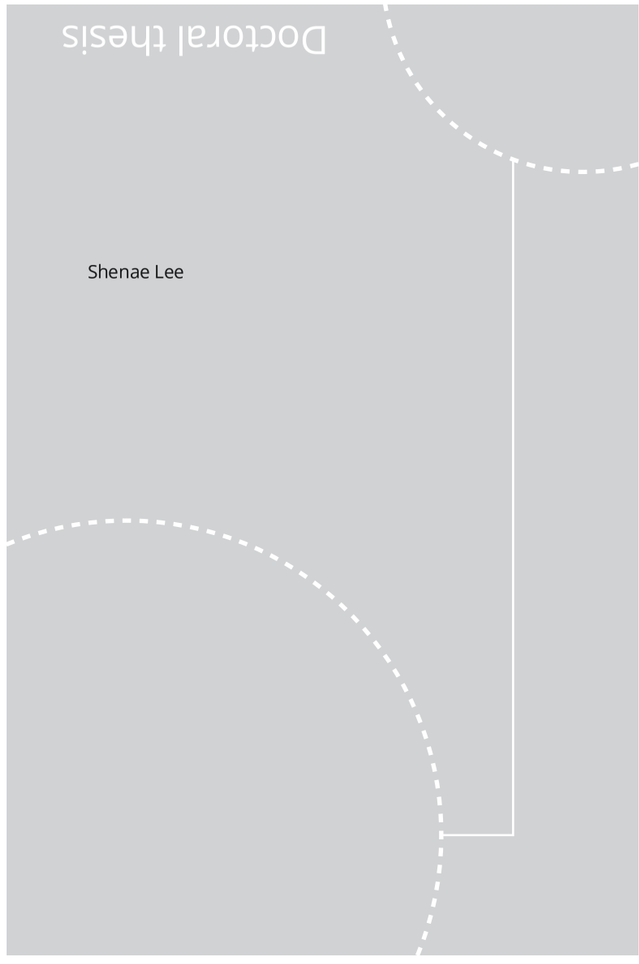
Doctoral theses at NTNU, 2020:134

Shenae Lee

# Safety performance of hazardous systems:

## Approaches to risk estimations for operations and design

Doctoral thesis



Shenae Lee

ISBN 978-82-326-4616-6 (printed ver.)
ISBN 978-82-326-4617-3 (electronic ver.)
ISSN 1503-8181

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology
Thesis for the Degree of
Philosophiae Doctor
Faculty of Engineering
Department of Mechanical and Industrial
Engineering

Doctoral theses at NTNU, 2020:134

NTNU
Norwegian University of
Science and Technology

Shenae Lee

# Safety performance of hazardous systems:

## Approaches to risk estimations for operations and design

Thesis for the Degree of Philosophiae Doctor

Trondheim, May 2020

Norwegian University of Science and Technology
Faculty of Engineering
Department of Mechanical and Industrial Engineering

NTNU
Norwegian University of
Science and Technology

**NTNU**
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Engineering
Department of Mechanical and Industrial Engineering



ISBN 978-82-326-4616-6 (printed ver.)
ISBN 978-82-326-4617-3 (electronic ver.)
ISSN 1503-8181

Doctoral theses at NTNU, 2020:134

Printed by NTNU Grafisk senter

# i. Preface

This thesis is submitted to the Norwegian University of Science and Technology (NTNU) for partial fulfilment of the requirements for the degree of Philosophiae Doctor.

The work was carried out at the Department of Mechanical and Industrial Engineering at NTNU, in Trondheim, Norway. Professor Nicola Paltrinieri from the Department of Mechanical and Industrial Engineering at NTNU and Professor Anne Barros from CentraleSupelec were the supervisor and co-supervisor respectively.

The target audience of this work includes researcher and practitioners interested in the following areas: safety risk assessment and management, barrier management, Oil and Gas and process industry.

## ii. Summary

Safety of chemical and petroleum process installations have received increased legislative and academic attention in most countries, to enhance protection for people from adverse effect of activities involving materials with dangerous properties. This may represent vigilance of current society against the potential for major process accidents such as explosion, fire, and toxic release which may result in fatalities and injuries. Despite knowledge on what characterizes a major accident is enhanced through experiences with past accidents, severe process accidents continue to occur until recently.

This PhD study focuses on the safety challenges associated with the risk contribution from changes in plant design and operations, and suggests advanced methodologies for safety and risk analysis. The models and methods developed aim to support both industry practitioners and risk analysts. Operators of systems handling hazardous materials may confront with difficulties when making safety-related decisions. The cost for risk control and protective measures can be high, and therefore the control measures should be selected based on plant-specific contexts. For this reason, the industry ought to aim for better understanding of risk, instead of focusing on compliance to standards and regulations. However, this is challenging, because event scenarios involving major hazards are rare. This work therefore suggests representative case studies where available information and data are prerequisite for both constructing models and running the model for obtaining results.

The results of this PhD study show how safety can be enhanced by continuous monitoring of safety barrier performance, based on forward-looking risk indicators as well as retrospective risk indicators for Dynamic Risk Analysis. However, modeling works based on Bayesian Networks, Multi-Phase Markov model and Petri Nets can be relatively challenging for a company and their adoption in practical application may still be in question. Thoughtful discussion on uncertainties and sensitivity analyses represent further required works for this research. In addition, operational modes of technical systems and their interaction with human operators should also be addressed in a more integrated manner.

Despite these limitations, the proposed methodologies may provide insights on how to select and apply prevalent techniques of risk analysis in real industry cases. Furthermore, illustrations of the models and approaches in example cases lays the foundations for advances in safety and risk analysis. More importantly, this PhD study is expected to encourage continual learning about risk and safety analysis in the relevant industry sectors.

## iii. Acknowledgments

First, I would like to thank my supervisor, Professor Nicola Paltrinieri from the Department of Mechanical and Industrial Engineering at NTNU, for his patient guidance and dedicated support throughout this PhD study. Nicola's encouragement has been a momentum to finish this PhD.

I am indebted to my co-supervisor Professor Anne Barros from CentraleSupelec. Supervision meetings with Anne were always inspirational and provided me new perspectives on research.

I would like to express my sincere gratitude to Professor Mary Ann Lundteigen from Department of Engineering Cybernetics at NTNU, for her feedback and contribution in improving our papers. I am deeply thankful to her for sharing her personal experience about pursuing PhD.

A special thank you to Professor Yiliu Liu from the Department of Mechanical and Industrial Engineering at NTNU for having me as his course assistant during my master's study and encouraging me to take a PhD.

I am grateful to Professor Hyungju Kim at the Department of Maritime operations at University of South-Eastern Norway, for his help and sincere advice on research and life.

Thank you to my colleagues at the department, Aibo, Ariful, Bahareh, Behnaz, Federico, Elena, Ewa, Giusi, Haavard, Himanshu, Jon Martin, Lin, Liu, Marta, Michael, Nanda, Tom Ivar, Xinge, and Xingheng for our time together at the office and offering me advice.

I am grateful to Renny for his support and encouragement. At times when everything seemed dark, his advice helped me to push myself forward. I am deeply thankful to Lina for her warm thoughts for me. Thank you to Ingri for playing music with me and encouraging me to join Midtnorsk symphony orchestra.

I want to thank my best friend Jiwoo, for sending me hand-written letters from Korea and Australia and having trust in me.

Finally, I must thank my family for their support and encouragement throughout this PhD.

# iv. Table of contents

# v. Figures

## vi. Tables

## vii. Abbreviations

ARAMIS: Accidental Risk Assessment Methodology for Industries

Bayesian Networks: BN

BOP: Blowout Preventer

BORA-release: Barrier and Operational Risk Analysis of hydrocarbon releases

CSA: Canadian Standard Association

DRA: Dynamic Risk Analysis

E/H: Electro-Hydraulic

E: Evidence

EEPE: Electrical / Electronic / Programmable Electronic

EPA: Environmental Protection Agency

ETA: Event Tree Analysis

FPSO: Floating Production Storage and Offloading unit

FT: Function Test

FTA: Fault Tree Analysis

IEC: International Electrotechnical Commission

ISO: International Organization for Standardization

LOPA: Layer Of Protection Analysis

Oil&Gas: Oil and Gas

ORIM: Organizational Risk Influence Model

PFD: Probability of Failure on Demand

PhD: Philosophiae Doctor

PN: Petri Nets

PSA: Petroleum Safety Authority

PSV: Pressure Safety Valve

QRA: Quantitative Risk Assessment

R&D: Research and Development

RB: Risk Barometer

RIF: Risk Influencing Factor

risk-OMT: risk modelling through integration of organizational, human and technical factors

TEC2O: method for the evaluation of technical, operational and organizational aspects

## viii. Thesis structure

This doctoral thesis is written in the format of a collection of articles, commonly known as compilation thesis. The thesis consists of two parts:

Part I, which interrelates the articles and presents the research results in a coherent entity;

Part II, which consists of the articles forming the backbone of this thesis.

The articles are stand-alone and can be read in any order. Although one may prefer to skip Part I and start with reading Part II, I suggest otherwise.

# ix. Publications

This thesis includes the following publications, the full texts of which are presented in Part II:

*Table ix-1 Overview of Articles included in this PhD thesis*

| Article ID | Title |
|---|---|
| Article I | Dynamic assessment of safety barriers preventing escalation in offshore Oil&Gas |
| Article II | Validation of dynamic risk analysis supporting integrated operations across systems |
| Article III | An approach to model risk contribution from periodic testing and maintenance of safety systems |
| Article IV | Modelling hazardous event scenarios for decision support |
| Article V | A new design concept of Blowout Preventer for decision support |

In the following, the details of the articles included in the thesis are presented together with the Authors' contributions.

Article I

Roberto Bubbico, Shenae Lee, Daniel Moscati, Nicola Paltrinieri, **Dynamic assessment of safety barriers preventing escalation in offshore Oil&Gas**, Safety Science, Volume 121, 2020, Pages 319-330.

The authors of this publication are reported in alphabetic order and their contributions are the following.

The second (I) and third authors initiated the research idea. I identified the state of the art and the research gaps on the basis of which I defined the research approach. Under my supervision, the third author developed the Bayesian networks and we presented the results in a meaningful way. The other authors provided feedback on the analysis. I wrote the manuscript and the co-authors supervised the work.

Article II

Shenae Lee, Gabriele Landucci, Genserik Reniers, Nicola Paltrinieri, **Validation of Dynamic Risk Analysis Supporting Integrated Operations Across Systems**, Sustainability, Volume 11, 2019.

The authors' contributions are the following.

I and the second author initiated the research idea. I identified the state of the art and its gaps, I designed and conducted the case study. The second, third and fourth authors provided me with support and expert feedback. I wrote the manuscript and the co-authors supervised the work.

Article III

Shenae Lee, Anne Barros, Mary Ann Lundteigen, Nicola Paltrinieri. **An approach to model risk contribution from periodic testing and maintenance of safety systems**. *(Under review for publication in Journal of Loss Prevention in the Process Industries)*.

The authors' contributions are the following.

I and the second author initiated the research idea. I defined the state of the art and designed the case study under the supervision of the second author. The second author provided relevant feedback on the Multi-phase Markov model. The third author supported with safety function expertise and the last author gave insightful feedback on the modelling. I wrote the manuscript and the co-authors supervised the work.

Article IV

Shenae Lee, Yiliu Liu, Nicola Paltrinieri. 2017. **Modelling hazardous event scenarios for decision support**. 27th European Safety and Reliability Conference ESREL. Ljubljana, Slovenia.

The authors' contributions are the following.

I initiated the research idea together with the other coauthors. I identified the state of the art and its gaps, I designed and run the case study. I wrote the manuscript and the co-authors supervised the work and provided feedback.

Article V:

Shenae Lee, Mary Ann Lundteigen, Nicola Paltrinieri, Yiliu Liu, Magne Rød, John Dale, 2017, **A new design concept of Blowout Preventer for decision support.** 27th European Safety and Reliability Conference ESREL. Ljubljana, Slovenia.

The authors' contributions are the following.

I initiated the research idea. I identified the state of the art and the research gaps on the basis of which I defined the research approach. The second, third and fourth authors provided feedback on the analysis. I wrote the manuscript and the other co-authors supervised the work supporting with valuable comments.

# Part I – Main report

# 1 Introduction

In Europe, enterprises processing or storing a large amount of hazardous substances are obliged to demonstrate that their facility meets the safety requirements in accordance with the Seveso directive III (European Parliament and Council, 2012). Equivalent regulations may be found in other countries, such as the United States and Australia (Rausand, 2011). These directives focus on identifying major accident hazards that pose risk to humans and providing necessary protection against them, to avoid the reoccurrence of severe accidents similar to the past major accidents in industry (Paltrinieri et al., 2012).

The safety and risk analyses required by regulations provide a basis for safety-related decision making. The overall purpose of such analyses addresses the decision on whether existing level of protection is adequate or additional safety functions are needed to reduce the risk to a tolerable level. Required safety functions are performed by technical systems like pressure relieving devices or the remedial actions of operators in dangerous situations (Paltrinieri et al., 2014a). We may refer to them as safety barriers, i.e. any physical or non-physical means planned to prevent, control or mitigate undesired events or accidents (Sklet, 2006). Risk analysis and estimation can be used to determine what types of safety barriers are needed in a specified accident scenario and the desired performance of these barriers.

One of the main challenges in such analyses has been to obtain accurate values for risk estimates, which can arise from the inherent aspect of risk concerning the probability of future events (i.e. unwanted accident events), and their potential consequences (Creedy, 2011). It may therefore be important to learn lessons from the experience of past accidents, and to reflect them in the analyses (Paltrinieri et al., 2019). Furthermore, new design features and operation concepts has enabled increased amount of safety related data collected by enhanced safety management systems (Gran et al., 2012). This implies that it may be possible to collect information related to the factors that contribute to the safety and risk, including, technical degradations, the effectiveness of tests and maintenance, and the operational strategies in the presence of component failures.

Many of the currently adopted approaches in practical applications are not able to capture all these aspects (Paltrinieri and Khan, 2016). In addition, it is of vital importance to establish validity of these methods to support adaptation in the industries (Lee et al., 2019). In this context, this PhD thesis address issues related to aspects of risk based on quantitative analyses approaches. Furthermore, the result of such analyses can be used as a basis for supporting decision-making for design and operation of hazardous systems, to enhance their safety performance throughout its lifespan.

The remainder of Part I of this thesis is organized as follows: Chapter 2 gives an overview of the relevant research background. Section 3 presents the research challenges and questions that form the basis of this study. Section 4 sets forth the research objectives. Section 5 explains the research approach. Section 6 presents the methods used for this study. Section 7 states the contributions from different articles. Section 8 discusses the findings. Finally, conclusions are presented in Section 9.

# 2 Background

The explosion at the Flixborough plant in 1974 and the chemical release at the Seveso plant in 1976 initiated safety legislation in Europe, referred to as the Seveso Directive (European Council, 1996; European Parliament and Council, 2012, 1982; Paltrinieri and Reniers, 2017). The directive was amended and revised following a number of severe process accidents with devasting effects, including the 1984 Bhopal toxic gas release, the 1986 Sandoz fire, the 2001 Toulouse explosion and the 2005 Buncefield explosion (Buncefield Major Incident Investigation Board and Books, 2008; Paltrinieri et al., 2012). Currently, the Seveso iii Directive (European Parliament and Council, 2012) is effective. Moreover, for offshore installations, a notable accident was the fire and explosion at the Piper Alpha platform in 1988. The lessons from the accident investigation (Cullen, 1990) initiated relevant regulatory response in the United Kingdom and in the US. A recent accident with safety implications was the blowout in the Deepwater Horizon rig in 2010 (BP, 2010), which led to safety recommendations and EU directive on offshore safety (Haugen, 2018).

The lessons learned from past accidents enhanced our understanding on what characterizes a major accident. Primary and intermediate causes are typically failures in several important safety barrier, including technical, operational and organizational barriers. Such impediments to the intended safety functions may also arise from the fact that the combination of hazards and hazardous events may be difficult to accurately foresee in a risk analysis stage (Aven, 2007; Paté-Cornell, 1993). In addition, performance of barriers in real operating contexts and in different operational modes may not be considered in conventional risk analysis. For this reason, a detailed level of analysis on possible accident scenarios, as well as to specify performance targets for the safety barriers in such scenario may be necessary, to be capable of supporting decisions on safety and risk problems. This implies that both barrier analyses need to reflect up-to-date risk information, such that the risk estimates are realistic for decision making on costly risk reducing measure.

Quantitative risk analyses are performed to provide the indication on how safe the system will be during a specified operational life. The amount of risk reductions necessary are derived from comparing the estimated risk level with risk acceptance criteria. The gap between estimated level of risk, and the highest

tolerable level of risk is the necessary risk reduction. In relation to quantitative criteria, for instance, the frequency of a specified hazardous event (accident scenario), and potential fatalities needs to be expressed in quantitative terms. The triplet definition of risk, stating that risk is expressed by a set of events, their frequency and consequence spectrum, is useful for this purpose (Kaplan and Garrick, 1981).

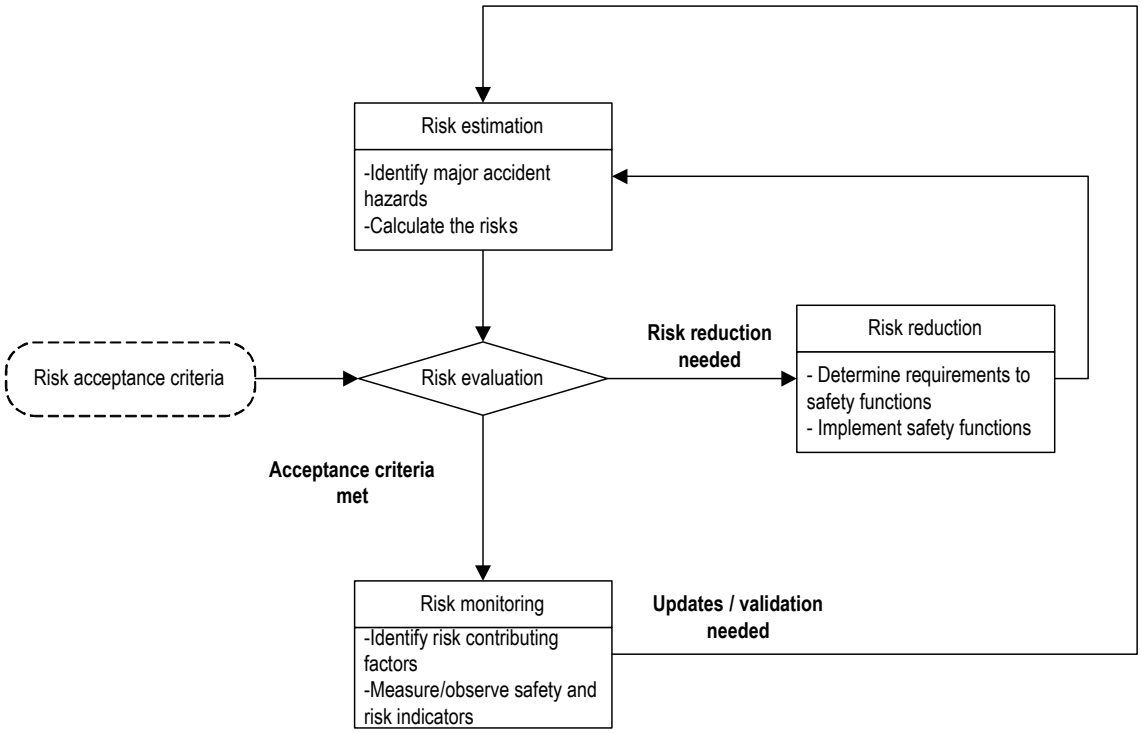



*Figure 2-1 Framework for iteration of safety and risk assessment*

## 2.1 Representative standards and guidelines

Several generic risk management standards and guidelines can be found in literature (Paltrinieri et al., 2013). For instance, the following documents presents practices applied in various fields:

1. ISO 31000 Risk Management Standard (International Organization for Standardization (ISO), 2018);
2. CSA-Q850, Risk Management Guideline for Decision Makers (Canadian Standard Association, 2009);
3. EPA Guidelines for Ecological Risk Assessment (EPA, 1998); and

4. Z-013 Risk and Emergency Preparedness Assessment Standard (NORSOK, 2010).

The analysis of these approaches highlights the lack of a widely accepted universal paradigm, as risk management, more than a self-standing discipline, is still mostly intended as an interdisciplinary field (Paltrinieri et al., 2013). However, some steps are integrated in every risk management model, such as: pre-assessment, risk assessment, tolerability and acceptability judgment, risk management, and risk communication. The treatment of uncertainties is generally addressed, even though the richness of recommendations and practices for treating them varies across the approaches. Finally, constant monitoring is a recurrent step in all risk management models presented above.

The general requirements for QRA in the Norwegian oil and gas industry expressed by the Z-013 standard (NORSOK, 2010) address the identification of hazardous situations and potential accident events, from initiating events to final outcomes. These accident sequences are then to be analyzed to provide an overall picture of risk, presented in a way that is suitable for the various target groups/users and their specific needs and uses. This is aimed at supporting the choice and design of risk-reducing measures, whose performance is required to be monitored and maintained (PSA, 2016).

The Accidental Risk Assessment Methodology for Industries in the context of the Seveso II directive (ARAMIS) (Andersen et al., 2004) provides a guideline to identify the accident scenarios related to the hazardous equipment in a process plant and quantify the associated risk. It was developed with the main objectives to identify a set of reference scenarios in relation to the operations of the selected hazardous equipment. ARAMIS suggests the use of a bow-tie diagram, obtained by a combination of a fault tree and an event tree.

Another important source to consider is the standard for safety instrumented systems for process industry IEC 61511 (IEC, 2016). The standard focuses on safety-related systems based on EEPE (electrical / electronic / programmable electronic) technology, but the quantification approach can also be applied to safety systems based on different technologies. The standard includes guidelines on how to use the Layer

Of Protection Analysis approach and allocate the safety integrity levels. In this case, a safety function is implemented by a protection layer and is intended to achieve or maintain a safe state for the process, with respect to a specified hazardous event. A protection layer may be a technical system or an operator's response to alarm or a corrective action. Possible accident sequence and barrier functions are often represented in a fault tree and an event tree to quantify the probability of event frequency. An important aspect of IEC61511 is the safety lifecycle approach, which encompasses from early design phase to operation and maintenance and requires iteration of analysis on safety function performances.

## 2.2 Approaches for modelling risk during operations

The risk models applied to the design phase QRAs are suitable for reflecting the technical design of an installation. These models, however, have a limited focus on changes in the operating and environmental conditions and their potential impact on risk. As a result, new methods and models have been developed for the quantitative analysis of changes in risk levels, which is referred to as dynamic risk analysis (DRA) in the process industry. DRAs are performed in the operational phase to update the risk level over a certain interval based on operational experiences and field data or predict the risk level for the upcoming period based on precursor data (Landucci and Paltrinieri, 2016).

Numerous representative DRA methods have been developed for safety-critical sectors, and their features are outlined briefly in Table 2.1. These methods extend the existing QRA models by explicitly incorporating organizational and operational factors. They have proved useful in periodic updates of QRA results by reflecting changes in the parameters and assumptions of QRAs. Further developments of these methods employ machine learning techniques (Paltrinieri et al., 2019).

A number of methods for dynamic risk analysis is based on the variation in safety barrier performance (Paltrinieri and Khan, 2016) and it integrates the Bayesian theory for the barrier management and, ultimately, risk assessment. In fact, the use of Bayesian networks for barrier management is a relatively innovative way to evaluate probabilities of possible barrier failures. This approach can take advantage of

model flexibility and possibility to update with new available data. It allows updating barrier probability of failure and, in turn, frequency of outcoming events, based on incidents and near misses occurred within the system (Paltrinieri et al., 2014b). This allows investigating how barrier performance influences the overall level of risk during the lifecycle of the facility, considering the information present in literature and collected by the national authorities.

Within the Norwegian oil and gas sector, the focus of operational risk analysis has been put on developing risk models that can consider Risk influencing factors (RIFs). Examples include the barrier and operational risk analysis of hydrocarbon releases (BORA-release) (Aven et al., 2006; Sklet et al., 2006), and the risk modelling through integration of organizational, human and technical factors (risk-OMT) (Gran et al., 2012). These methods use categories of generic RIFs to modify probabilities in the fault trees. On the other hand, the Organizational Risk Influence Model (ORIM) (Øien, 2001) suggests controlling risk during operation based on organizational indicators.

Table 2.1 Main features of risk analysis used in the design and operations phases

| **Phase** | **Design** | **Operations** | |
|---|---|---|---|
| | | Bayesian updating | RIF and indicator-based approach |
| **Model construction** | Event tree and fault tree | Updating of event tree and fault tree, via updating parameters in the probability distributions | Updating of event probability or important QRA parameters based on quantification of RIFs and indicators |
| **Main advantage** | Well suited for design related decisions related to major accident | Reflecting actual performance and failure causes based on data from operational experience<br><br>Possible to update when new information is collected | Suitable for incorporating the influence of organizational, human and technical factors<br><br>Suitable for using set of indicators (both risk-based and safety performance-based) |
| **Main disadvantage** | Model assumptions made in the design phase can be inadequate | With the absence of data, updating is not possible, and the choice of probability distribution is subjective | Modeling can be complex |

# 3 Research challenges and questions

## 3.1 Risk effects from potential changes in design and operation aspects of facility

Modeling approaches employed in the quantitative risk analysis for design process are suited to give the risk estimates and safety performance measures that are averaged over a long period of time (Aven, 2008; Haugen et al., 2016). During the operational phase, various information related to the factors that influence the risk and safety level of the plant can be collected (Hauge et al., 2015). This may include up-to-date status of barrier, escalation potential associated with a specific hazardous event and dynamic environmental conditions. However, risk contributions from such factors may not be catered for in the approaches to quantify risk commonly used at the design stage.

**Research challenge 1:** *Risk estimates are subjected to vary due to the changes in the operational and technical aspects.*

**Question 1.1:** *What type of methods may be developed to include the key factors that can affect changes in risk level? How do we quantify the effect of these factors? How can we establish the validity of such methods as well and their results?*

**Question 1.2:** *How can we make use of information on actual performance of safety barriers and undesired events that are collected during operations?*

## 3.2 Reliability assessments of safety systems

Major hazards accidents can arise from dangerous deviations and hazardous events that may occur during process plant operations. To reduce major accident risks, the effects of these undesired events may be mitigated by using engineered safety systems which can be added to the process equipment. These safety systems are designed to activate the intended safety functions in response to a specified demand. Periodic testing and maintenance are an important means to detect and correct hidden failures for attaining the desired performance of low-demand safety functions (Jin and Rausand, 2014; Rausand and Høyland, 2003).

The effectiveness of testing and maintenance strategies can be considered in calculation of PFD, by using parameters that express the effectiveness of testing and maintenance, for instance, test coverage (Lundteigen and Rausand, 2008), degradation by testing (Wu et al., 2018), and the impact of different repair policies (Srivastav et al., 2020).

Maintenance activity in a process plant can be hazardous operations that can introduce failures with the potential to cause new types of hazardous events and accident scenarios. This may require reliability models that can reflect important attributes that can influence the performance of safety system, for instance, different failure modes, different testing and maintenance strategies. For example, tests may introduce extra stresses to the system, and maintenance errors may induce dangerous failure modes. These errors are due to manual interventions, especially in relation to the isolation procedure, which is hazardous operation that may lead to a loss of containment.

**Research challenge 2:** *Limited focus is given to the modeling of adverse risk impact of testing and maintenance.*

**Question 2.1:** *How can we determine the testing and maintenance strategies (e.g. interval, maintenance activities) to achieve desired safety function performance?*

**Question 2.2:** *What may be the suitable performance measures with respect to failures during normal operations as well as maintenance?*

## 3.3 Modelling of event sequences based on operational experiences

The initial probability/frequency of hazardous events and accident scenarios may be over-estimated or under-estimated, as it may be practically infeasible to obtain the data directly related to the occurrence of such event. For a plant without enough operational experiences, in particular, the primary estimation for the probability of a potential accident may be based on the approximation of the design and operational features of the plant to the industry average level. It may therefore be necessary to update such probability estimates, based on the additional information on the changes in the design and operation of plant that can

be acquired through operational experiences. This may require a model that is capable of incorporating a set of data from both generic and plant specific sources that is relevant for the causal relations and temporal orders of events in an accident scenario. However, commonly used approaches (e.g. fault tree and event tree analysis) are limited to model readily foreseeable sequence of events, and it may difficult to update such models based on additional information.

**Research challenge 3:** *Standard fault tree and event tree analysis may not be fully suited to update based on operational experiences.*

**Question 3.1:** *If we acquired detailed information about the causal and temporal dependencies between the events in an accident scenario, what approaches can be used?*

**Question 3.2:** *What type of approaches may be suitable to cater for the information collected during operations to obtain updates of risk estimate?*

# 4 Research objectives

## 4.1 Definition of objectives

The main objective of this work is to identify the aspects that can influence the level of risk related to a specified accidents scenario, and to suggest how to reflect these aspects in calculating risk estimates. A particular focus is given to the factors that affects performance of critical safety functions whose failure have major contribution to the risk estimates. Sub-objectives are defined with link to three research challenges in the previous chapter. Each article includes suggested approaches in relation to these objectives that are illustrated in the case study (e.g. research objective 1 is defined in accordance with the research challenge 1).

**Research objective 1.** *Simplify the quantification of possible changes in the estimate for risk level during operations.*

Sub-objective 1.1. Suggest a risk analysis method to measure the change in risk and propose validation approaches to justify the adoption of the suggested methods in practical applications.

Sub-objective 1.2. Suggest an approach based on Bayesian networks, to make use of data related to undesired events and safety barrier performance in the operating stage to update the risk estimates.

**Research objective 2.** Estimate the reliability performance of safety functions.

Sub-objective 2.1 Model the effect of periodic testing and maintenance on dangerous failures and faults in safety system functions.

Sub-objective 2.2 Model the time-dependent behaviors of safety systems and use the model to obtain important performance measures.

**Research objective 3.** *Use operational experiences in the development of event scenarios.*

3.1 Identify causal or temporal sequence among events that constitutes a potential accident scenario, based on the information obtained from past accidents investigations and failure data

3.2 Propose an improved approach to model causal or temporal sequence to support understanding of selected scenarios

## 4.2 Overview of articles and research objectives

Figure 4-1 presents the relationships between the articles and the research objective that are stated in the section 4.1.

Article I and Articles II reflect on the aspects of risk that changes due to the changes in the operating conditions, with a particular focus on the changes in the barrier performances. The event sequence depicted Article I and Articles II are rather simple, since the main focus is not to identify the chain of event in detail but including key causal factors that contributes to the changes in the risk estimate. On the contrary, Article IV, both causal and temporal sequence in the event scenario is modeled on a more detailed level, because the model is based on the accident path that we already know from the investigation report. The main objective is to demonstrate how to model the event sequence leading to the specified hazardous events.

Articles III and Article V are linked to the objective 3, and both the studies include quantification of the influence of periodic testing and maintenance onto the performance of safety systems. The articles suggest analytical formula to calculate reliability performance of safety function. Article III aims to model the time-dependent behavior of safety systems and reliability performance measures during normal operations and the maintenance phase respectively, in order to provide a basis for decision making on testing interval. The case study in Article V is performed in a close collaboration with a company working on an advanced design concept where periodic testing and maintenance frequency, as well as the time spent for testing and maintenance, can be reduced. Modelling of two types of regular testing with different intervals is modelled.

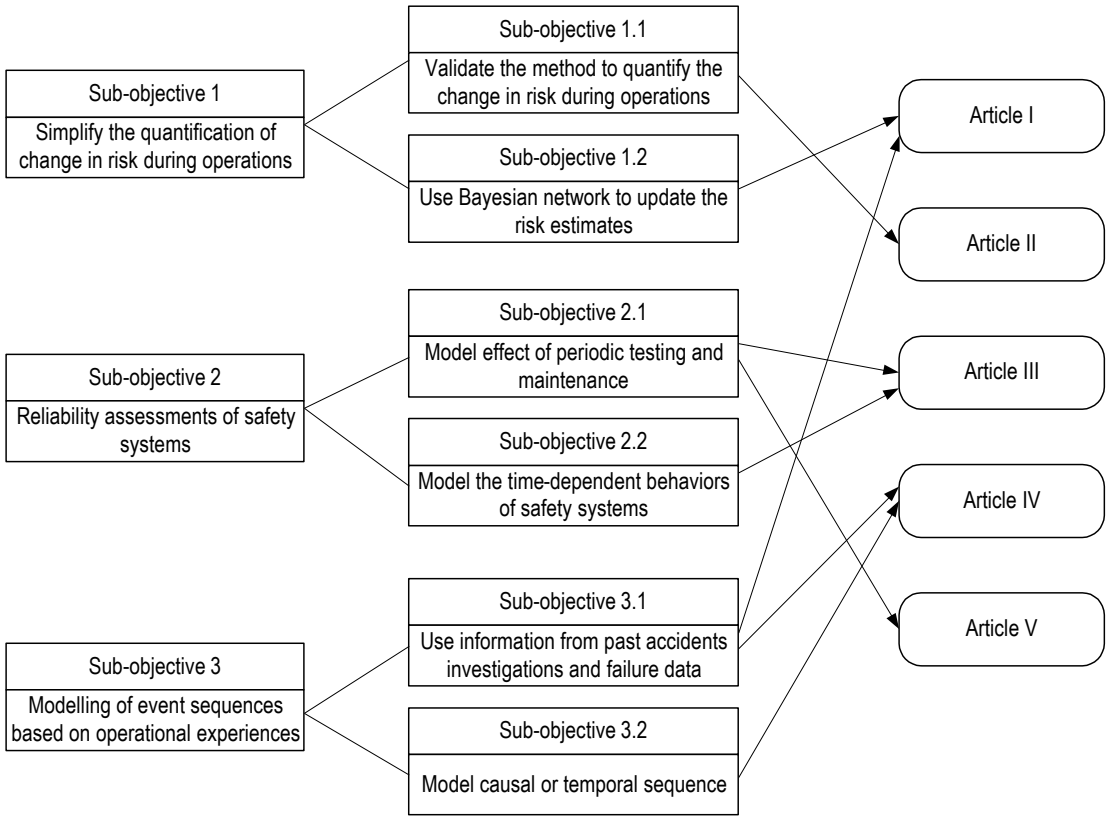



*Figure 4-1 Relationships between the research objectives and the articles*

## 4.3 Research scope

This PhD study aims to improve the approach for estimating the risk associated with major accident hazards related to processes within chemical and petroleum installations. The main objective has been to develop new approaches and/or extend existing ones to treat risk-contributing key factors, taking into account aspects related to design, as well as operations and maintenance. The focus is on obtaining probability estimates, and therefore modeling consequences falls out of the main research scope. In addition, updating acceptance criteria (during the operations) is not explicitly addressed, although it is important in terms of risk control point of view. Finally, underlying and root causes whose quantification is characterized by important uncertainties is not modelled or discussed.

# 5 Research approach

## 5.1 Research classification

Research is defined as a process that acquires new knowledge (Bock and Scheibe, 2001). English verb 'to know' can be translated into French as 'connaitre' or 'savoir'. The word connaitre can be used when describing the familiarity with something, and the word savoir can be used when describing the ability to know how to do something. This PhD study focused on not only methods and concepts within risk analysis field, but also on how to utilize them in the course of conducting research.

The Frascati Manual (Gaillard, 2010) defines three type of research: basic research, applied research, and experimental development.

1. *Basic research* refers to experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts, without any particular application or use in view;
2. Applied research refers to original investigation undertaken in order to acquire new knowledge. It is, however, directed primarily towards a specific, practical aim or objective;
3. Experimental development refers to systematic work, drawing on knowledge gained from research and practical experience and producing additional knowledge, which is directed to producing new products or processes or to improving existing products or processes.

This PhD study can be classified as basic research, and further, into 'oriented basic research'. Oriented basic research is or directed towards some broad fields of general interest, with the explicit goal of a range of future applications. Oriented basic research is carried out with the expectation that it will produce a broad base of knowledge likely to form the basis of the solution to recognized or expected current or future problems or possibilities. Oriented basic research may be distinguished from "pure basic research". Pure basic research is carried out for the advancement of knowledge, without seeking economic or social benefits or making an active effort to apply the results to practical problems or to transfer the results to sectors

responsible for their application. The new approaches developed in this PhD study is expected to form a basis of the solution to the recognized current problems (i.e. challenges related to safety and risk analysis experienced in the industries), without a specific and practical objective as a starting point. This PhD study does not involve experiments, but rather theoretical work that use of existing theories and method to develop new approaches and models to meet the research objectives that are defined thorough this PhD study.

Every R&D activity must meet the following criteria (Gaillard, 2010):

- Novelty criteria – the work should aim at new findings;
- Creativity criteria – the work should be based on original not obvious concepts;
- Uncertainty criteria – the outcome, cost and time allocation should not be known a priori;
- Systematic criteria – the work should be planned and budgeted; and
- Transferability and/or reproducibility criteria – the new knowledge should be transferrable in order to allow other researchers to reproduce the same findings in their R&D activities.

The research activities of this PhD study aimed at meeting the aforementioned criteria. In fact:

- Novelty: different methods for quantifying risk contribution from barrier failures, undesired events, and key causal factors, as well as indicators are aimed at clarifying the safety and risk aspects of hazardous systems that are not well understood by conventional safety and risk analysis. For example, Article V related safety issues associated with new design and operation concepts of BOPs.
- Creativity: each article in this PhD study suggests application of new methods and concepts. For example, Article III propose a safety performance measure during maintenance phase, which is not typically considered, and therefore it provides additional support to decision making.

- Uncertainty: the process and results of the research were uncertain. For instance, during this PhD study, new ideas for utilizing relevant methods were generated, and these work results were not known until the modeling and approaches were completely developed and applied.
- Systematic approach: records of the research progress and relevant outcomes have been collected, categorized, evaluated and published from the very beginning of the PhD to ensure a systematic approach.
- Transferability and/or reproducibility: the research outcomes are published in peer-reviewed journals and conference proceedings where transferability and reproducibility are required as criteria. In addition, the result of Article II on validations approaches adapted for dynamic risk analysis explicitly address this aspect.

## 5.2 Research approach

Research approach is a way to systematically solve the research problem. It is necessary for the researcher to know not only the research methods/techniques but also the overall approach (Kothari, 2004). This PhD study aims to support researchers in their search of methods or techniques, pointing at their relevance and significance. This work contributions allow researchers to understand the assumptions underlying various techniques and the applicability criteria of certain techniques and procedures.

Thus, this work research approach does not only focus on the research methods, but also considers the logic behind the methods and explains the reason for using a particular method or technique, so that the research results represent a generalized lesson for the whole domain.

## 5.3 Quality assurance

A reality check was conducted for some of the works in Table ix-1. This consists in the test on a real case-study of the methods and concepts proposed. This allows for comparison with operating experience of the interested systems.

Expert judgment to examine the research process behind the study was always conducted for the works in Table ix-1. Supervision by the PhD supervisors was constantly sought to assure realistic expectations, detailed documentation and significance in the results.

Independent peer review was received for all the works as they are published in either peer-reviewed journals or peer-reviewed conference proceedings. The people conducting the review are recognized as experts in the considered domain. The comments from these peer-reviewed process have allowed an important improvement in the quality of these works.

# 6 Methods used

The definition of the research approach laid the foundations for an appropriate selection of methods for the study. Methods are here defined as the composition of techniques and/or procedures that are suitable for meeting the research objectives in section 4. The choice of methods and techniques takes also into account the data sets available for this PhD study. The various articles constituting the study use different research methods that are commonly used for risk and reliability analyses. The methods the reason why they were selected are presented in the following – further explanation of the methods is provided by articles I-V.

