's users such as the operations personnel. Another positive note is that the nodes are represented by probability density functions rather than single values. Probability density functions represent all possible values which an event might take. The BNs are a superior method for dealing with lacking data as data can be represented through uniform probability distributions within broad bounding values of the parameters. The BNs could also be easily updated based on observations made by the operations personnel to more accurately represent risk. Uncertainty is minimized by including several data sources such as different physical models, frequency and expert opinions. The lack of feedback loops due to BNs being acyclic graphs is a drawback, however feedback loops can be included in separate models outside the network to generate conditional probability tables.

5.4 Opportunities and limitations of current state-of-the-art

5.4.1 Opportunities

There are several opportunities that are made possible by DRA, but they do suffer from several limitations. In terms of the design phase, hazard and scenario identification and discovery in addition to accident modelling can be improved by gathering and processing information that is generated during operations such as near misses, mishaps, incidents and accidents and applying it in the design of new operations [60]. Paltrinieri, Tugnoli [61] for instance developed a dynamic procedure for atypical scenario identification (DyPASI) for HAZID of new undiscovered hazards during the operations.

Another possibility, according to Pasman and Rogers [62] is the transparent comparison between design alternatives, determining the utility or dis-utility of different choices based on the cost or benefit of consequences using BN. Pasman and Rogers [63] continued by making Layer of Protection Analysis (LOPA) more effective and the QRA more transparent and flexible by using Bayesian approaches to weigh gains and costs versus risk.

DRA allows better visualization of the risk picture through graphs of risk vs time, BNs or risk barometers depicting instantaneous real-time risk levels. Better visualization and increased transparency is highly beneficial in the decision-making process. Decisions are no longer made based on the static QRA, but rather by considering future development of the risk picture for more long term robust design choices [64].

The effect of the interaction between human, organizational and technical elements in an operation can be more easily and accurately modelled. Monitoring these effects over time can improve decisions made in relation to the effect versus cost of safety programs and inattention to safety [65].

In terms of the operation, the most notable opportunity is to monitor the effect of additional safety measures based on an updated picture of the risk. Furthermore, monitoring the how the picture of risk varies over time due to other factors such as reliability, maintenance and parallel planned activities can be used to determine whether to continue with the operation or not in relation to risk acceptance criteria. The Risk Barometer developed by the Center for Integrated Operations in the Petroleum industry, continuously monitors how the risk picture changes based on the existing QRA and the indicators that assess the state of risk influencing factors [43]. The risk picture is then visualized analogously to how pressure fluctuations are visualized in a barometer [66].

5.4.2 Limitations

Limitations are related to complications surrounding condition monitoring. For DRA to work, condition monitoring must monitor much more than technical variables such as reliability and failure rates. It is unclear what exactly needs to be monitored in order to produce a living risk picture. This depends firstly on how the risk picture is represented. Risk can be represented as probabilities; probabilities and consequences; probabilities, consequences and uncertainty. It is tempting to display the risk picture using conventional means such as FAR values. The current DRA methods seem to concentrate on providing a living risk picture for single events or the aggregation of several events into a single risk level. Although transparency is often quoted as an opportunity, there is no explicit mention of using the transparency for learning and awareness purposes. Falck, Flage [14] suggest that the knowledge concerning how variables and uncertainty parameters that alone or in combinations have an impact on risk level and how they can be controlled and measured are of more value during an operation than the risk level alone.

It should be noted that most of the current techniques under development. Several limitations have not yet been addressed such as for DyPASI where dynamics are captured by continually collecting relevant data to detect emergent new hazards. Paltrinieri, Khan [67] applied DyPASI and DRA methods was applied to the analysis of Gallatin metal dust accidents to demonstrate the effectiveness. While successful, the methods are heavily contingent on a proper safety culture, reporting and a high level of vigilance for recording process performances and incidents. For Bayesian networks, the current difficulty is the lack of specific support for developing the networks [63, 64]. Although, ETs, FTs and Bowties can be used, the structure is limited and restricted from the beginning. BNs can incorporate much more complex and flexible relationships than conventional methods. The flexibility can be considered as a two-edged sword as using conventional methods as a crutch to save time might be tempting, but this does limits the benefits of using BNs in the first place. The vast number of possible ways to build the net and the fact that it must be tested to check if the model is realistic can make the task challenging.

6 Ensuring safety compliance

In subsection 4.3 four suggestions were made to increase SA to enable forward reasoning and subsequently ensure safety compliance. BDRA possesses the necessary functionalities to create a system that fulfils the four suggestions. First, the possibilities of using BDRA for SA is discussed in terms of the suggested method that was arrived at in subsection 4.3. Second, the suggested stages of development and implementation are discussed. Third, the most apparent challenge of implementing BDRA for SA is discussed.

6.1 Possibilities of using dynamic risk assessment for situational awareness

(i) increasing the perception of the elements in the environment by visualizing the interdependency between hazardous elements

The aim is to provide a visualized graphical database showing the explicit dependencies between all hazardous elements within a system such as a drilling rig. Ideally this database would include all the aggregated knowledge that exists across all FTs ETs, Bowties, HAZOPS, FMEAs, mathematical and physical models to visualize how every identified hazard in some way or another affects one another. The database would visualize the likelihood of hazard occurrence based on the reliability of the systems components, the interaction of components and human-system interactions. Bayesian Networks are ideal for this purpose due to their innate flexible representation of causal dependencies with arcs and nodes. This graphical representation of causal relationship makes the otherwise fragmented and unorganized information more understandable. Causal relationships can be found by inspecting a hazard node. By tracing the connective arcs, every other directly or indirectly connected hazard can be found. Depending on the how detailed and extensively the Bayesian Network is populated, unknown causal relationships could be identified.

One of the drawbacks of BNs is that there are no specific semantics to guide the model development and to guarantee the model coherence [64]. There are no clear methodologies for converting the QRAs into graphical representations in a BN. However, it is impractical to consider modelling the entire QRA in a BN in the first place. A more practical approach is to begin with the HAZOPs, FMEAs, FTs and ETAs that already exists to build a qualitative BN model [53, 68, 69]. It is not necessary for the purpose of creating SA to calculate probability distributions for the elements in the BN. It is more important to build a model where the conditional probabilities between hazard elements can be observed and highlighted.