Article I. Bayesian networks were selected for two main reasons: 1) to make use of recorded failure data, and 2) to model escalation scenarios by exploiting the capability of modelling causal sequence between nodes and including nodes that can have multiple variable states.

Article II. A set of fundamental validation methods (Suokas, 1985) were selected as appropriate validation for DRA is still an unexplored domain: reality check (comparison with operating experience of corresponding installations), benchmark (comparison with a parallel analysis of the same installation or activity), and peer review (examination of the output of the risk analysis by technical experts).

Article III. Multi-phase Markov was selected because: 1) testing and maintenance cannot be modeled by Markov and 2) to describe impact of maintenance errors. In addition, analytical to quantify time-dependent system state probabilities.

Article IV. The use of Petri Nets was selected over the use of fault trees to explicitly model causal and temporal order of set of events in the scenario, for example, to include activities such as inspections, remedial action of operators.

Article V. Petri Nets were selected for reliability assessment to evaluate testing intervals and reach redundancy.

## 6.1 Bayesian Networks

Bayesian networks represent a useful formalism in the risk analysis domain due to their ability to model probabilistic data with dependencies between events (Weber et al., 2012). The Bayes theorem has the advantage to use new evidence to update probabilities of events, for instance, deviations from normal operations, physical phenomena and, in particular, failure of safety barriers in an accident scenario. Prior probability is estimated in several ways, such as statistical analysis of historical data or data collected from inspection/condition monitoring, deductive reasoning by means of quantitative risk analysis techniques, or expert judgment (Khakzad et al., 2016). On the other hand, relevant information used to update prior probabilities become available during operation of the system under consideration , such as deviations from design parameters, near misses, or incidents.

Considering an event $\theta_f$, a safety barrier failure, the prior probability of the event $P(\theta_f)$ , can be updated considering evidence E by using Bayes theorem, as follows:

$$P(\theta_f|E) = \frac{P(\theta_f) \cdot P(E|\theta_f)}{\sum_{\theta_f} P(\theta_f) \cdot P(E|\theta_f)} \quad \text{(Eq. 1)}$$

$P(\theta_f|E)$ is the posterior probability given the evidence E, and the likelihood $P(E|\theta_f)$ (probability distribution of evidence given that $\theta_f$ has occurred). An example evidence can be represented by recorded failures, and the occurrence of an early warning of the safety barrier failure (Paltrinieri et al., 2014b; Scarponi et al., 2016). However, an early warning does not provide complete certainty for barrier failure.

BNs have two types of items to represent the uncertainty of evidence (Fenton et al., 2016):

- virtual evidence that uses the likelihood ratio to represent the uncertainty of evidence; and
- soft evidence that uses likelihood ratio as the target posterior distribution.

However, their distinction is excluded from the scope of this work, which will refer to the more generic term of “uncertain evidence”. Evidence imposed on the events of barrier failure $\theta_f$ and success $\theta_s$ can be specified by the weights $w_f$ and $w_s$ such that:

$$P(\theta_f|E) = w_f; \qquad P(\theta_s|E) = w_s; \qquad w_f + w_s = 1 \qquad \text{(Eq. 2)}$$

Uncertain evidence is implemented in many commercial BN software packages, such as AgenaRisk® (Agena Ltd, 2019). Multiple pieces of evidence, causes and effects are correlated within a single potential accident scenario. A Bayesian network is a graphical model, which describes the causal relationships between a set of variables. The variables are represented as nodes, and the dependence between the two corresponding variables is depicted by an arrow between them, denominated *edge*. A *parent node* has a direct influence on a *child node.* A *root node* has no parent nodes (root cause), while a *leaf node* has no child nodes (final accident outcome). Considering n variables $\theta_i$, such as the sequence of unwanted events and failed safety barriers leading from the root cause $\theta_1$ to a final accident outcome $\theta_{n+1}$, the probability distribution of the final outcome $P(\theta_{n+1})$ is expressed by the chain rule, as follows:

$$P(\theta_{n+1}) = \prod_{i=1}^{n} P(\theta_i|\, Parents\ (\theta_i)) \qquad \text{(Eq. 3)}$$

For this reason, the update based on new evidence of any probability distribution $P(\theta_i)$ along the chain leads to an updated probability distribution of the final outcome.

## 6.2 Validation methods

### 6.2.1 Reality check

Comparison against past accidents and disturbances that occurred in installations similar to the object of study may determine the risk analysis capability of identifying hazards and contributors. Past accident analysis is an extensively employed tool for preliminary hazard identification in chemical and process facilities (CCPS - Center for Chemical Process Safety, 1992). Real incidents and near-miss accidents can be used to assess whether a DRA technique has the capability of identifying complete accident scenarios (Aven and Krohn, 2014; D, 2009).

### 6.2.2 Benchmark

A comparison with other recognized risk analysis methods can be employed to test whether the analysed method is suitable for a specific application area. The activity of benchmarking primarily refers to the comparison of results from the two methods and allows identifying similarities and/or specificities on how the input data are processed. Fundamental aspects are the sensitiveness of the methods with respect to input changes (reflecting operational variations) and the overall conservativeness of their assessment.

### 6.2.3 Peer review

Rosqvist and Tuominen (Rosqvist and Tuominen, 2004) introduce a specific peer review process for formal safety assessment. This addresses the ultimate goal of the peer review of reducing uncertainty, which may be related to completeness, coherence, and accuracy. Coherence within risk assessment objectives and modelling is important, as they are the foundations of the study. Any incompleteness in the previous steps of risk assessment introduces a latent bias in the following steps. Accuracy in the evaluation of prior parameters and the risk index is essential to obtaining the correct definitions of safety barriers and their effect on risk. Incompleteness in the definition of safety barriers may negatively affect the redundancy of safety systems and the total installation safety.

## 6.3 Multi-phase Markov model

A Markov diagram is a state transition diagram that illustrates various system states and possible transitions between the states. In a Markov model, the time evolution of a system is assumed to be a stochastic process that fulfill the Markov property. Dynamic behavior of system (e.g. repair of a component, sequence-dependent failures) can be considered in a Markov model. A Markov analysis can provide range of reliability performance measures (e.g. average proportion of time spent in each state, visit frequency to each state). A Markov analysis is difficult for a system with a large number of states. The assumption that both time to failure and the repair time are exponentially distributed may not be realistic. Classical Markov model is not suitable for modeling periodic tests and maintenance. A system may possess the Markov property only within a certain time frame but does not fulfill the Markov property at different points in time.

For example, the system is subjected to periodic testing and maintenance actions on predefined time points, and the state may change after the execution of these actions. Such a process with the deterministic causes for state transitions may not have time-homogeneous transition probabilities, and thus cannot be modelled by using a standard Markov chain. One reason is that the time period spent for the testing and maintenance represents a different condition than normal operation period, such that the process may have different transition rates. To take this into account, we may use a multi-phase Markov model where we define a finite number of state spaces, so that each state space corresponds to a phased time period (e.g. normal operation period, and maintenance phase), and has its own transition rate matrix (Innal et al., 2016).

## 6.4 Fault tree analysis

A fault tree is constructed through a top-down or deductive reasoning about the potential causes of a specified hazardous event (i.e. the TOP event) (Rausand, 2011). Logic gates are used to connect the TOP event, intermediate casual events, down to primary level causes (i.e. basic events). FTA can be used to investigate the reasons for why a specified hazardous event could occur. FTA provides the combination of technical and human failures in detail. Relative criticality of the basic events (e.g. failures event) can be assessed.

FTA can handle large size systems. Time-dependent features (e.g. maintenance interventions) is difficult to be modelled in FTA. All events in a fault tree have binary states. Multi-states events (e.g. physical states of the hazardous substance) may not be handled. FTA is not suitable for explicit modeling of the temporal order of failures in an event scenario.

## 6.5 Petri Nets

A Petri Net is bipartite graph where two types of nodes, places (states or conditions) and transitions are connected via directed arcs (IEC, 2012; Nivolianitou et al., 2004), which can be used to represent dynamic behaviors of a system. A place can contain a number of tokens. A change in the distribution of tokens in a Petri Net represent a change in the system state. A Petri Net allows for detailed modelling of dynamic

system behaviours. A Petri Net can model both stochastic events and events that occur at a deterministic time. Specific conditions for state changes can defined, to model an event scenario in a particular causal or temporal order, including the possibility to model cascading failures.

# 7 Main results

## 7.1 Contribution to objective 1

### 7.1.1 Sub-objective 1.1. Validation of risk estimates obtained during operations

Dynamic risk analysis (DRA) refers to models and methods that have capability to capture changes in technical and operational aspects during the operational phase, and to quantify their effect on risk. DRA is expected to solve some of safety challenges by supporting decisions related to risk control, which cannot be supported by conventional risk analysis. However, DRA models and methods have not been extensively adopted and limited attention is given to establish their validity in practical applications.

Article II chose a DRA method denominated as Risk Barometer (RB) and a relevant case study. RB is an indicator-based method, and the change in risk is derived from measurement of indicators, as illustrated in Figure 7-1. Three validation methods are suggested to illustrate how validity can be established for DRA methods: i) reality check, ii) benchmark, and iii) peer review. The benefits of the suggested methods are the completeness and quality of the evaluation. The effectiveness was demonstrated by a specific validation study: the application of RB on a case study on sand erosion integrity in a virtual oil and gas cluster including a FPSO unit. The results from a past accident analysis confirmed the criticality of erosion/corrosion scenarios, as identified by the RB. Moreover, the dynamic nature of the event, which legitimizes the use of dynamic tools such as RB, was highlighted. The benchmark evaluation showed excellent conformity within the results from the RB and TEC2O (method for evaluation of technical, operational and organizational) factors, which validates the applicability of the RB indicators for the event with a loss of containment. A specific procedure for peer review that involves experts from the industrial domain confirmed the suitability of the RB in actual field applications.

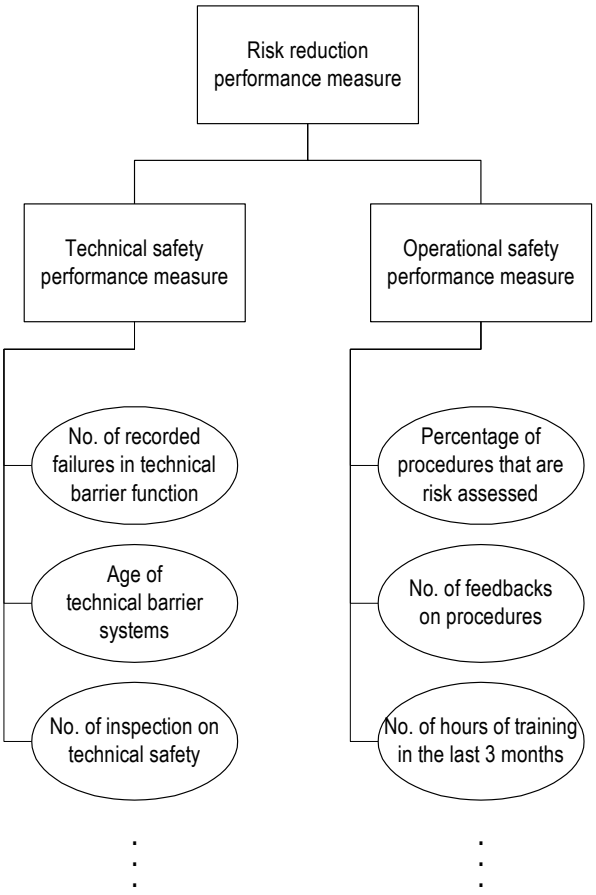



*Figure 7-1 Illustration of possible indicator set*

### 7.1.2 Sub-objective 1.2. Use of Bayesian network for risk estimation update

Oil&Gas activities in the arctic and subarctic regions are high risk operations, due to the several challenges related to the harsh where it is important protect sensitive environment from any adverse impact of petroleum activities, and therefore retaining a persistent high focus on the safety and risk management is important. For this reason, Bayesian Networks and safety barrier assessment is suggested, to be capable of regularly iterating dynamic risk assessment to support risk management of critical systems. The method is applied to the potential escalation scenario arising from leaks of different sizes on a Norwegian Oil&Gas production platform located in the Barents Sea. Risk data on the Norwegian petroleum activities are used as evidence to simulate continuous update of risk assessment throughout the years. The case study showed the benefits and limitations of such an approach. Accurate modelling of potential accident scenarios is

possible through BNs, but time-consuming. The approach allows for drill-down capabilities, which enhance support of operations and definition of risk mitigating measures. However, the data used for dynamic risk assessment has a pivotal role, as data quality and quantity may sensibly affect the outcome. Fortunately, the Oil&Gas industry is generally committed to improving collection of field data for the assessment of safety barrier performance. Finally, it must be mentioned that this approach represents a potential response to "pulses of risk", in which system deviations and resilient reactions are processed by iteration of dynamic risk management for an effective strategy controlling risk in critical cases, such as Oil&Gas production in the arctic and sub-arctic regions.

## 7.2 Contribution to objective 2

### 7.2.1 Sub-objective 2.1 Inclusion of the effect of periodic testing and maintenance on dangerous failures and faults in safety system functions

In Article V, two types of periodic testing are modelled in reliability quantification of Blowout Preventer (BOP) system. All BOP systems today are operated with Electro-Hydraulic (E/H) controls, and the record shows high number of failures and malfunctions involving hydraulic components (e.g. leakages). The current BOP systems require two types of regular tests, and Function Test (FT) is required to be carried out every 7 days - 21 days. Failures of BOP systems have made significant contributions to non-productive time of drilling rigs. This paper introduces a new concept of electro-mechanically operated BOP, which seems to be a candidate to improve reliability and availability of the BOP. The main interest of this paper is to shed light on the new features of the electrical BOP system versus current art qualitatively. In addition, this contribution proposes a quantitative method for obtaining the BOP availability analysis which may be used in the decision-making about designing optimal BOP systems.

In Article III, a model that can include two main types of failures of low-demand safety systems is developed. An illustrative case of PSVs that are subjected to periodic maintenance in the offshore plants, are used. Periodic testing and maintenance for PSVs are carried out on a regular basis to ensure the desired performance of risk reduction during normal operations phases (Okoh et al., 2016). As opposed to this, the

errors made during the maintenance phases of PSVs are claimed to be a key causal factor to introduce additional risk). The failures that can be caused by the errors in the maintenance interventions (i.e. external leakages), are distinguished from the random failures during normal operation (i.e. failure to open on demand). The main focus is to describe and quantify the negative effect of maintenance action on the system states, based on Multi-Phase Markov model (ISO/TR12489, 2013; Rausand, 2014). The main focuses are 1) to include failure events and faults of the safety systems induced by maintenance 2) to express the probability of maintenance errors in terms of transition probabilities 3) to calculate the time-dependent state probabilities of the safety system. The focus of a modeling approach to quantify the influence of periodic testing and maintenance onto the system states.

### 7.2.2 Sub-objective 2.2 Modelling of time-dependent behaviors of barriers, and use of the model to obtain important performance measures

In Article III, specific analytical formulas are suggested to obtain the frequency of hazardous events (i.e. external leakage) which can serve as a performance indicator of major risks. In addition, a commonly used reliability measure, the mean PFD of the main safety function is obtained. The major benefit of attaining these two performance measures is to enable risk-informed decision-makings regarding 1) the length of interval between the two periodic testing and maintenance 2) the improvement in human and organizational factors in maintenance activity. Further improvement may be to consider regarding the time delays in maintenance interventions, for example, due to delayed repair, by extending the model with additional phases.

## 7.3 Contribution to objective 3

### 7.3.1 Sub-objective 3.1 Modelling of scenario based on the information obtained from past accidents investigations and failure data

Quantifying the probability of hazardous events is an important step to achieve the overall risk estimate, and the reasonable value for probability estimate desired. For this reason, Petri Nets are selected to explicitly

model causal and temporal sequence as a tool to calculate a hazardous event frequency based on simulation. From the fact that we are interested in modeling the accident path that we already know, Petri Nets can be more suitable. The model includes two possible initiating events, and important safety barriers including operator activities.

### 7.3.2 Sub-objective 3.2 Improved approach to model causal or temporal sequence to support understanding of selected scenarios

The analysis focuses on one of the most critical accident scenarios for an offshore platform with limited space for escape (Bucelli et al., 2018): the scenario of escalation due to fire in the process area. Bayesian networks theory is implemented to calibrate and update the scenario frequency during the years by means of the AgenaRisk® software (Agena Ltd, 2019). The escalation initiating event considered within the Bayesian network is the hydrocarbon leak. Such event is particularly important for the Goliat platform located in the Barents Sea due to the environmental impact it may lead to, even without ignition. Moreover, information on hydrocarbon leaks are relatively available on scientific literature, as it is possible to rely on a considerable amount of data (Fossan and Opstad, 2016), while escalations are rare events for which probabilistic analysis is challenging. For this reason, modelling escalation from leak events may be beneficial.

# 8 Discussion and further works

## 8.1 Discussion to objective 1

DRA models tend to focus on specific cases that are usually associated with major hazard scenarios not adequately modeled in conventional technical QRAs for the design phase. The reason may be that the information related to such scenarios may not be sufficient, or due to the aspects that change with time during the operational phase. DRA models and methods arise from the need for providing updates on risk level during operations, and therefore use of simplified scenario modelling rather than complex one as suggested in the Article I, and Article II seems pragmatic. In this way, more amount of available data and information of different type can be utilized for updating. Article I uses observations (e.g. barrier failure record, leak event record) to directly update the node probabilities in the constructed Bayesian network. On the other hand, Article II uses information related to risk changes, derived from a suggested set of indicators, and this implies that the relation between the indicator and barriers may not be direct. For this reason, the suggested validation approaches are important, especially for the approaches to be adopted in the practical applications. This allows building consensus and trust in DRA techniques, as they represent a concrete solution for the implementation of integrated and safety-supported operations across the geographical, organizational and disciplinary boundaries of the oil and gas industrial systems.

## 8.2 Discussion to objective 2

Aven (Aven, 2017) affirms that reliability assessments can be viewed as a special type of risk assessment where the consequence are linked to technical system failures. Safety and reliability assessments are performed to support decisions related to design and operation of safety systems. Testing and maintenance in general enhance the reliability of safety functions, such that the probability of accidents can be reduced. However, it is also important to lessen the negative impact of maintenance, such as the introduction of additional failures and occurrence of accident during maintenance (Aven, 2008). In both Article III and Article V, particular focus is given to the effect of periodic testing and maintenance, but with different

practical implications. The quantification model in Article V is limited to the effect of two types of testing onto a typical safety performance function (PFD) of a safety barrier, while Article III suggests two performance measures, in normal operation and maintenance respectively. Article V focuses on the design features of safety barrier systems, as a key influence factor of the safety function performance. On the other hand, Article III focuses on the maintenance error made by operators, as a main contributor to the adverse risk impact.

## 8.3 Discussion to objective 3

Case study in Article IV is performed based on thorough reviews on the literatures related to the Buncefiled accident (Buncefield Major Incident Investigation Board and Books, 2008), which resulted from a tank overfilling scenario. In other words, we already know the chain of events that we want to model. By using Petri Nets, we may support decision making related to such scenario. For example, maintenance resources in a site are expected to be limited (e.g. fewer operators) in the next month due to the holiday season. The manager decides to extend the inspection interval and wants to understand how this decision influences the frequency of hazardous event. This can be simulated by changing input parameter or minor modifications in the initial Petri Nets. On the other hand, the BN based model in Article I has different updating regimes and is based on observations and knowledge that have gained through operations. This enables iteration and continuous updates whenever relevant data is made available, implying that such BN-based method may be used to monitor risk trend in a designated period.

# 9 Conclusions

The models and methods proposed in this work are intended to benefit both industry practitioners and risk analysts. Operators (management) of hazardous systems in their facilities at hand may confront with difficulties of making safety-related decisions against major accidents hazards. The cost for risk control and protective measures can be high, and therefore the control measures should be selected based on plant-specific operations contexts. This implies that screening of (unwanted) events that are not relevant for the safety of the individual plant is very important, and this should be well reflected in long-term risk analyses, as well as daily risk registers. In other words, the industries ought to aim for better understanding of risk, instead of focusing on compliance to standards and regulations. However, this is challenging, because event scenarios involving major hazards are rare. We therefore suggest representative case studies where available information and data are prerequisite for both constructing models and running the model for obtaining results.

The overall implications for industry, regarding the methods and models that were developed in the course of this PhD study, were that engineers and managers can enhance safety by continuous monitoring of their safety performance. This may be based on forward-looking risk indicators as well as retrospective risk indicators for Dynamic Risk Analysis. However, more advanced modelling based on Bayesian Networks, Multi-Phase Markov process and Petri Nets can be relatively challenging for a company. Moreover, this PhD study is not initiated from particular safety issues or a decision context in mind. Especially, as the considered models are focused on probabilities and frequencies, without any quantitative analysis on consequences. This, thus, does not provide a full risk picture. For this reason, adoption of such models in practical application is still in question.

Thoughtful discussion on uncertainties as well as constructed sensitivity analyses are activities that are still required for this research. In comparison to reliability modeling, especially in the field of safety-instrumented systems, the level of detail is not in high resolution. For instance, different operational modes of equipment and safety barriers, component failures, and their degradations are not comprehensively

treated. In addition, the interaction between the technical systems and the human operators, and cognitive aspects of human operators should also be addressed in a more integrated manner.

Despite these limitations, the proposed approaches may provide insights on how to select and apply prevalent techniques of risk analysis in real industry cases. Furthermore, illustrations of the models and approaches in example cases lays the foundations for advances in safety and risk analysis. More importantly, this PhD study is expected to encourage continual learning about risk and safety analysis in the relevant industry sectors.

# References

Agena Ltd, 2019. agenarisk.com, AgenaRisk. Cambridge, United Kingdom.

Andersen, H., Casal, J., Dandrieux, A., Debray, B., De Dianous, V., Duijm, N.J., Delvosalle, C., Fievez, C., Goossens, L., Gowland, R.T., Hale, A.J., Hourtlous, D., Mazzarotta, B., Pipart, A., Planas, E., Prats, F., Salvi, O., Tixier, J., 2004. ARAMIS - Accidental Risk Assessment Methodology for Industries in the Context of the SEVESO II Directive.

Aven, T., 2017. Improving the foundation and practice of reliability engineering. Proc. Inst. Mech. Eng. Part O J. Risk Reliab. https://doi.org/10.1177/1748006X17699478

Aven, T., 2008. A semi-quantitative approach to risk analysis, as an alternative to QRAs. Reliab. Eng. Syst. Saf. 93, 790–797. https://doi.org/10.1016/j.ress.2007.03.025

Aven, T., Krohn, B.S., 2014. A new perspective on how to understand, assess and manage risk and the unforeseen. Reliab. Eng. Syst. Saf. 121, 1–10.

Aven, T., Sklet, S., Vinnem, J.E., 2006. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). Part I. Method description. J. Hazard. Mater. 137, 681–691.

Bock, P., Scheibe, B., 2001. Getting It Right. Academic Press, Cambridge, Massachusetts.

BP, 2010. Deepwater Horizon Accident Investigation Report, Internal BP Report.

Bucelli, M., Landucci, G., Haugen, S., Paltrinieri, N., Cozzani, V., 2018. Assessment of safety barriers for the prevention of cascading events in oil and gas offshore installations operating in harsh environment. Ocean Eng. 158, 171–185. https://doi.org/10.1016/J.OCEANENG.2018.02.046

Buncefield Major Incident Investigation Board, Books, H.S.E., 2008. The Buncefield Incident 11 December 2005: The Final Report of the Major Incident Investigation Board. HSE Books, Bootle, UK.

Canadian Standard Association, 2009. CSA Q850 Risk Management: Guideline for Decision-Makers.

Toronto, Canada.

CCPS - Center for Chemical Process Safety, 1992. Guidelines for hazard evaluation procedures, 2nd (with. ed. American Institute of Chemical Engineers - Center of Chemical Process Safety, New York, NY.

Creedy, G.D., 2011. Quantitative risk assessment: How realistic are those frequency assumptions? J. Loss Prev. Process Ind. 24, 203–207. https://doi.org/http://dx.doi.org/10.1016/j.jlp.2010.08.013

Cullen, L., 1990. The Public Inquiry into the Piper Alpha Disaster - Volume I and II. London.

D, S., 2009. Dragon-Kings, Black Swans and the Prediction of Crises. ETH Zurich, Chair of Systems Design.

EPA, 1998. Guidelines for ecological risk assessment. EPA/630/R095/002F. U.S. Environmental protection agency, Risk Assessment Forum, Washington, DC.

European Council, 1996. Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances. Off. J. L 10, 13–33.

European Parliament and Council, 2012. Directive 2012/18/EU of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC - Seveso III. Off. J. Eur. Union 1–37.

European Parliament and Council, 1982. Council Directive 82/501/EEC of 24 June 1982 on the major-accident hazards of certain industrial activities. Off. J. Eur. Union 1–18.

Fenton, N., Neil, M., Lagnado, D., Marsh, W., Yet, B., Constantinou, A., 2016. How to model mutually exclusive events based on independent causal pathways in Bayesian network models. Knowledge-Based Syst. 113, 39–50. https://doi.org/10.1016/J.KNOSYS.2016.09.012

Fossan, I., Opstad, A.S., 2016. Process leak for offshore installations frequency assessment model - PLOFAM. Bergen, Norway.

Gaillard, J., 2010. Measuring Research and Development in Developing Countries: Main Characteristics and Implications for the Frascati Manual. Sci. Technol. Soc. 15, 77–111. https://doi.org/10.1177/097172180901500104

Gran, B.A., Bye, R., Nyheim, O.M., Okstad, E.H., Seljelid, J., Sklet, S., Vatn, J., Vinnem, J.E., 2012. Evaluation of the Risk OMT model for maintenance work on major offshore process equipment. J. Loss Prev. Process Ind. 25, 582–593.

Hauge, S., Okstad, E., Paltrinieri, N., Edwin, N., Vatn, J., Bodsberg, L., 2015. Handbook for monitoring of barrier status and associated risk in the operational phase. SINTEF F27045. Center for Integrated Operations in the Petroleum Industry, Trondheim, Norway , Norway.

Haugen, S., 2018. Safety in Offshore Platforms—Use of QRA in the Norwegian Offshore Industry. https://doi.org/10.1016/bs.mcps.2018.05.001

Haugen, S., Edwin, N.J., Vinnem, J.E., Brautaset, O., Nyheim, O.M., Zhu, T., Tuft, V.L., 2016. Activity-based risk analysis for process plant operations. Inst. Chem. Eng. Symp. Ser. 2016-Janua.

IEC, 2016. IEC 61511 Functional safety - Safety instrumented systems for the process industry sector. International Electrotechnical Commission, Geneve, Switzerland.

IEC, 2012. IEC 62551 Analysis techniques for dependability - Petri net techniques. Geneve, Switzerland.

Innal, F., Lundteigen, M.A., Liu, Y., Barros, A., 2016. PFDavg generalized formulas for SIS subject to partial and full periodic tests based on multi-phase Markov models. Reliab. Eng. Syst. Saf. 150, 160–170. https://doi.org/10.1016/J.RESS.2016.01.022

International Organization for Standardization (ISO), 2018. Risk Management. ISO 31000:2018.

Jin, H., Rausand, M., 2014. Reliability of safety-instrumented systems subject to partial testing and common-cause failures. Reliab. Eng. Syst. Saf. 121, 146–151.

Kaplan, S., Garrick, B.J., 1981. On The Quantitative Definition of Risk. Risk Anal. 1, 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

Khakzad, N., Yu, H., Paltrinieri, N., Khan, F., 2016. Reactive Approaches of Probability Update Based on Bayesian Methods, in: Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application. pp. 51–61. https://doi.org/10.1016/B978-0-12-803765-2.00005-6

Kothari, C., 2004. Research methodology: methods and techniques, New Age International. https://doi.org/http://196.29.172.66:8080/jspui/bitstream/123456789/2574/1/Research%20Methodology.pdf

Landucci, G., Paltrinieri, N., 2016. Dynamic evaluation of risk: From safety indicators to proactive techniques. Chem. Eng. Trans. 53. https://doi.org/10.3303/CET1653029

Lee, S., Landucci, G., Reniers, G., Paltrinieri, N., 2019. A validation approach for dynamic risk analysis techniques. Saf. Sci. (In Press.

Lundteigen, M.A., Rausand, M., 2008. Partial stroke testing of process shutdown valves: How to determine the test coverage. J. Loss Prev. Process Ind. 21, 579–588.

Nivolianitou, Z.S., Leopoulos, V.N., Konstantinidou, M., 2004. Comparison of techniques for accident scenario analysis in hazardous systems. J. Loss Prev. Process Ind. 17, 467–475. https://doi.org/http://dx.doi.org/10.1016/j.jlp.2004.08.001

NORSOK, 2010. Risk and emergency preparedness assessment. Z-013. Oslo, norway, Norway.

Øien, K., 2001. A framework for the establishment of organizational risk indicators. Reliab. Eng. Syst. Saf. 74, 147–167. https://doi.org/10.1016/S0951-8320(01)00068-0

Paltrinieri, N., Comfort, L., Reniers, G., 2019. Learning about risk: Machine learning for risk assessment. Saf. Sci. 118, 475–486. https://doi.org/https://doi.org/10.1016/j.ssci.2019.06.001

Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M., Cozzani, V., 2012. Lessons Learned from Toulouse and Buncefield Disasters: From Risk Analysis Failures to the Identification of Atypical Scenarios Through a Better Knowledge Management. Risk Anal. 32. https://doi.org/10.1111/j.1539-6924.2011.01749.x

Paltrinieri, N., Hauge, S., Albrechtsen, E., 2013. Risk management models in an integrated operations context, in: Transactions of the American Nuclear Society. pp. 1854–1857.

Paltrinieri, N., Hauge, S., Dionisio, M., Nelson, W.R., 2014a. Towards a dynamic risk and barrier assessment in an IO context, in: Safety, Reliability and Risk Analysis: Beyond the Horizon - Proceedings of the European Safety and Reliability Conference, ESREL 2013.

Paltrinieri, N., Khan, F., 2016. Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application, 1st ed, Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application. Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-803765-2.01001-5

Paltrinieri, N., Khan, F., Amyotte, P., Cozzani, V., 2014b. Dynamic approach to risk management: Application to the Hoeganaes metal dust accidents. Process Saf. Environ. Prot. 92. https://doi.org/10.1016/j.psep.2013.11.008

Paltrinieri, N., Reniers, G., 2017. Dynamic risk analysis for Seveso sites. J. Loss Prev. Process Ind. 49. https://doi.org/10.1016/j.jlp.2017.03.023

PSA, 2016. Trends in risk level in the petroleum activity (RNNP) [WWW Document]. URL http://www.psa.no/about-rnnp/category911.html

Rausand, M., 2011. Risk assessment - theory, methods and applications, Statistics in practice. https://doi.org/10.1093/ntr/nts290

Rausand, M., Høyland, A., 2003. System reliability theory: models, statistical methods, and applications. John Wiley & Sons.

Rosqvist, T., Tuominen, R., 2004. Qualification of Formal Safety Assessment: an exploratory study. Saf. Sci. 42, 99–120. https://doi.org/10.1016/S0925-7535(03)00005-5

Scarponi, G.E., Paltrinieri, N., Khan, F., Cozzani, V., 2016. Reactive and Proactive Approaches: Tutorials and Example, in: Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application. https://doi.org/10.1016/B978-0-12-803765-2.00007-X

Sklet, S., 2006. Safety barriers: Definition, classification, and performance. J. loss Prev. Process Ind. 19, 494–506.

Sklet, S., Vinnem, J.E., Aven, T., 2006. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). Part II: Results from a case study. J. Hazard. Mater. 137, 692–708.

Srivastav, H., Barros, A., Lundteigen, M.A., 2020. Modelling framework for performance analysis of SIS subject to degradation due to proof tests. Reliab. Eng. Syst. Saf. 195, 106702.

Suokas, J., 1985. On the reliability and validity of safety analysis. ampere University of Technology, Tampere, Finland.

Weber, P., Medina-Oliva, G., Simon, C., Iung, B., 2012. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Eng. Appl. Artif. Intell. 25, 671–682. https://doi.org/http://dx.doi.org/10.1016/j.engappai.2010.06.002

Wu, J., Wu, C., Cao, S., Or, S.W., Deng, C., Shao, X., 2018. Degradation data-driven time-to-failure prognostics approach for rolling element bearings in electrical machines. IEEE Trans. Ind. Electron. 66, 529–539.

# Part II – Articles

# Article I

Roberto Bubbico, Shenae Lee, Daniel Moscati, Nicola Paltrinieri, **Dynamic assessment of safety barriers preventing escalation in offshore Oil&Gas**, Safety Science, Volume 121, 2020, Pages 319-330.

Safety Science 121 (2020) 319–330

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

# Dynamic assessment of safety barriers preventing escalation in offshore Oil&Gas

Roberto Bubbico[a], Shenae Lee[b], Daniel Moscati[a], Nicola Paltrinieri[b,*]

[a] Department of Chemical, Materials and Environmental Engineering, "Sapienza" University, Rome, Italy
[b] Department of Mechanical and Industrial Engineering, NTNU, Trondheim, Norway

ARTICLE INFO

*Keywords:*
Dynamic risk analysis
Safety barrier analysis
Oil&Gas
Extreme environment

ABSTRACT

Oil&Gas activities in the arctic and subarctic regions are characterized by several challenges related to the harsh but sensitive environment in which they are carried out. The weather may deteriorate facility components at a higher rate, and delay operations, emergency and evacuation procedures. Moreover, these regions host unique ecosystems, and their preservation is a worldwide priority. For this reason, a comprehensive and systematic approach for risk analysis is necessary to prevent major accidents and comply with Arctic pollution control. A novel approach for dynamic risk assessment and management, based on Bayesian Networks and safety barrier assessment, is suggested. The method is applied to the Goliat Oil&Gas platform located in the Barents Sea and risk data on the Norwegian petroleum activities are used as evidence to simulate continuous update of risk assessment throughout the years. The case study shows the benefits and limitations of such approach. Accurate modelling of potential accident scenarios is possible through BNs, but time-consuming. The approach allows for drill-down capabilities, which enhance support of operations and definition of risk mitigating measures. However, the data used for dynamic risk assessment has a pivotal role, as data quality and quantity sensibly affect the outcome. Fortunately, the Oil&Gas industry is committed to improving collection of field data for the assessment of safety barrier performance. This approach represents a strategy to process deviations and resilient reactions, regularly iterating dynamic risk assessment to support risk management of critical systems, such as the Oil&Gas production in the arctic and sub-arctic regions.

## 1. Introduction

Despite the constant growth within the field of renewable energy (Granata et al., 2016; The solar foundation, 2016), as of today, the world energy demand is mainly fulfilled by fossil fuels (IEA - International Energy Agency, 2016). While energy consumption in western countries is bounded by uncertain economic growth (US Energy Information Administration, 2018), countries with strong economic growth, particularly in Asia, account for more than 60% of the world total projected increase in energy consumption from 2015 through 2040 (US Energy Information Administration, 2017). Increasing Energy demand drives oil & gas (O&G) exploration companies to search for novel reservoirs within the Arctic and sub-Arctic regions, along Norwegian, American and Russian continental shelves. However, this explorations bring also a series of critical challenges to address.

### 1.1. Oil&Gas production in the arctic and subarctic regions and related risks

The interest of oil and gas (O&G) industry on arctic and subarctic regions is driven by promising resources (Barabadi et al., 2015; Bercha et al., 2003; Gao et al., 2010; Musharraf et al., 2013; Song et al., 2016). The United States Geological Institute estimates 22% of world hydrocarbon reserves within these areas and approximately 84% of such sources is expected to be found in offshore areas (Bird et al., 2008; Bucelli et al., 2018, 2017b). Despite the fact that low oil prices have recently clouded the overall industry focus on these regions (Gulas et al., 2017), the slow price resurgence is set to reverse this trend. In fact, decreasing production of a Nordic country such as Norway has increased the national attention in Arctic Oil&Gas (Gulas et al., 2017). In 2016, the platform on Goliat field started production. The field is located 85 km Northwest of Hammerfest, North of Russia and Norway,

* Corresponding author.
*E-mail address:* nicola.paltrinieri@ntnu.no (N. Paltrinieri).

https://doi.org/10.1016/j.ssci.2019.09.011
Received 18 November 2018; Received in revised form 30 June 2019; Accepted 9 September 2019
Available online 20 September 2019

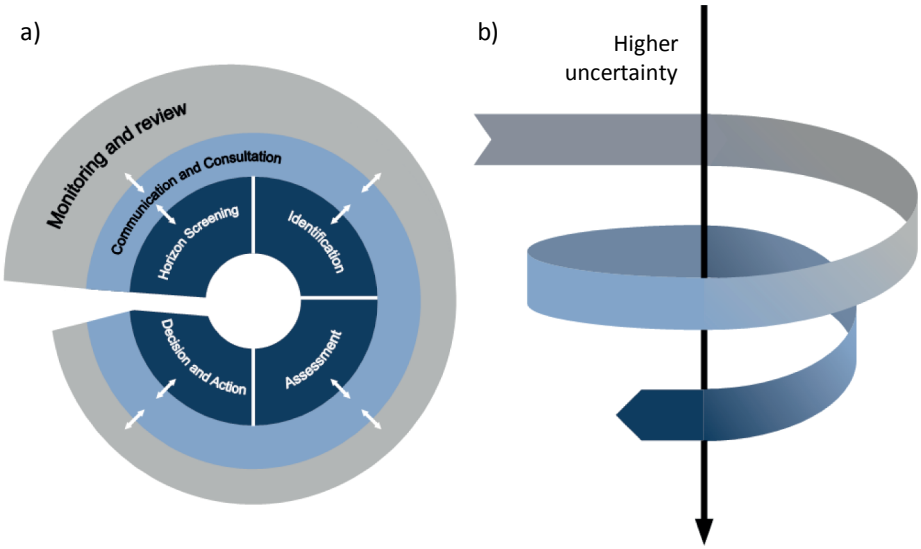



**Fig. 1.** Dynamic risk management framework: (a) two-dimensional version, and (b) three-dimensional version. Adapted from (Grøtan and Paltrinieri, 2016).

and is the first oil field to be developed in the Barents Sea (Eni Norge, 2015). The production license is owned by ENI Norge, with 65%, and by Statoil, with 35%. The Goliat field has two separate main reservoirs, Kobbe and Realgrunnen, characterized by low pressure. The recoverable reserves amount to 174 million barrels (28 $Mm^3$). The field is expected to be in production for fifteen years, but field life may be extended with new discoveries (Eni Norge, 2015).

However, one of the challenges of arctic and subarctic regions is represented by their climate, characterised by long, usually very cold winters, and short, cool to mild summers (Bucelli et al., 2017b, 2017a; Paltrinieri et al., 2017). Snow and ice are often present in many different forms. Such harsh climate is associated with remoteness, long distances from customer and supplier's markets. Climate has considerable influence on the choice of design, operations, and maintenance (Barabadi et al., 2015), as operations may be delayed by harsh weather, and maintenance would have to focus on components that are quickly deteriorating due to severe conditions (Barabadi et al., 2015; Gao et al., 2010; Landucci et al., 2017). In particular, special attention is needed due to the uncertainty on the influence of Arctic low temperature on offshore platform mechanical properties, which represents a topic for further investigation (Yan et al., 2016). On the other hand, in case of loss of integrity and, consequently, oil spill, its spreading and weathering would be substantially reduced in cold and icy conditions (Nevalainen et al., 2017). As oil decomposes slowly in cold latitudes, the recovery rate in Arctic regions sensibly decreases (Brandvik et al., 2006). Harsh weather intensifies the uncertainty on the response to such major events. As stated by Nevalainen et al. (2017), an oil spill in these regions is likely to remain in the environment for a relatively long time, prolonging the related environmental harm (Arctic Council, 2007).

Rich and important ecosystems are located in the Arctic and sub-Arctic regions (Barabadi et al., 2015; Gao et al., 2010). The Barents Sea, located off the northern coasts of Norway and Russia, is relatively shallow and free from ice during the year, due to high salt level and warm Gulf Stream currents from the Atlantic Ocean. This improves its biodiversity and supports abundant fish stocks as well as high concentration of nesting seabirds and a diverse community of sea mammals (Larsen et al., 2004). Such characteristics make the Barents Sea (together with the Kara Sea) one of the World Wildlife Fund (WWF) marine ecoregions for global conservation (Olson and Dinerstein, 2002), and its coast a high priority area for biodiversity maintenance (Larsen et al., 2004). These ecosystems consist of relatively short food webs making trophic interactions comparatively simple (Kaiser et al., 2011). This implies that population changes in just one key species may have strong cascading effects in the entire ecosystem (Hop and Gjøsæter, 2013; Palumbi et al., 2008).

A number of authors discuss risk-based design enhancing safety of operations in harsh environment (Gao et al., 2010; Paik et al., 2011; Vinnem, 2014). Other works suggest relatively more advanced approaches for the assessment of safety barriers within harsh environment (Bucelli et al., 2018, 2017a; Paltrinieri et al., 2017), where safety barriers are defines as "technical, operational and organizational elements intended individually or collectively to reduce the possibility for a specific error, hazard or accident to occur, or limit its harm/disadvantages" (Petroleum Safety Authority, 2013). As reminded by Bucelli et al. (2017a), releases of flammable hydrocarbons on an Oil& Gas Arctic platform have the potential to escalate into major events with serious multiple consequences for operators, environment and asset. Within this context, a comprehensive and systematic approach for risk analysis, which can rely on a robust modelling basis, is still missing. In addition, it should not be forgotten that another purpose of risk analysis is demonstrating the compliance with Arctic governance and environmental pollution control, which are rightfully strict and are set to further strengthen, as invoked by Gulas et al. (2017).

Quantitative Risk Assessment (QRA) is the most common approach to assess the risk of oil loss of containment. However, criticisms have directed towards this approach. Creedy (2011) states that the estimation of event frequencies, such as releases, still appears to be largely based on values from several decades ago, while Apostolakis (2004) underlines that probabilities of these events cannot be realistically calculated. Moreover, such uncertainties have little chance of being overcome as this approach is intrinsically static (Villa et al., 2016a, 2016b). In fact, it precludes possible updates and integrations of the overall risk figures on a frequent basis. For this reason, in the last years, several studies have been devoted to the development of novel approaches for dynamic risk assessment and management (Paltrinieri et al., 2014b, 2013, 2011, 2010; Paltrinieri and Hokstad, 2015).

Fig. 1 shows the two- and three-dimensional versions of the framework developed to support dynamic risk management (Dynamic Risk Management Framework – DRMF) (Grøtan and Paltrinieri, 2016; Paltrinieri et al., 2019). The two-dimensional version has a characteristic shape, showing an iterative risk management process that is open to the outside, opposing self-sustained processes by including external experience and early warnings through monitoring and review activities. DRMF suggests communication of this new information, with possibly the support of experts (communication and consultation), for:

(i) improved investigation of overall issues (horizon screening), (ii) delineation of related hazards (identification), (iii) assessment of associated risk (assessment) and, (iv) ultimately, support for risk-informed decision-making and focused safety operation (decision and action). Such a process would not only continuously improve the current risk picture, but also limit uncertainties in its management, as represented by the three-dimensional version of DRMF. A centripetal iteration from the external phase of monitoring and review (represented in grey in Fig. 1) to the final phases of assessment and decision (represented in blue in Fig. 1) implies an additional transition along a third dimension, which may be identified as the increment of knowledge for risk analysis (Aven and Krohn, 2014), or, as shown in Fig. 1, the decrease of uncertainty about potential unwanted scenarios (Grøtan and Paltrinieri, 2016; Paltrinieri et al., 2017).

Technical and operational performance of safety barriers on Oil& Gas facilities is a critical aspect to continuously monitor and assess, not only within sensitive areas (Bercha et al., 2003; Gao et al., 2010). The Norwegian Petroleum Safety Authority (PSA) requires yearly performance assessment of safety barriers on all the Norwegian Oil&Gas installations (PSA, 2018). The present study is aimed at providing a methodology for dynamic risk assessment based on the variation in safety barrier performance, which will be dedicated to offshore Oil&Gas facilities in sensitive areas. Such method is inspired by previous relevant studies (Paltrinieri and Khan, 2016), and it integrates the Bayesian theory for the barrier management and, ultimately, risk assessment. In fact, the use of Bayesian networks for barrier management is a relatively innovative way to evaluate probabilities of possible barrier failures. This approach can take advantage of model flexibility and possibility to update with new available data. It allows updating barrier probability of failure and, in turn, frequency of outcoming events, based on incidents and near misses occurred within the system (Paltrinieri et al., 2014a). This allows investigating how barrier performance influences the overall level of risk during the lifecycle of the facility, considering the information present in literature and collected by the national authorities.

## 2. Safety barriers in offshore Oil&Gas

Sklet (2006) defines a safety barrier as a physical and/or non-physical means planned to prevent, control or mitigate undesired events or accidents. It may range from a single technical unit or a single action to a complex and structured socio-technical system.

Each barrier is characterized by one or more specific functions. Delvosalle et al. (2006) summarises barrier functions as follows:

- Avoidance. Removing all potential causes of accidents by changing design.
- Prevention. Reducing probability of a hazardous event or reducing its consequences.
- Control. Limiting deviations from the normal operation and also delimiting emergency situations.
- Protection. Protecting assets from consequences of hazardous event.

The barrier function may be considered as the purpose of the safety barrier. This function is realized by several measures or solutions which are defined as barrier elements. Every element by itself is not able to reduce the overall risk, but it performs a specific role within the barrier system. Barrier elements could be divided in three categories: technical, operational and organizational. A technical element is an equipment or a system (sensor, a transmitter or a valve). An operational element is an action or activity to be carried out by personnel. An organizational element is a role or functions attributed to personnel (Petroleum Safety Authority, 2013).

A barrier system is a structured collection of barrier elements designed and implemented to perform one or more barrier functions. Often “barrier system” and “safety barrier” are two different words for the same meaning. Barrier systems may be decomposed in elements. Every element perform a certain sub-function. If a barrier system reduces the probability of a hazardous event, it is named frequency-reducing barrier or proactive barrier. If a barrier system reduces the consequence of a hazardous event, it is named consequence-reducing barrier or reactive barrier (Sklet, 2006).

Barrier systems can be classified as passive, if they do not require any solicitation in terms of human activation, information signals or energy source. Passive barriers must be inspected routinely in order to monitor their state and their capability to respond to the identified hazards. On the contrary, they can be defined active, if they need at least one among human activation, information signals or any energy source, to perform their protective function. In case of active barriers, all the necessary signals must be detectable when activation is required. Active barriers must be fail-safe and tested, by either self-testing or regular function testing (Sklet, 2006). Human actions is another kind of barrier. The effectiveness of this barrier relies on the knowledge of the operator in order to reach the purpose. Human actions include the use of senses, communication, thinking, physical activities and also rules, guidelines and emergency plans (Delvosalle et al., 2006).

According to PSA, performance requirements shall be established for the safety barriers on an Oil&Gas installation (Petroleum Safety Authority, 2013). According to Sklet (2006) and relevant standards, the performance of a safety barrier may be defined by three parameters:

- Probability of failure on demand (PFD), for which special reference is made to IEC 61,508 (International Electrotechnical Commission, 2010) and NOGA 070 (Norwegian Oil Industry Association, 2004), as the recommended standards for specification, design and operation of Safety Instrumented System (SIS).
- Functionality/effectiveness, which is the ability to perform a specified function under given technical, environmental, and operational conditions. The barrier effectiveness addresses the effect that the barrier has on the event or accident sequence. The potential degree of fulfilment may be expressed as the probability of successful function execution or the percentage of successful function execution (Sklet, 2006).
- Time to respond, which is the time from solicitation of the barrier to the end of the response (Sklet, 2006).

### 2.1. Safety barriers against escalation

One of the main events triggering escalation is primary fire (Landucci et al., 2015). For this reason, the study focuses on technical safety barriers related to fire scenarios.

Barriers used to prevent escalation in process plants can be divided in active barriers, passive barriers, and human actions (Hourtolou and Bernuchon, 2004). Active barriers require a sequence of detection, diagnosis, decision, and action. The sequence is performed by a detection system, a logic solver or an electro-mechanical device, and a mechanical or instrumented system – or alternatively a human (Hourtolou and Bernuchon, 2004).

The main scopes of active fire protection systems are (Landucci et al., 2015):

- To mitigate fire exposure of target that could be equipment or structures. It can be done keeping a water film on exposed surfaces to cool them and absorb radiant heat preventing material loss of strength.
- To isolate and empty the target vessel, reducing the potential loss and consequent damages due to release of inventory in undesirable locations.
- Control of the primary fire and prevention of fire spread in nearby units.

On the basis of these scopes, active fire protection systems can be

divided in two categories (Landucci et al., 2015):

1. Systems for the delivery of fire-fighting agents such as water or foam. They can be fixed, semi-fixed, mobile and portable systems.
2. Emergency Shutdown (ESD) Systems and Blowdown (BD).

The most common way to deliver fire-fighting agents (usually simply water or water with some additives) is by means of the deluge system. The effect of this barrier system is multiple. It can reduce likelihood of escalation by controlling fires dimensions, providing cooling of equipment near to the fire, and reducing consequences of a gas explosion if activated before the ignition (van Wingerden, 2000). The deluge system can be used to cover a whole process area providing non-specific coverage of pipework and equipment; it can protect a specified equipment or structural elements providing a dedicated coverage, or it can be used to form a water curtain that can reduce thermal radiation and control smoke and dangerous gasses dispersion.

The purpose of the ESD system is to prevent escalation of abnormal conditions into a major hazardous event and to limit the extent and duration of any such event that may occur. To perform this safety function, ESD valves shall isolate and sectionalise the installations in a fast and reliable manner, in order to reduce the total amount of released hydrocarbons in the event of a leakage (NORSOK, 2008). ESD valves are actuated valves which are closed when triggered by a signal during emergency conditions. ESD can also command the execution of other automatic actions, for instance main power generator shut down and possible ignition sources isolation (NORSOK, 2008), in order to avoid more severe consequences.

The BD drains liquid from the vessels by opening a certain number of blowdown valves (BDVs). Its main purposes are (NORSOK, 2008):

- in the event of fire, to reduce the pressure in process segments, reducing the risk of rupture and escalation;
- to reduce the leak rate and leak duration and thereby ignition probability;
- in some cases, to avoid leakage at process upsets;
- to route gases from atmospheric vent lines.

The BD is considered the primary means of protection and its intervention time should be reduced as much as possible to limit the need for passive fire protection.

Natural and mechanical ventilation can also be considered a preventing fire escalation measure (NORSOK, 2008). In fact, it dilutes flammable gas concentrations and reduces the size of flammable gas clouds. In case of fire, it dilutes harmful concentration of smoke and toxic gasses, ensuring acceptable environment for evacuation or intervention. Natural ventilation can be considered a passive protection. On the contrary, mechanical ventilation is an active measure as it is activated by engines triggered by fire and gas detection.

In offshore platforms also passive barriers have a key role in preventing escalation due to fire. In particular we can mention passive fire protection (PFP) system. For instance, the objective of passive fire protection is to reduce heat transfer to equipment, structures, and enclosures, while limiting escalation (ISO, 2015). Fire division is used to avoid that fire and explosion escalade into surrounding areas. Fire divisions are made by fire walls and blast walls, ensuring that thermal effects, propagation of fire and explosion overpressure are prevented. Critical structures, piping and equipment components shall have adequate fire resistance with regard to load bearing properties, integrity and insulation properties during a dimensioning fire and contribute in reducing consequences in general (NORSOK, 2008). Containment basins can be also considered barrier elements preventing escalation. They can be located under one or more vessels to contain potential liquid releases, preventing propagation into other areas. A drainage system is often connected to basins. Pressure Safety Valves (PSVs) and rupture disks are considered passive barriers because they open only by the energy of the fluid to be released. They prevent vessel rupture caused by overpressure. Another escalation preventing measure is ignition source control (ISC) that shall minimize the likelihood of ignition of flammable liquids and gases following a loss of containment.

Human barriers are organizational and operational measures aiming to prevent escalation. These barriers include specific procedures during both normal operations and emergency response, and can be divided in two categories (Hauge et al., 2016):

- Procedures to be activated in order to prevent failure or an unwanted event to occur. In this case, the time to perform the procedure is not critical.
- Procedures to be activated after the occurrence of a failure event. In this case, time is critical for the success of the barrier element.

### 2.2. Data collection in Oil&Gas

Most of the conventional Health, Safety and Environment (HSE) management approaches and hazard identification systems in the Oil& Gas are incapable of agile and automated data integration in decision making (Tarrahi and Shadravan, 2016). Application of data analytics in the Oil&Gas industry is in an experimental stage, with much of the early work focused on data-intensive computing and how Input/Output data loading can be managed efficiently. The challenging physical environment in the Arctic and the need to limit the number of personnel in hazardous and remote locations led to the development of some degree of automation within the Oil&Gas rigs (Feblowitz, 2012). In this context sophisticated sensors technologies coupled with powerful data-analytics can be used for early detection of anomalies and malfunctions. In fact, a possible alternative to curative maintenance can be the preventive maintenance, consisting in detecting anomalous behaviour and prevent further consequences. To this end, monitoring equipment is needed and it is possible using data from sensors. Nevertheless, data collected are often difficult to exploit in order to generate relevant information.

Tools for collecting, systematizing and presenting critical information on safety barrier performance are operative only on the most advanced Oil&Gas platforms (Eni Norge, 2018; Paltrinieri et al., 2017). Several Oil&Gas companies operating on the Norwegian continental shelf (NCS) have developed such concepts, but only a few have implemented them (Hauge et al., 2016). For instance, the system used on the Goliat platform measures and monitors over 10 600 technical components in real time, in order to outline the status of major accident-critical barriers for use in daily priorities (Eni Norge, 2018). The barrier panel provides data from the maintenance management system and control system. The information can be aggregated in several different views, tailored to different user groups. The barrier status panel contributes to increased risk awareness, both in daily status meetings, and as decision support during work planning and approval (Eni Norge, 2018; Paltrinieri et al., 2017).

## 3. Method

Several techniques are available for accident scenario modelling and safety assessment. For instance, a review of 62 risk analysis methodologies for industrial plants is provided by Tixier et al. (2002). As discussed, traditional techniques may not be suitable for dynamic risk management. They are incapable to manage multi-state variables, which are often encountered in process system modelling, or do not take into account the variability of risk level over time. For this reason, attention has been recently focused on dynamic techniques. As clarified by Yang et al. (2017), dynamic approaches are addressed by research on:

1. real-time risk analysis, focusing on real-time input data and high-frequency update;

2. dynamic risk analysis, focusing on the methodologies of risk analysis designed to be dynamic and updatable; and
3. operational risk analysis, focusing on the continuous support to safety-critical operations provided by risk analysis.

Given that dynamic risk analysis deals with the methodological perspective of the issue (Paltrinieri and Khan, 2016) regardless of the specificities of its use, the related literature has been reviewed to identify a suitable technique for this work. Several approaches aim to comprehensively describe socio-technical systems. In this regard, system dynamics was used by Garbolino et al. (2016) for risk assessment of industries dealing with hazardous substances. In addition, preliminary methodologies are developed in collaboration with industry, such as the Risk Barometer (Hauge et al., 2015). Other methods are defined based on the API 581 standard on risk based inspection (American Petroleum Institute, 2016), such as the Frequency modification methodology based on Technical Operational and Organizational factors (TEC2O) (Landucci and Paltrinieri, 2016). The mentioned approaches are defined as proactive by Scarponi and Paltrinieri (2016) and include in the analysis early deviations from the optimal condition also in terms of operational and organizational factors, which have a lower degree of causality on a potential accident and, thus, a relatively uncertain connection. On the other hand, reactive approaches, mainly focusing on technical factors, respond to an event that is directly associated with the overall risk picture and is presumably closer in time to a potential accident, if not to an accident itself (Scarponi and Paltrinieri, 2016). For instance, contributions to dynamic risk analysis by means of the Monte Carlo method can be found in literature (Noh et al., 2014). The Petri nets method is also used to improve risk analysis and capture dynamic sequences (Zhou et al., 2017; Zhou and Reniers, 2017). The application of Bayesian networks (Lee et al., 2017) also falls in the group of reactive approaches and provides sound statistical theories to dynamic risk analysis. Moreover, it allows updating the risk picture of the system by considering information on past events that indicate failure or success of safety barriers (Scarponi and Paltrinieri, 2016), as the barriers can be modelled by network nodes. For this reason, the application of Bayesian networks is considered for this study.

### 3.1. Bayesian networks

Bayesian networks represent a useful formalism in the risk analysis domain due to their ability to model probabilistic data with dependencies between events (Weber et al., 2012). The Bayes theorem has the advantage to use new evidence to update probabilities of events deviating from normal operations, physical phenomena and, in particular, failure of safety barriers in an accident scenario. Prior probability is estimated in several ways, such as statistical analysis of historical data or data collected from inspection/condition monitoring, deductive reasoning by means of quantitative risk analysis techniques, or expert judgment (Khakzad et al., 2016). On the other hand, relevant information used to update prior probabilities become available during the plant lifecycle, such as deviations from design parameters, near misses, or incidents.

For instance, a safety barrier failure $\theta_f$ is updated considering evidence E and the likelihood function $L(E|\theta_f)$ (probability distribution of evidence given that $\theta_f$ has occurred) as follows:

$$P(\theta_f|E) = \frac{P(\theta_f)L(E|\theta_f)}{\sum_{\theta_f} P(\theta_f)L(E|\theta_f)} \quad (1)$$

where the safety barrier failure $\theta_f$ is a discrete random variable, $P(\theta_f)$ is its probability distribution, and $P(\theta_f|E)$ is the updated (posterior) probability distribution given the evidence E. An example evidence can be represented by the occurrence of an early warning of the safety barrier failure (Paltrinieri et al., 2014a; Scarponi et al., 2016). However, an early warning does not provide complete certainty for barrier failure.

BNs have two types of items to represent the uncertainty of evidence (Fenton et al., 2016):

- virtual evidence that uses the likelihood function to represent the uncertainty of evidence; and
- soft evidence that uses likelihood ratio as the target posterior distribution.

This work generally uses virtual evidence. However, considered the philosophical concern about whether soft evidence has any rational meaning in the real world (Pearl, 2014) and that the two types of evidence are often confused with each other (Fenton et al., 2016), their distinction is excluded from the scope of this work, which will refer to the more generic term of “uncertain evidence”. Evidence imposed on the events of barrier failure $\theta_f$ and success $\theta_s$ (but independent from them) can be specified by the weights $w_f$ and $w_s$ such that:

$$L(E|\theta_f) = w_f; \quad L(E|\theta_s) = w_s; \quad w_f + w_s = 1 \quad (2)$$

This can be extended to other events $\theta_i$ for i = 1,…,n.

Uncertain evidence is implemented in many commercial BN software packages, such as AgenaRisk® (Agena Ltd, 2019). The latter is used for this study and only requires to set appropriate weights $w_i$ to describe the likelihood function of uncertain evidence.

Multiple pieces of evidence, causes and effects are correlated within a single potential accident scenario. Bayesian networks can graphically represent such interactions, as it explicitly describes dependencies between a set of variables through an acyclic graph. Uncertain variables (deviating events, physical phenomena, or safety barrier failures) are represented as nodes, while causation or influential dependence is depicted by an arrow between them, denominated *edge*. A *parent node* affects a *child node*. A *root node* has no parent nodes (root cause), while a *leaf node* has no child nodes (final accident outcome). Considering n variables $\theta_i$, such as the sequence of unwanted events and failed safety barriers leading from the root cause $\theta_1$ to a final accident outcome $\theta_{n+1}$, the probability distribution of the final outcome $P(\theta_{n+1})$ is expressed by the chain rule, as follows:

$$P(\theta_{n+1}) = \prod_{i=1}^{n} P(\theta_i|Parents(\theta_i)) \quad (3)$$

For this reason, the update based on new evidence of any probability distribution $P(\theta_i)$ along the chain leads to an updated probability distribution of the final outcome.

## 4. Case study

The methodology was applied to a real reference case study in the Goliat oil field (Norway), which represents a relevant example of innovative facility operating offshore in the Arctic sensitive region. The information about this platform is gathered exclusively from public sources and the results obtained are derived from theoretical simulations.

### 4.1. Characteristics of the installation

Goliat installation is a circular geostationary Floating Production Storage and Offloading (FPSO) unit. It is the largest and most complex of its kind and it was specifically designed to ensure safe and reliable production in the harsh conditions of the Barents Sea (Eni Norge, 2016). It is possible to identify seven main areas on the FPSO, as depicted in Fig. 2. Production is supported by a subsea system of 22 wells: 12 production wells, 7 water injectors and 3 gas injectors.

The extracted crude oil is processed, stabilized, stored and then directly offloaded from the FPSO to shuttle tankers through the

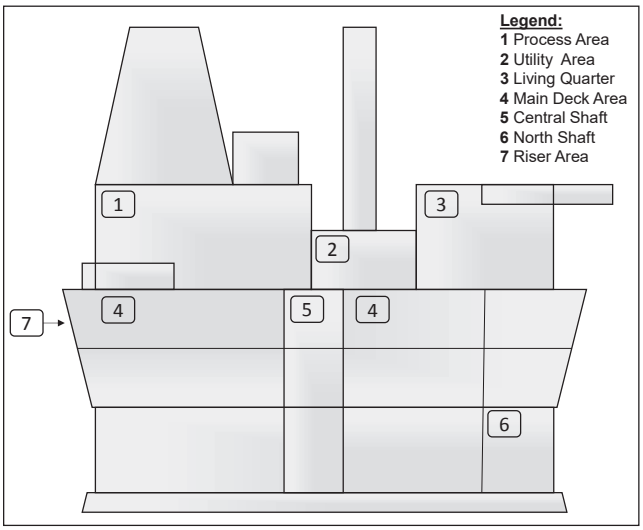



**Fig. 2.** Main areas on Goliat FPSO (adapted from Rekdal and Hansen, 2015).

offloading station (Bjørnbom, 2011). The offloading system is one of the safest and most reliable offloading system ever fabricated for offshore operations. The distance between the shuttle tanker and the platform is greater than in similar installations and video cameras and a light system are in place for frequent status monitoring of the offloading hose (Eni Norge, 2015).

### 4.2. Analysis

A specific Bayesian network is created for the case study. Relevant data from the yearly PSA reports on performance of safety barriers in the Norwegian Oil&Gas sector ("Trends in risk level in the petroleum activity" (PSA, 2018)) are used to update prior probabilities. A period from 2010 to 2016 was considered. The reports use one or more risk indicators to measure the status of most defined hazard and accident conditions. This shows how the various contributors to risk are developing, both collectively and for the individual defined hazard and accident conditions (PSA, 2018).

The analysis focuses on one of the most critical accident scenarios for an offshore platform with limited space for escape (Bucelli et al., 2018): the scenario of escalation due to fire in the process area. Bayesian networks theory is implemented to calibrate and update the scenario frequency during the years by means of the AgenaRisk® software (Agena Ltd, 2019). The escalation initiating event considered within the Bayesian network is the hydrocarbon leak. Such event is particularly important for the Goliat platform also due to the environmental impact it may lead to, even without ignition. Moreover, information on hydrocarbon leaks are relatively available on scientific literature, as it is possible to rely on a considerable amount of data (Fossan and Opstad, 2016), while escalations are rare events for which probabilistic analysis is challenging. For this reason, modelling escalation from leak events may be beneficial. Furthermore, an analysis of leaks causes would have required specific information about the process area of Goliat, which are not publicly available.

The analysis considers the safety barriers and related barrier elements depicted in Fig. 3, derived from previous studies of safety barriers on the Goliat platform (Bucelli et al., 2017a; Hansen, 2015). As the focus is on escalation, the safety barrier on escalation prevention is broken down into its barrier elements.

The escalation probability due to fire or explosion is estimated based on the probabilities of failure on demand of the considered safety barriers. Eq. (3) is used to obtain frequencies of escalation in Goliat.

$$f_{esc} = f_{ie}\ p_{esc} \tag{3}$$

where $f_{esc}$ is the escalation frequency, $f_{ie}$ is the frequency of the initiating event, and $p_{esc}$ is the probability of escalation obtained from the Bayesian network.

The unwanted events and safety barriers considered in the case study (Fig. 3) are further discussed in the following.

#### 4.2.1. Process leak

PSA records leaks with minimum flow rate of 0.1 kg/s and classifies them in three categories (Carlsen, 2015):

- Small, from 0.1 to 1 kg/s,
- Medium, from 1 to 10 kg/s, and
- Large, higher than 10 kg/s.

Leak data considered are only from the NCS offshore platforms. Hydrocarbon leaks may be gas or liquid. Moreover, partial vaporization may occur during a liquid release. For this reasons, three possible leak states should be considered: gas, liquid, and two-state. The case of two-state leak is often complex to analyse from a statistical point of view, mostly because the gas and liquid fractions are uncertain as they depend on a number of factors typical for each accidental scenario. The PSA reports (Carlsen, 2015; Tuntland, 2011) classify leaks in two categories: Liquid, and Gas/two-state. Also the ARAMIS project main deliverable (Delvosalle et al., 2004) shows a correspondence between gas and two-state categories, suggesting the same types of consequences after their occurrence: toxic cloud, environmental damage, and jet fire.

In case of delayed ignition, an aerosol puff can turn into a gas puff. As mentioned by the Health and Safety Executive (Health and Safety Executive, 2014), the airborne liquid particles receive energy from the external environment to transit from liquid phase to vapour or gas state. Moreover, the phenomenon of rainout (generation of a pool caused by condensation of little drops from a two-state cloud) is not considered in this model. However, further evaluation is needed to understand whether the release conditions in subarctic climate would anyway favour significant airborne dispersion over rainout.

#### 4.2.2. Leak detection

Leak detection is necessary to mitigate leak potential consequences. The probability of failure on demand of appropriate detectors is calculated based on the relevant Norwegian standard (Norwegian Oil Industry Association, 2004) and appropriate assumptions on the leak size in accordance with PSA leak categories.

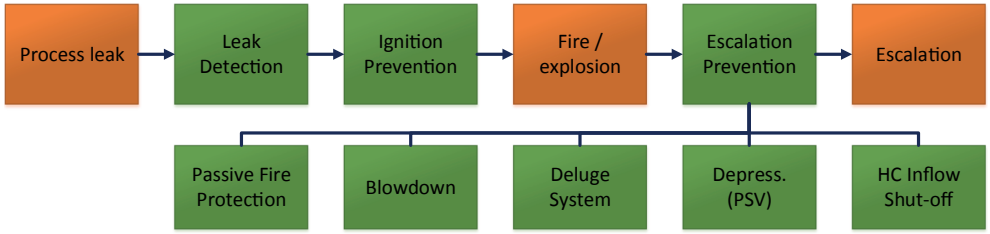



**Fig. 3.** Scenario considered in the case study. Unwanted events in orange and safety barrier elements in green. PSV and HC stand for, respectively, Pressure Safety Valve and hydrocarbon. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

#### 4.2.3. Ignition prevention

The most common ignition sources in Offshore Oil&Gas platforms are (Eckhoff and Thomassen, 1994): open flames, hot surfaces, metal particle sparks from impact or manual works, electric sparks and arcs, electrostatic discharges, and jet of hot gases.

Different preventing measures can be adopted to contrast such ignition sources, such as connection to the grounding system, isolation, and shields. However, for the sake of simplicity, specific correlations between leak rate and probability of ignition (Lund et al., 2007) were used for this barrier.

#### 4.2.4. Fire/explosion

The unwanted fire and explosion events considered are: jet fire, flash fire, pool fire, and vapour cloud explosion (VCE). Jet fire is a flammable gas leak from pressurized equipment or pipeline that is ignited immediately after the release starts. If the ignition is not immediate, a flammable cloud is generated, leading to flash fire or VCE in case of delayed ignition. Flash fire occurs when the flammable cloud burns in an open space, generating only a radiating and convective heat flux. Due to its short duration, no damages to structures and equipment are assumed to occur. On the contrary, VCE may occur in case of confinement of the burning flammable cloud, and this may affect structures and equipment by means of the overpressure it generates.

The occurrence of these fire and explosion events depends on several conditions specific of a certain accident mechanism and event (Uijt de Haag and Ale, 1999). The occurrence probabilities used for this event refer to the *Guidelines for quantitative risk assessment (Purple Book)* (Uijt de Haag and Ale, 1999).

#### 4.2.5. Passive fire protection

It is one of the barrier elements of escalation prevention. It shall ensure that relevant structures, piping and equipment components have adequate fire resistance with regard to load bearing properties, integrity and insulation properties, and contribute in reducing the consequences in general (NORSOK, 2008). Cott (1994) reports an inventory of PFD values for these barriers.

#### 4.2.6. Blowdown

Blowdown is the main measure to avoid an equipment catastrophic collapse due to a process fire scenario. It allows pressure relief avoiding exceeding maximum design load of the equipment and reduces inventory inside the vessel or equipment involved in a certain fire scenario. Reduction of hydrocarbon inventory prevents severe consequences in case of rupture of equipment lapped by flames or stroke by a burst overpressure avoiding ignition of further flammable substances. Blowdown is considered to be the primary means of protection. Blowdown time should be reduced as much as possible to limit the need for passive fire protection, which are only to be considered as a supplement to blowdown (NORSOK, 2008). According to the IEC 61508 Standard (International Electrotechnical Commission, 2010), the maximum PFD for a blowdown valve is 0.01. To correctly perform the blowdown function, we need a series of $n$ valves and a logic unit to succeed. The number of valves $n$ depends on the extent of fire or explosion event, which is in turn affected by the leak dimension. An updated value for the blowdown valve PFD is reported every year in the PSA reports (PSA, 2018). Probability of failure of the logic unit can be found in NOGA 070 (Norwegian Oil Industry Association, 2004) and it is equal to 0.0044.

#### 4.2.7. Deluge system

The deluge system is an active protection measure that has the task to reduce fire heat loads on equipment and structures. In this way, it can reduce probability of escalation and can be considered a barrier element of escalation prevention. Its failure modes can be failure in the pump activation, failure to open deluge valves and clogged deluge system, due to, for example, ice. According to the IEC 61508 Standard (International Electrotechnical Commission, 2010), the maximum deluge system PFD should be equal to 0.1. The system includes logic unit, fire water pump, fire water diesel engine, electric generator, electric motor, and deluge valve (Norwegian Oil Industry Association, 2004). NOGA 070 (Norwegian Oil Industry Association, 2004) estimates the PFD for a single deluge valve equal to 0.01. PSA also provides a yearly updated PFD values for the deluge valve (PSA, 2018).

#### 4.2.8. Depressurization

This barrier element of escalation prevention is intended to be performed by PSVs. When, for any reason, vessel pressure increases without control, the first depressurization safety function is performed by one or more PSVs. According to ISO 4126 (ISO, 2013) a safety valve is a valve which automatically discharges a quantity of the fluid in case of overpressure. After restoring normal pressure conditions, the PSV shall close automatically. In this model, only fire scenarios are considered and the cause of overpressure is due to the increasing internal temperature of the vessel affected by a fire. A PSV can fail for different reasons, such as clogging. We can consider that a single PSV is installed for each piece of equipment. This hypothesis is conservative as it does not take into account the possibility of redundancy. Also in this case, the number of PSVs and the overall depressurization PFD depend on the extent of fire or explosion event, which is in turn affected by the leak dimension. The PFD of a PSV can be found in PSA reports (PSA, 2018).

#### 4.2.9. Hydrocarbon inflow shut-off

The purpose of the ESD system is to prevent escalation of abnormal conditions into a major hazardous event and limit its extent and duration (NORSOK, 2008). The escalation prevention barrier element is performed by ESD valves that isolate the affected equipment. The system is activated by the detection of hydrocarbon leak on installation (Norwegian Oil Industry Association, 2004). In FPSO units, such as Goliat, riser emergency shutdown valves (RESDV) are an essential risk reduction measure. They isolate the topside from well and subsea pipeline, reducing the potential for loss of containment. The main failure mode is related to imperfect closure of the valve. PSA reports (PSA, 2018) provide the yearly probability to fail the closure test.

#### 4.2.10. Escalation

This event represents the scope of the analysis performed through the Bayesian network. In this case, we consider part of escalation every damage to equipment, physical passive barriers, firewalls and structures caused by fire and explosion events. This may lead to propagation of fire and explosions and further catastrophic events, such as Boiling Liquid Expanding Vapour Explosions (BLEVEs) and fireballs. The main mechanisms causing escalation to other areas are (Vinnem, 2014):

- Heat impact from external flames;
- flames passing through penetrations and openings in the floor, walls or roof; and
- failure of segregating walls.

In the analysis of this case study, the escalation event is considered to happen if a relevant fire or explosion event occurs and the escalation prevention function fails, i.e. none of the escalation prevention barrier elements succeeds.

### 4.3. Evidence

Specific data for the Goliat platform are not available due to a twofold reason: it recently started its production (March 2016) and specific data on its safety barriers are not public. For this reason, production start for Goliat is assumed in 2010. This allowed using the PSA reports on trends in risk level from 2010 to 2016 (PSA, 2018), reporting relevant evidence for the BN nodes. However, such evidence is uncertain as it is referred to the whole petroleum activity in Norway.

**Table 1**
Evidence weights for the considered hydrocarbon leak sizes, based on (PSA, 2018).

| Leak size (kg/s) | Leak size probability | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 |
| 0.1–1 | 7.20E-01 | 7.21E-01 | 7.17E-01 | 7.22E-01 | 7.22E-01 | 7.18E-01 | 7.08E-01 |
| 1.0–10 | 2.46E-01 | 2.47E-01 | 2.44E-01 | 2.40E-01 | 2.37E-01 | 2.43E-01 | 2.54E-01 |
| > 10 | 3.39E-02 | 3.24E-02 | 3.94E-02 | 3.80E-02 | 4.07E-02 | 3.93E-02 | 3.78E-02 |

**Table 2**
Evidence weights for the considered safety barrier PFDs (success = 1 − PFD), based on (PSA, 2018). HC stands for hydrocarbon.

| Safety Barrier | Leak size (kg/s) | PFD | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 |
| Leak detection | 0.1–1 | 1.44E-02 | 1.44E-02 | 1.44E-02 | 1.64E-02 | 1.64E-02 | 1.64E-02 | 1.84E-02 |
| | 1.0–10 | 4.48E-03 | 4.48E-03 | 4.48E-03 | 4.51E-03 | 4.51E-03 | 4.51E-03 | 4.55E-03 |
| | > 10 | 4.40E-03 | 4.40E-03 | 4.40E-03 | 4.40E-03 | 4.40E-03 | 4.40E-03 | 4.40E-03 |
| Blowdown | 0.1–1 | 2.34E-02 | 4.84E-02 | 3.34E-02 | 2.14E-02 | 2.54E-02 | 1.94E-02 | 2.24E-02 |
| | 1.0–10 | 9.59E-02 | 2.06E-01 | 1.41E-01 | 8.66E-02 | 1.05E-01 | 7.72E-02 | 9.12E-02 |
| | > 10 | 1.79E-01 | 3.67E-01 | 2.59E-01 | 1.62E-01 | 1.96E-01 | 1.45E-01 | 1.71E-01 |
| Deluge system | / | 7.69E-03 | 1.87E-01 | 6.69E-03 | 3.22E-02 | 1.57E-02 | 1.37E-02 | 8.19E-03 |
| Depressurization | 0.1–1 | 1.50E-02 | 1.40E-02 | 1.50E-02 | 2.00E-02 | 1.70E-02 | 2.30E-02 | 1.80E-02 |
| | 1.0–10 | 7.28E-02 | 6.81E-02 | 7.28E-02 | 9.61E-02 | 8.22E-02 | 1.10E-01 | 8.68E-02 |
| | > 10 | 1.40E-01 | 1.32E-01 | 1.40E-01 | 1.83E-01 | 1.58E-01 | 2.08E-01 | 1.66E-01 |
| HC inflow shut-off | / | 2.25E-02 | 3.25E-02 | 2.10E-02 | 1.70E-02 | 1.25E-02 | 1.30E-02 | 2.00E-02 |

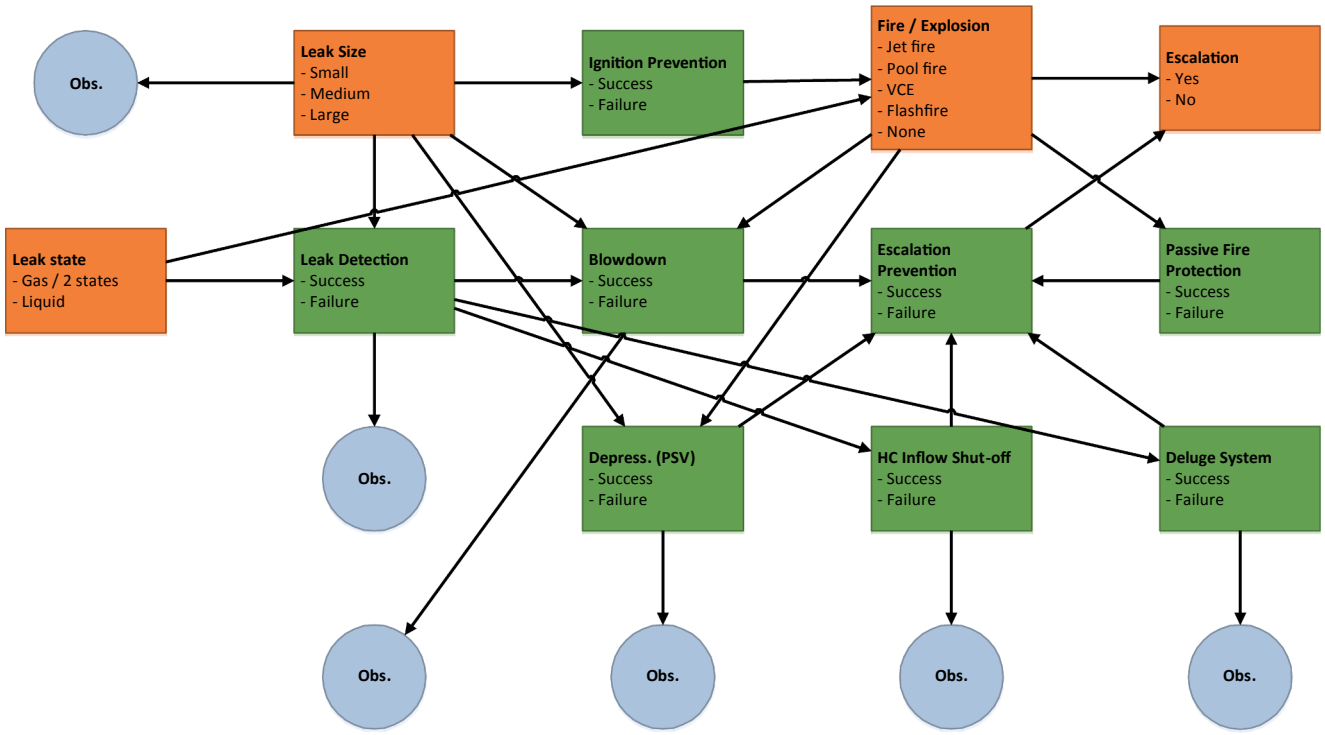



**Fig. 4.** Bayesian network for the case study. Unwanted events in orange and safety barrier elements in green. PSV and HC stand for, respectively, Pressure Safety Valve and hydrocarbon. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Tables 1 and 2 report the uncertain evidence weights used to yearly update the respective BN nodes.