(ii) increasing the comprehension of the situation by highlighting only the most relevant information to the task at hand

The abovementioned visualization of causal relationships can result in extremely large and complex global networks. This will have the opposite effect of what is the goal of implementing BNs. How operations personnel can interface with the BN is highly important and the design of the graphical model should be user focused. A hierarchical structure is recommended when possible as it allows a top down view of the system. BNs can be structured in a hierarchically using Object Oriented Bayesian Networks (OOBN). OOBNs are a specific class of BNs [70] which simplifies models by providing a top-down structure of the network. A generic structure of an OOBN can be seen in Figure 6.1. Weber and Jouffe [71] successfully used a OOBN to model the dependency between several failure modes of components and the impact, in terms of reliability, of several decisions made on the maintenance of a highly complex system.

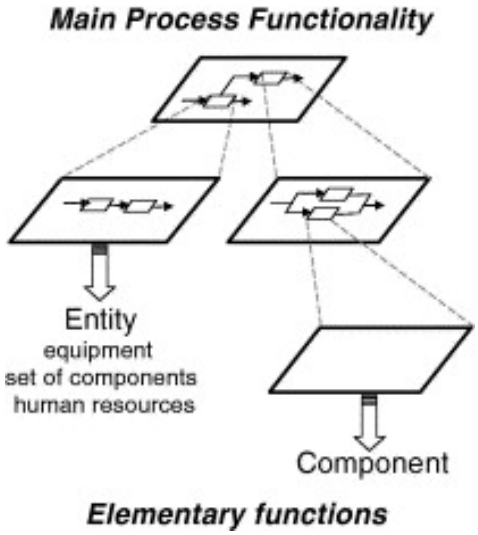

Figure 6.1 Functional decomposition Source: [71]

(iii) allow operations personnel to project future status by updating the interdependency between hazardous events according to intent

To aid with forward reasoning and for extra decision support, BNs can be updated given manual inputs by its users. This is done by manually changing the probability for a hazard to occur to 100 % and observe how this affects other hazards in the network. By providing evidence that a certain component such as a valve should fail could represent that the valve is taken offline for maintenance. The implications of taking the valve offline could have unforeseen repercussions for hazards that were unknown before providing evidence. In theory, before commencing an activity or making a

decision, scenario analyses could be undertaken by providing evidence in the BN to observe repercussions that would otherwise be considered insignificant or be unknown to the people involved.

(iv) implemented decisions and actions should be used to update the situation such that unintentional deviations can be discovered

One of the major issues regarding safety compliance is that it is often unintentional and occurs unknowingly to the operations personnel. However, the functionality of BDRA allows for the discovery of unknown mistakes such that reactionary measures can be taken.

Within the network certain activities or components can have binary states which affect other nodes in the network. For example, hot work can either be ongoing or not. If it is, the likelihood for ignition in case of a gas leak should increase and vice versa. In a similar manner, components or equipment that is either offline or online during maintenance will have a similar effect on other elements in the system and can be observed in the network. Continuously updating the state of these variables during the operation will allow operators and operations personnel to continuously be aware of any fluctuations of the risk level and the cause of such fluctuation. An illustration of how the risk picture fluctuates in relation to activities, performance, interactions, decisions, etc. can be seen in Figure 6.2. The transparency of BNs can not only calculate the risk fluctuations, but also visualize what is causing the fluctuations. By correlating abnormal trends or fluctuations in the BN variables with ongoing or past activities unknown mistakes might be uncovered.

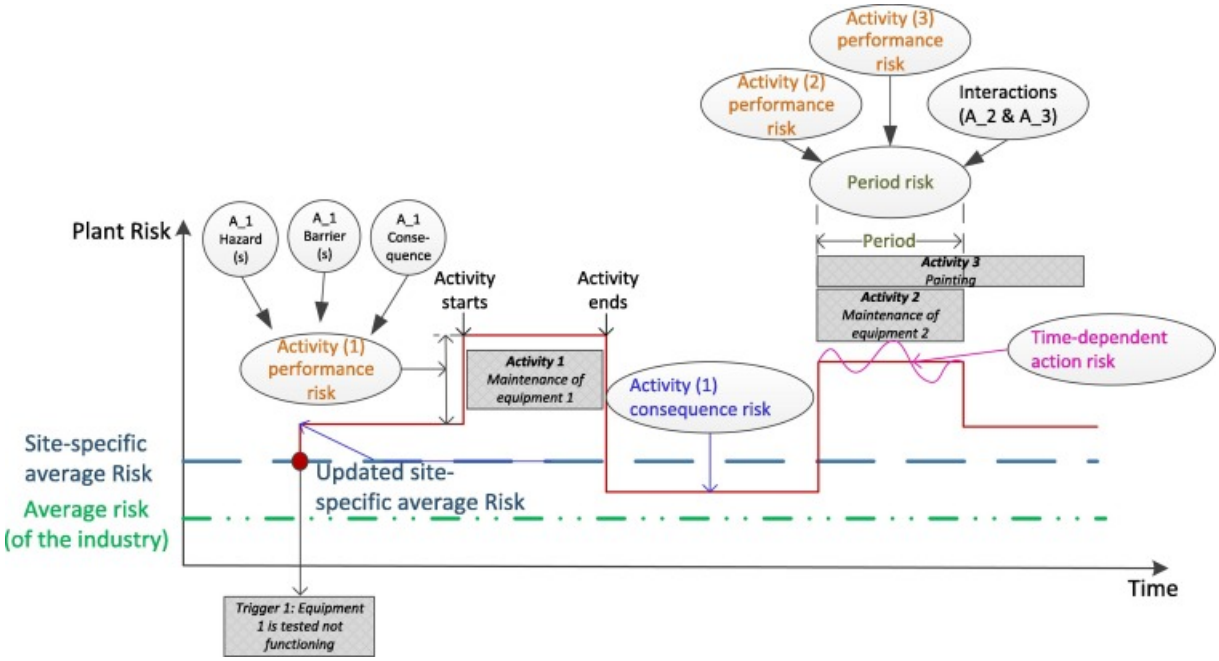

Figure 6.2 Illustration of how risk fluctuates in relation to activity levels. Source: [37]

6.2 Suggested development stages:

Even though BDRA have a theoretic potential to be a suitable tool for raising operational SA with regards to risk, the current state-of-the-art is limited and no commercially viable technologies have been successfully developed. Because of this, it is useful to consider how the abovementioned possibilities can be developed and implemented.

The most important aspect to consider during development is the visualization. The current focus of DRA is to update the

- numerical value of risk to compare it with predefined risk acceptance criteria,
- to predict future trends based on planned activities
- to identify the most risk inducing activities such as maintenance
- or to measure the deteriorating reliability of barriers.