## 5. Results

Fig. 4 depicts the Bayesian network defined for the case study, representing the relationships among the scenario events and safety barriers discussed in Section 4.2. Fig. 5 shows the calculated escalation frequencies and probabilities for the period 2010–2016. Frequencies are obtained from equation 3, using the event probabilities from the Bayesian network and the related yearly leak frequencies from (PSA, 2018) averaged by the number of production units surveyed every year. 2011 shows the highest frequency of escalation, which is demonstrated by the associated probability net of the yearly leak frequency values. Fig. 6 allows understanding that Escalation Prevention is the safety barrier that affects the most the final event of escalation, as it generally

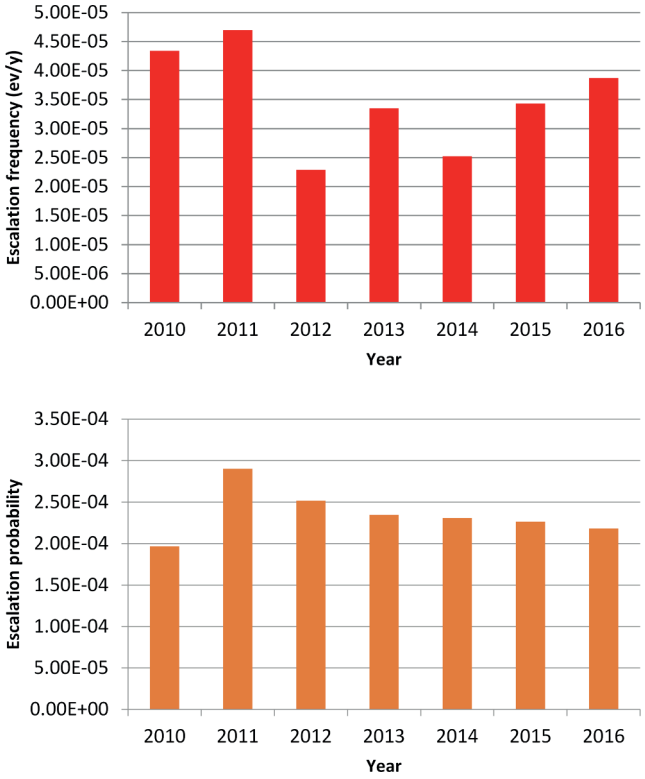



**Fig. 5.** Calculated escalation frequencies and probabilities within the period 2010–2016.

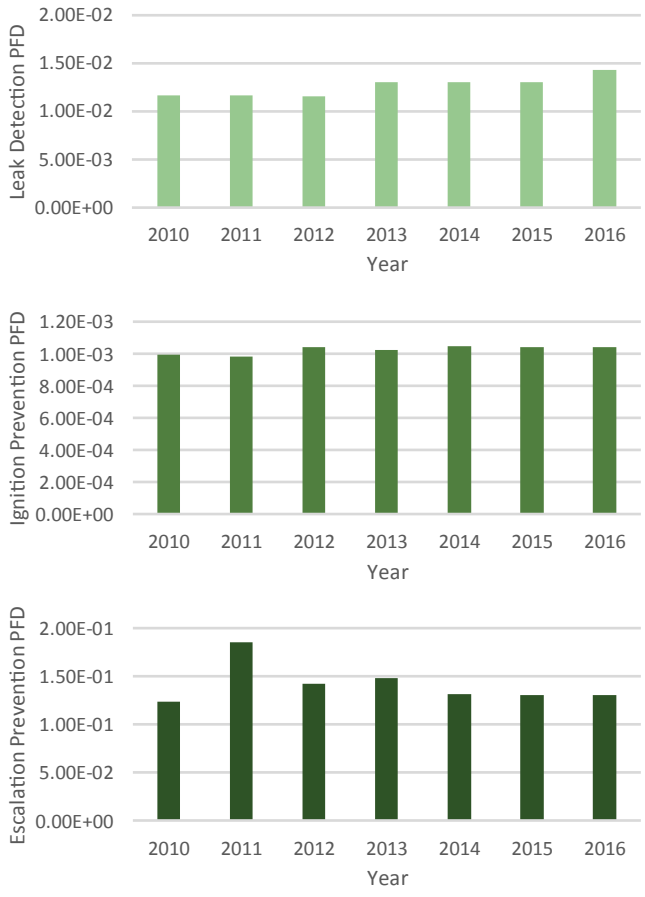



**Fig. 6.** Calculated safety barrier PFD values within the period 2010–2016.

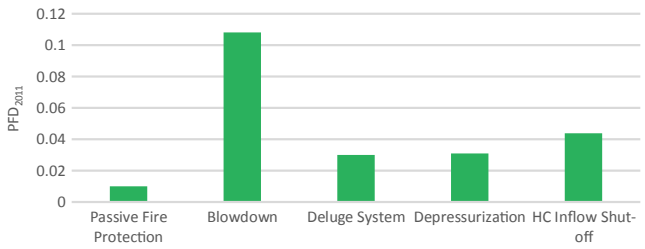



**Fig. 7.** Calculated PFD values of barrier elements for the safety barrier "Escalation Prevention in 2011.

presents the highest PFD. In particular, Escalation Prevention has record high in 2011. For this reason, Fig. 7 reports the PFD values of the Escalation Prevention barrier elements in 2011, from which we can evince that the Blowdown barrier element has the highest weight and its performance may relatively affect the overall escalation frequency.

## 6. Discussion

One of the first important results obtained from the study is represented by the BN itself. In fact, the network depicted in Fig. 4 is developed from the linear and simplified sequence of events and barriers in Fig. 3. BN unwanted events are described with an increased level of detail, which allows for more reliable modelling, but also for time-consuming analyses. "Process leak" is split in two BN nodes describing its size and physical state, while specific states are defined for "Fire/Explosion" to address the different physical phenomena that may occur in case of ignition. Interconnectivity among the BN nodes allows considering an increased number of dependencies. For instance, the "leak detection" barrier depends on "process leak" and affects "ignition prevention" in a linear scenario sequence, while a BN considers it as a child of "leak size" and "leak state" and parent of the "escalation prevention" barrier elements except "depressurization". Such structure allows for definition of complex interdependencies existing in a real accident scenario (Weber et al., 2012).

As mentioned by Edwin et al. (Edwin et al., 2016), drill-down capability is an important feature for dynamic risk analysis tools. The overall risk is a function of the status and condition of the different safety barriers and associated barrier elements. Drill-down capability enables moving through the hierarchy of the model and its different barrier elements. If the risk underlying causes are traced, we can provide intuitive understanding of variation causes and support definition of priorities related to risk mitigation and control.

Fig. 5 shows the final result of escalation frequency for the Goliat platform throughout the years considered. Despite the fact that this overall value remains within the same order of magnitude, some fluctuations can be identified. In particular, the escalation frequency is at its highest point in 2011, while the lowest frequency value is experienced the year after (2012). It is worth reminding that the data used for the analysis are real data from the Norwegian Oil&Gas petroleum activities and such a value change may reflect an actual reaction from critical conditions imposed by PSA. Such effective improvement is possible only if the weak links are identified.

As the escalation frequency is calculated through equation 3, a potential user of a dynamic risk assessment tool would be interested in understanding whether it is the frequency of the initiating event (i.e. the leak frequency) or the escalation probability affecting 2011 overall result. For this reason, Fig. 5 shows also the escalation probability, which is at its maximum as well. This indicates relatively poor performance of the safety barriers mitigating hydrocarbon leak. Fig. 6 shows relatively stable values of PFD for the safety barriers throughout the years, except for the escalation prevention, which reports the maximum PFD in 2011. This highlights the influence of this barrier performance on the overall frequency of escalation. Finally, if the single

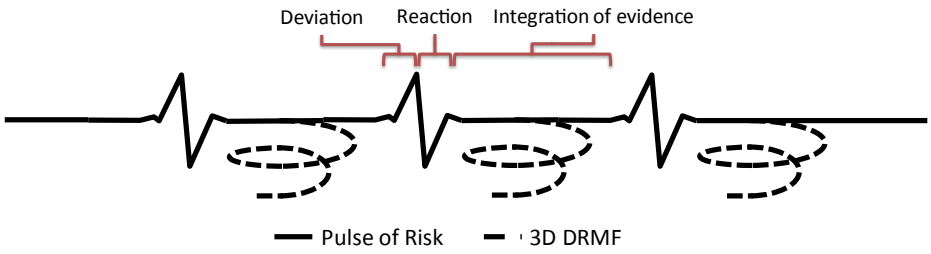



**Fig. 8.** DRMF as response to pulse of risk.

barrier elements are also studied, specific criticalities can be identified. For instance, Fig. 7 reports poor performance for the blowdown barrier element during 2011, and, consequently, indicates need for improvement.

Another aspect to consider is the quantity and quality of data used as input to dynamic risk assessment methods. In this case, the quality of data is (supposedly) high as the source is PSA, but they represent evidence that may sensibly affect the final analysis outcome. Moreover, it should be reminded that these statistics refer to a period preceding the start of Goliat productions and were used for the sake of demonstrating the effectiveness of such approach. Dynamic risk assessment would be hard to justify if little or no data are available, but this industry trend is in favour of data collection, as demonstrated by the ENI barrier panel project.

This study shows how dynamic risk assessment allows assessing risk variation also due to observed presence of resilience. Resilience is about dealing with the unexpected and the unprecedented and dynamism is the intrinsic premises for it (Grøtan and Paltrinieri, 2016). As discussed in Section 1, Oil&Gas production in arctic and sub-arctic regions may be characterized by the emergence of unexpected events, whose control assumes increasingly critical connotations due to the sensitive environment in which they occur. Continual performance variability due to intrinsic adaptations may be the norm rather than the exception. However, evidence on resilient episodes may be represented by barrier successes and may have various implications (Paltrinieri et al., 2017), such as positive effects in terms of evidence of enhanced processes of preclusion, mitigation or recovery. Even the opposite (series of failures) may signify a turning point due to accumulated learning.

Resilient episodes are better assessed within their context (Grøtan and Paltrinieri, 2016). For instance, the evidence collected for a single BN node eventually affects a larger portion of the network. A model such as BN is needed for the safety management process to identify and grasp such occasions. A “drift into failure” (Snook, 2002) might as well be a “drift into success” and a manifestation of resilience as a positive outcome of complex system properties. The drift metaphor is recurrent and recursive in the sense that technical revisions and redesigns, failures, incidents, accidents and recoveries may represent such occasions. BN analysis is used in this study to derive risk-related knowledge from resilient functioning.

Fig. 8 depicts how dynamic risk management (Fig. 1) may be performed as a response to a “pulse of risk” (Grøtan and Paltrinieri, 2016), i.e.:

- an expansion phase indicating a deviation from optimal system conditions, followed by
- a contraction representing the resilient reaction.

Examples of such pulses are provided by the near misses from the yearly PSA reports, such as leaks (expansion) that were successfully controlled (contraction). Collected evidence would trigger iteration of dynamic risk management. Newly assessed risk levels would call for overall re-organization and general improvement, as suggested for the blowdown barrier element after the analysis of its 2011 performance. This “Pulse of Risk” approach concurs into the shift of the DRMF perspective: from a two-dimension process designed to continuously integrate exogenous information, to a three-dimension process iterated to re-orient the overall risk management, for a flexible but comprehensive response to the challenges imposed by Oil&Gas production in arctic and subarctic regions.

## 7. Conclusions

A novel approach for dynamic risk assessment and management is suggested by this work. A method based on BNs and safety barrier assessment is used to carry out the approach indicated by DRMF (Grøtan and Paltrinieri, 2016). The method is applied to the Goliat Oil&Gas platform located in the Barents Sea and risk data on the Norwegian petroleum activities are used as evidence to simulate continuous update of risk assessment throughout the years. The case study showed the benefits and limitations of such an approach. Accurate modelling of potential accident scenarios is possible through BNs, but time-consuming. The approach allows for drill-down capabilities, which enhance support of operations and definition of risk mitigating measures. However, the data used for dynamic risk assessment has a pivotal role, as data quality and quantity may sensibly affect the outcome. Fortunately, the Oil&Gas industry is generally committed to improving collection of field data for the assessment of safety barrier performance. Finally, it must be mentioned that this approach represents a potential response to “pulses of risk”, in which system deviations and resilient reactions are processed by iteration of dynamic risk management for an effective strategy controlling risk in critical cases, such as Oil&Gas production in the arctic and sub-arctic regions.

## Acknowledgement

This research was supported by the project Lo-Risk (“Learning about Risk”), funded by the Norwegian University of Science and Technology – NTNU (Onsager fellowship).

## References

Agena Ltd, 2019. agenarisk.com, AgenaRisk. Cambridge, United Kingdom.
American Petroleum Institute, 2016. API 581 Risk-based Inspection Methodology, third ed.
Apostolakis, G.E., 2004. How useful is quantitative risk assessment? Risk Anal. 24, 515–520. https://doi.org/10.1111/j.0272-4332.2004.00455.x.
Arctic Council, 2007. Arctic Oil and Gas. Oslo, Norway.
Aven, T., Krohn, B.S., 2014. A new perspective on how to understand, assess and manage risk and the unforeseen. Reliab. Eng. Syst. Saf. 121, 1–10.
Barabadi, A., Tobias Gudmestad, O., Barabady, J., 2015. RAMS data collection under Arctic conditions. Reliab. Eng. Syst. Saf. 135, 92–99.
Bercha, F., Brooks, C., Leafloor, F., 2003. Human performance in arctic offshore escape, evacuation and rescue. In: Proceedings of the Thirteenth International Offshore and Polar Engineering Conference, Honolulu, Hawaii, USA. International Society of Offshore and Polar Engineers (ISOPE), Cupertino, Ca, USA, pp. 2755–2762.
Bird, K.J., Charpentier, R.R., Gautier, D.L., Houseknecht, D.W., Klett, T.R., Pitman, J.K., Moore, T.E., Schenk, C.J., Tennyson, M.E., Wandrey, C.J., 2008. Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle. USGS Fact Sheet 2008-3049. https://doi.org/USGS Fact Sheet 2008-3049.
Bjørnbom, E., 2011. Goliat – Leak detection and monitoring from template to satellite. In: Eni Norge.
Brandvik, P.J., Sorheim, K.R., Singsaas, I., Reed, M., 2006. Short state-of-the-art report on oil spills in ice-infested waters. Oil behaviour and response options, Trondheim,

Norway.
Bucelli, M., Landucci, G., Haugen, S., Paltrinieri, N., Cozzani, V., 2018. Assessment of safety barriers for the prevention of cascading events in oil and gas offshore installations operating in harsh environment. Ocean Eng. 158, 171–185. https://doi.org/10.1016/J.OCEANENG.2018.02.046.
Bucelli, M., Paltrinieri, N., Landucci, G., 2017a. Integrated risk assessment for oil and gas installations in sensitive areas. Ocean Eng. https://doi.org/10.1016/j.oceaneng.2017.12.035.
Bucelli, M., Paltrinieri, N. Landucci, G. Cozzani, V., 2017. Safety barrier management and risk assessment: integration for safer operations in the Oil & Gas industry (2017). In: Institution of Chemical Engineers Symposium Series, 2017-May (162).
Carlsen, F., 2015. Summary report 2014 - Norwegian Continental Shelf. Trends in risk level in the petroleum activity, Stavanger, Norway.
Cott, B.J., 1994. Guidelines for safe automation of chemical processes, Center for chemical process safety, American Institute of Chemical Engineers, 1993, 424 + xxiv pages, American Institute of Chemical Engineers, New York, New York. ISBN 0-8169-0554-1. Price: US $120.00. Can. J. Chem. Eng. 72, 767–768. https://doi.org/10.1002/cjce.5450720432.
Creedy, G.D., 2011. Quantitative risk assessment: How realistic are those frequency assumptions? J. Loss Prev. Process Ind. 24, 203–207. https://doi.org/10.1016/j.jlp.2010.08.013.
Delvosalle, C., Fiévez, C., Pipart, A., 2004. ARAMIS D1C - APPENDIX 5 Methodology for the building of generic event trees (MIMAH).
Delvosalle, C., Fievez, C., Pipart, A., Debray, B., 2006. ARAMIS project: a comprehensive methodology for the identification of reference accident scenarios in process industries. J. Hazard. Mater. 130, 200–219.
Eckhoff, R.K., Thomassen, O., 1994. Possible sources of ignition of potential explosive gas atmospheres on offshore process installations. J. Loss Prev. Process Ind. 7, 281–294. https://doi.org/10.1016/0950-4230(94)80041-3.
Edwin, N.J., Paltrinieri, N., Østerlie, T., 2016. Risk Metrics and Dynamic Risk Visualization. In: Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application. https://doi.org/10.1016/B978-0-12-803765-2.00013-5.
Eni Norge, 2018. Digitalisering av sokkelen - Norskutviklet verktøy overvåker Goliat-produksjonen i sanntid [WWW Document]. Eni Norge Nyheter og Media.
Eni Norge, 2016. Goliat - Eni Norge [WWW Document].
Eni Norge, 2015. Goliat Blend [WWW Document].
Feblowitz, J., 2012. The big deal about big data in upstream oil and gas. IDC Energy Insights 1–11.
Fenton, N., Neil, M., Lagnado, D., Marsh, W., Yet, B., Constantinou, A., 2016. How to model mutually exclusive events based on independent causal pathways in Bayesian network models. Know.-Based Syst. 113, 39–50. https://doi.org/10.1016/J.KNOSYS.2016.09.012.
Fossan, I., Opstad, A.S., 2016. Process leak for offshore installations frequency assessment model. PLOFAM. Bergen, Norway.
Gao, X., Barabady, J., Markeset, T., 2010. An approach for prediction of petroleum production facility performance considering Arctic influence factors. Reliab. Eng. Syst. Saf. 95, 837–846.
Garbolino, E., Chery, J.-P., Guarnieri, F., 2016. A simplified approach to risk assessment based on system dynamics: an industrial case study. Risk Anal. 36, 16–29. https://doi.org/10.1111/risa.12534.
Granata, G., Paltrinieri, N., Mingotti, N., 2016. Dust Hazards And Safety Measures Related To Photovoltaic Panel Recycling. Flogen Star OUTREACH.
Grøtan, T.O., Paltrinieri, N., 2016. Dynamic Risk Management in the Perspective of a Resilient System. In: Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application, https://doi.org/10.1016/B978-0-12-803765-2.00020-2.
Gulas, S., Downton, M., D'Souza, K., Hayden, K., Walker, T.R., 2017. Declining arctic ocean oil and gas developments: opportunities to improve governance and environmental pollution control. Mar. Policy 75, 53–61. https://doi.org/10.1016/J.MARPOL.2016.10.014.
Hansen, H.N., 2015. Goliat Barrier Management. In: Barrierestyring i Praksis. ESRA, Oslo, Norway.
Hauge, S., Øien, K., SINTEF, 2016. Guidance for barrier management in the petroleum industry [WWW Document].
Hauge, S., Okstad, E., Paltrinieri, N., Edwin, N., Vatn, J., Bodsberg, L., 2015. Handbook for monitoring of barrier status and associated risk in the operational phase. SINTEF F27045. Center for Integrated Operations in the Petroleum Industry, Trondheim, Norway, Norway.
Health and Safety Executive, 2014. Flammable mist from accidental hydrocarbon releases offshore. Buxton, United Kingdom.
Hop, H., Gjøsæter, H., 2013. Polar cod (Boreogadus saida) and capelin (Mallotus villosus) as key species in marine food webs of the Arctic and the Barents Sea. Mar. Biol. Res. 9, 878–894.
Hourtolou, D., Bernuchon, E., 2004. ARAMIS D1C- APPENDIX 9 Assessment of the performances of safety barriers.
IEA - International Energy Agency, 2016. Key world energy statistics.
International Electrotechnical Commission, 2010. IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.
ISO, 2015. Iso 13702: Petroleum and natural gas industries — Control and mitigation of fires and explosions on offshore production installations— Requirements and guidelines. Int. Stand.
ISO, 2013. ISO 4126-1 Safety devices for protection against excessive pressure - Part 1: Safety valves. Geneve, Switzerland.
Kaiser, M.J., Attrill, M.J., Jennings, S., Thomas, D.N., Barnes, D.K.A., 2011. Marine ecology: processes, systems, and impacts. Oxford University Press.
Khakzad, N., Yu, H., Paltrinieri, N., Khan, F., 2016. Reactive Approaches of Probability Update Based on Bayesian Methods. In: Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application, https://doi.org/10.1016/B978-0-12-803765-2.00005-6.
Landucci, G., Argenti, F., Tugnoli, A., Cozzani, V., 2015. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. Reliab. Eng. Syst. Saf. 143, 30–43.
Landucci, G., Bonvicini, S., Cozzani, V., 2017. A methodology for the analysis of domino and cascading events in Oil & Gas facilities operating in harsh environments. Saf. Sci. 95, 182–197. https://doi.org/10.1016/j.ssci.2016.12.019.
Landucci, G., Paltrinieri, N., 2016. A methodology for frequency tailorization dedicated to the Oil & Gas sector. Process Saf. Environ. Prot. 104, 123–141. https://doi.org/10.1016/j.psep.2016.08.012.
Larsen, T., Nagoda, D., Andersen, J.R., 2004. The Barents Sea ecoregion: A biodiversity assessment. WWF's Barents Sea Ecoregion Programme.
Lee, S., Liu, Y., Paltrinieri, N., 2017. Modelling hazardous event scenarios for decision support. Saf. Reliab. Theory Appl.
Lund, J.K., Christensen, J.A., Wiklund, J., Sagvolden, T., Scandpower, 2007. Ignition Modeling in Risk Analysis. Kjeller, Norway.
Musharraf, M., Khan, F., Veitch, B., Mackinnon, S., Imtiaz, S., 2013. Human factor risk assessment during emergency condition in harsh environment. In: Proceedings of the ASME 2013 32nd International Conference on Ocean, Offshore and Arctic Engineering (OMAE 2013), June 9-14, 2013, Nantes, France. American Society of Mechanical Engineers, New York, NY, pp. 1–9. https://doi.org/10.1115/OMAE2013-10867.
Nevalainen, M., Helle, I., Vanhatalo, J., 2017. Preparing for the unprecedented — towards quantitative oil risk assessment in the Arctic marine areas. Mar. Pollut. Bull. 114, 90–101. https://doi.org/10.1016/J.MARPOLBUL.2016.08.064.
Noh, Y., Chang, K., Seo, Y., Chang, D., 2014. Risk-based determination of design pressure of LNG fuel storage tanks based on dynamic process simulation combined with Monte Carlo method. Reliab. Eng. Syst. Saf. 129, 76–82. https://doi.org/10.1016/j.ress.2014.04.018.
NORSOK, 2008. S-001: Technical safety. Oslo, Norway.
Norwegian Oil Industry Association, 2004. Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry. Nor. Oil Ind. Assoc. 070.
Olson, D.M., Dinerstein, E., 2002. The global 200: priority ecoregions for global conservation. Missouri Bot. Gard. Press 89, 199–224. https://doi.org/10.2307/3298564.
Paik, J.K., Czujko, J., Kim, B.J., Seo, J.K., Ryu, H.S., Ha, Y.C., Janiszewski, P., Musial, B., 2011. Quantitative assessment of hydrocarbon explosion and fire risks in offshore installations. Mar. Struct. 24, 73–96.
Paltrinieri, N., Comfort, L., Reniers, G., 2019. Learning about risk: machine learning for risk assessment. Saf. Sci. 118, 475–486. https://doi.org/10.1016/j.ssci.2019.06.001.
Paltrinieri, N., Cozzani, V., Wardman, M., Dechy, N., Salzano, E., 2010. Atypical major hazard scenarios and their inclusion in risk analysis and safety assessments. In: Reliability, Risk and Safety: Back to the Future, pp. 588–595.
Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M., Cozzani, V., 2013. Towards a new approach for the identification of atypical accident scenarios. J. Risk Res. 16, 337–354. https://doi.org/10.1080/13669877.2012.729518.
Paltrinieri, N., Grøtan, T.O., Bucelli, M., Landucci, G., 2017. A case of dynamic risk management in the subarctic region, in: Risk, Reliability and Safety: Innovating Theory and Practice. Proceedings of the 26th European Safety and Reliability Conference, ESREL 2016.
Paltrinieri, N., Hokstad, P., 2015. Dynamic risk assessment: Development of a basic structure. In: Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014, pp. 1385–1392.
Paltrinieri, N., Khan, F., 2016. Dynamic Risk Analysis in the Chemical and Petroleum Industry, Dynamic Risk Analysis in the Chemical and Petroleum Industry. In: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application. Butterworth-Heinemann, https://doi.org/10.1016/B978-0-12-803765-2.01001-5.
Paltrinieri, N., Khan, F., Amyotte, P., Cozzani, V., 2014a. Dynamic approach to risk management: application to the Hoeganaes metal dust accidents. Process Saf. Environ. Prot. 92. https://doi.org/10.1016/j.psep.2013.11.008.
Paltrinieri, N., Scarponi, G.E., Khan, F., Hauge, S., 2014b. Addressing dynamic risk in the petroleum industry by means of innovative analysis solutions. Chem. Eng. Trans. https://doi.org/10.3303/CET1436076.
Paltrinieri, N., Tugnoli, A., Bonvicini, S., Cozzani, V., 2011. Atypical scenarios identification by the DyPASI procedure: application to LNG. Chem. Eng. Trans. 24, 1171–1176. https://doi.org/10.3303/CET1124196.
Palumbi, S.R., McLEOD, K.L., Grünbaum, D., 2008. Ecosystems in action: lessons from marine ecology about recovery, resistance, and reversibility. Bioscience 58, 33–42.
Pearl, J., 2014. Probabilistic reasoning in intelligent systems: networks of plausible inference. Elsevier.
Petroleum Safety Authority, 2013. Principles for barrier management in the petroleum industry. PSA, Stavanger, Norway.
PSA, 2018. List of RNNP reports. Stavanger, Norway.
Rekdal, O., Hansen, H.N., 2015. Goliat Barrier Management - ERSA Norge. March 25, 2015 [WWW Document].
Scarponi, G.E., Paltrinieri, N., 2016. Comparison and Complementarity between Reactive and Proactive Approaches. In: Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application, https://doi.org/10.1016/B978-0-12-803765-2.00008-1.
Scarponi, G.E., Paltrinieri, N., Khan, F., Cozzani, V., 2016. Reactive and Proactive Approaches: Tutorials and Example. In: Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the

Perspective of Industrial Application, https://doi.org/10.1016/B978-0-12-803765-2.00007-X.
Sklet, S., 2006. Safety barriers: definition, classification, and performance. J. loss Prev. Process Ind. 19, 494–506.
Snook, S.A., 2002. Friendly fire: The accidental shootdown of US Black Hawks over northern Iraq. Princeton University Press.
Song, G., Khan, F., Wang, H., Leighton, S., Yuan, Z., Liu, H., 2016. Dynamic occupational risk model for offshore operations in harsh environments. Reliab. Eng. Syst. Saf. 150, 58–64.
Tarrahi, M., Shadravan, A., 2016. Advanced big data analytics improves. HSE Manage.
The solar foundation, 2016. National Solar Jobs Census. Washington, DC, US.
Tixier, J., Dusserre, G., Salvi, O., Gaston, D., 2002. Review of 62 risk analysis methodologies of industrial plants. J. Loss Prev. Process Ind. 15, 291–303. https://doi.org/10.1016/S0950-4230(02)00008-6.
Tuntland, Ø., 2011. Risikonivå i petroleumsvirksomheten Norsk sokkel 2010. Stavanger, Norway.
Uijt de Haag, P.A.M., Ale, B.J.M., 1999. Guidelines for quantitative risk assessment (Purple Book). The Hague (NL).
US Energy Information Administration, 2018. Annual Energy Outlook 2018 with projections to 2050. Washington, DC, US.
US Energy Information Administration, 2017. EIA projects 28% increase in world energy use by 2040. Washington, DC, US.
van Wingerden, K., 2000. Mitigation of gas explosions using water deluge. Process Saf. Prog. 19 (3), 173–178.
Villa, V., Paltrinieri, N., Khan, F., Cozzani, V., 2016a. Towards dynamic risk analysis: a review of the risk assessment approach and its limitations in the chemical process industry. Saf. Sci. 89. https://doi.org/10.1016/j.ssci.2016.06.002.
Villa, V., Paltrinieri, N., Khan, F., Cozzani, V., 2016b. A Short Overview of Risk Analysis Background and Recent Developments. In: Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application, https://doi.org/10.1016/B978-0-12-803765-2.00001-9.
Vinnem, J.E., 2014. Offshore Risk Assessment vol 1. Principles, Modelling and Applications of QRA Studies, 3rd ed. Springer-Verlag, London, UK.
Weber, P., Medina-Oliva, G., Simon, C., Iung, B., 2012. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Eng. Appl. Artif. Intell. 25, 671–682. https://doi.org/10.1016/j.engappai.2010.06.002.
Yan, J.-B., Liu, X.-M., Liew, J.Y.R., Qian, X., Zhang, M.-H., 2016. Steel–concrete–steel sandwich system in Arctic offshore structure: materials, experiments, and design. Mater. Des. 91, 111–121. https://doi.org/10.1016/J.MATDES.2015.11.084.
Yang, X., Haugen, S., Paltrinieri, N., 2017. Clarifying the concept of operational risk assessment in the oil and gas industry. Saf. Sci. https://doi.org/10.1016/j.ssci.2017.12.019.
Zhou, J., Reniers, G., 2017. Petri-net based cascading effect analysis of vapor cloud explosions. J. Loss Prev. Process Ind. 48, 118–125. https://doi.org/10.1016/J.JLP.2017.04.017.
Zhou, J., Reniers, G., Zhang, L., 2017. A weighted fuzzy Petri-net based approach for security risk assessment in the chemical industry. Chem. Eng. Sci. 174, 136–145. https://doi.org/10.1016/J.CES.2017.09.002.

# Article II

Shenae Lee, Gabriele Landucci, Genserik Reniers, Nicola Paltrinieri, **Validation of Dynamic Risk Analysis Supporting Integrated Operations Across Systems**, Sustainability, Volume 11, 2019.

*sustainability*

MDPI

*Article*

# Validation of Dynamic Risk Analysis Supporting Integrated Operations Across Systems

**Shenae Lee [1], Gabriele Landucci [2], Genserik Reniers [3,4,5] and Nicola Paltrinieri [1,*]**

[1] Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology NTNU, S.P. Andersens veg 3, 7031 Trondheim, Norway; shenae.lee@ntnu.no
[2] Department of Civil and Industrial Engineering, University of Pisa, Largo Lucio Lazzarino 2, 56126 Pisa, Italy; gabriele.landucci@unipi.it
[3] Faculty of Applied Economics, University of Antwerp Operations Research Group ANT/OR, 2000 Antwerp, Belgium; G.L.L.M.E.Reniers@tudelft.nl
[4] Center for Corporate Sustainability (CEDON), HUB, KULeuven, 1000 Brussels, Belgium
[5] Safety Science Group, TU Delft, 2628 BX Delft, The Netherlands
* Correspondence: nicola.paltrinieri@ntnu.no

Received: 25 October 2019; Accepted: 21 November 2019; Published: 28 November 2019


**Abstract:** Dynamic risk analysis (DRA) is a novel industrial approach that aims to capture changes in operational conditions over time and quantify their effect on risk. This aspect may be advantageous for providing insight into the causal factors that have substantial risk contributions and supporting decisions related to risk control. Some DRA methods were developed by the oil and gas industry to support the integration of work processes and the cooperation across virtual clusters, e.g., between offshore and onshore systems and/or oil company and supplier. However, DRA has not been extensively adopted and limited attention is given to its validity in practical applications. The objective of this article is to illustrate how this validity can be established based on common validation approaches for risk analysis. The case study focuses on a DRA method named risk barometer that was developed to support integrated operations across the oil and gas industrial systems. The outcome of this study may serve as a basis for the validation of other DRA methods, the use of DRA in practical cases, and ultimately the achievement of integrated operations (IO) capabilities.

**Keywords:** Validation; dynamic risk analysis; oil and gas; integrated operations; risk barometer; TEC2O; reality check; benchmark; peer review.

## 1. Introduction

Quantitative risk assessment (QRA) has been extensively employed in the design phase of hazardous process facilities to ensure compliance with safety requirements. These requirements may be defined as acceptance criteria that express a tolerable risk level. Conventional QRA studies provide risk estimates and support decisions that are related to the design of an industrial installation [1–3]. The risk models applied to the design phase QRAs are suitable for reflecting the technical design of an installation. These models, however, have a limited focus on changes in the operating and environmental conditions and their potential impact on risk. As a result, new methods and models have been developed for the quantitative analysis of changes in risk levels, which is referred to as dynamic risk analysis (DRA) in the process industry. DRAs are performed in the operational phase to update the risk level over a certain interval based on operational experiences and field data or predict the risk level for the upcoming period based on precursor data [4]. However, appropriate validation for DRA is still an unexplored domain. For this reason, this study aims to suggest a set of relevant approaches.

Numerous representative DRA methods have been developed for safety-critical sectors, such as the oil and gas (O&G) sector: The organizational risk influence model (ORIM) [5], the barrier and operational risk analysis of hydrocarbon releases (BORA-release) [6,7], and the risk modeling through integration of organizational, human and technical factors (risk-OMT) [8]. These methods extend the existing QRA models by explicitly incorporating organizational and operational factors. They have proved useful in periodic updates of QRA results by reflecting changes in the parameters and assumptions of QRAs. Further developments of these methods employ machine learning techniques [9]. However, a specific challenge when using these methods is the ability to provide relevant input data [10,11], and therefore, the use of these models is difficult in practical cases. For this reason, a new DRA method named risk barometer (RB) was developed in the context of integrated operation (IO) concepts, also known by O&G companies as Field of the Future (BP), Smart Fields (Shell), eOperations and eField [12]. These concepts refer to the integration of people, work processes and information technology to make smarter decisions and achieve extended operational lifetime, reduced costs, and improved safety, production and recovery rates. It is enabled by global access to real-time information, collaborative technology, and integration of multiple expertise across disciplines, organizations, and geographical locations [12,13] representing virtual industrial clusters. IO concepts enable access to an increasing amount of real-time data related to safety barrier performance and operational conditions [14], which underlie the Risk Barometer (RB) method [15]. The RB method is mainly applied to O&G, but DRA is not limited to this domain [16]. Analogously, safety barriers are not only widespread within O&G, but they are also becoming a pivotal concept for other industries [17], as they are generically defined as physical or non-physical means that are planned to prevent, control, or mitigate undesired events or accidents [18].

The primary aim of the RB method is to use this dataset as a basis for continuously capturing the changes in operational conditions and dynamic aspects of risk in an improved way. In many cases, a lack of detailed knowledge about the relation between the actual risk level and the associated causal factors may exist. For this reason, the risk level is calculated by considering the contributions from the involved safety barriers. In this way, time for processing information and calculating the risk can be reduced, which may enable a more frequent update of the risk [15]. Note that the RB method emphasizes visualizing the results. Thus, the results are understood by the operational personnel [15]. Despite these practical benefits, the RB method may disregard certain contributors to risk or be based on unrealistic assumptions [19]. Therefore, investigating whether the RB method is suitable for quantitative analysis of risk in the relevant operational and decision context is essential.

This standpoint is particularly pertinent to the validity concept for risk analysis, which can be established based on an argument. It is referred to as cost-effective usefulness: Quantification of risk provides safety benefits compared with other methods that are based on qualitative approaches [20]. For example, the existing QRAs used in design can provide quantitative risk measures, which are used to prove compliance to regulations that concern the safe design in the long term [20–22]. New DRA methods, such as the RB method, can quantify the changes in the total risk level in a shorter time, which may not be obtained by traditional QRA. This finding provides decision support regarding barrier performances and safe operations [15,21]. If we consider also the IO context in which the RB has been developed, the main issues concerning its validity are detailed as follows:

- Is the method capable of identifying major accident scenarios and the critical safety barrier?
- Is the modeling approach suitable for capturing the changes in the operations and updating the risk level over time based on the collected data?
- Are the results similar compared with other recognized DRA methods?
- Are the outcomes sufficiently realistic to be applicable for industrial cases?
- Is the method functional to the achievement of sustainable integrated operations across systems?

As Cumming [23] states, the validation procedures for risk analysis techniques are limited. For this reason, a set of fundamental validation approaches were selected from Suokas' work [24] to address DRA issues: (i) Reality check (comparison with operating experience of corresponding installations), (ii) benchmark (comparison with a parallel analysis of the same installation or activity), and (iii) peer review (examination of the output of the risk analysis by technical experts).

Goerlandt et al. [21] present these approaches for establishing the pragmatic validity of risk analysis. The authors state that the first approach concerns the validity of a generic analysis method and can be applied to validate the results of a specific risk assessment. The second approach is primarily intended for evaluating the coverage of an analysis method and the reliability of the results in terms of analysis content and outcome [25]. The third approach can be applied to specific risk analysis and builds on the personal experience of individuals having technical expertise on the considered phenomena, practitioners, or risk analysis experts [21].

We illustrate how these approaches may be used to establish the validity of a DRA method when applied to a specific accident scenario. The RB method is considered for this purpose, but the approaches can be applied to any DRA technique.

After this introductive section, Section 2 describes the dynamic risk analysis method and the validation approaches. Section 3 illustrates the case-study used in this work. In Section 4, we report the results from the validation process of the considered dynamic risk analysis method. Sections 5 and 6 present the discussion and concluding remarks.

## 2. Methods

Validity for risk analysis can have several meanings that are debatable. Therefore, a focus on certain aspects of validity, considering the objectives, expected results, and limitations of risk analysis methods, may be necessary [24]. As a result, familiarization with the dynamic risk analysis method is essential to select adequate approaches for validation, which can be considered a primary step in the process (Figure 1). Subsequently, one validation approach should be adopted. Further iterations to analyze the DRA method validity through parallel approaches are possible and suggested for comprehensive results (Figure 1).

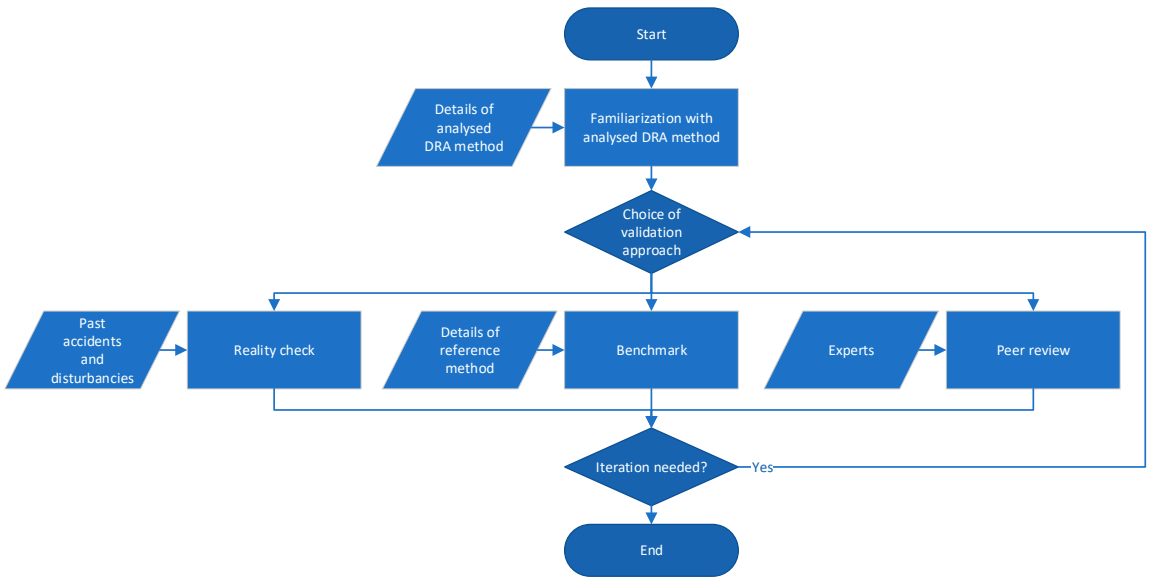



**Figure 1.** Flowchart for dynamic risk analysis (DRA) validation.

### *2.1. Familiarization with the Risk Barometer Dynamic Risk Analysis Method*

As previously mentioned, RB is a DRA method defined to enable IO concepts for risk assessment. Despite its practical benefits, the RB method may rely on incorrect assumptions and/or present limitations on the definition of contributors to risk. For these reasons, the validation of this method is investigated. This section introduces the main characteristics of the risk barometer method. The RB method is suitable for frequent updates of the risk level and involving practitioners in the risk model development. The risk model used in the RB takes into account the status of most critical barriers, whose performance has a significant impact on risk. The information related to the status of these barriers is collected by a set of indicators [26]. The RB method consists of seven main steps [15]:

**Step 1: Select scenarios.** This step aims to select hazardous events and accident scenarios that match installation-specific interests. In some cases, relevant guidelines and standards may be applied for this step. For instance, the methodology for identification of major accident hazards (MIMAH) [27] can be implemented to identify hazards and represent the associated accident paths in a Bowtie diagram. A Bowtie diagram analysis is easily comprehended by practitioners and can be conducted in cooperation with installation personnel [28].

**Step 2: Review relevant data sources.** To identify barriers and indicators that are relevant to the scenario defined in step 1, available data sources, including generic industry data, plant-specific data, and interviews with personnel and judgments, should be reviewed. No single source can provide sufficient information to perform a risk analysis [15], and therefore, combining both qualitative information and quantitative information from various references is essential.

**Step 3: Identify safety barriers and associated installations.** Safety barriers and the associated installations that are linked to the scenario in step 1 are identified. Ensuring that critical safety barriers are taken into account, which should be supported by the information obtained in Step 2, is important. The result of step 3 can be presented by adopting the form of objective trees, which is extensively employed in nuclear facilities [14,29,30]. The top level of an objective tree is a specific safety objective, which can be achieved by the safety functions listed on the lower level. The challenges related to achieving each safety function and the mechanism that causes these challenges are listed. On the lowest level of the tree, a provision that denotes a set of barriers to prevent/mitigate the mechanism is listed [31].

**Step 4: Evaluate the importance of barrier installations.** In the RB method, critical safety barriers are defined as barriers whose performance has a relatively high impact on the risk level. To evaluate the criticality of barriers, risk contributions from performance variations of barriers are assessed.

**Step 5: Select indicators to assess barrier status.** In step 5, a set of key performance indicators is developed to measure the performance of the associated barriers. Step 2 can be iterated for indicator selection as discussions and reviews with operational personnel may confirm which indicator is available and can be collected during operations.

**Step 6: Establish a risk model based on the aggregation of scaled indicators.** As shown by Table 1, each indicator is translated into a mutually comparable score value that is defined on a standardized scale (e.g., 1 to 6). This translation can be obtained by an interpolation function (e.g., linear, geometric, or logarithmic). Weighted summations of these scores quantify the barrier performance. The safety barrier performance expressed on this scale is translated into the barrier failure probability. The iteration of the bow-tie analysis with new failure probability values enables the risk measure to be updated.

**Step 7: Visualization.** The results from the RB method need to be presented to the decision-makers and operational personnel, so that information about risks is used to support decisions. Adequate presentation formats can facilitate the communication of risk information. Typical formats include time-series trends, radar charts, tabular formats, and criticality plots. The RB method can provide a graphical representation of its underlying risk model using the mentioned formats and detailed information about risk contribution from model elements [32].

**Table 1.** Aggregation of scaled indicators.

| Model Level | Aggregation Rule |
| --- | --- |
| ***Indicator*** | Indicator measure $x$ translated into indicator score $s$ (both for barrier $i$) via interpolation function S. |
| | $s_i = \mathrm{S}(x_i)$ (1) |
| ***Barrier performance*** | Barrier performance ($B_i$) of barrier $i$ obtained by the weighted sum of the indicator scores. |
| | $B_i = \sum w_{i,j} \cdot s_{i,j}$ (2) |
| ***Failure Probability*** | Barrier performance $B_i$ translated into failure probability $FP_i$ via direct proportionality P. |
| | $FP_i = \mathrm{P}(B_i)$ (3) |

## 2.2. Validation Approaches

This section presents three validation approaches for risk analysis [24] that are considered for validation of a DRA method, such as the RB.

### 2.2.1. Reality Check

Comparison against past accidents and disturbances that occurred in installations similar to the object of study may determine the risk analysis capability of identifying hazards and contributors. Past accident analysis is an extensively employed tool for preliminary hazard identification in chemical and process facilities [33]. This study was inspired by this tool to provide insights that validate the results from a DRA and eventually identify issues beyond the scope of this study, which should have been addressed but have remained unidentified and unassessed. Real incidents and near-miss accidents can be used to assess whether an RB has the capability of identifying complete accident scenarios [34,35]. In addition, we may gain insight into the extent to which the RB method can identify causal factors. For example, a comparison may reveal that the method performs well in identifying technical component failures rather than human errors in different operational situations [24]. Based on what was suggested by Paltrinieri et al. [36], the past accident data analysis applied in this work adopts the following databases:

- Online Major Accident Reporting System (eMARS) by the Major Accident Hazards Bureau (MAHB) of the European Commission's Joint Research Centre (JRC) [37];
- Analysis Research and Information on Accidents (ARIA) by the French Ministry of Environment [38].
- Major Hazard Incident Data Service by Health and Safety Executive (MHIDAS) [39]

Google Scholar, web search engine of scholarly literature by Google [40].

### 2.2.2. Benchmark

A comparison with other recognized DRA methods can be employed to test whether the analyzed method is suitable for a specific application area. The activity of benchmarking primarily refers to the comparison of results from the two methods and allows identifying similarities and/or specificities on how the input data are processed. Fundamental aspects are the sensitiveness of the methods with respect to input changes (reflecting operational variations) and the overall conservativeness of their assessment.

Statistic metrics are to be used for comparison of results. The kurtosis and skewness metrics are important descriptors of a data distribution shape. Kurtosis shows whether the distribution is peaked or heavy-tailed relatively to a normal distribution [41]. This suggests whether the technique has a rather constant evaluation of risk during the period considered (peaked distribution) or it is subject to

large variations (heavy-tailed distribution). For this reason, kurtosis comparison is an indication of the relative sensitiveness. Skewness measures the degree of asymmetry of the distribution. The skewness for a normal distribution is zero, while positive skewness values indicate data that are skewed right (the right tail is long relative to the left tail), and vice versa [41]. This provides an overall picture of how the technique has evaluated risk during the period considered. This metric comparison describes relative conservativeness.

**Reference method for comparison.** A recognized DRA method that has specific similarities to the analyzed method should be considered. This study uses the frequency modification methodology based on technical, operational, and organizational factors (TEC2O) [42] as it is based on the collection and evaluation of key performance indicators and was developed for the O&G domain. TEC2O is a consolidated method while RB is a method that has mainly been defined and used for specific industrial applications [15]. For this reason, validation by TEC2O was deemed to be not only appropriate but also functional to strengthening the RB methodology. In this work, this method is exclusively functional to the benchmark approach and, for this reason, is introduced in this section.

TEC2O focuses on updating the likelihood of hydrocarbon release from the equipment on O&G installations, which is a common application area of the two methods. Both methods use a set of indicators that are related to operational and technical causal factors. Indicator measurements are quantified on a standardized discrete scale and are important input parameters for both methods. The impact of indicators on the risk is calculated based on a weighted sum of the indicator values in both methods. However, the differences between RB and TEC2O should be noted. The RB identifies accident scenarios and the associated safety barriers, whereas TEC2O focuses on single equipment items included in the current QRA. The RB emphasizes on capturing the changes in the risk level, such that most indicators in the RB are related to the performance of safety barriers based on field data. Indicators of TEC2O are selected from a set of generic indicators that are related to the specific equipment characteristics. An extensive description of the method is reported elsewhere [4,42–44]. The key elements are summarized in the following section.

The fundamental relationship in the TEC2O method enables us to update the leak frequency as follows:

$$F(t) = F_0 \times \mathrm{TMF} \times \mathrm{MMF} \tag{4}$$

where $F(t)$ is the timely updated accident frequency, $t$ is the time, $F_0$ is the baseline frequency value, TMF is the technical modification factor and MMF is the management modification factor. TMF and MMF are obtained by combining different scores, which are produced by monitoring the quantitative indicators. The TEC2O procedure is depicted in Figure 2.

TMF aims to synthetically account for the lifecycle of equipment to penalize "old" units, which may be more prone to leaks and failure due to aging, erosion and/or corrosion phenomena. Moreover, external factors (environmental issues, seismic zone, and harsh weather areas) are considered. TMF only contributes as a worsening element since the failure likelihood of typical mechanical and electrical components or systems increases with time, with an increasing rate that approaches (or in some cases extends) the end of the design life. TMF is based on four subfactors, as indicated in Figure 2a. Periodical monitoring of related indicators statuses enables an average score to be assigned to each of the four subfactors. The weighted combination of the scores enables the total technical score ($\varepsilon$) to be determined and converted to the TMF.

The evaluation of the MMF is based on the concept of resilience and follows the resilience-based early warning indicators (REWI) methodology [45]. Managerial aspects are related to the definition of the safety procedures, training, and competencies of the operators, safety culture, frequency of maintenance operations and communication at different levels of the organization. To introduce a quantitative evaluation of these factors, the REWI method proposes the use of indicators, which are quantitative parameters, so they can be monitored, modified and updated in time. According to [45], the MMF is divided into two main subfactors (Figure 2b): An operational subfactor and an organizational subfactor. Periodical monitoring of related indicators statuses enables an average score

to be assigned to each subfactor. The weighted combination of the scores enables the total technical score (μ), which is converted to the MMF.

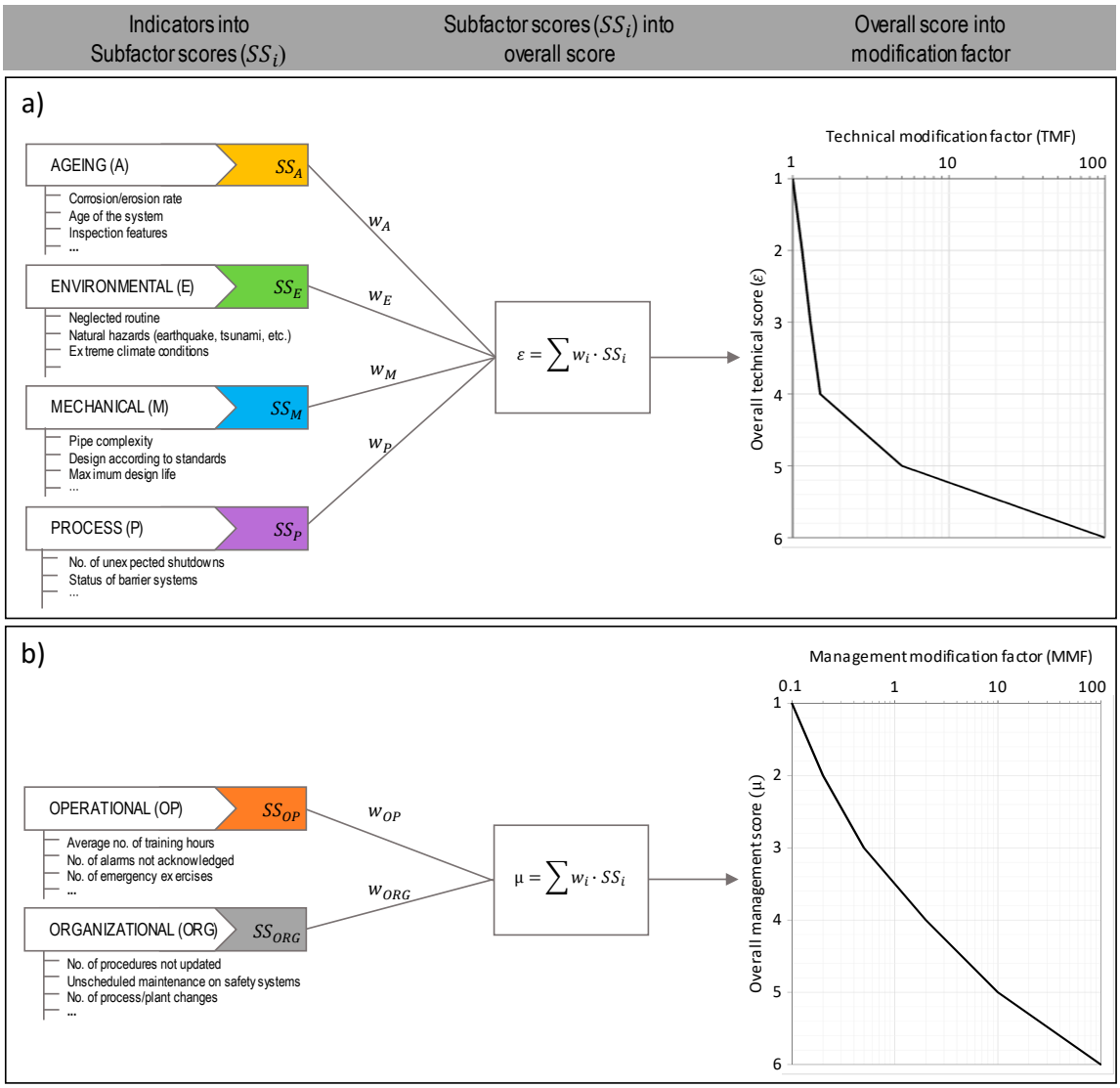



**Figure 2.** Schematization of the procedure for the application of technical, operational, and organizational factors (TEC2O): (**a**) Evaluation of technical modification factor technical modification factor (TMF), (**b**) evaluation of management modification factor management modification factor (MMF). Adapted from [42].

### 2.2.3. Peer Review

Rosqvist and Tuominen [46] introduce a specific peer review process for formal safety assessment. In this work, an adapted version of this process is implemented for validation of the DRA method. The results of this process should be reviewed by experts and operational personnel inasmuch as information from any QRA model should be peer-reviewed before accepted to be used for decision-making. A set of pivotal items are suggested in Table 2 to lay the foundations of the peer-review process. These items address the ultimate goal of the peer review of reducing uncertainty, which may be related to completeness, coherence, and accuracy. Coherence within risk assessment objectives and modeling is important, as they are the foundations of the study. Any incompleteness in the previous steps of risk assessment introduces a latent bias in the following steps. Accuracy in the evaluation of prior parameters and the risk index is essential to obtaining the correct definitions of safety barriers and their

effect on risk. Incompleteness in the definition of safety barriers may negatively affect the redundancy of safety systems and the total installation safety.

**Table 2.** Pivotal elements for peer review.

| Item | Object of Review | Comment |
|---|---|---|
| Objectives | Risk acceptance criteria (e.g., ALARP). | Acceptance criteria should match the external requirements (i.e., regulations and standards). |
| Hazards/scenarios | Set of unwanted events. | A relative lack of process experience may negatively affect this item [47]. |
| Safety barriers | Safety barriers defined for the set of unwanted events. | Whether the barrier systems included in the analysis can realize the desired risk reduction should be validated. |
| Model | Barrier modeling, including risk indicators. | Whether the safety barriers are well interpreted by the barrier system, subsystems, and related models should be assessed. |
| Prior parameter values | Prior parameter values that are considered in barrier modeling | Step formed in a formulated procedure, typically including [48] (1) preparation, (2) elicitation, and (3) calibration. |
| Risk index | Results | Whether the presentation of the risk level is appropriate for the purpose and provides concrete support to operations that directly control the process should be assessed. |

## 3. Case Study

The O&G industry is gradually implementing IO strategies to support work processes [12,13,49–53]. This implies important changes compared to traditional operations where O&G production was almost totally managed by the platforms with little or no interaction with external parties. Now the boundaries of the system are reshaped by using available digital infrastructures and real-time data to monitor operations and control processes remotely. The exchange of information over large distances without significant delay and the use of high-quality collaboration technology connects different actors and increases access to expert knowledge.

This is particularly important in complex installations characterized by numerous wells connected through flowlines to a floating production storage and offloading (FPSO) unit. The FPSO exports to trading tankers and collaborates with nearby drilling platforms, onshore facilities to process and distribute the product, and a number of contractors collaborating and depending on each other within the operations (Figure 3). Such installations may represent a virtual cluster of organizations with multiple expertise across disciplines, organizations, and locations [12,13].

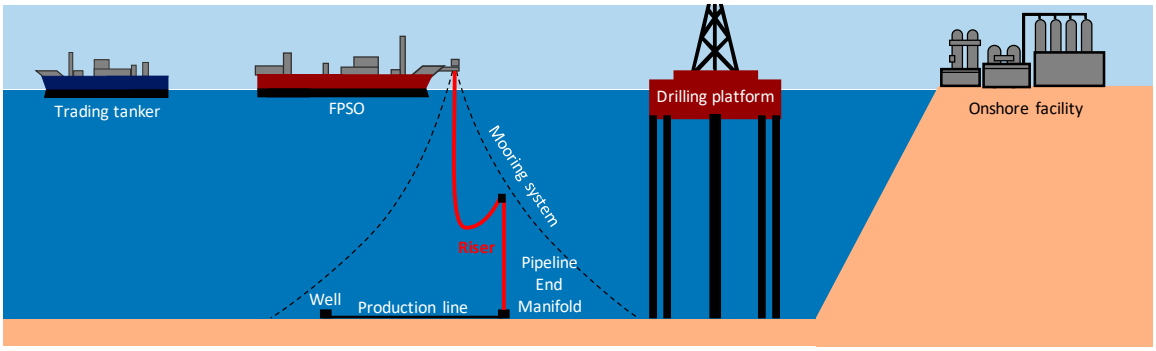



**Figure 3.** Representation of the installation considered for the case study and identification of the reference equipment for the analysis (riser).

Although the geographical location has progressively become secondary for the abovementioned aspects, it is still critical for what concerns production. For instance, installations producing from oil

wells in soft formations commonly require appropriate precautions, such as control of sand or fines with fluids [54]. Sand does not have economic value and can plug wells, erode and corrode equipment, and reduce well productivity. In certain producing regions, sand control completions generate considerable operational expenses. Paltrinieri et al. [14,44] have previously suggested DRA strategies to effectively control the potential loss of containment due to oil sands. Continuous monitoring is essential for providing effective management of the safety barriers in place, regardless of the managers' physical location. Due to these specific criticalities, this case is considered for the validation of the RB. The case is based on the results from a project with a major oil company within the overall framework of the Center for Integrated Operations in the Petroleum Industries [55]. Details are provided elsewhere [14,15,29,49].

### *3.1. Description of the Installation*

The case study is based on a sand erosion issue in a real offshore oil production installation with multiple topside modules. A multi-jointing yard and marine supply base support the FPSO operations from onshore. The production installation is located subsea and connected with a spread-moored FPSO, which is used as a hub to process and store the fluids produced from the subsea wells. Figure 3 shows a representation of the facility that is considered for the case study. The analysis focuses on the riser of the FPSO (highlighted in red in Figure 3) and its material degradation due to the processes of erosion/corrosion. The riser is a piping system in which a multiphase stream (e.g., containing oil, gas, and water) is sent from the wells to the preliminary treatment on the on-board process facility.

An excessive sand production rate, i.e., an increase in both sand production and flow velocity that exceeds a critical threshold, causes pipeline material degradation. Sensors to detect oil sand are usually employed [14,44]:

- An acoustic sand detector (ASD) performs online monitoring and provides immediate information. The ASD records the noise produced by sand carried in the process flow. The detectors are placed subsea on the outside of the flow line bends and detect the noise made when sand collides with the pipeline wall.
- An erosion probe, i.e., a metallic surface inserted in the well stream is physically eroded by passing sand particles. This detector is placed topside and only reports accumulated effects over a longer time period.

One of the main safety measures that are used to prevent sand erosion at the root of the problem is the gravel pack. A gravel pack is a downhole filter that is held in place with a properly sized screen. In case the gravel pack is not sufficient and excessive sand production is detected, a specific sand response procedure should be performed.

A sand response procedure that is based on sensor-based monitoring [14,44] is also employed as a prevention measure. This procedure implies that if sand is detected and its rate exceeds a specific threshold, the flow line should be choked back until the sand production rate is acceptable. Generally, the acoustic sand detector is used for dynamic monitoring, and the erosion probe represents subsequent confirmation of the results.

A corrosive environment and sand deposit may also cause pipeline material degradation due to corrosion. The gravel pack is a safety measure for this scenario, as it can prevent sand production and sand deposit where the flow is slowed by line bends. Injection of appropriate chemicals into the fluids to inhibit corrosion (chemical treatment) is another safety measure that is defined to prevent a corrosive environment, which may be based on sensor detection of oil corrosiveness. Moreover, cleaning pigs to run within the riser can be employed if a sand deposit is expected from the results of the sand detectors.

### *3.2. FPSO Lifecycle*

The study focuses on the operations during the FPSO lifecycle, which is assumed to be 25 years. For this reason, the evolution of 87 items that describe the installation's technical, operational

and organizational factors was simulated within this period. To avoid specific organizational and maintenance management implications, the following main assumptions are considered in the application:

- no personnel change, and
- no equipment replacement throughout the entire time period.

Table 3 illustrates a selection of the simulated items, which are not indicators but details that describe the evolution of the technical, operational and organizational factors that represent the FPSO lifecycle for a period of 25 years (for this reason, no measuring time is reported). The definition of these items was inspired by the aspects considered by the REWI method [56]. The DRA techniques that were considered in this study (RB and TEC2O) are based on indicators that are similar but not identical (e.g., they may be based on a different measuring time, the indicators are reported in Tables S1 and S2 in the Supplementary Materials) and the items in Table 3 are the basis for their definitions. While most of the technical items are simulated based on literature and statistical sources [57,58], the operational and organizational items are simulated using sinusoidal trends with a randomly changing mean value to reproduce the relative unpredictability. Time evolution is described using a hyperbola function and initial indicators values are set equal to the values reported by Øien and Sklet [59].

**Table 3.** Selection of representative items describing the installation technical, operational, and organizational factors.

| Technical, Operational and Organizational Items |
| --- |
| • Age of the technical barrier system |
| • Amount of overtime worked |
| • Average availability of critical safety systems |
| • Average no. of exercises completed by operating personnel |
| • Average no. of hours of training |
| • Average no. of risk issues/cases discussed during weekly management meetings |
| • Average no. of safety job analyses performed by operating personnel |
| • Fraction of operating procedures that are risk assessed |
| • Fraction of serious loss of barriers that are adequately treated |
| • Fraction of work processes/procedures verified/tested in simulators |
| • Inspection results |
| • Loss of technical barrier signal |
| • Maximum no. of control and safety functions in bypass |
| • No. of alarms that are not acknowledged within 1 min or disabled (without acknowledgment) |
| • No. of cases in which a decision to respond is delayed or experts are not alerted |
| • No. of cases in which communication among actors is inadequate |
| • No. of different persons who facilitate/lead safety job analyses |
| • No. of emergency preparedness exercises |
| • No. of feedbacks on procedures (tracked in the management system) |
| • No. of hours of simulator training for operating personnel |
| • No. of internal audits/inspections that address technical safety |
| • No. of overrides of safety systems |
| • No. of overrides of safety systems extended to next shift |
| • No. of outdated procedures |
| • No. of red traffic signals in the system for barrier control |
| • No. of risk issues communicated to the entire organization |
| • No. of times that critical ICT systems fail or are inoperable |
| • No. of toolbox meetings |
| • No. of violations for authorized entrance of systems |
| • No. of visual inspections of real or simulated suspended bypasses |

**Table 3.** *Cont.*

| Technical, Operational and Organizational Items |
| --- |
| • No. of years of personnel experience with this system<br>• Number of unscheduled maintenance operations on safety systems (including possible maintenance call-backs)<br>• Overdue inspections<br>• Portion of a company that actively uses the risk register<br>• Portion of operating personnel who are informed about risk analyses<br>• Portion of operating personnel who receive training<br>• Portion of operating personnel who take risk courses<br>• Temporary repairs that become permanent and neglected routine<br>• Unexpected shutdowns<br>• ... |

## 4. Results

### *4.1. RB Application*

**Step 1: Scenario definition.** A hazardous event was defined as material degradation of the riser wall. The hazard is the presence of sand particles in the hydrocarbon flow from the well. The two identified events that cause degradation are (i) erosion due to excessive sand production with exceeding velocity, and (ii) corrosion due to sand under-deposit combined with corrosive environment.

After the identification of possible event sequences, barriers are considered. The existing proactive barriers include the gravel pack, the sand response procedure, pigging, and chemical treatment. Reactive barriers to degradation caused by erosion and corrosion are operational strategies and erosion/corrosion allowance. The final outcomes are listed as follows: (1) Loss of containment, (2) loss of production, and (3) unscheduled repair. The total result of Step 1 is presented in the bowtie diagram depicted in Figure 4.

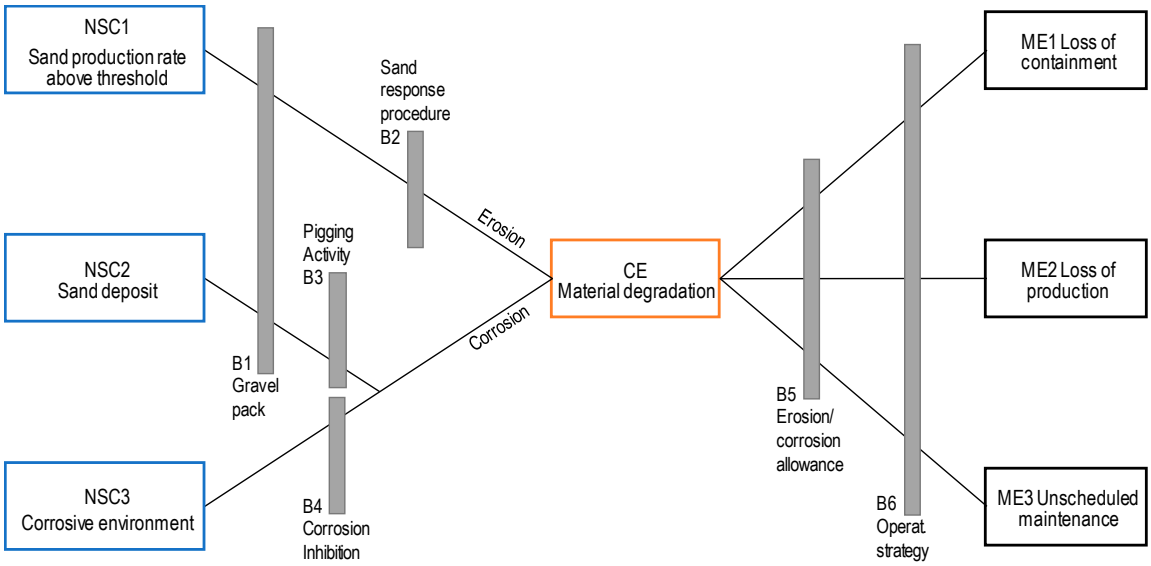



**Figure 4.** Bowtie diagram for a case of sand erosion and corrosion in offshore oil production. NSC = necessary and sufficient condition, B = barrier, CE = critical event, and ME = major event [27,60].

**Step 2: Review of relevant information sources.** Specific information about the case was obtained from three workshops with the major oil company (participants listed in Table 4), which enabled a set of indicators to be identified based on the barrier systems and their relative importance.

**Table 4.** Workshop participants from the major oil company.

| Participants | Main Responsibilities |
| --- | --- |
| Regional risk coordinator | Business owner for the risk management tool, including managing users, training, data and the developers. Working on risk team to review regional risks with the line and feed them up through the company annually for chief operating officers to review. |
| Threats Advisor Manager | Management of the advisor system. |
| Threats Advisor System Project Management Office Lead | Ensuring compliance with intellectual property and legal including technology project processes, branding, and marketing. |
| Subsea Integrity Engineer | Improving the integrity management system for subsea operations team. |
| Material Engineer | Integrity management system for subsea operations team. |

Furthermore, the generic information employed for this step includes studies of sand production during extrusion of hydrocarbon [54], risk indicators [4,26,42,61–63], and expression of barrier criticality [19,29,49,64–68].

**Step 3: Establishment of barrier functions and systems.** The first degradation event sequence refers to erosion caused by an excessive amount of sand in which the critical threshold velocity of the oil flow is exceeded (NSC1). The involved safety function is "prevent erosion", which is achieved by two safety barriers: B1 filtering sand particles with a gravel pack, and B2 sand response procedure after the detection of excessive sand. Two barrier elements are used for sand detection, i.e., ASD and erosion probe. The second degradation event sequence refers to corrosion, which may occur with sand under deposit (NSC2) in a corrosive environment (NSC3). The safety function, in this case, is "prevent corrosion", which is achieved by three safety barriers: B1 gravel pack, B3 cleaning pigs, and B4 corrosion inhibitor. The major event of loss of containment is prevented by B5 (erosion/corrosion allowance) and B6 (operational strategy). The results of this step are represented by the objective tree depicted in Figure 5.

**Step 4: Evaluation of relative importance of safety barriers.** As the QRA is not available, the results from Steps 1–3 are used to perform a qualitative evaluation of the safety barriers and define their relative importance. A qualitative evaluation of the safety barriers is presented as follows:

B1. The gravel pack (i.e., physically installed to prevent sand in the well fluid to flow to the production unit) is a passive barrier system. This system applies to the excessive sand production rate (NSC1) and sand deposit (NSC2).
B2. The sand response procedure (i.e., operator intervention as a response to excessive sand production rate detected by ASD and erosion probe) consists of technical and operational barrier systems that apply to the sand production rate (NSC1) and can prevent sand erosion.
B3. Pigging activity (i.e., the pigging equipment removes sand deposits in the riser) is a technical barrier that applies to the sand deposit (NSC3). However, it cannot prevent corrosion.
B4. Inhibition (i.e., injection of corrosion inhibitors) is an operational barrier that applies to a corrosive environment (NSC2) but cannot prevent the corrosion phenomenon.
B5. Pipe wall allowance (i.e., increased design thickness of the riser wall) is a passive technical barrier that can mitigate material degradation (CE).
B6. Operational strategy (i.e., modification of production strategy) is an operational barrier that mitigates degradation (CE) and is the last barrier for preventing the final major events of release (ME1), loss of production (ME2), and unscheduled maintenance (ME3).

The following criteria are also considered for the definition of the barrier relative importance.

1. A safety barrier should be active (controllable) to be considered in the RB model. For simplicity, passive barriers are considered a constant factor as their degradation is not within the primary

scope of the RB application. The RB primary scope is to provide operational support for actions that can directly control the process.

2. The relative importance of a safety barrier within the RB model increases with its proximity to the final major event. This importance is demonstrated by the sensitivity analysis performed on barrier $i$ by assessing its Birnbaum-like measure $I^B(i) = \frac{\partial R}{\partial FP_i}$ (Figure 6), where $R$ is the total risk and FP is the barrier failure probability [15,69]. The failure of a safety barrier at the beginning of a sequence of barriers can be considered relatively less critical than the failure of the last safety barrier that separates the target from a major accident.
3. The relative importance of a safety barrier within the RB model also increases with the number of unwanted events that it can address. This importance is demonstrated by the sensitivity analysis of barrier $i$ that was performed by assessing the Birnbaum-like measure [15,69] (Figure 6).

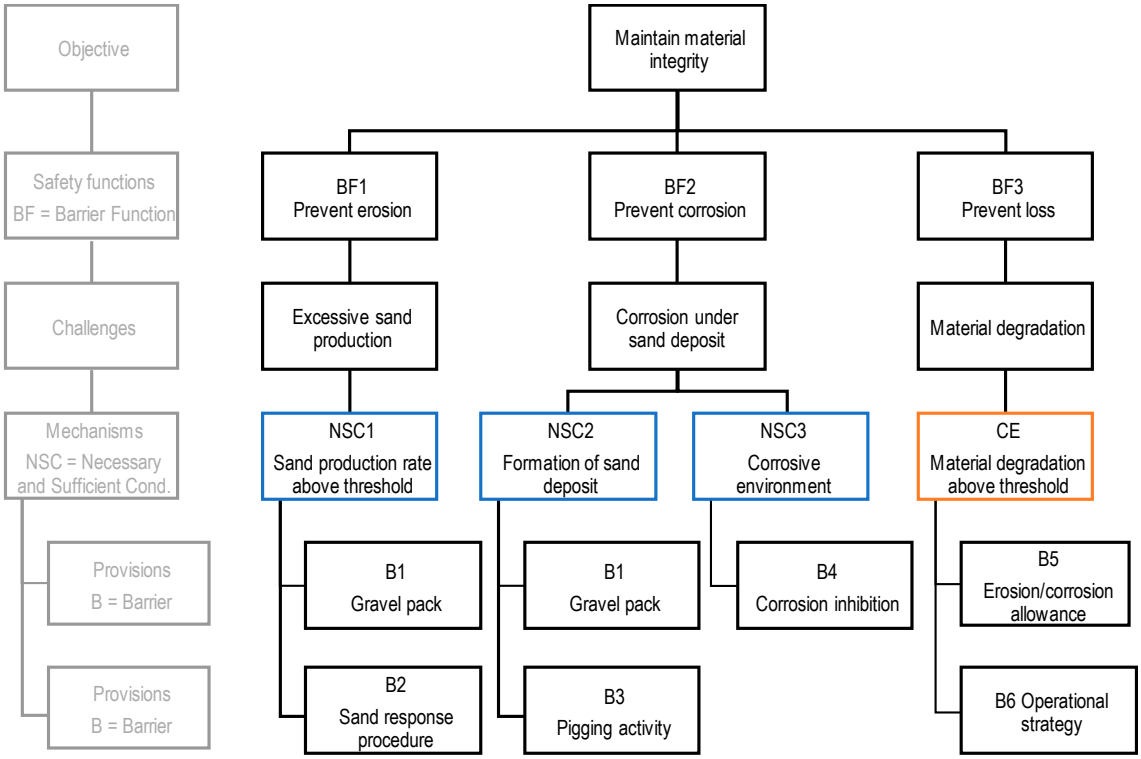



**Figure 5.** Objective tree for a case of sand erosion and corrosion in offshore oil production. BF = barrier function, NSC = necessary and sufficient condition, B = barrier.

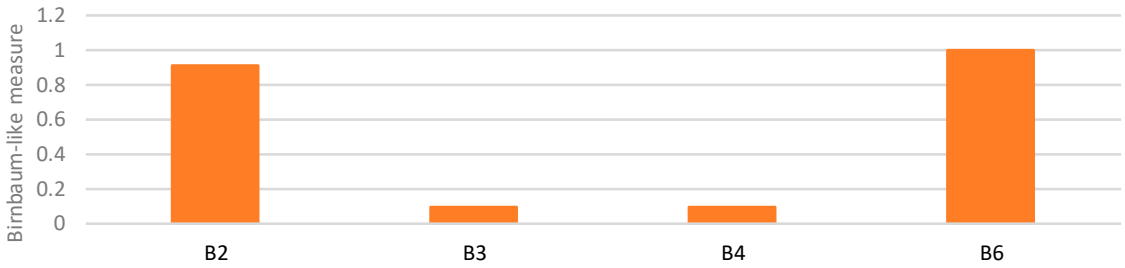



**Figure 6.** Birnbaum-like measures for the barriers B2 (sand response procedure), B3 (pigging), B4 (inhibitor), and B6 (operational strategy), considering generic FPs from the ARAMIS guidelines (Accidental Risk Assessment Methodology for Industries in the context of the Seveso II directive) [70].

Based on the qualitative evaluation and the mentioned criteria, the relative importance of the barriers is defined and expressed by the ranking in Table 5.

**Table 5.** Ranking of safety barriers, which expresses their relative importance within the Risk Barometer (RB) (B3 and B4 are equally ranked third).

| Ranking | Barrier |
|---|---|
| 1 | B6. Operational strategy |
| 2 | B2. Sand response procedure |
| 3 | B3. Pigging B4. Inhibitor |

**Step 5: Establishment of barrier performance indicators.** Sets of barrier performance indicators are defined based on the information collected during the workshops with the major oil company involved in the case study (Table S1). For instance, the indicators defined for the barrier "sand response procedure" are shown in Table 6. Due to the lack of frequency values for the NSCs, a constant status is assumed to focus on barrier performance variations.

**Table 6.** Example of the indicator set for the "sand response procedure" barrier.

| Barrier Element | Indicator | Comment |
|---|---|---|
| ASD | • Age of the technical barrier system.<br>• Loss of technical barrier signal in the last three months | ASD is mounted in inhospitable conditions that impede maintenance activities. |
| Erosion Probes | • Loss of technical barrier signal in the last three months<br>• Overdue inspections | Overdue inspections indicate odd functioning, while signal loss reduces the probe performance. |
| Manual well-flow sampling | • No. of feedback on procedures (tracked in the management system)<br>• Fraction of operational procedures that have been risk-assessed<br>• Average no. of hours of training in the last three months | This barrier requires laboratory equipment and adequate procedures by personnel. |
| Response to sand detection | • No. of feedbacks on procedures (tracked in the management system)<br>• Fraction of operational procedures that have been risk-assessed<br>• Fraction of work processes/procedures verified/tested in simulators<br>• Average no. of hours of training in the last three months<br>• Portion of operating personnel who receive training in the last three months<br>• No. of hours of simulator training for operating personnel each month | This barrier requires compliance to adequate procedure by personnel. |

**Step 6: Establishment of a risk model.** The established risk model is based on the bowtie diagram in Figure 4. For simplicity, indicator weights were considered uniform, but assessment using the analytical hierarchy process (AHP) based on personnel's feedback is necessary for further refinement [71]. Linear interpolation was used to obtain the indicator measure as the items mentioned in Section 3.2 were expressively simulated to facilitate the definition of indicators. However, other simulation functions may be used in case of sparse data. The gravel pack (B1) and erosion/corrosion allowance (B5) are passive barriers. For this reason, they were omitted (Step 4), as shown by Figure 7. Moreover, the model focuses on the worst-case consequence: Loss of containment (ME1). Risk is defined as the risk of loss of containment.

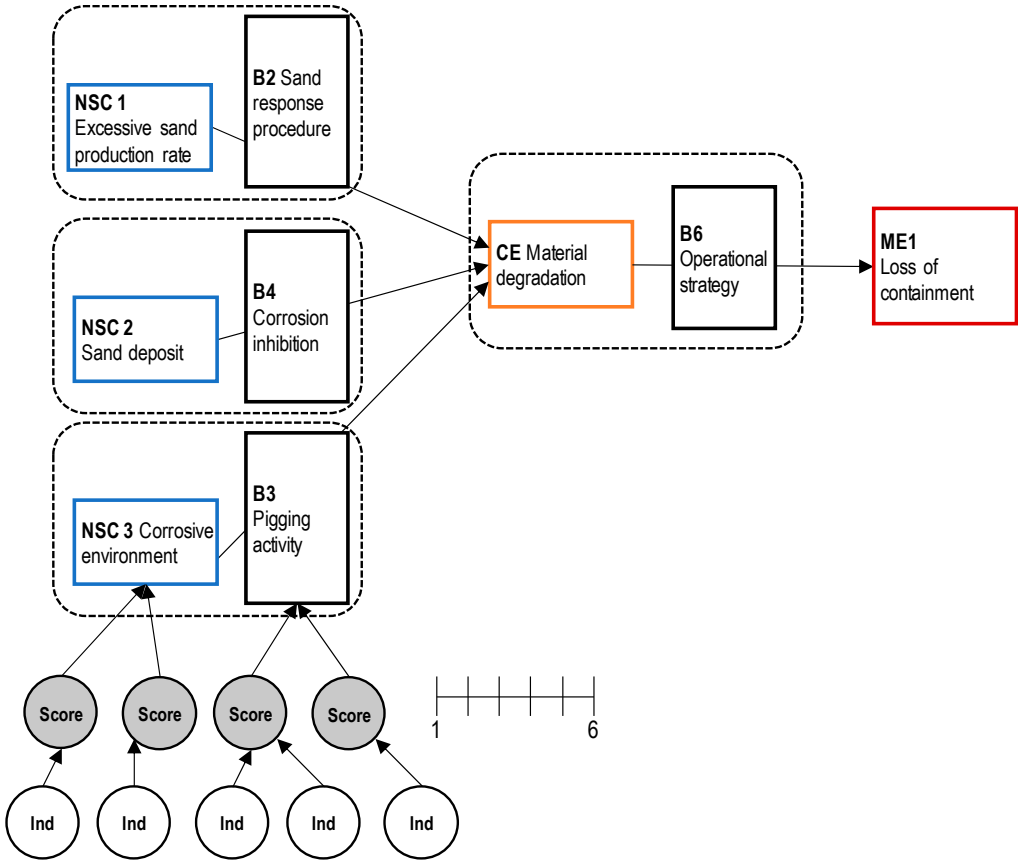



**Figure 7.** Graphical representation of the risk model for the RB. NSC = necessary and sufficient condition, B = barrier, CE = critical event, and ME = major event.