There does not seem to be any focus on explicitly visualizing the risk assessment knowledge in a manner that provides spatial and temporal SA.

6.2.1 Stage 1: Qualitative visualization

The first stage should be concentrated on the development of the Bayesian Network. More precisely, the BN needs to include all causal relationships, hazards and relevant variables. The aim is to visualize the dependencies. The probability distributions are not important as the emphasis is to create a visual database that easily conveys SA. Visualization does not need to be implemented using a BN at the first stage. And any graphical representation of causal models can be used. However, the graphical model should be easily convertible to a BN for the next development stage.

This first stage of the development is analogous to the hazard identification stage of traditional risk assessment. This should be based on the QRA, if available, as the aggregated knowledge gained during that process is highly likely to create a rudimentary network structure. As the tools used in the QRA are limited due to Boolean logic and binary states, it is expected that the remaining work is to identify causal dependencies that were not possible to consider using the conventional tools. In other words, the development should be concentrated on the efficient identification of causal risk factors and possible relationships.

Technologies and methods that can discover multivariate cause and effect relationships from large databases should be considered such as TETRAD.

TETRAD is an ongoing program that uses artificial intelligence techniques to help an investigator to perform systematic search for alternative causal models using whatever relevant knowledge may be available [72]. TETRAD has been in development since the 1980s and is an open source platform

that searches for and creates causal statistical models from large databases. [73]. TETRAD is for example used to perform many of the functions in commercial programs such as Hugin. Hugin is a commercial software for analysis using Bayesian Networks [74]. Technologies like TETRAD could be adapted to assist or even automate the network development of BNs based on available risk knowledge. However, this assumes that the risk data, information and knowledge is structured in a digital database which is currently not the case. Digitalizing the collective risk knowledge is currently an on-going process according to DNV GL.

6.2.2 Stage 2: Implement probability distributions

This stage aims to implement basic inference in the graphical causal model and the model should be converted to a OOBN. The purpose is to see the effect of how intended actions will affect the nodes in the network. If the intended action is to perform maintenance on a valve, the valve will be unavailable for the duration of the maintenance. An offline valve will influence other elements in the technical system. Knowing if the risk is relatively higher or lower is enough to know what to consider. The emphasis should be on this functionality. It is not necessarily important that the causal dependencies are an accurate representation of the risk. For the purpose of awareness, the relationships and the relative differences based on updated information given by the operator regarding intended activities or actions.

6.2.3 Stage 3: Holistic real time risk monitoring

Throughout development, it is important that real time risk monitoring can be implemented when the limitations of real time risk monitoring have been addressed. The probability distributions for all nodes, or critical nodes to start off with, will at this stage be an accurate representation of the actual risk picture based on advanced state-of-the-art condition monitoring. At this stage, the discovery of potentially harmful mistakes or acts of non-compliance that were unknowingly made by the operations personnel can be discovered. The decisions and actions that interact with the system in question could be detected by analyzing and detecting abnormal fluctuations in the network.

6.3 Current main identified challenges

So far, only the possibilities of BDRA for increased SA has been discussed with few mentions of explicit challenges. However, there does exist significant challenges that need to be overcome. The main challenges are related to the availability of data. This is due to the current risk assessment latent conditions discussed in subsection 3.7. The current risk management paradigm of basing most of the decisions concerning both design and operations on comprehensive QRAs is a challenge.

Modelling Instantaneous Risk for Major Accident Prevention (MIRMAP) is a publicly financed project by the Research Council of Norway, Gassco and Statoil. MIRMAP attempts to *"explore the concept of instantaneous major hazard risk and how this can be analyzed in living risk analysis, as a basis for better decision support in an operational setting*" [75]. The project has focused on work-order preparation and planning by modelling fluctuations in risk based on the planned activity level. The fluctuating risk as illustrated in Figure 6.2, can be smoothed by planning activities based on how they influence the risk level. Although the focus of this project is not on providing better SA for the operations personnel, MIRMAP is quantitative and based on relevant information that exists in the QRA. It is therefore safe to assume that the amount of work is required to develop MIRMAP is indicative of the amount of work required to implement the BDRA for SA. According to Haugen [75], the effort of developing MIRMAP is on a similar order of conducting a QRA. According to Vinnem [16], the budget of a detailed QRA is 2500 man-hours and can take up to 5 months. As the QRA is still required for safe design, developing MIRMAP in addition to the QRA would be uneconomical and unfeasible. Implementing MIRMAP violates the ALARP principle.

This is likely due to how the information and knowledge is stored and presented. The use of reports and consultancies results in a highly fragmented knowledgebase among several individuals or groups. This makes it immensely difficult for anyone to convert the available information into a visual representation of the knowledge focusing on SA. Furthermore, even though artificial intelligence applications such as TETRAD are available for deep learning and knowledge extraction, they still require a data to be stored digitally. This can be considered the first and most important challenge to overcome because it not only enables BDRA for SA, but many other DRA possibilities such as MIRMAP.

Using artificial intelligence to overcome this challenge is likely to be the optimal solution. Recent algorithmic development and the exponential increase of computing power and availability of data has triggered successful applications across a wide range of domains. In e-commerce, Amazon have disrupted their market with personalized recommender systems. In the field of medicine, artificial intelligence is used for more precise diagnostics and personalized treatment recommendations [76]. Lawyers are able to reduce their research time from days to hours by applying artificial intelligence techniques [77]. 'Deep Learning' algorithms have enabled highly accurate image, text and speech recognition systems that are fueling a renaissance in the areas of robotics, with particularly well-known cases being self-driving cars and digital personal assistants.

7 Conclusion and further work

7.1 Conclusion

The premise for this thesis is that the safety of process plants, such as an offshore drilling rig, is based on the performance of its operations personnel. Operations personnel must comply with certain safety policies and procedures to initiate and maintain the safety functions. However, safety is only guaranteed if personnel do not make mistakes unknowingly or deliberately. It was therefore necessary to consider new methods to better ensure compliance. It was hypothesized that it is likely that the risk assessment findings could be better used to ensure safety compliance during the operation phase in the same way it is used as decision support during the planning phase.

To be able to understand how information from the risk assessment can be used to better ensure safety compliance, it was necessary to evaluate which factors affects safety compliance and what the consequences of non-compliance are. This was approached by reviewing the causes of major accidents both specifically in the offshore industry and more general, with focus on what affects the behavior and decisions of the personnel.

It was determined that the causes of major accidents stem from aggregated errors made by humans both during planning and operation. Evidence suggests that non-compliant behavior is firstly caused by the failure to recognize the meaning or reasoning behind safety policies and procedures. Secondly, non-compliant behavior is caused by operations personnel that are not applying forward reasoning to account for unknown risks. In other words, operations personnel lack relevant decision support and information that enables them to make the necessary considerations regarding the consequences of their decisions and actions. This implies that the risk assessments are not providing the necessary information to operations personnel.

A review and evaluation of the risk assessments was conducted and revealed that vast amounts of information which can provide operations personnel with the means to perform forward reasoning exists. However, this information is not available during operations as it exists in databases, reports and assessments that are not easily accessible. Furthermore, the risk information is based on assumptions and approximations prior to operations. Current risk assessment techniques fail to consider emergent operational information for a more updated and accurate risk picture. Operations personnel therefore also lack the means of observing abnormal trends. The bottom line is that the information to better ensure safety compliance does exist within the knowledge generated in the risk assessment, but it is not easily available to operations personnel.

A review of decisional situations that could lead major risks made it clear that operations personnel lack situational awareness. A lack of situational awareness directly impacts the ability for a person to

make the right decisions and conduct forward reasoning. Increased situational awareness, DRA functionality and Bayesian Networks could lead to better operational compliance by:

- spatially and temporally visualize the interdependency between hazard elements
- highlight the most important information for the task at hand and allow operations personnel to test how their intended actions or decisions will impact the system in terms of risk
- provide a live updated view of risk such that abnormal trends can be identified and human mistakes avoided.

7.2 Future work

It should be noted that the reasoning used throughout this thesis to reach the different conclusions is based on exploratory research. This limited the research to the author's interpretations and evaluations of several research papers and other available knowledge in order to draw conclusions. The resulting conclusions, inferences and recommendations are more tentative than final and should be regarded as such. More conclusive research would have required a concrete method such as the one presented in this thesis.

Three suggestions for future work are presented:

(i) The functionality of a BDRA for SA outlined in this thesis should be proven in future work. It is important to show how SA can easily be communicated using a BN by building and testing a functional model. For example, a BN model that shows the dependencies of a P&ID for a system can be built. The effects of the different failure modes identified in a HAZOP will have on the different elements in the P&ID can be shown.

(ii) Furthermore, research into what specifically affects human behavior and safety compliance is needed. It is likely that revisiting accident investigations and interviewing operations personnel will provide more insight into the issue. This should be supported by research into user friendly design specifically aimed at making situational awareness intuitive for operations personnel.

(iii) More research regarding the digitalization of risk assessment findings is needed. Specifically, the risk assessments need to be accessible in databases where state-of-the-art artificial intelligence techniques can be applied. Methods that are capable of aggregating data and information that exists in different formats should be looked into in order to take advantage of the knowledge that already exists in the different QRA-reports. In the long run, it is likely that risk information will become increasingly more digitalized. This will solve many of the major challenges regarding unavailability of information that are discussed in this thesis.

Bibliography

1. Group, D.H.S., *Final report on the investigation of the Macondo well blowout.* Center for Catastrophic Risk Management, University of California at Berkeley, 2011.
2. Eltervåg, A., et al., *Prinsipper for barrierestyring i petroleumsvirksomheten - Barrierenotat 2017*. 2017, Petroleumstilsynet, PSA.
3. Hauge, S. and K. Øien, *Guidance for barrier management in the petroleum industry.* SINTEF F27608, 2016.
4. PSA. *RNNP 2016: serious incidents cause concern*. Petroleum Safety Authority 2016 [cited 2016 May 5.]; Available from: http://www.psa.no/summary-report-2016/category1264.html.
5. PSA. *Reversing the trend*. Petroleum Safety Authority 2017 [cited 2017 May 5.]; Available from: http://www.psa.no/main-issue-2017/category1245.html.
6. Bell, J. and N. Healey, *The Causes of Major Hazard Incidents and How to Improve Risk Control and Health and Safety Management: A Review of the Existing Literature*. 2006: Health and Safety Laboratory.
7. Reason, J., *Managing the risks of organizational accidents*. 1997: Routledge.
8. Simpson, G., C. Tunley, and M. Burton, *Development of human factors methods and associated standards for major hazard industries*. 2003: HSE books.
9. Venkatasubramanian, V., *Systemic failures: challenges and opportunities in risk management in complex systems.* AIChE Journal, 2011. **57**(1): p. 2-9.
10. Carlsen, I.M., et al., *Årsaksforhold og tiltak knyttet til brønnkontrollhendelser i norsk petroleumsvirksomhet*. 2012, SINTEF: Petroleumstilsynet.
11. Hauge, S., et al., *Risk of Major Accidents: Causal Factors and Improvement Measures Related to Well Control in the Petroleum Industry*. 2013, Society of Petroleum Engineers.
12. Gordon, R.P., *The contribution of human factors to accidents in the offshore oil industry.* Reliability Engineering & System Safety, 1998. **61**(1-2): p. 95-108.
13. Wagenaar, W.A., P.T. Hudson, and J.T. Reason, *Cognitive failures and accidents.* Applied Cognitive Psychology, 1990. **4**(4): p. 273-294.
14. Falck, A., R. Flage, and T. Aven. *Risk assessment of oil and gas facilities during operational phase*. in *Safety and Reliability of Complex Engineered Systems—Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015*. 2015.
15. ISO, I., *31000: 2009 Risk management–Principles and guidelines.* International Organization for Standardization, Geneva, Switzerland, 2009.
16. Vinnem, J.E., *Offshore Risk Assessment*. Springer Series in Reliability Engineering. 2014: Springer London.
17. Lawley, H., *Operability studies and hazard analysis.* Chemical Engineering Progress, 1974. **70**(4): p. 45-56.
18. Scandpower Risk Management, *An assessment of safety, risks and costs associated with subsea pipeline disposals*. 2004: Scandpower , Kjeller, Norway.
19. British Standard, B., *IEC61882: 2002 Hazard and operability studies (HAZOP studies)-Application Guide*. 2002, British Standards Institution.“This British Standard reproduces verbatim.
20. Ericson, C., *Fault Tree Analysis–A History from the Proceeding of the 17th International System Safety Conference*. 1999, Orlando.