**Step 7: Visualization.** The total result of the RB application is the trend of the loss of containment risk for 25 years (300 months), as shown in Figure 8, considering the FPSO lifecycle simulation (Section 3.2).

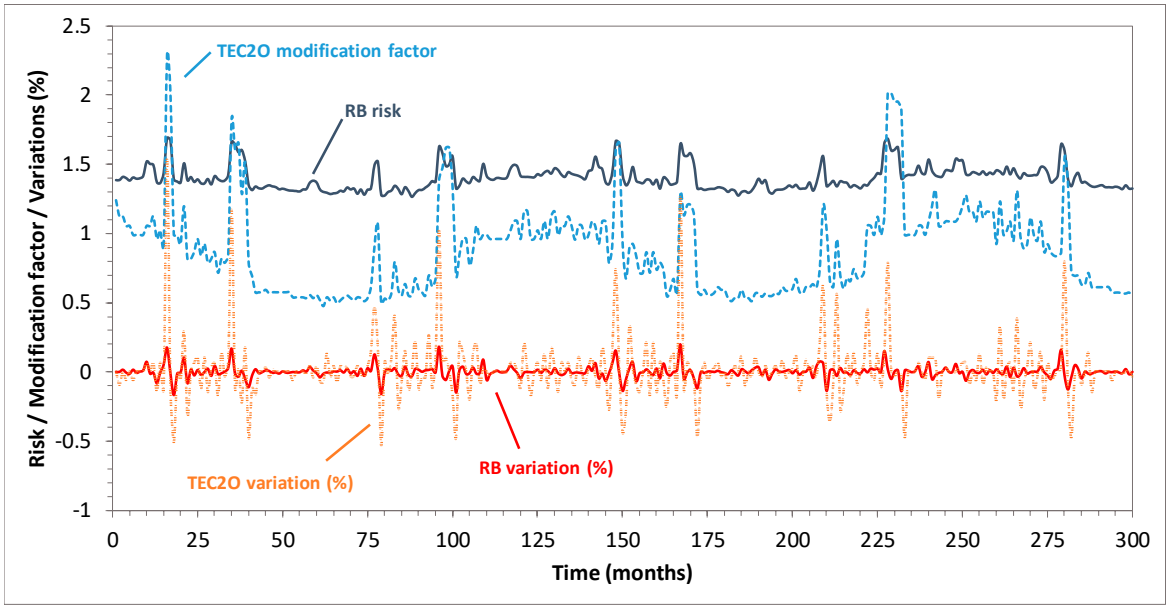



**Figure 8.** Trends of RB loss containment risk (1–6 score), TEC2O adimensional frequency modification factor, and respective percentage variations.

### *4.2. Reality Check*

Several queries were performed in the search and considered different combinations of the following keywords: "Corrosion", "erosion", "sand oil", "hydrocarbon leak", "hydrocarbon release", "oil leak", "oil leakage", "offshore pipeline", "oil pipeline", and "pipeline". In addition, the results were manually filtered based on their relevance to the case.

While the eMARS database [37] did not provide relevant information, one relevant event was identified from a search on ARIA [38]. The search on MHIDAS [39] generated two relevant reports on corrosion events and two reports on offshore oil releases. However, the results from these databases provided only limited information about the purpose of this work.

The search on Google Scholar [40] revealed further sources of information, such as the following reports on accidents in the petroleum offshore industry:

Doc. 1. "Riser and pipeline release frequencies" by the International Association of Oil and Gas Producers [72];
Doc. 2. "Offshore hydrocarbon releases statistics and analysis" by Health and safety Executive [73];
Doc. 3. "Hydrocarbon leak on Oseberg A on 17 June 2013" by the Norwegian Petroleum Safety Authority [74].

Document 1 reports failure mechanisms and relative occurrence percentages for offshore pipelines. In 36% of the cases analyzed by the document, corrosion is the main failure mechanism. Document 2 does not specifically focus on one type of equipment, such as pipelines. However, the document reports a record of approximately 1600 equipment faults that occurred between 1 October 1992 and 31 March 2002. Almost 20% of the faults were caused by corrosion/erosion. Document 3 by Oseberg A focuses on a gas hydrocarbon leak that occurred on an offshore facility on 17 June 2013. This report indicates that sand production was the direct cause of the accident: "The main reason that the test manifold blown line was able to develop over time and eventually cause a gas leak was that an adequate review of the plant had not been conducted to verify that it could handle sand production".

This past accident data analysis provides an overview of the sand production issues within the O&G sector. The collected data indicate the criticality of the causes and consequences of erosion/corrosion. These data match the scenario events identified by the RB, which confirm its ability to address major accident hazards. In particular, document 3 highlights the dynamic aspects of the hazardous event and implies that continuous monitoring of risk associated with erosion/corrosion risks is necessary.

### *4.3. Benchmark*

Despite similar inputs for RB and the parallel method TEC2O, a comparison of their results may not be straightforward. The RB method provides an adimensional value of risk level, while the TEC2O final result is an updated leakage frequency associated with the FPSO riser. For this reason, the adimensional TEC2O frequency modification factor (FMF) was used to represent the method results:

$$\mathrm{FMF} = \mathrm{TMF} \times \mathrm{MMF} \tag{5}$$

Figure 8 shows the RB risk and TEC2O FMF for a period of 25 years. The results from both methods follow a total common trend, as most of the peaks match. Moreover, both curves have sinusoidal behavior, which is accentuated in TEC2O FMF. This finding reflects the contribution of operational and organizational indicators, which were simulated by sinusoidal curves. The percentage variations in the RB risk and TEC2O FMF confirm the trend conformity. Note that the RB expresses the risk level on a scale from 1 to 6, while TEC2O FMF can range from $10^{-1}$ to $10^{4}$. Considering these ranges, the RB results indicate a more conservative method, as TEC2O FMF eventually produces a negligible variation of the leakage frequency for the FPSO riser.

Considering that the two techniques have processed similar sets of input data, a kurtosis comparison shows how the techniques evaluate changes in controlling loss of containment. A pointed

distribution suggests that the control of the loss of containment has a constant performance, as its risk or FMF are not subject to large variations. In this case, the RB kurtosis shows a situation that is less stable than that of TEC2O (Figure 9 and Table 7).

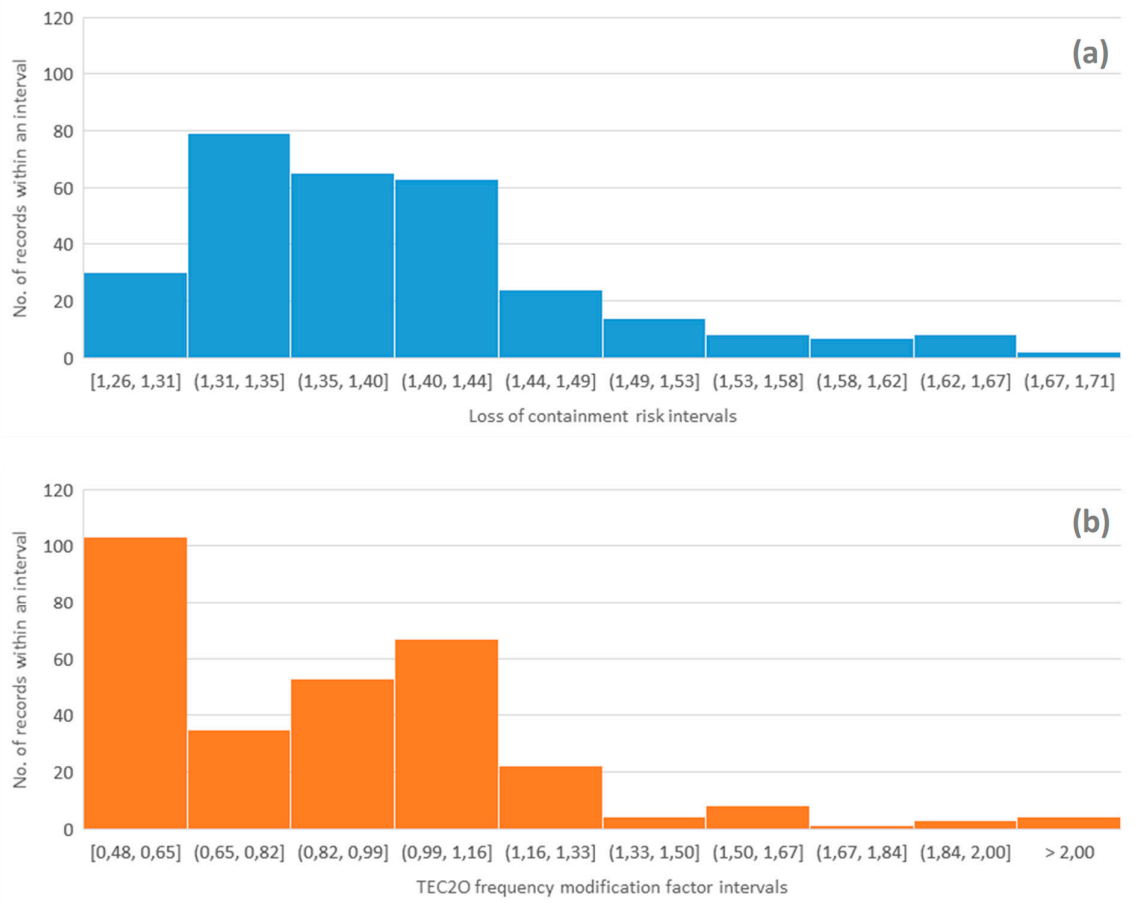



**Figure 9.** (**a**) Distribution of RB loss of containment risk, and (**b**) distribution of TEC2O frequency modification factor.

**Table 7.** Kurtosis and skewness of RB loss of containment risk and TEC2O frequency modification factor distributions.

| Method | Kurtosis | Skewness |
|---|---|---|
| Risk Barometer | 1.433 | 1.235 |
| TEC2O | 2.383 | 1.298 |

The skewness comparison (Figure 9 and Table 7) shows how the techniques evaluate the performance in the loss of containment control based on similar sets of input data. Positive skewness indicates a positive performance of loss of containment control, as the associated risk or FMF have relatively low values. In this case, the skewness values of both techniques are positive and similar, TEC2O is slightly higher.

Considering that TEC2O presents higher values of both kurtosis and skewness, we can affirm that the technique generally reports a more positive and stable evaluation for the case (despite a few higher peaks in its derivative, Figure 8), which confirms that RB is a more conservative technique that flags higher levels of risk.

For both methods, the selected set of indicators (i.e., main model inputs) will affect the selection of data to collect during the operation on a daily basis. Despite the careful selection of the matching

indicators for the RB and TEC2O, the methods have different approaches to the translation of physical parameters (e.g., pipeline thickness and age) and qualitative information (e.g., inspection effectiveness) to the standardized range (1–6). The RB presents the relative changes in the risk level, while TEC2O has greater relevance to the existing QRA results (i.e., last updated leak frequency) as a basis.

### *4.4. Peer Review*

The pivotal elements in Table 2 are considered and critically discussed, assuming the perspective of peer reviewers.

**Objectives.** Risk acceptance criteria for this case were initially established by the major oil company. However, an external requirement may be compliance with a decreasing trend in historical leak frequency with time for installations on the Norwegian continental shelf after year 2000 [75]. Moreover, changes in practices, procedures, regulations, or emerging risks associated with design modifications (e.g., new technology) may produce alternative criteria. For this reason, assessment of the validity of the acceptance criteria needs to be iterated with a focus on the coherence between the objectives and the application of the RB in practical cases.

**Hazards/set of events.** Identification of hazards and unwanted events included in the case study was also facilitated and subsequently validated by the company experts. However, changes to the equipment and plant during operations, such as the introduction of new technologies or the collection of previously disregarded risk notions, may require a review for completeness of hazard identification. Techniques such as the methodology for the identification of major accident hazards (MIMAH) [27] may provide generic accident scenarios and establish a basis for peer review. In addition, dynamic procedure of atypical scenarios identification (DyPASI) [28] can be adopted to consider atypical unwanted events.

**Safety barriers.** The RB model is related to the bowtie diagram defined by the hazard identification phase. This structure is also the result of workshops and follow-up communications with the involved oil company. Further validation may be sought by the Norwegian Petroleum Safety Authority principles for barrier management in the petroleum industry [68].

**Model.** The accident investigation report of the Macondo blowout accident [76] showed that some barriers had limited ability in performing the desired functions before the catastrophic event. The barrier structure should reflect the relationship between function and systems, which highlights its capabilities and limitations. The model is intentionally revisable to favor expert judgment input, but total coherence is needed. Sets of predefined indicators, such as the REWIs, may be used by peer reviewers for comparative assessment [62]. The weights assigned to the indicators have been considered uniform in this work due to limited feedback from the company, and accurate weighing enables further model refinement. This weighing is possible via AHP, which is valid only if the weight judgment is coherent [71].

**Parameter values.** Partial sets of risk indicators (input) can negatively affect the model and assessed risk. This work considers only a representative set of indicators and related values. A detailed integration is necessary for industrial applications. For instance, accurate human reliability indicators may be integrated by the SPAR-H (standardized plant analysis risk-human reliability analysis) method to estimate human error probabilities in the petroleum industry [77–79].

**Risk index.** RB enables drill-down capabilities, which indicates that the user can understand the cause of risk changes, which may reside in anomalous barrier performance. RB ensures that guidance given to operational staff and experts across systems pertains to parameters that can be directly controlled. The risk level is expressed by a barometer-type visualization and a trend over time. Results that accurately and proactively reflect critical conditions should not only be indicated by these risk indexes but also support user decision-making. The RB is explicitly designed to easily adapt to the user's needs [32,80] based on the feedback collected within the involved company.

## 5. Discussion

### *5.1. Lessons Learned*

This validation study for the RB method has addressed both the challenges that may be encountered in the validation of novel techniques and the issues associated with dynamic risk analysis. The research questions defined in Section 1 were addressed as follows:

**Capability of identifying major accident scenarios and safety barriers.** This issue highlights the correct identification of the accident scenarios that are subsequently modeled by the method. The reality check performed in this study provides an initial confirmation of the criticality of the scenarios considered by RB due to the similarities with past accidents [38,39]. The failure mechanisms of erosion and corrosion and the sand erosion causality are confirmed by a non-negligible number of minor events [72] with a well-reported accident in 2013 [73]. Moreover, the dynamic aspects of the accident scenarios are highlighted by an accident report, which suggests continuous risk monitoring [74]. The actual peer review for the RB application was performed in collaboration with the major oil company involved in the case study [15]. Company experts provided their feedback in an iterative process to confirm or suggest improvements in the description of the potential accident scenarios and the involved safety barriers. This application is ideal and enables continuous and effective validation. Further validation may be sought in other studies [27] or authority documents [68]. In addition, the method for dynamic hazard identification (DyPASI) [17,28] is a tool to iteratively improve the identification of accident scenarios and related safety barriers to satisfying the peer review requirements.

**Suitability for capturing changes in the operations and updating risk.** The validation by benchmarks highlighted this aspect of the RB, which is essential for DRA. Both TEC2O and RB aim to provide a dynamic estimation of the likelihood of hazardous materials release (namely, the leak frequency in TEC2O and the loss of containment in RB). However, the differences between TEC2O and RB should be noted. TEC2O focuses on single equipment items, while RB includes important safety barriers in a determined hazardous scenario. TEC2O selects risk indicators, which are gathered from a provisional generic set that is based on specific equipment characteristics. RB focuses on risk indicators that are specific to barriers and aims to provide the risk level variation. For both methods, the selected set of indicators (i.e., main model inputs) affect the selection of data to collect daily during operations. However, the methods have different approaches in the translation of physical parameters (e.g., pipeline thickness and age) and qualitative information (e.g., inspection effectiveness) to a value within the standardized range (1–6). TEC2O has systematic procedures for processing sub factors based on collected data [42], while the RB is based on interpolation functions. Both methods use a weighted sum approach to aggregate information. TEC2O has more relevance to the existing QRA results (i.e., the last updated leak frequency) and pursues a periodic update of the frequency based on both quantitative data and qualitative data collected during the operation or in the design/manufacturing features. However, RB can provide a visualized presentation of the barrier status and risk level, as it is based on a hierarchical structure of safety barriers inspired by the objective tree and bowtie diagram. Concerning the peer review, the collection of actual feedback on the RB model for updating risk was not possible but its design is intentionally revisable to promote and consider expert judgment. A peer review was performed for RB risk visualization, which was iteratively developed based on the needs of the involved major oil company.

**Comparison of results with another DRA method.** The benchmark showed that the RB results follow a trend that is comparable with the TEC2O FMF, as the peaks match the curves that have a sinusoidal behavior. The measures of kurtosis and skewness from statistics are also applied in the benchmark validation. The RB has a relatively unstable performance if compared with TEC2O, while the skewness values of both techniques are positive and similar. In general, conformity between the results from the RB and TEC2O is observed. However, it has to be noted that RB is considerably more conservative than TEC2O. A conservative approach may be preferable as it enhances prevention. If needed, appropriate weight calibration may attenuate this feature and prevent unnecessary warnings.

**Realistic outcomes for industrial application.** The RB peer review process for the case study has helped and demonstrated the usefulness of the industrial application as the development of a technique in collaboration with a company enables a continuous review to satisfy the company's needs. However, the peer review for this application was not complete as it primarily addressed the aspects of hazard identification, safety barrier definition, and the use of risk indexes. In general, discussing this issue addresses the accuracy and cost-usefulness claims expressed by Rae et al. [20]:

- Are the numbers sufficiently accurate to support decision-making? The benchmark results for this study show that RB has the potential to support and even improve decision-making compared with the TEC2O factors. As mentioned by Weinberg [81], "one of the most powerful methods of science (experimental observations) is inapplicable to the estimation of overall risk." The reverse is also not true, as perfectly reliable measurement may be invalid if the wrong results are consistently obtained. Thus, a benchmark can rebut but not confirm the accuracy claim. Although the resulting numbers are comparable, they are more accurate in principle despite the application of a reality check, as uncertainty about the produced numbers, dominant scenarios, and relative importance of contributing factors remain [21].
- Is the safety benefit from the DRA technique measurably better than a traditional QRA? In this case, usefulness is required for tracking the changes in risk over time [20], which is demonstrated by the results. These results confirm the requirements highlighted by Goerlandt et al. [21], which demonstrate how the RB (i) summarizes evidence from different sources via an extensive set of indicators, (ii) aims to facilitate communication among stakeholders with its risk visualization solutions and provide a platform for reflection and discussion, (iii) highlights areas of uncertainty by its drill-down capabilities, where additional information or research is necessary, and (iv) complements operational experience as demonstrated by the quality control of this study.

**Sustainable operations across systems.** Andersen and Mostue [12] review a series of risk analysis and risk management approaches for the petroleum industry from the perspective of applicability to IO concepts. On a generic level, they confirm that risk analysis methods are mostly used in design and modification projects and not during daily operation. Concerning IO, they show that they are mainly perceived as challenges by the operators. IO are considered to give good opportunities in the follow up of major accident risk for daily operations. However, a specific focus on human and organizational factors is required for a complete risk assessment within the IO framework.

The systematic validation approach in this contribution may have the benefit to build consensus in DRA and lead to confident sharing of evaluated risk levels across O&G virtual clusters. The tool has the potential to facilitate risk-informed collaboration between reservoir management, drilling, production optimization, operation and maintenance, logistics and HSE (health, safety, and environment). This represents a cornerstone to build effective communication practices and collaborative work processes between offshore and onshore organizations. The suggested validation approach explicitly addresses the method capabilities to monitor operations, which indirectly points to the need for monitoring human and organizational factors mentioned.

Overall, DRA validation within the IO framework entails the opportunities of improving DRA techniques and their consultation for daily activities from the perspective of the utilization of cross-system collaboration platforms.

### *5.2. Future Developments*

In the RB, the emphasis is placed on defining and quantifying risk indicators related to the causes of a hazardous event. The set of indicators is linked to operational decisions that are associated with maintenance planning based on both conditions of the components and the deviations made by operators and management. A set of indicators is desired to be valid, or the indicator must measure the most important aspects of the associated barrier systems or performance-influencing factors [15]. In the case of human and organizational factors, the validation can be improved by using real-case data

and comparing the outcomes of the method with the results from the human reliability analysis (HRA). This comparison may require a redefinition of the risk indicators set compared with the performance shaping factors (PSF) or adjustment of specific indicators values based on a task analysis for validation. Novel information systems may enable improvement in the reporting of planners, operators, and management, which can facilitate defining case-specific indicators [82] and relating the indicators to a generic HRA human error event for validation. For technical indicators, both the RB and TEC2O factors have the potential for improvement by taking into account the behaviors of the process systems influenced by dynamic operational and environmental conditions. Machine learning [9,69,83] can be qualitatively structured to provide reasoning between risk indicators (e.g., casual factors, incidences, testing result) and the safety barrier performance, and sensitivity analysis can be applied to rank the importance of the indicators.

## 6. Conclusions

In this work, an advanced approach to support the validation of DRA techniques dedicated to the process industry was illustrated. The validation approach relies on three parallel strategies: (i) Reality check, (ii) benchmark, and (iii) peer review.

The benefits of the suggested approach are the completeness and quality of the evaluation. These benefits are ensured by the application of different kinds of methods, which were previously proposed only for standard risk analysis. The effectiveness was demonstrated by a specific validation study. The RB, which is a novel method developed for DRA in the framework of O&G installations, was analyzed by the application of a case study to address sand erosion integrity in virtual O&G cluster, including an FPSO unit. The results from a past accident analysis confirmed the criticality of erosion/corrosion scenarios, as identified by the RB. Moreover, the dynamic nature of the event, which legitimizes the use of dynamic tools such as RB, was highlighted. The benchmark evaluation showed excellent conformity within the results from the RB and TEC2O factors, which validates the applicability of the RB indicators for the event with a loss of containment. A specific procedure for peer review that involves experts from the industrial domain confirmed the suitability of the RB in actual field applications.

This allows building consensus and trust in DRA techniques, as they represent a concrete solution for the implementation of integrated and safety-supported operations across the geographical, organizational, and disciplinary boundaries of the O&G industrial systems.

**Supplementary Materials:** The following are available online at http://www.mdpi.com/2071-1050/11/23/6745/s1, Table S1: RB indicators, Table S2: RB indicators.

**Author Contributions:** Supervision, G.L., G.R. and N.P.; Writing—original draft, S.L. and G.L.; Writing—review & editing, S.L. and N.P.

**Funding:** This research received no external funding.

**Acknowledgments:** The authors would like to thank Michele Filippetti, whose work inspired this study.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Haugen, S.; Edwin, N.J.; Vinnem, J.E.; Brautaset, O.; Nyheim, O.M.; Zhu, T.; Tuft, V.L. Activity-Based Risk Analysis for Process Plant Operations. 2016. Available online: https://www.icheme.org/media/11793/hazards-26-paper-56-activity-based-risk-analysis-for-process-plant-operations.pdf (accessed on 26 November 2019).
2. Yang, X.; Haugen, S.; Paltrinieri, N. Clarifying the concept of operational risk assessment in the oil and gas industry. *Saf. Sci.* **2018**, *108*, 159–268. [CrossRef]
3. Pasman, H.J.; Rogers, W.J.; Mannan, M.S. Risk assessment: What is it worth? Shall we just do away with it, or can it do a better job? *Saf. Sci.* **2017**, *99*, 140–155. [CrossRef]
4. Landucci, G.; Paltrinieri, N. Dynamic evaluation of risk: From safety indicators to proactive techniques. *Chem. Eng. Trans.* **2016**, *53*, 169–174. [CrossRef]

5. Øien, K. A framework for the establishment of organizational risk indicators. *Reliab. Eng. Syst. Saf.* **2001**, *74*, 147–167. [CrossRef]
6. Sklet, S.; Vinnem, J.E.; Aven, T. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). Part II: Results from a case study. *J. Hazard. Mater.* **2006**, *137*, 692–708. [CrossRef]
7. Aven, T.; Sklet, S.; Vinnem, J.E. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). Part I. Method description. *J. Hazard. Mater.* **2006**, *137*, 681–691. [CrossRef]
8. Gran, B.A.; Bye, R.; Nyheim, O.M.; Okstad, E.H.; Seljelid, J.; Sklet, S.; Vatn, J.; Vinnem, J.E. Evaluation of the Risk OMT model for maintenance work on major offshore process equipment. *J. Loss Prev. Process Ind.* **2012**, *25*, 582–593. [CrossRef]
9. Paltrinieri, N.; Comfort, L.; Reniers, G. Learning about risk: Machine learning for risk assessment. *Saf. Sci.* **2019**, *118*, 475–486. [CrossRef]
10. Bucelli, M.; Okstad, E.; Paltrinier, N.; Cozzani, V. Advanced methods for risk analysis with integrated perspective. In Proceedings of the Safety and Reliability—Theory and Applications—Proceedings of the 27th European Safety and Reliability Conference, ESREL 2017, Portorož, Slovenia, 18–22 June 2017; pp. 1335–1342. [CrossRef]
11. Bucelli, M.; Paltrinieri, N.; Landucci, G. Integrated risk assessment for oil and gas installations in sensitive areas. *Ocean Eng.* **2018**, *150*, 377–390. [CrossRef]
12. Andersen, S.; Mostue, B.A. Risk analysis and risk management approaches applied to the petroleum industry and their applicability to IO concepts. *Saf. Sci.* **2012**, *50*, 2010–2019. [CrossRef]
13. Foss, B. Real-time production optimization and reservoir management at the IO center. *IFAC Proc. Vol.* **2012**, *45*, 7–12. [CrossRef]
14. Paltrinieri, N.; Hauge, S.; Dionisio, M.; Nelson, W.R. Towards a dynamic risk and barrier assessment in an IO context. In Proceedings of the Safety, Reliability and Risk Analysis: Beyond the Horizon—Proceedings of the European Safety and Reliability Conference, ESREL 2013, Amsterdam, The Netherlands, 29 September–2 October 2013.
15. Hauge, S.; Okstad, E.; Paltrinieri, N.; Edwin, N.; Vatn, J.; Bodsberg, L. *Handbook for Monitoring of Barrier Status and Associated Risk in the Operational Phase*; SINTEF F27045; Center for Integrated Operations in the Petroleum Industry: Trondheim, Norway, 2015.
16. Villa, V.; Paltrinieri, N.; Khan, F.; Cozzani, V. Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry. *Saf. Sci.* **2016**, *89*, 77–93. [CrossRef]
17. Paltrinieri, N.; Reniers, G. Dynamic risk analysis for Seveso sites. *J. Loss Prev. Process Ind.* **2017**, *49*, 111–119. [CrossRef]
18. Sklet, S. Safety barriers: Definition, classification, and performance. *J. loss Prev. Process Ind.* **2006**, *19*, 494–506. [CrossRef]
19. Scarponi, G.E.; Paltrinieri, N. Comparison and Complementarity between Reactive and Proactive Approaches. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application*; Elsevier: Amsterdam, The Netherlands, 2016; ISBN 9780128038239. [CrossRef]
20. Rae, A.; Alexander, R.; McDermid, J. Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment. *Reliab. Eng. Syst. Saf.* **2014**, *125*, 67–81. [CrossRef]
21. Goerlandt, F.; Khakzad, N.; Reniers, G. Validity and validation of safety-related quantitative risk analysis: A review. *Saf. Sci.* **2017**, *99*, 127–139. [CrossRef]
22. Kirchsteiger, C. On the use of probabilistic and deterministic methods in risk analysis. *J. Loss Prev. Process Ind.* **1999**, *12*, 399–419. [CrossRef]
23. Cumming, R.B. Is Risk Assessment A Science? *Risk Anal.* **1981**, *1*, 1–3. [CrossRef]
24. Suokas, J. *On the Reliability and Validity of Safety Analysis*; Ampere University of Technology: Tampere, Finland, 1985; ISBN 9513823954.
25. Suokas, J.; Rouhiainen, V. Quality control in safety and risk analyses. *J. Loss Prev. Process Ind.* **1989**, *2*, 67–77. [CrossRef]
26. Paltrinieri, N.; Landucci, G.; Nelson, W.R.; Hauge, S. Proactive Approaches of Dynamic Risk Assessment Based on Indicators. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application*; Elsevier: Amsterdam, The Netherlands, 2016; ISBN 9780128038239. [CrossRef]

27. Delvosalle, C.; Fievez, C.; Pipart, A.; Debray, B. ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. *J. Hazard. Mater.* **2006**, *130*, 200–219. [CrossRef]
28. Paltrinieri, N.; Tugnoli, A.; Buston, J.; Wardman, M.; Cozzani, V. DyPASI methodology: From information retrieval to integration of HAZID process. *Chem. Eng. Trans.* **2013**, *32*. [CrossRef]
29. Paltrinieri, N.; Hauge, S.; Nelson, W.R. Dynamic barrier management: A case of sand erosion integrity. In Proceedings of the Safety and Reliability of Complex Engineered Systems—Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015, Zurich, Switzerland, 7–10 September 2015.
30. Nelson, W.R.; Van Scyoc, K. Focus on mission success: Process safety for the Atychiphobist. *J. Loss Prev. Process Ind.* **2009**, *22*, 764–768. [CrossRef]
31. IAEA. *Assessment of Defence in Depth for Nuclear Power Plants*; Safety Reports Series No. 46; IAEA: Vienna, Austria, 2005.
32. Edwin, N.J.; Paltrinieri, N.; Østerlie, T. Risk Metrics and Dynamic Risk Visualization. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry*; Elsevier: Amsterdam, The Netherlands, 2016; pp. 151–165. [CrossRef]
33. CCPS—Center for Chemical Process Safety. *Guidelines for Hevaluation Procedures*, 2nd ed.; American Institute of Chemical Engineers—Center of Chemical Process Safety: New York, NY, USA, 1992.
34. Aven, T.; Krohn, B.S. A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 1–10. [CrossRef]
35. Sornette, D. Dragon-Kings, Black Swans and the Prediction of Crises. *Int. J. Terraspace Sci. Eng.* **2009**, *2*, 1–18.
36. Paltrinieri, N.; Tugnoli, A.; Buston, J.; Wardman, M.; Cozzani, V. Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool. *J. Loss Prev. Process Ind.* **2013**, *26*, 683–695. [CrossRef]
37. Major Accident Hazards Bureau—MAHB. *Emars*; MAHB: Brussels, Belgium, 2018.
38. BARPI—Bureau for Analysis of Industrial Risks and Pollutions. *Analysis Research and Information on Accidents—ARIA*; BARPI: Paris, France, 2018.
39. AEA technology—Major hazards assessment unit. *MHIDAS—Major Hazard Incident Data Service*; AEA technology: Oxfordshire, UK, 2003.
40. Google LLC Google Scholar. Available online: https://scholar.google.com/ (accessed on 20 December 2018).
41. NIST/SEMATECH e-Handbook of Statistical Methods. Available online: http://www.itl.nist.gov/div898/handbook/ (accessed on 22 November 2019).
42. Landucci, G.; Paltrinieri, N. A methodology for frequency tailorization dedicated to the Oil & Gas sector. *Process Saf. Environ. Prot.* **2016**, *104*, 123–141. [CrossRef]
43. Landucci, G.; Paltrinieri, N. Proactive monitoring of risk-based indicators: Example of application in the Oil & Gas integrated operations. *Inst. Chem. Eng. Symp. Ser.* **2018**, 163.
44. Paltrinieri, N.; Landucci, G.; Salvo Rossi, P. Real-time data for risk assessment in the offshore oil&gas industry. In Proceedings of the International Conference on Offshore Mechanics and Arctic Engineering—OMAE, Trondheim, Norway, 25–30 June 2017; Volume 3B. [CrossRef]
45. Øien, K.; Massaiu, S.; Tinmannsvik, R.K.; Størseth, F. Development of early warning indicators based on Resilience Engineering. In Proceedings of the 10th International Conference on Probabilistic Safety Assessment and Management 2010, PSAM 2010, Seattle, WA, USA, 7–11 June 2010; Volume 3, pp. 1762–1771.
46. Rosqvist, T.; Tuominen, R. Qualification of Formal Safety Assessment: An exploratory study. *Saf. Sci.* **2004**, *42*, 99–120. [CrossRef]
47. Paltrinieri, N.; Dechy, N.; Salzano, E.; Wardman, M.; Cozzani, V. Towards a new approach for the identification of atypical accident scenarios. *J. Risk Res.* **2013**, *16*, 337–354. [CrossRef]
48. Hokstad, P.; Øien, K.; Reinertsen, R. Recommendations on the use of expert judgment in safety and reliability engineering studies. Two offshore case studies. *Reliab. Eng. Syst. Saf.* **1998**, *61*, 65–76. [CrossRef]
49. Paltrinieri, N.; Hokstad, P. Dynamic risk assessment: Development of a basic structure. In Proceedings of the Safety and Reliability: Methodology and Applications—Proceedings of the European Safety and Reliability Conference, ESREL 2014, Wrocław, Poland, 14–18 September 2014; pp. 1385–1392.
50. Foss, B. Process control in conventional oil and gas fields—Challenges and opportunities. *Control Eng. Pract.* **2012**, *20*, 1058–1064. [CrossRef]
51. Yang, X.; Haugen, S. Risk information for operational decision-making in the offshore oil and gas industry. *Saf. Sci.* **2016**, *86*, 98–109. [CrossRef]

52. Baraldi, P.; Mangili, F.; Zio, E.; Gola, G.; Nystad, B.H. A hybrid ensemble approach for process parameter estimation in offshore oil platforms. In *Uncertainty Modeling in Knowledge Engineering and Decision Making*; World Scientific: Singapore, 2012; pp. 1227–1232.
53. Taylor, C.; Sarshar, S.; Larsen, S. How IO leaders can use technology to enhance risk perception and communication. In Proceedings of the SPE Intelligent Energy Conference & Exhibition; Society of Petroleum Engineers, Utrecht, The Netherlands, 1–3 April 2014.
54. White, D.P.; Price-Smith, C.J.; Whaley, K.S.; Keatinge, P. Breaking The Completions Paradigm: Delivering World Class Wells In Deepwater Angola. In Proceedings of the SPE Russian Oil and Gas Technical Conference and Exhibition, Moscow, Russia, 28–30 October 2008. [CrossRef]
55. IO Center Center for Integrated Operations in the Petroleum Industries. Available online: www.iocenter.no (accessed on 25 October 2019).
56. Øien, K.; Massaiu, S.; Tinmannsvik, R.K. *Guideline for Implementing the REWI Method*; SINTEF Technology and Society: Trondheim, Norway, 2012.
57. Filippetti, M. Innovative Tools for Dynamic Risk Analysis. Master's Thesis, University of Bologna, Bologna, Italy, 2014.
58. Department of Energy and Climate Change Well Data Index. Available online: https://www.gov.uk/government/organisations/department-of-energy-climate-change (accessed on 22 November 2019).
59. Øien, K.; Sklet, S. *Metodikk for Utarbeidelse av Organisatoriske Risikoindikatorer*; SINTEF: Trondheim, Norway, 2001.
60. Delvosalle, C.; Fiévez, C.; Pipart, A. *ARAMIS D1C—Appendix 5 Methodology for the Building of Generic Event Trees (MIMAH)*; Faculté Polytechnique de Mons, Major Risk Research Centre: Mons, Belgium, 2004.
61. Paltrinieri, N.; Cozzani, V.; Øien, K.; Grøtan, T.O. Prevention of atypical accident scenarios through the use of resilience based early warning indicators. In Proceedings of the Advances in Safety, Reliability and Risk Management—Proceedings of the European Safety and Reliability Conference, ESREL 2011, Troyes, France, 18-22 September 2011.
62. Paltrinieri, N.; Tugnoli, A.; Øien, K.; Cozzani, V. Synergy between DyPASI and well-known safety indicator methodologies in the prevention of atypical accident scenarios. In Proceedings of the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012, Helsinki, Finland, 25–29 June 2012; Volume 5.
63. Park, J. Investigating a homogeneous culture for operating personnel working in domestic nuclear power plants. *Reliab. Eng. Syst. Saf.* **2016**, *156*, 256–265. [CrossRef]
64. Bucelli, M.; Paltrinieri, N.; Landucci, G.; Cozzani, V. Safety barrier management and risk assessment: Integration for safer operations in the Oil & Gas industry. In Proceedings of the Institution of Chemical Engineers Symposium Series, Birmingham, UK, 10–12 May 2017.
65. Paltrinieri, N.; Grøtan, T.O.; Bucelli, M.; Landucci, G. A case of dynamic risk management in the subarctic region. In Proceedings of the Risk, Reliability and Safety: Innovating Theory and Practice—Proceedings of the 26th European Safety and Reliability Conference, ESREL 2016, Glasgow, Scotland, 25–29 September 2016.
66. Paltrinieri, N.; Khan, F.; Cozzani, V. Coupling of advanced techniques for dynamic risk management. *J. Risk Res.* **2015**, *18*, 910–930. [CrossRef]
67. Paltrinieri, N.; Scarponi, G.E.; Khan, F.; Hauge, S. Addressing dynamic risk in the petroleum industry by means of innovative analysis solutions. *Chem. Eng. Trans.* **2014**, *36*, 451–456. [CrossRef]
68. Petroleum Safety Authority. *Principles for Barrier Management in the Petroleum Industry*; PSA: Stavanger, Norway, 2013.
69. Scarponi, G.E.; Paltrinieri, N.; Khan, F.; Cozzani, V. Reactive and Proactive Approaches: Tutorials and Example. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application*; Elsevier: Amsterdam, The Netherlands, 2016; ISBN 9780128038239. [CrossRef]
70. Andersen, H.; Casal, J.; Dandrieux, A.; Debray, B.; De Dianous, V.; Duijm, N.J.; Delvosalle, C.; Fievez, C.; Goossens, L.; Gowland, R.T.; et al. *ARAMIS—Accidental Risk Assessment Methodology for Industries in the Context of the SEVESO II Directive*; Faculté Polytechnique de Mons, Major Risk Research Centre: Mons, Belgium, 2004.
71. Saaty, T.L. The analytic hierarchy process. *Eur. J. Oper. Res.* **1990**, *48*, 9–26. [CrossRef]

72. Association of Oil&Gas Producers. *Riser & Pipeline Release Frequencies*; Association of Oil&Gas Producers: London, UK, 2010.
73. HSE-Health Safety Executive. *Offshore Hydrocarbon Releases Statistics and Analysis*; HSE-Health Safety Executive: London, UK, 2002.
74. Petroleum Safety Authority. *Hydrocarbon Leak on Oseberg A on 17 June 2013*; Petroleum Safety Authority: Stavanger, Norway, 2014.
75. Fossan, I.; Opstad, A.S. *Process Leak for Offshore Installations Frequency Assessment Model—PLOFAM*; Lloyd's Register: Bergen, Norway, 2016.
76. Tinmannsvik, R.K.; Albrechtsen, E.; Bråtveit, M.; Carlsen, I.M.; Fylling, I.; Hauge, S.; Haugen, S.; Hynne, H.; Lundteigen, M.A.; Moen, B.E.; et al. *Deepwater Horizon-Ulykken: Årsaker, Lærepunkter og for-Bedringstiltak for Norsk Sokkel. [The Deepwater Horizon Accident: Causes, Learning and Recommendations for the Norwegian Continental Shelf]*; SINTEF: Trondheim, Norway, 2011.
77. Massaiu, S.; Paltrinieri, N. Human Reliability Analysis: From the Nuclear to the Petroleum Sector. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application*; Elsevier: Amsterdam, The Netherlands, 2016; ISBN 9780128038239. [CrossRef]
78. Paltrinieri, N.; Massaiu, S.; Matteini, A. Human Reliability Analysis in the Petroleum Industry: Tutorial and Examples. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry*; Butterworth-Heinemann: Oxford, UK, 2016; pp. 181–192. [CrossRef]
79. Bye, A.; Laumann, K.; Taylor, C.; Rasmussen, M.; Øie, S.; van de Merwe, K.; Øien, K.; Boring, R.; Paltrinieri, N.; Wærø, I. *The Petro-HRA Guideline*; Institutt for energiteknikk: Kjeller, Norway, 2017.
80. Bucelli, M.; Salvo Rossi, P.; Paltrinieri, N.; Utne, I.B. A system engineering approach to subsea spill risk management. *Saf. Sci.* **2020**, in press.
81. Weinberg, A.M. Reflections on Risk Assessment. *Risk Anal.* **1981**, *1*, 5–7. [CrossRef]
82. Paltrinieri, N.; Hauge, S.; Albrechtsen, E. *Risk Management Models in an Integrated Operations Context*; Transactions of the American Nuclear Society: Chicago, IL, USA, 2013; Volume 109.
83. Khakzad, N.; Yu, H.; Paltrinieri, N.; Khan, F. Reactive Approaches of Probability Update Based on Bayesian Methods. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application*; Elsevier: Amsterdam, The Netherlands, 2016; pp. 51–61. ISBN 9780128038239. [CrossRef]


# Article III

Shenae Lee, Anne Barros, Mary Ann Lundteigen, Nicola Paltrinieri. **An approach to model risk contribution from periodic testing and maintenance of safety systems**. *(Under review for publication in Journal of Loss Prevention in the Process Industries)*.