21. Ericson, C.A., *Event tree analysis.* Hazard Analysis Techniques for System Safety, 2005: p. 223-234.

22. Stamatis, D.H., *Failure mode and effect analysis: FMEA from theory to execution*. 2003: ASQ Quality Press.

23. de Ruijter, A. and F. Guldenmund, *The bowtie method: A review.* Safety Science, 2016. **88**: p. 211-218.

24. NORSOK Standard Z-013 2001, *Risk and emerency preparedness analysis Rev. 2*. 2001, Norwegian Technology Centre.

25. Størseth, F., R. Rosness, and G. Guttormsen, *Exploring safety critical decision-making.* Reliability, risk and safety: Theory and applications, 2010: p. 1311-1317.

26. Ferdous, R., et al., *Methodology for computer aided fuzzy fault tree analysis.* Process Safety and Environmental Protection, 2009. **87**(4): p. 217-226.

27. Ferdous, R., et al., *Methodology for Computer-Aided Fault Tree Analysis.* Process Safety and Environmental Protection, 2007. **85**(1): p. 70-80.

28. Khan, F.I., R. Sadiq, and T. Husain, *Risk-based process safety assessment and control measures design for offshore process facilities.* Journal of hazardous materials, 2002. **94**(1): p. 1-36.

29. Bartlett, L.M., E.E. Hurdle, and E.M. Kelly, *Integrated system fault diagnostics utilising digraph and fault tree-based approaches.* Reliability Engineering & System Safety, 2009. **94**(6): p. 1107-1115.

30. Khoo, L., S. Tor, and J. Li, *A rough set approach to the ordering of basic events in a fault tree for fault diagnosis.* The International Journal of Advanced Manufacturing Technology, 2001. **17**(10): p. 769-774.

31. Khakzad, N., F. Khan, and P. Amyotte, *Quantitative risk analysis of offshore drilling operations: A Bayesian approach.* Safety science, 2013. **57**: p. 108-117.

32. Abimbola, M., F. Khan, and N. Khakzad, *Dynamic safety risk analysis of offshore drilling.* Journal of Loss Prevention in the Process Industries, 2014. **30**: p. 74-85.

33. Rathnayaka, S., F. Khan, and P. Amayotte, *Accident modeling and risk assessment framework for safety critical decision-making: application to deepwater drilling operation.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of risk and reliability, 2013. **227**(1): p. 86-105.

34. Janbu, A.F. *Safety up to speed: DNV GL takes dynamic risk assessment to the next level*. 2017 [cited 2017 May 25.]; Available from: https://www.dnvgl.com/news/safety-up-to-speed-dnv-gl-takes-dynamic-risk-assessment-to-the-next-level-90820.

35. Khakzad, N., F. Khan, and P. Amyotte, *Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches.* Reliability Engineering & System Safety, 2011. **96**(8): p. 925-932.

36. Abimbola, M., et al., *Safety and risk analysis of managed pressure drilling operation using Bayesian network.* Safety science, 2015. **76**: p. 133-144.

37. Yang, X. and S. Haugen, *Classification of risk to support decision-making in hazardous processes.* Safety Science, 2015. **80**: p. 115-126.

38. Kongsvik, T., et al., *Decisions and decision support for major accident prevention in the process industries.* Journal of Loss Prevention in the Process Industries, 2015. **35**: p. 85-94.

39. Klein, G., *Naturalistic decision making.* Human Factors: The Journal of the Human Factors and Ergonomics Society, 2008. **50**(3): p. 456-460.

40. Endsley, M.R., *Designing for situation awareness: An approach to user-centered design*. 2016: CRC press.

41. Hafver, A., et al., *Maintaining Confidence - Dynamic risk management for enhanced safety.* DNV GL Group Technology and Research Position Paper, 2017.

42. Kalantarnia, M., F. Khan, and K. Hawboldt, *Dynamic risk assessment using failure assessment and Bayesian theory.* Journal of Loss Prevention in the Process Industries, 2009. **22**(5): p. 600-606.

43. Villa, V., et al., *Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry.* Safety Science, 2016. **89**: p. 77-93.

44. Paltrinieri, N., F. Khan, and V. Cozzani, *Coupling of advanced techniques for dynamic risk management.* Journal of Risk Research, 2015. **18**(7): p. 910-930.

45. Meel, A., et al., *Operational risk assessment of chemical industries by exploiting accident databases.* Journal of Loss Prevention in the Process Industries, 2007. **20**(2): p. 113-127.

46. Meel, A. and W.D. Seider, *Real-time risk analysis of safety systems.* Computers & Chemical Engineering, 2008. **32**(4): p. 827-840.

47. Meel, A. and W.D. Seider, *Plant-specific dynamic failure assessment using Bayesian theory.* Chemical engineering science, 2006. **61**(21): p. 7036-7056.

48. Pariyani, A., et al., *Dynamic risk analysis using alarm databases to improve process safety and product quality: Part I—Data compaction.* AIChE Journal, 2012. **58**(3): p. 812-825.

49. Pariyani, A., et al., *Dynamic risk analysis using alarm databases to improve process safety and product quality: Part II—Bayesian analysis.* AIChE Journal, 2012. **58**(3): p. 826-841.

50. Ayello, F., et al., *Quantitive Assessment of Corrosion Probability—A Bayesian Network Approach.* Corrosion, 2014. **70**(11): p. 1128-1147.

51. Bhandari, J., et al., *Risk analysis of deepwater drilling operations using Bayesian network.* Journal of Loss Prevention in the Process Industries, 2015. **38**: p. 11-23.

52. Khakzad, N., *Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures.* Reliability Engineering & System Safety, 2015. **138**: p. 263-272.

53. Khakzad, N., F. Khan, and P. Amyotte, *Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network.* Process Safety and Environmental Protection, 2013. **91**(1): p. 46-53.

54. Koch, G., et al., *Corrosion threat assessment of crude oil flow lines using Bayesian network model.* Corrosion Engineering, Science and Technology, 2015. **50**(3): p. 236-247.

55. Mkrtchyan, L., L. Podofillini, and V.N. Dang, *Bayesian belief networks for human reliability analysis: A review of applications and gaps.* Reliability engineering & system safety, 2015. **139**: p. 1-16.

56. Neil, M., D. Häger, and L.B. Andersen, *Modeling operational risk in financial institutions using hybrid dynamic Bayesian networks.* The Journal of Operational Risk, 2009. **4**(1): p. 3.

57. Kalantarnia, M., F. Khan, and K. Hawboldt, *Modelling of BP Texas City refinery accident using dynamic risk assessment approach.* Process Safety and Environmental Protection, 2010. **88**(3): p. 191-199.

58. Jensen, F.V., *An introduction to Bayesian networks*. Vol. 210. 1996: UCL press London.

59. Khakzad, N., S. Khakzad, and F. Khan, *Probabilistic risk assessment of major accidents: application to offshore blowouts in the Gulf of Mexico.* Natural hazards, 2014. **74**(3): p. 1759-1771.

60. Al-Shanini, A., A. Ahmad, and F. Khan, *Accident modelling and analysis in process industries.* Journal of Loss Prevention in the Process Industries, 2014. **32**: p. 319-334.

61. Paltrinieri, N., et al., *Dynamic procedure for atypical scenarios identification (DyPASI): a new systematic HAZID tool.* Journal of Loss Prevention in the Process Industries, 2013. **26**(4): p. 683-695.

62. Pasman, H.J. and W.J. Rogers, *Risk assessment by means of Bayesian networks: a comparative study of compressed and liquefied H 2 transportation and tank station risks.* international journal of hydrogen energy, 2012. **37**(22): p. 17415-17425.

63. Pasman, H. and W. Rogers, *Bayesian networks make LOPA more effective, QRA more transparent and flexible, and thus safety more definable!* Journal of Loss Prevention in the Process Industries, 2013. **26**(3): p. 434-442.

64. Weber, P., et al., *Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas.* Engineering Applications of Artificial Intelligence, 2012. **25**(4): p. 671-682.

65. Ale, B., et al., *Towards BBN based risk modelling of process plants.* Safety Science, 2014. **69**: p. 48-56.

66. Paltrinieri, N., et al., *Addressing dynamic risk in the petroleum industry by means of innovative analysis solutions.* Chemical Engineering Transactions, 2014. **36**: p. 451-456.

67. Paltrinieri, N., et al., *Dynamic approach to risk management: application to the Hoeganaes metal dust accidents.* Process Safety and Environmental Protection, 2014. **92**(6): p. 669-679.

68. Bobbio, A., et al., *Improving the analysis of dependable systems by mapping fault trees into Bayesian networks.* Reliability Engineering & System Safety, 2001. **71**(3): p. 249-260.

69. Bearfield, G. and W. Marsh. *Generalising event trees using Bayesian networks with a case study of train derailment*. in *International Conference on Computer Safety, Reliability, and Security*. 2005. Springer.

70. Koller, D. and A. Pfeffer. *Object-oriented Bayesian networks*. in *Proceedings of the Thirteenth conference on Uncertainty in artificial intelligence*. 1997. Morgan Kaufmann Publishers Inc.

71. Weber, P. and L. Jouffe, *Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN) ☆.* Reliability Engineering & System Safety, 2006. **91**(2): p. 149-162.

72. Glymour, C., R. Scheines, and P. Spirtes, *Discovering causal structure: Artificial intelligence, philosophy of science, and statistical modeling*. 1987: Academic Press.

73. Glymour, C., et al. *About Tetrad*. 2017 [cited 2017 June 4.]; Available from: http://www.phil.cmu.edu/tetrad/index.html.

74. Hugin. *Main website*. 2017 [cited 2017 June 4.]; Available from: http://www.hugin.com/.

75. Haugen, S., *MIRMAP – Modelling Instantaneous Risk for Major Accident Prevention*. 2017, NTNU Department of Marine Technology: Presentation RAMS Seminar 2017.

76. Bennett, C.C. and K. Hauser, *Artificial intelligence framework for simulating clinical decision-making: A Markov decision process approach.* Artificial intelligence in medicine, 2013. **57**(1): p. 9-19.

77. McGinnis, J.O. and R.G. Pearce, *The great disruption: How machine intelligence will transform the role of lawyers in the delivery of legal services.* 2014.

Appendix A The Safety System

The risk for major accidents in the oil and gas industry is often perceived as reasonably low [3]. The reason for this is the design of a robust system through a layered and independently redundant risk reducing measures. This is a safety system and consists of technical, organizational and operational safety functions designed to either mitigate the likelihood of initiating events, the propagation of the chain of events due to the initiating event or potential consequences [2]. For a blowout, the hydrostatic pressure from the mud column inhibits the unwanted flow of gas into the well bore, the blow out preventer stops the potential sudden influx of gas from reaching the surface and evacuation policies mitigate potential fatalities in case of the BOP fails.

The redundant nature of measures is often referred to as defense in depth and illustrated by the Swiss Cheese Model [7]. The defenses are the safety functions. Single failures can and will occur, but single failures should not be allowed to result in catastrophic events. Major accidents occur when all the safety functions simultaneously and inexplicably fail.

The risk safety system is illustrated in Figure A.1. In this definition, there is an important distinction between initiating events and the top level hazardous event. Initiating events are not considered as a hazardous accident, but may over time and in conjunction with other initiating events eventually lead to a top level hazardous event.

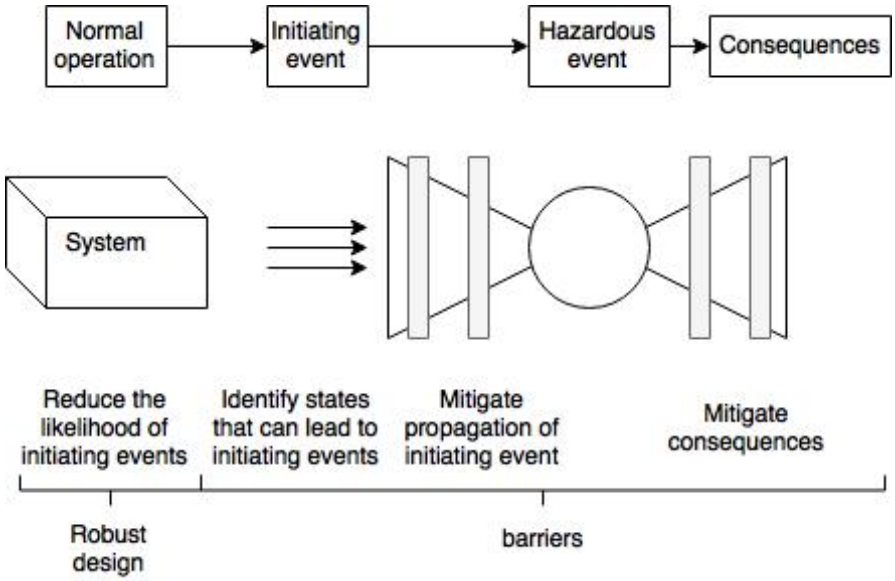

Figure A.1 Representation of the Risk Safety System

Appendix A.1 Robust design

Robust design mitigates the likelihood of initiating events. In other words, robust design ensures operation whereas barrier management restores normal operation in case of an abnormal event. Examples can be:

- Technical design makes it less likely for someone to make a mistake through optimal human-machine interfacing
- Quality material choice for enhanced reliability
- Detailed operation procedures that convey necessary information in a
- Training of personnel in different scenarios and identified possible operational variances that might occur to increase preparedness
- Increased structural integrity

This is not a new term in the risk management world, but is only recently being discussed by authorities such as PSA. Robust design is one of PSAs three goals for 2017 and is currently emphasizing the importance of considering this and encouraging operators to more explicitly consider robustness during planning and risk management. The goals are for operators to better respond to sudden changes or unexpected events.