# An approach to model risk contribution from periodic testing and maintenance of safety systems

Shenae Lee[1,*], Anne Barros[1], Mary Ann Lundteigen[2], Nicola Paltrinieri[1]

[1] Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology NTNU, S.P. Andersens veg 3, 7031, Trondheim (Norway)

[2] Department of Engineering Cybernetics, Norwegian University of Science and Technology, O.S. Bragstads plass 2E, Gløshaugen, 7034 Trondheim

* shenae.lee@ntnu.no

# Abstract

Safety functions are implemented in process plants to reduce the risk of major accidents that can arise from process demands. When the demands for a safety function occur infrequently, the function is operated in low-demand mode. An important reliability measure for a low-demand safety function is the average probability of dangerous failure on demand, which can indicate the inability of the safety system to achieve the required risk reduction. The dangerous failures that can impede a safety system from functioning on demand may occur as random events during normal operations and remain unknown. For this reason, periodic function testing and maintenance are an important means to reveal and correct dangerous undetected failures, for attaining the desired availability of the low-demand safety functions. However, human errors made during maintenance may induce new types of faults that have a potential to cause accidents, introducing additional risk. In addition, ineffective testing and maintenance action may not restore the safety functions to a desired level. To account for the risk contributions from such adverse effects of maintenance, the present study suggests an approach to quantify the negative impact of scheduled maintenance. Multi-phase Markov approach is utilized for modeling the states of a safety system with respect to the two main types of dangerous failures during operations and maintenance. The application of suggested model is demonstrated by a case study of pressure relief valves in offshore platforms that are subjected to testing and maintenance at regular intervals. The proposed model may provide an input to decision-making regarding the periodic testing and maintenance intervals, taking into account the desired reliability performance of safety functions, while keeping a persistent focus on safety and risk.



# Keyword

Multi-phase Markov approach, Periodic testing and maintenance, performance measures, Maintenance errors, Major hazard risks.

# 1 Introduction

Major hazards accidents can arise from dangerous deviations and hazardous events that may occur during process plant operations. To reduce major accident risks, the effects of these undesired events may be mitigated by using engineered safety systems which can be added to the process equipment. These safety systems are designed to activate the intended safety functions in response to a specified demand. Such a reactive safety function are said to be operated in demanded mode, and if the demand rate is less than once per year, the function is operated on low-demand mode (CCPS, 2015; IEC 61511, 2016). To quantify the reliability of a low-demand safety function and its risk reduction performance, probability of failure on demand (PFD) is calculated. The impediments to a safety function may occur at a random time, which causes the equipment to be unprotected against possible demands. Periodic testing and maintenance are an important means to detect and correct hidden failures for attaining the desired performance of low-demand safety functions (Jin and Rausand, 2014; Rausand and Høyland, 2004). The effectiveness of testing and maintenance strategies can be considered in calculation of PFD, by using parameters that express the effectiveness of testing and maintenance, for instance, test coverage (Lundteigen and Rausand, 2008), degradation by testing (Wu et al., 2018), and the impact of different repair policies (Srivastav et al., 2020).

Testing and maintenance in general enhances the reliability of safety functions, such that the probability of accidents can be reduced. However, it is also important to lessen the negative impact of maintenance, such as the introduction of additional failures and occurrence of accident during maintenance (Aven, 2008; Vatn and Aven, 2010). Maintenance activity in a process plant can be hazardous operations that can introduce failures with the potential to cause new types of hazardous events and accident scenarios. One main reason is that process isolations and re-start of the plant can give rise to external leakages, typically due to the errors related to isolation, blinding, and reinstatements (HSG 253, 2005; Vinnem et al., 2016a; Vinnem and Røed, 2015). In relation to this, immediate leakages of hazardous substances can occur, for example, due to the insecure isolation during the manual interventions for maintenance. External leakage may not directly impinge on the activation of safety function upon a demand, but may have harmful impact to the maintenance personnel present at the plant. Furthermore, the leakage may be ignited and lead to major accidents (e.g. fire and explosion)(Haugen, 2018).

More attention may need to be given to risk contributions from the maintenance errors, to be capable of continuously providing necessary protections against major accident hazards both in maintenance and operations phases. The maintenance induced failures are considered as a factor that can either influence the performance of the main safety functions, or introduce new hazards and initiating events (e.g. leakages) (Okoh and Haugen, 2014, 2013). The latter issue is considered in quantitative risk models developed for Norwegian offshore industry, with a focus on the causal sequences leading to the leakage events, and the factors that influence the frequency of leakages, especially to update the plant-specific risk picture (Gran et al., 2012; Øien, 2001; Sklet et al., 2006; Vinnem et al., 2009). However, these risk models do not explicitly include the effect of the test and maintenance on the safety systems states are not modelled to a detailed level, compared to the modeling approaches for SISs.

The objective of this paper is therefore to develop a model that can include two main types of failures of low-demand safety systems. An illustrative case of PSVs that are subjected to periodic maintenance in the offshore plants, are used. Periodic testing and maintenance for PSVs are carried out on a regular basis to ensure the desired performance of risk reduction during normal operations phases (Okoh et al., 2016). As opposed to this, the errors made during the maintenance phases of PSVs are claimed to be a key causal factor to introduce additional risk). The failures that can be caused by the errors in the maintenance interventions (i.e. external leakages), are distinguished from the random failures during normal operation (i.e. failure to open on demand). The main focus is to describe the negative effect of maintenance action on the system states, using Multi-Phase Markov approach (ISO/TR12489, 2013; Rausand, 2014). The main focuses are 1) to include failure events and faults of the safety systems induced by maintenance 2) to express the probability of maintenance errors in terms of transition probabilities 3) to calculate the time-dependent state probabilities of the safety system. The focus of a modeling approach to quantify the influence of periodic testing and maintenance onto the system states.

# 2. Theoretical background

## 2.1 Dangerous failures of safety functions in demanded mode

A safety system is said to operate in demanded mode, when it intended safety functions is only activated to respond to a demand. A demand refers to hazardous deviation from the normal operation that requires the safety function. The unavailability of the safety function to protect against a specified demand, may lead to safety consequences (Rausand, 2014). In case the demand rate for is not greater than once per year, the safety system operates in low-demand mode. A low-demand safety system may experience dangerous failures that may impede

the system from functioning in the presence of a demand. A dangerous failure results in a dangerous fault of a safety system that cause the inability to correctly react upon a demand (IEC60050-192, 2015; Rausand, 2014). A dangerous failure is classified as a dangerous undetected (DU) failure if it can be only revealed during testing or a real demand situation, which is major contributor to the unknown unavailability of a safety function (Jin and Rausand, 2014; Rausand, 2014). A reliability performance for a low-demand safety function is commonly measured by the average probability of dangerous failure on demand (PFD), which is unavailability of a safety function due to DU failures (Hauge et al., 2010). In relation to achieving the desired PFD, function testing and preventive maintenance at regular interval to reveal and correct possible DU failures. The requirement for the PFD of a safety function may be determined by the amount of the risk reduction that needs to be achieved by the safety function (Rausand, 2011).

## 2.2 Safety functions of pressure relief valves

Pressure relief valves (PSVs) are used to protect pressurized equipment (e.g. hydrocarbon containing vessel) against overpressure conditions with the potential to cause unwanted consequences, for example, a catastrophic rupture of vessel and release of toxic substances (API 521, 2014; ARAMIS, 2004). The essential safety function of PSV is to prevent the pressure increase from exceeding the specified allowed value. A PSV is designed to be actuated when its upstream pressure reaches the preset pressure, and to be in open position for reliving the excess pressure from the process equipment. The valve recloses when the normal condition has been restored. In addition, a PSV is intended to open rapidly for avoiding the pressure build-up (API 521, 2014). In relation to these required functions, the inability of a PSV to open at the set pressure point and within the predefined response time, which is defined as fail to open on demand (FTO), is taken into account in the calculation of the PFD (Hauge et al., 2010; OREDA, 2015). As FTO is a DU fault, a PSV is subjected to periodic function testing, and the length of the testing interval has a direct influence on the PFD value (Maher et al., 1988; Rausand, 2014).

A PSV would be removed from the plant section and transported to the workshop for bench testing, where the inlet of a PSV is applied a predefined pressure (e.g. 90% of the opening pressure) to verify the opening and reclosing within the preset pressure range, and seat leakage testing is also carried out (Gross, 2004; Hellemans, 2009). The removal of PSV for maintenance requires the isolation of the plant section that is protected by the valve during normal operation. The isolations (e.g. blank flanges, block valves, vent valves) are installed, and the section is emptied of the process medium (e.g. Hydrocarbon) by depressurizing, venting, and purging. The isolation plan also covers the plant reinstatement after reconnecting the PSV that has been tested and maintained. This includes removal of the isolations, leak testing and re-pressurization of the section (API RP 576, 2017; HSG 253, 2005; Norwegian Oil and Gas Association, 2018). Inadequate isolations procedures in relation to PSVs maintenance in the Norwegian offshore platforms have caused external leakages incidents (i.e. leak rate greater than 0.1kg/s), contributing to major accident risks (Vinnem and Røed, 2015). Both mechanical failures of isolation devices and human and organizational factors can cause leakages during the establishment of isolations or the removal of isolations. Notably, incident investigations indicate that human errors are the key factor that influence the performance isolations. Examples of human errors may include improper selection of isolation device, errors in leak testing of isolations, and incompliance to the reinstatement sequence (HSG 253, 2005).

## 2.3 Markov process and Multi-phase Markov process to model periodic testing and maintenance

The Markov approach can be used to analyze the system performance over time, for example to attain its average unavailability and visit frequency to a particular state. The system behavior may be defined by a finite number of states. If the evolution of a system is modeled by a Markov process, the changes of the system states is a stochastic process with memoryless property. In other words, the transition from one state to another state in the future is independent on the past, and depends only on the present state and the time for making the transition, and the process has time-homogeneous transition probabilities (Rausand, 2014; Rausand and Høyland, 2004).

A system may possess the Markov property only within a certain time frame but does not fulfill the Markov property at different points in time. For example, the system is subjected to periodic testing and maintenance actions on predefined time points, and the state may change after the execution of these actions. Such a process with the deterministic causes for state transitions may not have time-homogeneous transition probabilities, and thus cannot be modelled by using a standard Markov chain. One reason is that the time period spent for the testing and maintenance represents a different condition than normal operation period, such that the process may have different transition rates. To take this into account, we may use a multi-phase Markov approach where we

define a finite number of state spaces, so that each state space corresponds to a phased time period (e.g. normal operation period, and maintenance phase), and has its own transition rate matrix (Barros, 2016). Table 1 summarized main differences between the standard Markov and Multi-phase Markov approach.

Table 1 Main differences in assumptions for modeling testing and maintenance in standard Markov and Multiphase Markov

| Standard Markov approach | Multi-phase Markov approach |
|---|---|
| • The system behavior (i.e. the state probability distribution) is defined by single constant transition rate matrix.<br>• Maintenance activities are initiated immediately after the system has arrived a fault state.<br>• The time spent for the maintenance activities is exponentially distributed. | • The system behavior may be defined by different transition rate matrixes to reflect the different operating contexts (e.g. normal operation, test conditions)<br>• Periodic test and maintenance actions may occur at a deterministic time point, and the distribution of states may change as a result of such actions.<br>• The effect of each action can be described in the transition probability matrix that links two states.<br>• The length of the time spent for a testing or maintenance activity can be deterministic. |

# 3. Case Study

The demand for pressure reliving of by a PSV occurs when the basic process control and the emergency shutdown have failed in a typical overpressure scenario (IEC 61511, 2016). The industry standard for the average PFD for PSVs in the Norwegian petroleum sector is 0.04. PSVs are in general dismantled for inspection and maintenance tasks (e.g. repair, parts changes, calibration, and cleaning). Periodic testing for PSVs are performed at a regular testing interval, and the length of interval varies, for example, 1 to 2 years, or 6 months. With certain number of subsequent tests that do not reveal faults, the interval may be adjusted from 1 year to 2 years (PSA, 2016). However, periodic testing and maintenance of PSVs have been claimed to influence the occurrence of hydrocarbon releases in Norwegian offshore platforms (Vinnem et al., 2016b). One main reason is that the PSVs are removed from the process segment, which requires secure isolation of process before the PSV disconnection, as well as and proper reconnection following PSV maintenance. The errors in isolation and reinstatement following the PSV maintenance, for example, incorrect location of isolations, the breakdown of installed isolations device, and unauthorized removal of isolations would lead to external leakage state. External leakage (EL) can be considered as a dangerous failure (OREDA, 2015) in normal operation and maintenance phases, as the probability of ignition of released substances exists in both phases.

Table 2 Key characteristics of fault modes of PSVs and the containment envelope during PSV disconnection

| | Fail to open on demand | External leakages to environment |
|---|---|---|
| Potential hazardous event due to PSV fault | Overpressure exceeding the preset opening pressure of the PSV | Ignition of the external leakage |
| Performance measure | Average PFD | Frequency of external leakage |
| Performance influencing factor | Function test interval<br>Failure rate with respect to FTO | Frequency of maintenance<br>Leak control procedures |

# 4. Modelling

## 4.1 Modelling assumptions

The physical boundaries of the system included in the modeling is a self-actuating PSV, as well as the isolation devices (e.g. blinds, isolation valves) inserted during the time when the PSV is removed. The assumptions are made to take into account the two types of failures that can be introduced in the normal operations or the maintenance of a PSV. The possible states of a PSV is described in the table 3, and each of the six states is given

with a number, and in state 1, the system does not have any fault. The corresponding transition rate matrix is established. The state transition diagram is shown in the figure 1. The main assumptions include:

- PSV safety function operates in low-demand mode.
- Demands to the PSV only occur during normal operation phases.
- During normal operation phases, the failure mode FTO may occur due to some mechanisms related to physical faults (e.g. ageing). The deterioration process of PSV is the focus of this model, and therefore the failure rate is assumed to be constant.
- In the maintenance phase 2, the test may detect FTO with probability of $1-\gamma$. In the maintenance phase 3, the detected FTO may be repaired with probability of $1-\gamma$. We assume that the test and repair is carried out by the same maintenance engineer, such that human error probability (HEP) in the test and repair are the same.
- During normal operation phases, the failure mode EL can occur randomly due to unspecified mechanisms. EL faults are detected immediately during normal operation, their repair begins at once, and its duration is random and exponentially distributed. In this paper, it is assumed that mean repair time is 8 hours.
- FTO and EL are independent failure modes. During normal operation phases, these events may occur sequentially one after the other.
- A PSV is taken out from the process for testing and maintenance.
- During the maintenance phases, the failure mode EL can only be caused in a deterministic way, but does not occur as random events. In the maintenance phase 1 and 4 (maintenance preparation and reconnection, respectively), the failure mode EL occurs as a result of human errors, with the HEP value of $\alpha$. It is assumed that the isolation and reconnection are carried out by the same maintenance crew present in the plant section, such that the values of HEP for the test preparation and reconnection are the same.

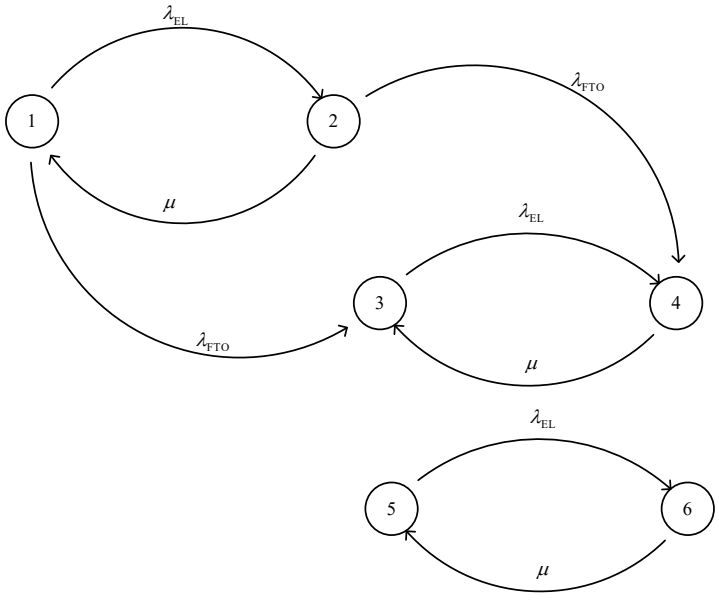



Figure 1 State transition diagram during normal operations

Table 3 Description of possible states

| System states | Description |
|---|---|
| 1 | The system is fully functioning. |
| 2 | The system has EL fault. |
| 3 | The system has FTO fault. FTO fault is undetected. |
| 4 | The system has EL fault and FTO fault. FTO fault is undetected. |

| | |
|---|---|
| 5 | FTO fault is detected. |
| 6 | FTO fault is detected, and the system has EL fault. |

Table 4 Description of time frames in normal operation, test, and maintenance phase of a PSV

| Time frame name | Event description | Duration |
|---|---|---|
| Normal operation phase | 1) The PSV is put into operation after the maintenance is finished<br>2) Planning of the maintenance work is carried out.<br>3) Repair action upon detection of fault state (i.e. leakage) | Length of the proof test interval (e.g. Typically 6 month, 1 year, 2 year according to the maintenance practice in Norwegian offshore installation) |
| Maintenance phase 1 | 1) Tasks for isolation, draining, venting, and purging of section are carried out, to prepare test<br>2) Operator errors may lead to the failure mode, leakages | Usually duration of one shift without any process deviation |
| Maintenance phase 2 | 1) Function test of PSV related to the failure mode FTO, under a specified test pressure | Average test time is typically less than 1 hour |
| Maintenance phase 3 | 1) Repair based on the result of the test | Mean time to repair |
| Maintenance phase 4 | 1) Tasks for removal of isolations and reconnecting PSV to a correct position after the repair are carried out<br>2) Equivalent controls to those used during installation of isolation are required | Usually Duration of one shift without any process deviation |

Four maintenance phases are suggested based on the impact of different testing and maintenance activities, as explained in the table 3. Each maintenance phase $j$ has the constant duration of $m_j$, $j = 1,2,3,4$, and the total time spent for all the test and maintenance activities is $m_{tot} = \sum_{j=1}^{4} m_j$. The transition probability matrix $\mathbf{M}_j$ (i.e. denoted as maintenance matrix) are used to describe the effect of maintenance phase $j$ on the state immediately after the phase $j$ (Rausand, 2014), as illustrated in the figure 2. For example, if the PSV is in state 3 (i.e. PSV has FTO fault), it is desired that the fault is detected in the test (i.e. the transition from state 3 to state 5 is made). However, due to the imperfectness of testing, the probability of the PSV remaining in the in state 3 exists, which is reflected in the 3rd column in the $\mathbf{M}_2$.

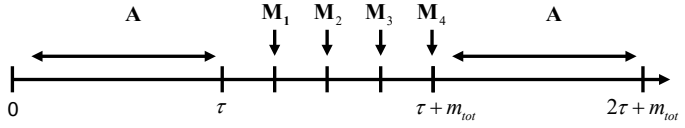



Figure 2. Each maintenance matrix $\mathbf{M}_j$ denotes the transition probabilities that are influence by testing and maintenance actions in each phase.

Transition rate matrix

$$A = \begin{pmatrix} -(\lambda_{EL} + \lambda_{FTO}) & \lambda_{EL} & \lambda_{FTO} & 0 & 0 & 0 \\ \mu & -(\mu + \lambda_{FTO}) & 0 & \lambda_{FTO} & 0 & 0 \\ 0 & 0 & -\lambda_{EL} & \lambda_{EL} & 0 & 0 \\ 0 & 0 & \mu & -\mu & 0 & 0 \\ 0 & 0 & 0 & 0 & -\lambda_{EL} & \lambda_{EL} \\ 0 & 0 & 0 & 0 & \mu & -\mu \end{pmatrix}$$

Maintenance matrix (transition probability matrix)

$$M_1 = \begin{pmatrix} 1-\alpha & \alpha & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1-\alpha & \alpha & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1-\alpha & \alpha \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \gamma & 0 & 1-\gamma & 0 \\ 0 & 0 & 0 & \gamma & 0 & 1-\gamma \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$M_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1-\gamma & 0 & 0 & 0 & \gamma & 1 \\ 1-\gamma & 0 & 0 & 0 & 0 & \gamma \end{pmatrix}$$

$$M_4 = \begin{pmatrix} 1-\alpha & \alpha & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1-\alpha & \alpha & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1-\alpha & \alpha \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

## 4.2 Analytical formulas

The analytical formulas that correspond to the state transition diagram in the previous section is derived in this section. The computation of the formula is implemented in the Matlab, and the result is presented in the section 4.3. We denote $X(t)$ the state of a system at time $t$, and the probability of being in the state $i$ at time $t$ is denoted as $P_i(t) = \Pr(X(t) = i)$. According to the assumptions, they system has six possible states, namely, state 1, state 2, … state 6. The state distribution at time $t$ can be denoted in a row vector, $\mathbf{P(t)} = \begin{bmatrix} P_1(t) & P_2(t) & P_3(t) & P_4(t) & P_5(t) & P_6(t) \end{bmatrix}$. The descriptions of the state $i$ are summarized in the table 4. The state probability at time $t = 0$, the system is put into operation. $P_1(0) = \Pr(X(0) = 0) = 1$, as the system is fully functioning in the beginning. The first test interval $t \in [0, T_1]$, with the length of $\tau$ is denoted as operation phase 1. In this interval, the time evolution of the system is described by the Markov process with the transition rate matrix $\mathbf{A}$. The state probabilities can be written as

$$\mathbf{P}(t) = \mathbf{P}(0)e^{t\mathbf{A}}, t \in [0, T_1] \qquad (1)$$

At time $t = T_1$, operation phase 1 ends, and the systems state is given by $\mathbf{P}(T_1) = \mathbf{P}(0)e^{T_1\mathbf{A}}$.

Immediately after the time $t = T_1$, a set of activities related to periodic testing and maintenance are performed in a predefined sequence. Immediately after the time $t = T_1$, maintenance phase 1 begins and the duration is $m_1$. At time $t = T_1 + m_1$, maintenance phase 1 ends. $T_1 + m_1^-$ denotes the time point immediately before $T_1 + m_1$ ,when the maintenance phase 1 finishes. Within time interval $t \in (T_1, T_1 + m_1^-]$, it is assumed that the state of the system does not change, and it is given as $\mathbf{P}(t) = \mathbf{P}(T_1),\ t \in (T_1, T_1 + m_1^-]$. The reason may be that the effects of test and maintenance actions cannot be observed yet. At the time point at $t = T_1 + m_1$, test and maintenance actions are complete, and their effects may become observable. Such effects of maintenance phase 1 onto the state of the system is described in $\mathbf{M}_1$. The system state at time $t = T_1 + m_1$ is given,

$$\mathbf{P}(T_1 + m_1) = \mathbf{P}(T_1 + m_1^-) \cdot \mathbf{M}_1 \qquad (2)$$

We may further define the system states as follows:

**Maintenance phase 2**

$$\mathbf{P}(t) = \mathbf{P}(T_1 + m_1),\ t \in [T_1 + m_1, T_1 + m_1 + m_2^-]$$
$$\mathbf{P}(T_1 + m_1 + m_2) = \mathbf{P}(T_1 + m_1 + m_2^-) \cdot \mathbf{M}_2 = \mathbf{P}(T_1 + m_1^-) \cdot \mathbf{M}_1 \cdot \mathbf{M}_2$$

**Maintenance phase 3**

$$\mathbf{P}(t) = \mathbf{P}(T_1 + m_1 + m_2), t \in [T_1 + m_1 + m_2, T_1 + m_1 + m_2 + m_3^-]$$
$$\mathbf{P}(T_1 + m_1 + m_2 + m_3) = \mathbf{P}(T_1 + m_1 + m_2 + m_3^-) \cdot \mathbf{M}_3 = \mathbf{P}(T_1 + m_1^-) \cdot \mathbf{M}_1 \cdot \mathbf{M}_2 \cdot \mathbf{M}_3$$

**Maintenance phase 4**

$$\mathbf{P}(t) = \mathbf{P}(T_1 + m_1 + m_2 + m_3), t \in [T_1 + m_1 + m_2 + m_3, T_1 + m_1 + m_2 + m_3 + m_4^-]$$
$$\mathbf{P}(T_1 + m_1 + m_2 + m_3 + m_4) = \mathbf{P}(T_1 + m_1 + m_2 + m_3 + m_4^-) \cdot \mathbf{M}_4 = \mathbf{P}(T_1 + m_1^-) \cdot \mathbf{M}_1 \cdot \mathbf{M}_2 \cdot \mathbf{M}_3 \cdot \mathbf{M}_4 = \mathbf{P}(0)e^{T_1\mathbf{A}_1} \cdot \mathbf{M}_1 \cdot \mathbf{M}_2$$

Immediately after $t = T_1 + m_1 + m_2 + m_3 + m_4$, or $t = T_1 + m_{tot}$, the operation phase 2 begins. After the time elapse of the periodic testing interval at time $t = T_1 + m_{tot} + \tau = T_2$, the operation phase 2 ends. In the interval $t \in (T_1 + m_{tot}, T_2]$ the time evolution of the unit is again described by the Markov process with the transition rate matrix. The same applies for the operation phase n.

The system state in the operation n, $t \in [T_{n-1} + m_{tot}, T_n], n = 1,2\ldots$ is given by

$$\mathbf{P}(t) = \mathbf{P}(0)\left(e^{\tau\mathbf{A}}\prod_{j=1}^{4}\mathbf{M}_j\right)^{n-1} e^{(t-(T_{n-1}+m_{tot}))\mathbf{A}}, t \in [T_{n-1} + m_{tot}, T_n] \quad (3)$$

Test and maintenance phase 1 just after $T_n$

$$\mathbf{P}(t) = \mathbf{P}(0)\left(e^{\tau\mathbf{A}}\prod_{j=1}^{4}\mathbf{M}_j\right)^{n-1} e^{\tau\mathbf{A}}, t \in [T_n, T_n + m_1^-]$$

$$\mathbf{P}(T_n + m_1) = \mathbf{P}(0)\left(e^{\tau\mathbf{A}}\prod_{j=1}^{4}\mathbf{M}_j\right)^{n-1} e^{\tau\mathbf{A}}\mathbf{M}_1$$

Maintenance phase $k$ after $T_n, k = 2,3,4$

$$\mathbf{P}(t) = \mathbf{P}(0)\left(e^{\tau\mathbf{A}}\prod_{j=1}^{4}\mathbf{M}_j\right)^{n-1} e^{\tau\mathbf{A}}\prod_{j=1}^{k-1}\mathbf{M}_j, t \in [T_n + m_1 + \ldots + m_{k-1}, T_n + m_1 + \ldots + m_{k-1} + m_k^-]$$

$$\mathbf{P}(T_n + m_1 + \ldots + m_k) = \mathbf{P}(0)\left(e^{\tau\mathbf{A}}\prod_{j=1}^{4}\mathbf{M}_j\right)^{n-1} e^{\tau\mathbf{A}}\prod_{j=1}^{k}\mathbf{M}_j$$

## 4.3 Results

### 4.3.1 Reliability measure during normal operation

The transition from state 1 (i.e. fully functioning state) to state 3 may occur, when the failure FTO occurs during normal operations. The time-dependent probability of being in state 3 is presented in the figure 3, where the length of test interval is 2 years (denoted τ), and the HEP value of 0.1. The time-dependent probability of state 3 increases within the interval between the two consecutive periodic maintenance, and it decreases after the maintenance activities. It is notated that the probability of being in state 3 is not zero after the first maintenance. One reason for this may be possible testing error that causes the PSV to remain in state 3, instead of jumping into state 5. Another reason is that the repair of the detected FTO fault may be imperfect or partial, implying that the transition from state 6 into state 1 does not occur.

The PSV is in the fault state with respect to FTO in state 3 and state 4, and these two states contribute to the failure of the main safety function. For this reason, the mean PFD with respect to FTO is calculated as the sum of the probability of being in state 3 and the probability of state 4 in the middle of the operation phase. Moreover, the effect of changing the test interval on the mean PFD is illustrated in the figure 4, during the 25 years of lifecycle. It is shown that the mean PFD value increases almost proportional to the length of the interval between two subsequent tests. Being PSVs maintenance interval usually 1 to 2 years (Vinnem et al., 2016b) in real

industry cases, the length of the interval 12 years (i.e. 2 times of periodic maintenance) may seem unrealistic. However, the changes in the test interval was carried out for demonstration. Until the year 9, the mean PFD achieve the safety integrity level (SIL) range 1. The change of HEP does not have significant effect on the mean PFD.

### 4.3.2 Performance measure with respect to failures during maintenance

The introduction of the leakages by maintenance can be illustrated in the time-dependent probability of being in state 2, as in the figure 3. The transition from state 1 to state 2 may take place due to the possible occurrence of EL failure. The probability of being in state 2 abruptly increases immediately after the maintenance phase 1 and the maintenance phase 4, since these phases may introduce EL failures. For the same reason, the transition from state 3 to the state 4, and the transition from state 5 to state 6 may occur after the maintenance phase 1 and the maintenance phase 4. On the other hand, the EL faults can be eliminated during the normal operation, and therefore, the mean FTO with respect to the EL fault is suitable performance indicator. Instead, we suggest using the sum of the number of visits to the leakage states (i.e. state 2, state 4, and state 6) during the installation lifespan, as shown in figure 5. The number of leakages decreases with the reduced frequency of periodic test and maintenance. In addition, the higher HEP is found to contribute to the higher number of leakages. The HEP values are selected in reference to generic values that are suggested in human reliability analysis studies and the relevant standards (IEC 61511, 2016; Kirwan, 1994; Williams, 1986). A conservative value for HEP implies that the tasks that require competence and skill, while lower HEP value can be assigned for the situations that are less demanding. However, adapting the HEP values to a specific maintenance task is outside the scope of this paper.

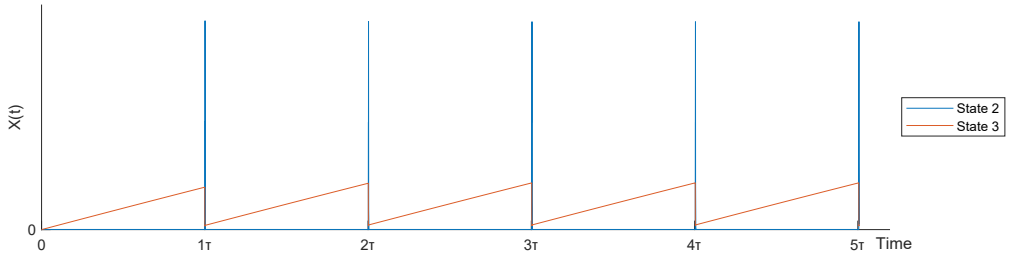



Figure 3 Time-dependent state probabilities (state 2 and state 3)

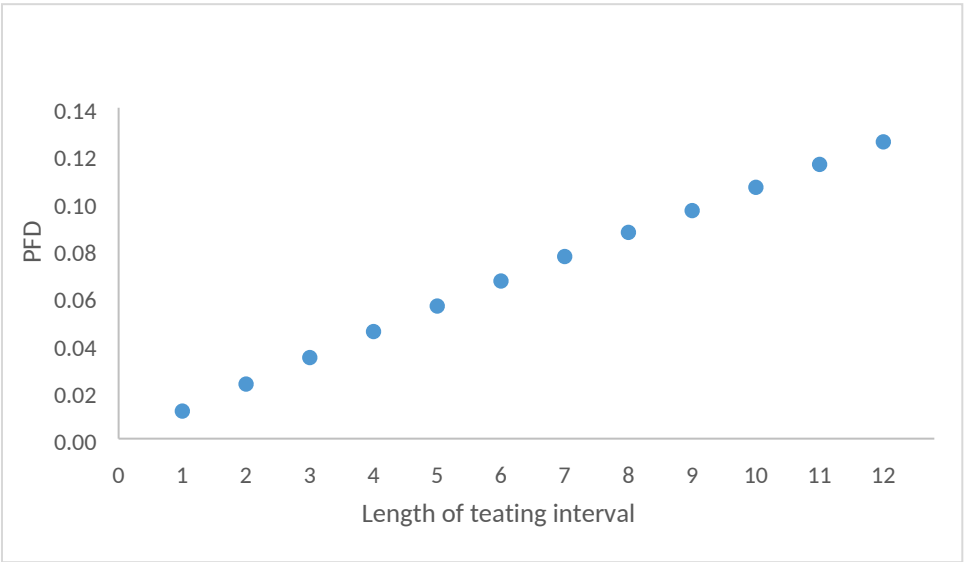



Figure 4. The maximum value of PFD with respect to FTO (state 3, state 4) with changing testing interval

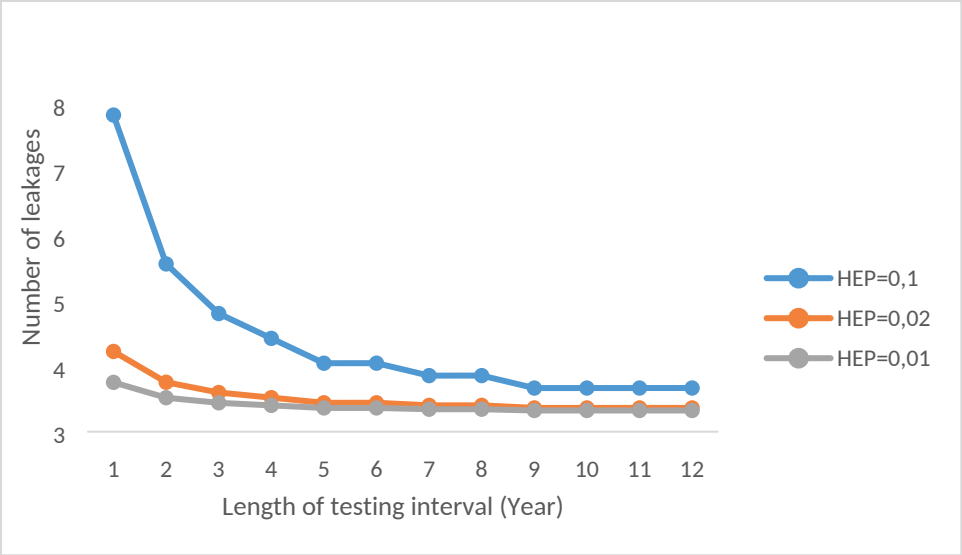



Figure 5. The number of visiting the leakage states corresponding to the changes in the length of the testing interval, and with changing the HEP values.

Table 5 Parameter denotation and description

| Denotation | Parameter value | Description | Data source |
|---|---|---|---|
| $\lambda_{FTO}$ | 2.2E-6 | Failure rate of the failure mode, FTO | PDS (Hauge et al., 2010) |
| $\lambda_{EL}$ | 1.5E-5 | Failure rate of the failure mode, EL | OREDA (OREDA, 2015) |
| $\mu$ | 0.125 | Repair rate of the valve with respect to the failure mode leakage during the operation | (HSG 253, 2005) |
| $\alpha$ | 0.01-0.1 | Probability of introducing leakages | Table 6 |
| $\gamma$ | 0.01-0.1 | Probability of imperfect test and repair | Table 6 |

Table 6 Human error probability (HEP) values from different data sources

| Human error probability | Value | Data source |
|---|---|---|
| Generic human error probability, lower bound | 0.01 | IEC61511(IEC 61511, 2016) |
| Fail to return the manually operated test valve to the correct configuration after maintenance/ General error of omission | 0.01 | Kirwan(1994) |
| Complex task requiring high level of comprehension and skill | 0.16 | Williams(1986) |
| Routine, highly practiced, rapid task, involving a relatively low level of skill | 0.02 | Williams(1986) |
| Generic human error probability, upper bound | 0.1 | IEC61511(IEC 61511, 2016) |
| Non-routine operation with other duties at the same time | 0.1 | Kirwan(1994) |

# 5. Concluding remarks

## 5.1 Implication from the results

It was shown that the mean PFD with respect to the failure mode FTO can be considered almost linearly proportional to the length of the interval between the two consecutive tests. The changes in the value of HEP does not impact the mean PFD with respect to FTO. It is also noted that after each maintenance, the mean PFD increases slightly, due to the testing and maintenance errors. In the maintenance interval ranging from 1 year to 9

year, the mean PFD is below 0.1. Second, the leak frequency, which represents the risk contributions from PSV during the maintenance phase was obtained. Higher HEP would lead to higher leak frequency, which implies that improvement in the quality of manual intervention would contribute to lower the risk to personnel at the plant section during maintenance. Furthermore, reducing the frequency of the periodic testing decreases the potential leakage, while the mean PFD is kept below 0.1, with the interval of 9 years. This may imply that we may find the optimal testing interval not only for based on the mean PFD value, but also attaining a lower leakage frequency.

## 5.2 Main benefits and further work

The proposed model is an illustration of how to quantify the influence of periodic testing and maintenance on the states of a safety system, based on multiphase Markov approach. The mean PFD of the main safety function during normal operation is obtained as a reliability measure. Furthermore, the number of occurrences of hazardous events (i.e. external leakages) is calculated, as a measure of the risk contribution from testing and maintenance errors. The suggested approach may be used to support decision-making regarding the periodic testing and maintenance intervals, considering the adverse impact of maintenance on safety and risk. Further improvement may be to consider the time delays in maintenance interventions, for example, due to delayed repair, by extending the model with additional phases.