Appendix A.2 Barrier management

According to a memo issued by the Petroleum Safety Authority (PSA), the purpose of barrier management is to [2]:

"…establish and maintain barriers so that the risk faced at any given time can be handled by preventing an undesirable incident from occurring or by limiting the consequences should such an incident occur. Barrier management includes the processes, systems, solutions and measures, which must be in place to ensure the necessary risk reduction through the implementation and follow-up of barriers."

It is important to recognize that there is a difference between establishing a solution that prevents errors, hazards and accidents from occurring and barriers that are intended to stop errors and hazards from developing into accidents. It does not matter how safely or robust a system is designed; errors, mistakes or slips will occur. Barriers only take affect when this occurs, i.e. during abnormal circumstances, to reduce the development towards an unwanted incident and to mitigate the consequences of the incident should it occur. Barriers are therefore a specific type of risk reducing measures.

Barriers are a hierarchical concept that consists of the overall function and sub-functions such as the barrier's intent, elements such as specific equipment, personnel or operation needed to uphold the function, performance requirements of the elements and performance influencing or shaping factors.

Depending in the barrier function, technical organizational and operational barrier elements are needed. How these different types interact is illustrated in figure A.2.

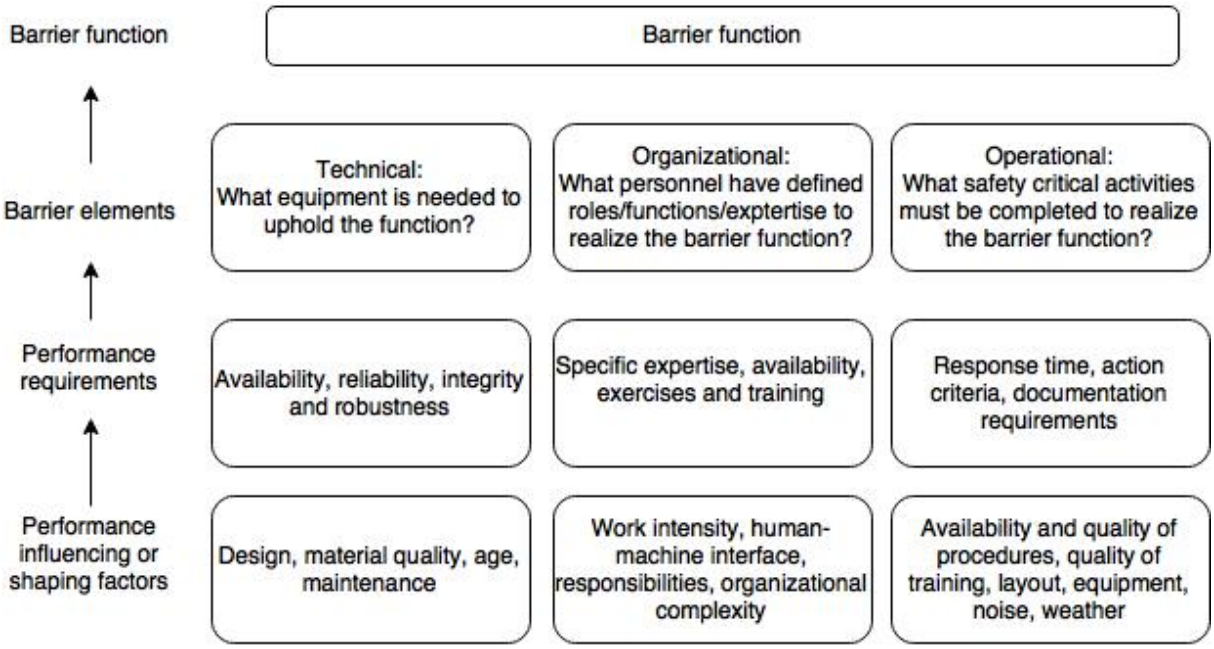

Figure A.2 Illustration of how a barrier function is upheld through the interaction between technical, organizational and operational elements. Adapted from Eltervåg, Hansen [2].

Appendix B Active and Latent Failures

As human error or mistakes are identified as the main underlying causes of major accidents, it is necessary to explore what James Reason calls the latent conditions that allow these errors and mistakes to be made.

James Reason's Swiss Cheese Model is often referred to when describing how the barrier system works in the oil and gas industry, Figure B.1. It illustrates that there are usually several layers of safety functions in place such that no single failure in the safety system can lead to potential losses. In the ideal world, each safety function is perfect such that all hazards are deflected; in reality, safety functions have weaknesses that are represented by the holes. Potential losses occur when the holes perfectly line up creating a viable trajectory. This indicates that for some inexplicable reason the hazard could bypass all safety functions via the ever-present weaknesses. Reason points out that a static image of the model is an inadequate representation. It is best represented by a moving picture where safety functions are continually moving, disappearing and appearing and the holes grows and shrinks. At some point in time the holes will line up allowing an accident trajectory.

The holes in the safety functions are referred to as active failures or latent conditions. Almost every single accident that occurs is can be traced back to a human or organizational mistake as people design manufacture, operate, maintain and manage complex technological systems. Reason divides how people affect the system into active failure on the "sharp end" of the spectrum and latent conditions on the opposite end. Active failures have a direct and immediate effect such as wrongly shutting down a critical safety system as what happened in Chernobyl. However, these are actually the consequences of what Reason calls latent conditions. They are the poorly designed procedures, inadequate man-machine-interface or maintenance failures that lie dormant in the system and can manifest into active failures given the right conditions and enough time. A wrongly perceived complete HAZID can be considered as a latent condition and maintenance done to trigger the accident by closing some valve that had an unknown adverse effect is the active failure. However, latent conditions can be traced deeper into the organization. The managerial decision to restrict the resources available for a more complete HAZID or the failure to use methods or tools that are more capable of identifying hazards are also latent conditions. The hierarchal or layered nature of latent conditions and the pathways they create is illustrated in Figure B.2.

It is reasonable as a measure to ensure compliance and safe behavior to remove the responsible latent conditions. However, they must first be identified.

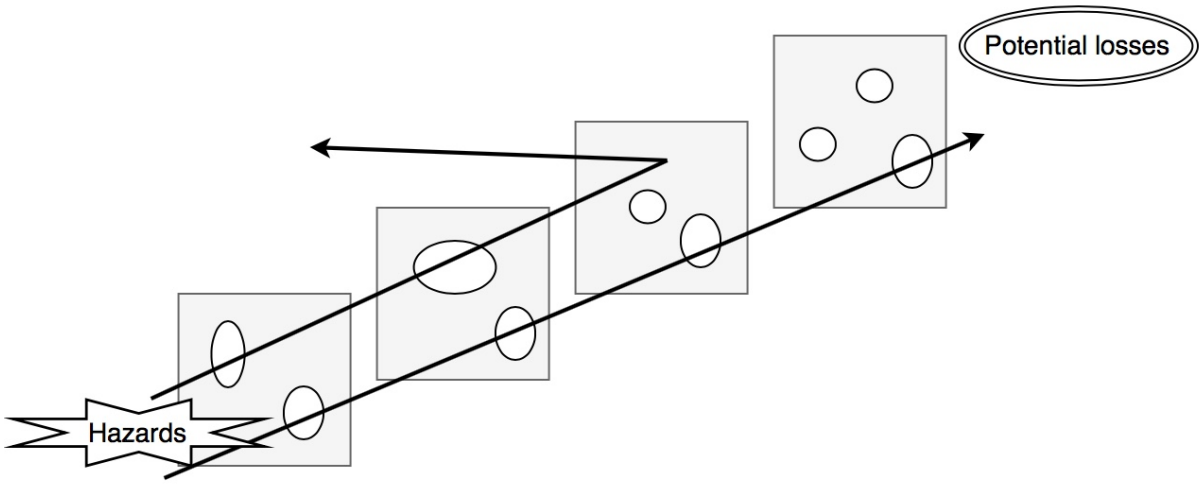

Figure B.1 The Swiss Cheese Model, adapted from Reason [7]

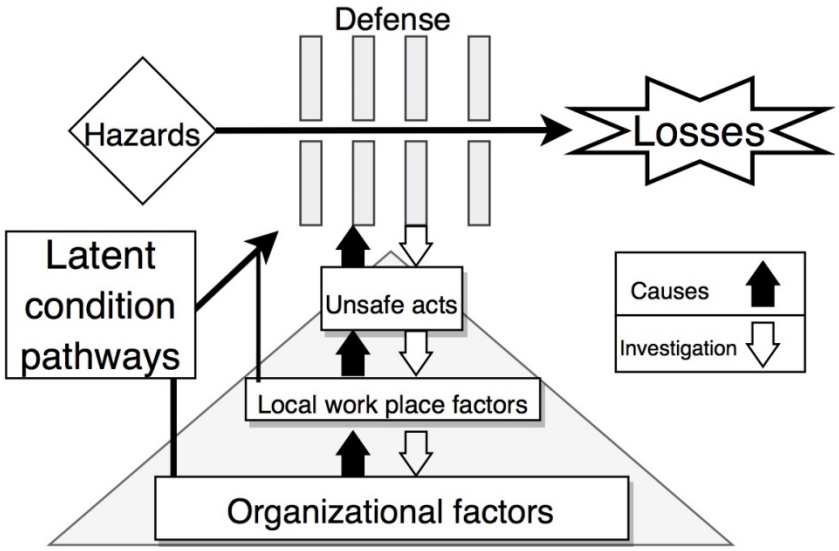

Figure B.2 The hierarchy of latent condition pathways [7]

Appendix C Presentation of the risk picture Norsok Z-013

Excerpt from NORSOK Standard Z-013 2001 [24]

5.6.3.3 Presentation of the risk picture

For the presentation of the risk picture the following requirements apply (if included in the scope):

(a) The main results and conclusions of any risk analysis shall be presented as risk for the activity in question, in accordance with the structure of the risk acceptance criteria (RAC) and for the relevant risk elements. The risk picture shall include
    (1) Ranking of risk contributors,
    (2) Identification of potential risk reducing measures,
    (3) Important operational assumptions/measures in order to control risk

(b) If required, the presentation of risk picture shall include dimensioning accidental loads;

(c) Presentation of possible measures that may be used for reduction of risk and their risk reducing effect;

(d) The analysis shall presented describe accident scenarios relevant for the assessment of the emergency preparedness

(e) Presentation of the sensitivity in the results with respect to variations in input data and crucial premises. The basis for the chosen sensitivity analyses shall be presented;

(f) The results of the QRA shall be traceable though the analysis report. It shall be possible to identify any mechanism/equipment that causes large risk contribution;

(g) Intermediate results shall be presented such that risk contributors can be traced though the report;

(h) Assumptions and premises of importance to the risk assessment results, to decisions related to future project development of with implications to operations/maintenance shall be documented;

(i) Assumptions premises and results shall be presented in a way suitable as input for defining performance requirements for safety and emergency preparedness measures lain later life cycle phases;

(j) Assumptions, premises and results for environmental risk shall be presented in a way suitable as input for the environmental preparedness and response analysis;

(k) All recommendations made in the analysis shall be listed separately with reference to calculations

5.6.3.4 Sensitivity analysis

The following requirements apply:

(a) Sensitivity analyses shall be carried out to include
    (1) Identification of the most important aspects and assumptions/parameters in the analysis
    (2) Evaluation of effects of changes in the assumptions parameters including the effect of any excessively conservative assumptions,
    (3) Evaluation of effects of potential risk reducing measures

(b) The input parameters to be considered for sensitivity analyses should, if relevant, include
    (1) Total manning and personnel distribution,
    (2) Leak frequencies
    (3) Probability of ignition
    (4) Performance (reliability, availability, functionality, etc.) of important barrier functions, systems and/or elements (technical, human and organizational) for personnel, environment and asset risk
    (5) Operational parameters such as the activity levels,
    (6) Environmental resources and their vulnerability
    (7) Spreading of contaminant