# Acknowledgement

The authors are grateful to Renny Arismendi for helpful guidance on using Matlab and valuable suggestions for improvement.

# References

API 521, 2014. Pressure-relieving and depressuring systems, American Petroleum Institute. Washington, DC.

API RP 576, 2017. Inspection of Pressure-relieving Devices. American Petroleum Institute, Washington, DC.

ARAMIS, 2004. Accidental risk assessment methodology for industries in the context of the Seveso II directive. Technical report EVSGI-CT-2001-00036, Fifth Framework Programme of the European Community, Energy, Environment and Sustainable Development, http://aramis . jr.

Aven, T., 2008. A semi-quantitative approach to risk analysis, as an alternative to QRAs. Reliab. Eng. Syst. Saf. 93, 790–797. https://doi.org/10.1016/j.ress.2007.03.025

CCPS, 2015. Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis. https://doi.org/10.1002/9781118948743

Gran, B.A., Bye, R., Nyheim, O.M., Okstad, E.H., Seljelid, J., Sklet, S., Vatn, J., Vinnem, J.E., 2012. Evaluation of the Risk OMT model for maintenance work on major offshore process equipment. J. Loss Prev. Process Ind. 25, 582–593.

Gross, R.E., 2004. Reliability testing of pressure relief valves, in: American Society of Mechanical Engineers, Pressure Vessels and Piping Division (Publication) PVP. https://doi.org/10.1115/PVP2004-2610

Hauge, S., Hokstad, P., Langseth, H., Hauge, S., Onshus, T., 2010. Reliability prediction method for safety instrumented systems-PDS Example collection, PDS Method Handbook.

Haugen, S., 2018. Safety in Offshore Platforms—Use of QRA in the Norwegian Offshore Industry. https://doi.org/10.1016/bs.mcps.2018.05.001

Hellemans, M., 2009. The Safety Relief Valve Handbook: Design and Use of Process Safety Valves to ASME and International Codes and Standards, The Safety Relief Valve Handbook: Design and Use of Process Safety Valves to ASME and International Codes and Standards. https://doi.org/10.1016/C2009-0-20219-4

HSG 253, 2005. The safe isolation of plant and equipment. Health and Safety Executive, London.

IEC 61511, 2016. Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Part 1-3., 2.1. ed. International Electrotechnical Commission, Geneva.

Jin, H., Rausand, M., 2014. Reliability of safety-instrumented systems subject to partial testing and common-cause failures. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/j.ress.2013.08.006

Kirwan, B., 1994. A Guide to Practical Human Reliability Assessment. Taylor & Francis, London.

Maher, S.T., Rodibaugh, R.K., Sharp, D.R., 1988. Relief valve testing interval optimization program for the cost-effective control of major hazards, in: Symposium on Preventing Major Chemical Accidents. Institution of Chemical Engineers, Oslo, Norway.

Norwegian Oil and Gas Association, 2018. Recommended practice for isolation when working on hydrocarbon systems.

Øien, K., 2001. Risk indicators as a tool for risk control. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/S0951-8320(01)00067-9

Okoh, P., Haugen, S., 2014. A study of maintenance-related major accident cases in the 21st century. Process Saf. Environ. Prot. https://doi.org/10.1016/j.psep.2014.03.001

Okoh, P., Haugen, S., 2013. Maintenance-related major accidents: Classification of causes and case study. J. Loss Prev. Process Ind. https://doi.org/10.1016/j.jlp.2013.04.002

Okoh, P., Haugen, S., Vinnem, J.E., 2016. Optimization of recertification intervals for PSV based on major accident risk. J. Loss Prev. Process Ind. https://doi.org/10.1016/j.jlp.2016.09.003

OREDA, 2015. Offshore reliability data handbook, 6th editio. ed. OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway.

PSA, 2016. RNNP: Risk Levels in Norwegian Petroleum Activities 2015 (in Norwegian). (Technical Report). Stavanger.

Rausand, M., 2014. Reliability of Safety-Critical Systems, Reliability of Safety-Critical Systems. https://doi.org/10.1002/9781118776353

Rausand, M., 2011. Risk assessment - theory, methods and applications, Statistics in practice. https://doi.org/10.1093/ntr/nts290

Rausand, M., Høyland, A., 2004. System Reliability Theory: Models, Statistical Methods, and Applications. Wescon/96. https://doi.org/10.1109/WESCON.1996.554026

Sklet, S., Vinnem, J.E., Aven, T., 2006. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). Part II: Results from a case study. J. Hazard. Mater. https://doi.org/10.1016/j.jhazmat.2006.03.027

Vatn, J., Aven, T., 2010. An approach to maintenance optimization where safety issues are important. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/j.ress.2009.06.002

Vinnem, J.E., Haugen, S., Okoh, P., 2016a. Maintenance of petroleum process plant systems as a source of major accidents? J. Loss Prev. Process Ind. 40, 348–356. https://doi.org/10.1016/j.jlp.2016.01.021

Vinnem, J.E., Haugen, S., Okoh, P., 2016b. Maintenance of petroleum process plant systems as a source of major accidents? J. Loss Prev. Process Ind. https://doi.org/10.1016/j.jlp.2016.01.021

Vinnem, J.E., Røed, W., 2015. Root causes of hydrocarbon leaks on offshore petroleum installations. J. Loss Prev. Process Ind. https://doi.org/10.1016/j.jlp.2015.05.014

Vinnem, J.E., Seljelid, J., Haugen, S., Sklet, S., Aven, T., 2009. Generalized methodology for operational risk analysis of offshore installations. Proc. Inst. Mech. Eng. Part O J. Risk Reliab. https://doi.org/10.1243/1748006XJRR109

Williams, J.C., 1986. HEART - a proposed method for assessing and reducing human errors., in: In Ninth Advances in Reliability Technology Symposium, Birmingham, UK.

# Article IV

Shenae Lee, Yiliu Liu, Nicola Paltrinieri. 2017. **Modelling hazardous event scenarios for decision support**. 27th European Safety and Reliability Conference ESREL. Ljubljana, Slovenia.

*Safety and Reliability – Theory and Applications – Čepin & Briš (Eds)*
*© 2017 Taylor & Francis Group, London, ISBN 978-1-138-62937-0*

# Modelling hazardous event scenarios for decision support

S. Lee, Y. Liu & N. Paltrinieri
*NTNU, Trondheim, Norway*

ABSTRACT: Quantitative risk analysis has been a successful tool to support decision-making related to the design of technical (safety) barriers. A quantitative risk model may comprise a combination of event trees and fault trees, which is a basis for causal and frequency analysis of accident scenarios. Fault tree analysis is a well-documented technique, and it is commonly used for casual analysis of hazardous events. Fault tree analysis, however, is not fully suitable for modelling dynamic systems where the status of barriers may change, depending on various operational decisions. This paper introduces Petri nets as a formalism to consider this aspect. Petri nets are employed to model the sequence to a hazardous event, considering the effect of testing, repair, and daily activities on the availability of safety barriers. A representative case of an atmospheric tank overfilling is considered. Moreover, the effect of decisions on the risk level is addressed from a perspective of decision-making support.

## 1 INTRODUCTION

The Seveso III directive (Directive 2012/18/EU) has recently been adopted to improve decision-making support for establishments that involve hazardous substances, for instance, chemical plants and storage sites. The directive endorses safety management policies to prevent major accidents similar to the cases of Buncefield in 2005 (BMIIB, 2008; COMAH, 2011), Enschede in 2000 (French Sustainable Development Ministry, 2009), and Sandoz in 1986 (Schwabach, 1989). The operator of a Seveso site classified as an upper-tier is assigned with obligatory documentation of safety report. The report serves several purposes including the description of the possible accident scenarios and the safety measures implemented to avoid such scenarios.

Representative methodologies for qualitative and quantitative assessment of reference accident scenarios in process industry were developed in the European project, ARAMIS (Accidental Risk Assessment Methodology for Industries in the Context of the Seveso II Directive) (Andersen et al., 2004). The modelling technique in ARAMIS is based on the bow-tie diagram where a fault tree is built on the left-hand side, and an event tree is built on the right-hand side. A bowtie is centered on the hazardous event, which is the TOP event of the fault tree.

Fault tree analysis and event tree analysis have been widely used in quantitative risk models. While fault tree analysis is effective in identifying possible causes of a hazardous event, it exhibits limited ability to reflect dynamic behavior of safety barriers that are affected by complex maintenance strategies. Fault trees are often combined with an event tree to represent pivotal events (Rausand, 2011). In this approach, individual fault trees may share basic events among each other, which are complicated to account for (Nývlt & Rausand, 2012). Moreover, Vinnem (2014) indicates that barriers are activated in a certain sequence in an event tree, and it is critical to decide the event sequence to describe a realistic accident scenario. The sequence, however, can be ambiguous, especially when some events occur simultaneously or repeatedly in several points in timeline (Nývlt & Rausand, 2012; Nývlt et al., 2015; Fajardo et al., 2010).

Nivolianitou et al. (2004) compares the use of fault trees, event trees, and Petri nets for qualitative accident scenario analysis. This study concludes that the event tree provides clear visualization of event agents, while the fault tree is the most effective in resolving primary causes of an undesired event. Besides, it is claimed that Petri nets are capable of expressing modelling assumptions, concurrent events, and events with deterministic durations.

Petri net modelling has attained growing recognition as a powerful tool for risk and reliability analysis, and its application is addressed in the standards IEC 61508 (2010) and IEC 62551 (2012). Petri nets can add new features to the traditional risk analysis by including both deterministic and stochastic events with different distributions. Petri net modeling is flexible such that it can replace fault trees, event trees, and Markov diagrams. For example, the AND-gate and the-OR gate of

a fault tree can be easily constructed by Petri nets (Rausand, 2011).

This contribution studies on the use of Petri nets to visualize causal relations and temporal sequences of events in a representative case of tank overfill. Although tank overfills have led to major accidents like the Buncefield case in recent years (Casey, 2016), the awareness of the consequences resulted from a tank overfilling incident is relatively low, as affirmed by Paltrinieri et al. (2013). The objective of this paper is to 1) introduce Petri nets for dynamic modelling of safety barriers 2) explore the potentials of using the result of Petri nets simulation for supporting safety-critical decision-making. We focus on modelling of two types of technical barriers for overfilling protection: an Automatic Gauging System (ATG) and a high level switch.

## 2 CASE STUDY

The aforementioned Buncefield accident is chosen for the case study. Two main lessons learned from this accident are 1) tank overfilling (loss of primary containment) should be prevented by Safety-Instrumented Systems (SISs) 2) the industry should agree to undertake a systematic assessment of tank overfilling risk (BMIIB, 2007; BMIIB, 2008; Chambers et al., 2009; PSLG, 2009).

BMIIB (2007) recommends that Buncefield-type sites should use an automatic overfill protection systems, which comprises of sensor (level detection), logic solver, and actuator (valve). BMIIB also states that methodologies to determine Safety Integrity Level (SIL) of such system should be agreed upon in reference to IEC 61511 (2016).

In case of the Buncefield accident, the level of the tank continued to rise, exceeding the threshold level. The floating level indicator remained in the same position, instead of rising with the tank liquid. Despite the fact that this 'stuck gauge' had been discovered repeatedly before the accident day, this problem had not been seriously taken into account. The supervisor decided not to carry out a thorough investigation, or take correct repair actions. Furthermore, the high level switch was inoperable, which led to the failure to close shutdown value.

## 3 MODELLING

### 3.1 *Tank overfilling protection systems*

To simplify the model, we choose to consider one tank with the ATG system, the high level switch, alarms, and an emergency shutdown valve that can be closed in case of an emergency. It should also be remarked that the modeling includes selected component states and events to avoid too big model in this paper. However, an analyst has no limitations in increasing the number of elements in Petri net to address more specific tasks, possible decisions during operations, and the states of the components.

Figure 1 shows the tank with three filling levels. In normal operations, Basic Process Control System (BPCS) is designed to keep the filling level below the 'normal capacity'. 'Maximum capacity' is the threshold level, and liquid filling beyond this level indicates overfilling. To reduce the probability of reaching the maximum capacity level, High-high alarm is designed to be activated shortly after the tank reaches 'Tank rated capacity'. The operators are supposed to take actions in response to the High-high alarm.

The ATG system is a part of BPCS that continuously monitors the tank level, and it can trigger the High alarm in case the filling level goes beyond the normal capacity. Servo-operated float gauges are the most commonly used technology for ATG systems. This type of equipment relies on many mechanical components, and it experiences degradation over time. Servo motors, gear train, and magnetic bearings are typically prone to the wear upon contact with chemicals, which normally causes erratic measurement or sticking of the float. On the other hand, the loss of BPCS function requires the high level switch to function. The switch is designed to trigger the alarm or automatically close the shutdown valve. To comply with IEC 61511 (2016), periodic testing of the safety functions performed by the two systems is required.

The operator should ensure that the overfill protection system will work as intended. Before the start of the liquid filling, the operator calculates the ullage of the tank, calibrates the gauge, and check the functioning of the associate valves. It is

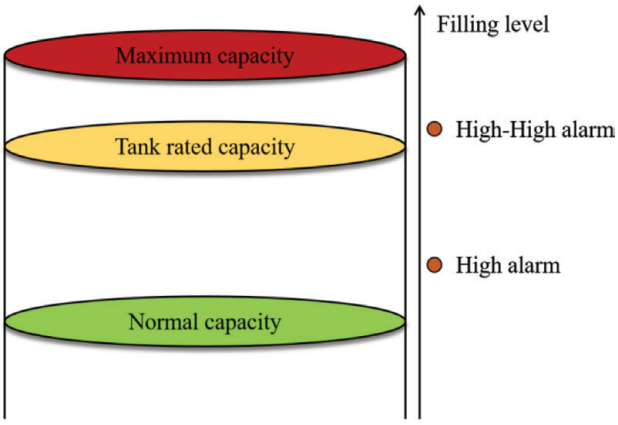



Figure 1. The tank levels set to prevent overfill.

also assumed that the operator routinely monitors the filling system at the regular intervals during the work shift to monitor the tank status.

### 3.2 *Petri nets*

Petri nets are a mathematical tool and a graphical that can be used to represent dynamic behaviors of a system. The elements of Petri nets are places, transitions, arcs, and tokens (in case of marked Petri nets). The symbol of a place is a circle, while a transition is drawn by a rectangular. Places represent local states or conditions, while transitions stand for occurrence of local events. The time to the event occurrence (firing of transition) can be stochastic or deterministic, which is depicted with different symbols. Places and transitions are connected by arcs with the shape of an arrow to model causal relations between them (IEC 62551, 2012). A place can be marked with tokens (a black dot), when the current state or condition is fulfilled. A simple example of a Petri net is shown in Figure 2.

Quantitative analysis of Petri nets is possible with Monte Carlo simulation, and this paper uses the program, GRIF workshop (GRIF, 2016). Petri nets have been used for a couple of decades to model behavior of periodically maintained systems to calculate the average availability (Signoret et al., 2013, Liu & Rausand, 2013). In GRIF, it is possible to utilize predicates for assigning preconditions and assertions to appoint the result of events. For example, filling operation can only be started when the safety systems are inspected, and the operator has not detected any abnormality. The predicates are: '?Abnormal = = 0, test = = 0', and the assertion is' !filling = 1', which are shown in in Figure 5.

### 3.3 *Modelling parameters*

Two initiating events are chosen, one is 'operator incorrect' and the other is 'ATG fails'. To utilize existing failure data (Chambers et al., 2009), the failure modes associated with the degradation of shut down valves and pipe line not included in the model, and thus exponential distribution is selected for the failure events. When the tank reaches the High level or the High-high level, it is assumed that the response should be made in 10 minutes. It is assumed that the number of tank filling is carried out 192 times per year, and the tank filling duration 12 hours. Routine visual inspection by the operator is assumed to be carried out at a regular interval (for example, every 2 hour) (PSLG, 2009). The input data is shown in Table 1.

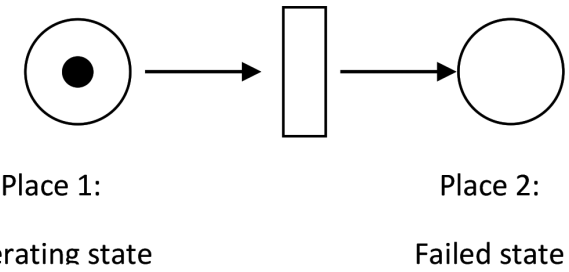



Figure 2. A simple Petri net with two places and one token.

The overview of the modelling for the tank status is shown in Figure 5. Table 2 shows the selected list of the tank states, and Table 3 shows selected list of events in the model.

#### 3.3.1 *Scenario 1*

The place 'Normal state' indicates that the tank filling is carried out with the expected velocity. No abnormal situation is found by the operator, and overfill protection systems are operable. In the normal situation, the token will stay in the place 'Normal state' for 12 hours. Afterwards, the transition 'filling_end' will be fired. The token moves to the 'Ready to fill', which means the tank is ready for another filling operation.

#### 3.3.2 *Scenario 2*

The transition 'Operator errors' is the event where the operator incorrectly calculates the tank ullage,

Table 1. Input data (PSLG, 2009; HSE, 2009).

| Transition | Parameters |
|---|---|
| Operator response | Delay, 10 minutes (0.17 hour) |
| Operator error | Failure rate, 0.00105/hour |
| ATG fail | Failure rate, 0.0000114/hour |
| Switch fail | Failure rate, 0.000004/hour |

Table 2. States of the tank.

| State (Marked with a token) | Description |
|---|---|
| Normal state | The tank level is normal |
| Abnormal | The tank level is abnormal due to the error in operational tasks |
| Level H | The tank level is high as a result of the ATG failure |
| Level HH | The tank level is at High-high level |
| Level H_Op | The tank level is at the High level as a result of operator mistake |
| Ready to fill | The tank filling level is normal |

Table 3. Description of events considered in the model.

| Event name (Transitions) | Description |
|---|---|
| Operator errors | The operator or supervisor makes a mistake in calculating filling time. |
| Operator intervenes | The operator makes actions based on own judgement. |
| H alarm response | The operator hears the alarm and take measures |
| H-H alarm response | The operator hears the alarm and take measures |
| Not detect H | The operator does not notice The High level |
| Not detect HH | The operator does not notice The High-high level |
| DU test | Periodic proof tests every six month |
| Gauge fails | Level indicator (gauge) fails |
| Switch fails | Switch fails to trigger shutdown |

* Selected events.

and the token moves to the place 'Abnormal'. In this situation, the operator may intervene and stop the process. In addition, the operator would calculate the ullage to start the filling again. If the operator does not manage to intervene and make proper response in the right time (this event is assumed to be stochastic in this case study), the filling level will reach the High level. At this point, there are two possibilities: 1) the High-level alarm sounds and the operator can stop the process 2) If the ATG had failed (either the failure is not detected or repair is not perfect), the alarm does not sound and the tank will be reaching High-high level. This frequency of this initiating is assumed to be: 192 times/year · 0.0480 = 9.22 per year (Chambers et al., 2009).

### 3.3.3 *Scenario 3*

The initiating event 'ATG failure' implies that the tank will reach beyond the normal capacity and the High alarm does not sound. There is nevertheless an opportunity for the operator to make actions without the aid of High alarm sound, which is denoted with the transition 'Operator intervene 2'. This means the operator discovers the abnormal situation by inspection, and makes the actions. If the correct actions cannot be made, the tank will stay in abnormal state and eventually reach the High-high level. After the liquid reaches the High-high level, there is still an opportunity to prevent overfilling. If the switch is working and alarm sounds at High-high level, the operator may take proper measures (e.g. close the shutdown valve). Otherwise, the tank will reach the overfill level.

### 3.3.4 *Barrier modelling*

The Petri nets for the ATG are shown in Figure 3. It is assumed that the ATG fail happens 0.1/year = $1.14 \cdot 10^{-5}$/hour (Chambers et al., 2009), which satisfies SIL 1 requirements with 6 month testing interval (PSLG, 2009). In addition, it is assumed that the periodic proof testing reveals all the dangerous undetected (DU) failures, while the repair time is assumed to be 8 hours. The Petri net model for the operational barrier is shown in Figure 4. The operator is assumed to carry out routine inspection. This allows the operator to compare the manually calculated filling level and

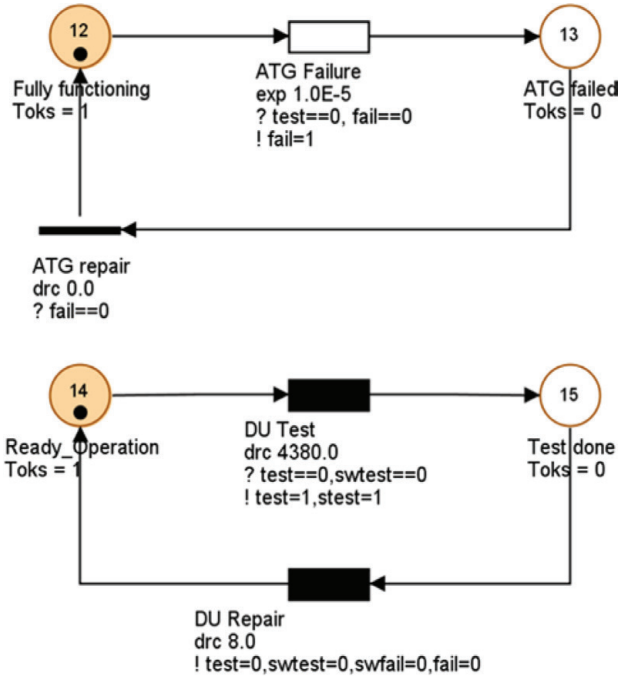



Figure 3. The Petri nets for technical barriers.

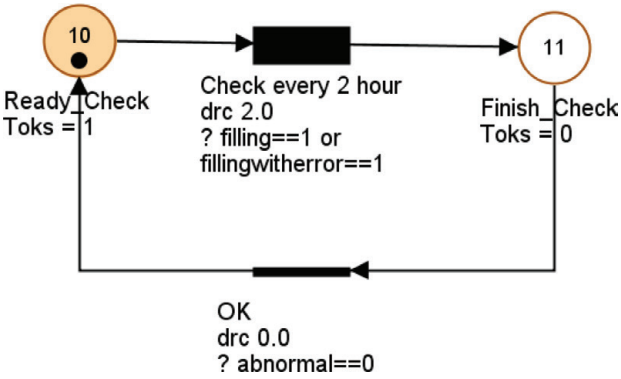



Figure 4. The Petri nets for operational barrier. The operator checks the status every 2 hour when tank filling has started, and responds to the abnormal situation.

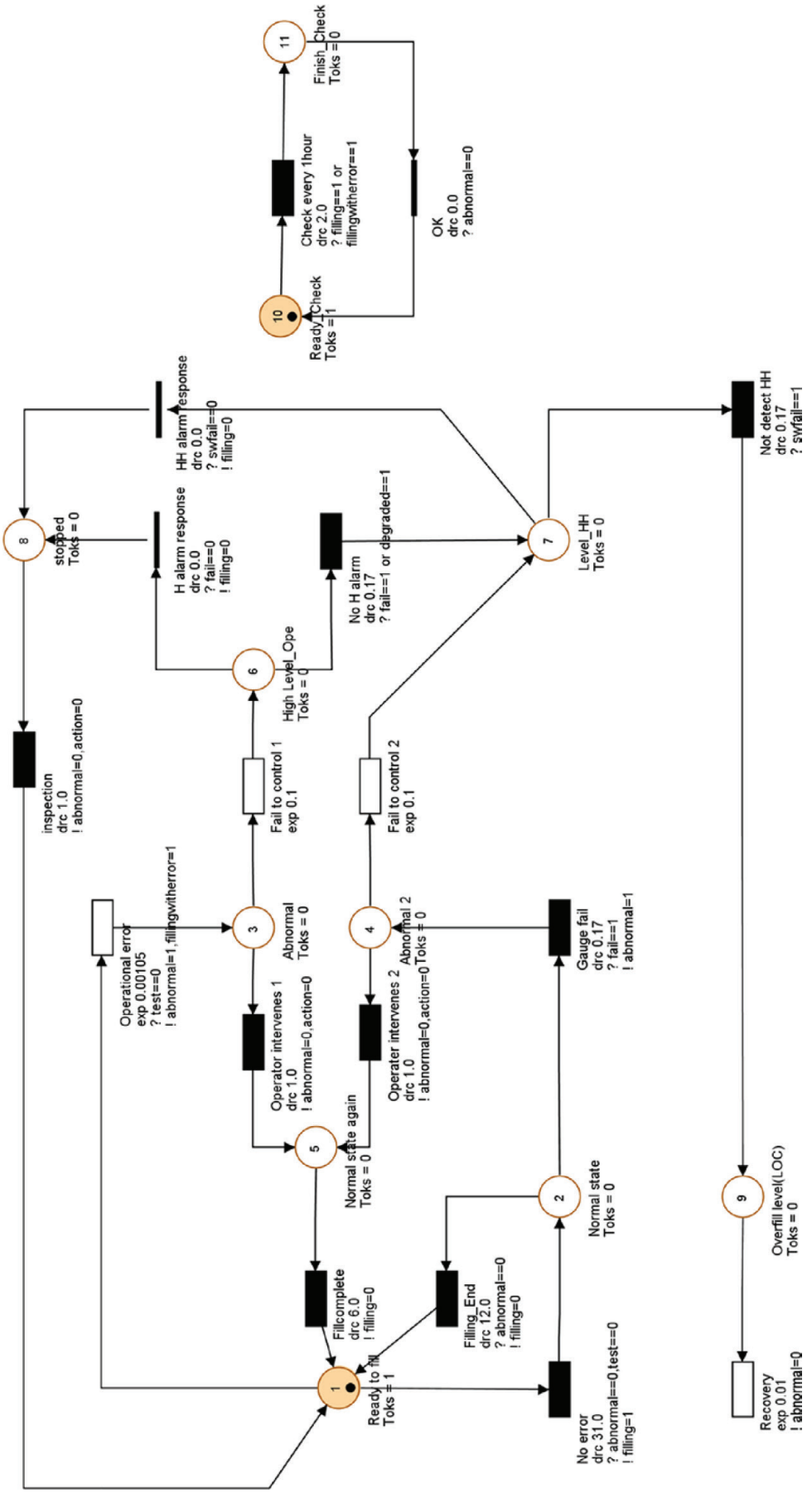



Figure 5. The Petri net modelling of the tank filling level.

actual filling level. It is also assumed that the operator records the discovered defects and reports them to the supervisor. In addition, the operator can make quick decision to immediately stop the procedure when she observes any abnormal system status. The transition 'Response' therefore has no delay, while the value to the variables are changing (action = 1, filling = 0) to denote that action is initiated and the filling will be immediately stopped.

## 4 RESULTS

### 4.1 *Simulation results*

The result of the simulation is shown in Table 4 and Table 5. The simulation was run on 1000 iterations.

Table 4. Average probability of each state.

| Name | Average token number |
|---|---|
| Ready to fill | 7,235E-01 |
| Normal state | 2,671E-01 |
| Abnormal | 1,531E-03 |
| Abnormal 2 | 1,409E-03 |
| Normal state again | 6,111E-03 |
| High Level_Ope | 2,952E-05 |
| Level_HH | 2,198E-05 |
| Stopped | 2,946E-04 |
| Ready_Check | 1,000E+00 |
| Finish_Check | 0,000E+00 |
| ATG functioning | 9,783E-01 |
| ATG failed: | 2,165E-02 |
| Switch functioning | 9,932E-01 |
| Switch failed | 6,764E-03 |

Table 5. Number of triggering of each event.

| Name | Number of triggers during period |
|---|---|
| Operational error | 7,6469 |
| Not detect HH | 0,0105 |
| HH alarm response | 1,2827 |
| H alarm response | 1,6631 |
| No error | 228,0482 |
| Response 1 | 13,6127 |
| Operator intervenes 1 | 5,9092 |
| Gauge fail | 5,4992 |
| Fail to control 1 | 1,7364 |
| Operator intervenes 2 | 4,2783 |
| No H alarm | 0,0733 |
| Fail to control 2 | 1,2199 |
| ATG Failure | 0,1098 |
| ATG repair | 0,0945 |
| Switch fail | 0,0334 |
| DU Test | 2 |
| DU Repair | 2 |

Each iteration has the length of 10000 hours. The average token number of each state, listed in Table 4 indicates long-term average probability of each state. For the ATG and the high level switch, the average token number can be understood as the average probability of failure on demand (PFD). It is shown that the ATG satisfies SIL 1, and the high level switch meets the requirements of SIL 2. Due to the structure of the Petri nets presented here, the overfill probability is dependent on the recovery time after an occurrence of tank overfill incident. Since the recovery time can vary depending on the consequence of the incident, we choose to calculate the overfill probability as below:

Frequency of overfill in 10000 hours
= Number of triggering 'Not detect HH'/10000
= 1.05E-06 (per hour)

The probability of the event in the model should be lower than industry-average overfill probability, because the model is limited to two initiating events and two safety barriers. A more complex model that includes more possible initiating events and safety functions is expected to give closer value to the real industrial case.

### 4.2 *Decision support*

Yang and Haugen (2015) addresses different types of risk associated with different types of decisions. A decision may have long-term or short-term effects on the risk level. For example, strategic decisions have long-time effects, and the risk is averaged over a relatively long time period. On the other hand, a short decision, for example, an approval of work orders for a single activity has short-term effects (i.e. the risk related to performing the work), and the average risk is not relevant.

To use Petri net modelling as an approach to operational decision support, different types of decisions can be understood as inputs to modelling assumptions (including input parameters). The assumptions are subjected to being changed over time with respect to management of change, maintenance strategies, barrier degradation. For example, maintenance resources in a site are expected to be limited (e.g. fewer operators) in the next month due to the holiday season. The manager decides to extend the inspection interval and wants to understand how this decision influences the probability of the state, tank level 'High-high' in a time frame of one month. The manager can run a new simulation with this new input, a new inspection interval. The duration of the new simulation is one month. Furthermore, new tasks or activities may need to be carried out corresponding to the results of inspection, maintenance backlogs, and new knowl-

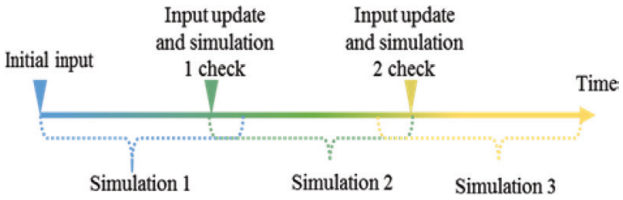



Figure 6. Updating of the model according to new inputs for new simulation result.

edge about the systems. The manager wants to assess the influence of performing the new activities in consideration for safe operation. The manager can make minor modifications in the initial Petri nets (e.g. adding or removing elements), and run a new simulation with duration of short-term, mid-term, or long-term. This aspect is schematized in the Figure 6.

## 5 DISCUSSION

One of the main challenges in Petri net modelling is the uncertainties in choosing the distributions for the transitions and input parameters. In particular, events associated with the errors and the decisions made by operators may not be straightforward to be included in the Petri nets. Petri nets in general have weaknesses, to include that the models tend to become so complex that the possible errors are hard to be discovered (Brissaud & Oliveira, 2012; Rausand, 2014). In other words, it may not be realistic to develop an exhaustive model with numerous places and transitions. Another challenge is to logically select and structure the elements (place, transitions, and arc connections) in Petri nets. This requires good understanding of both technical systems and operational situations, as one of the prerequisites of Petri net modelling.

## 6 SUMMARY AND CONCLUSION

Quantifying the probability of the hazardous event is an important step to achieve the overall risk picture, and the realistic probability value is highly desired for practical use of risk analysis. This paper suggests Petri nets as a tool to account time-dependent barrier performances to realistically calculate a hazardous event frequency. A tank overfilling scenario is chosen to be analyzed with Petri nets. The presented model is not exhaustive, in that the model selects two possible initiating events, in consideration of the two SISs amongst the technical barriers in tank filling operation. The operator activities are also simplified. Despite these limitations, we regard this work as a point of departure to demonstrate how Petri nets can be used for modelling hazardous events. In addition, the simulation result of the model can provide inputs to the managers in assessing the risk and safety implications of operational decisions, which represents a valuable support for safe operation.

## ACKNOWLEDGEMENT

The contributions from Professor S. Haugen are acknowledged. The authors are grateful for the valuable comments from X. Yang.

## REFERENCES

Andersen, H., Casal, J., Dandrieux, A., Debray, B., De Dianous, V., Duijm, N.J., 2004. ARAMIS—user guide. EC Contract number EVG1-CT-2001–00036.

Buncefield Major Incident Investigation Board (BMIIB). 2007. Recommendations on the design and operation of fuel storage sites. The Office of Public Sector Information, UK (2008)

Buncefield Major Incident Investigation Board (BMIIB). 2008. The Buncefield incident 11 December 2005, The Office of Public Sector Information, UK (2008)

Brissaud, F. and Luiz, F., 2015. Average probability of a dangerous failure on demand: Different modelling methods, similar results.

Casey, R. 2016. Storage tank overfilling and double failure. Loss Prevention Bulletin, (247):2–4.

Chambers, C. Wilday, J. & Turner, S. (2009) A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks. Health and Safety Laboratory, Harpur Hill Buxton Derbyshire SK17 9 JN,UK.

COMAH Competent Authority, 2011. Buncefield: why did it happen?. Retrieved on 18 December 2016 from http://www.hse.gov.uk/comah/buncefield/buncefield-report.pdf.

EU, 2012. SEVESO III. Directive 2012/18/EU Of The European Parliament And Of The Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC.

Fajardo, J.F., Perez, A.A.J., Alsina, S.S.M., & Ramirez-Marquez, J.E. (Eds.). 2010. Simulation methods for reliability and availability of complex systems. Springer Science & Business Media.

GRIF, 2016. http://grif-workshop.com/

Haugen, S. & Edwin.J.N. 2016. Dynamic risk analysis for operational decision support ESREL 2016. Taylor & Francis, 2016.

IEC 61508, 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission, Geneva.

IEC 61511, 2016. Functional Safety: Safety Instrumented Syystems for the Process Industry Sector, Part 1–3. International Electrotechnical Commission, Geneva.

IEC 62551, 2012. Analysis techniques for dependability—Petri net techniques. International Electrotechnical Commission, Geneva.

Liu, Y., & Rausand, M. 2013. Reliability effects of test strategies on safety-instrumented systems in different demand modes. Reliability Engineering & System Safety, 119, 235–243.

Nivolianitou, Z.S., Leopoulos, V.N., & Konstantinidou, M. 2004. Comparison of techniques for accident scenario analysis in hazardous systems. Journal of Loss Prevention in the Process Industries, 17(6), 467–475.

Nývlt, O., & Rausand, M. 2012. Dependencies in event trees analyzed by Petri nets. *Reliability Engineering & System Safety*, *104*, 45–57.

Nývlt, O., Haugen, S., & Ferkl, L. 2015. Complex accident scenarios modelled and analysed by Stochastic Petri Nets. *Reliability Engineering & System Safety*, *142*, 539–555.

Paltrinieri, N., Tugnoli, A., Buston, J., Wardman, M. and Cozzani, V., 2013. Dynamic procedure for atypical scenarios identification (DyPASI): a new systematic HAZID tool. Journal of Loss Prevention in the Process Industries, 26(4), pp.683–695.

Process Safety Leadership Group (PSLG), 2009. Safety and environmental standards for fuel storage sites. Final report. Retrieved on 18 December 2016 from http://www.hse.gov.uk/comah/buncefield/fuel-storage-sites.pdf.

Høyland, A. & Rausand, M., 2004. System reliability theory: models, statistical methods, and applications. NJ: Wiley-Interscience.

Rausand, M., 2011. Risk assessment: theory, methods, and applications. John Wiley & Sons.

Rausand, M., 2014. Reliability of safety-critical systems: theory and applications. John Wiley & Sons.

Schwabach, A. 1989. The Sandoz Spill: The Failure of International Law to Protect the Rhine from Pollution, 16 Ecology L.Q. Available at: http://scholarship.law.berkeley.edu/elq/vol16/iss2/3

Signoret, J.P., Dutuit, Y., Cacheux, P.J., Folleau, C., Collas, S., & Thomas, P. 2013. Make your Petri nets understandable: Reliability block diagrams driven Petri nets. Reliability Engineering & System Safety, 113, 61–75.

Total, 2016. GRIF Workshop: http://grif-workshop.com/

Vinnem, J.E., 2014. Offshore Risk Assessment vol 2. London: Springer.

Yang, X., Haugen, S., 2015. Classification of risk to support decision-making in hazardous processes. Safety Science, 80, 115–126

Liu, Y., & Rausand, M. 2013. Reliability effects of test strategies on safety-instrumented systems in different demand modes. Reliability Engineering & System Safety, 119, 235–243.

Nivolianitou, Z.S., Leopoulos, V.N., & Konstantinidou, M. 2004. Comparison of techniques for accident scenario analysis in hazardous systems. Journal of Loss Prevention in the Process Industries, 17(6), 467–475.

Nývlt, O., & Rausand, M. 2012. Dependencies in event trees analyzed by Petri nets. *Reliability Engineering & System Safety*, *104*, 45–57.

Nývlt, O., Haugen, S., & Ferkl, L. 2015. Complex accident scenarios modelled and analysed by Stochastic Petri Nets. *Reliability Engineering & System Safety*, *142*, 539–555.

Paltrinieri, N., Tugnoli, A., Buston, J., Wardman, M. and Cozzani, V., 2013. Dynamic procedure for atypical scenarios identification (DyPASI): a new systematic HAZID tool. Journal of Loss Prevention in the Process Industries, 26(4), pp.683–695.

Process Safety Leadership Group (PSLG), 2009. Safety and environmental standards for fuel storage sites. Final report. Retrieved on 18 December 2016 from http://www.hse.gov.uk/comah/buncefield/fuel-storage-sites.pdf.

Høyland, A. & Rausand, M., 2004. System reliability theory: models, statistical methods, and applications. NJ: Wiley-Interscience.

Rausand, M., 2011. Risk assessment: theory, methods, and applications. John Wiley & Sons.

Rausand, M., 2014. Reliability of safety-critical systems: theory and applications. John Wiley & Sons.

Schwabach, A. 1989. The Sandoz Spill: The Failure of International Law to Protect the Rhine from Pollution, 16 Ecology L.Q. Available at: http://scholarship.law.berkeley.edu/elq/vol16/iss2/3

Signoret, J.P., Dutuit, Y., Cacheux, P.J., Folleau, C., Collas, S., & Thomas, P. 2013. Make your Petri nets understandable: Reliability block diagrams driven Petri nets. Reliability Engineering & System Safety, 113, 61–75.

Total, 2016. GRIF Workshop: http://grif-workshop.com/

Vinnem, J.E., 2014. Offshore Risk Assessment vol 2. London: Springer.

Yang, X., Haugen, S., 2015. Classification of risk to support decision-making in hazardous processes. Safety Science, 80, 115–126

# Article V

Shenae Lee, Mary Ann Lundteigen, Nicola Paltrinieri, Yiliu Liu, Magne Rød, John Dale, 2017, **A new design concept of Blowout Preventer for decision support.** 27th European Safety and Reliability Conference ESREL. Ljubljana, Slovenia.

*Safety and Reliability – Theory and Applications – Čepin & Briš (Eds)*
*© 2017 Taylor & Francis Group, London, ISBN 978-1-138-62937-0*

# A new design concept of Blowout Preventer for decision support

S. Lee, M.A. Lundteigen, N. Paltrinieri & Y. Liu
*NTNU, Trondheim, Norway*

M. Rød & J. Dale
*Electrical Subsea and Drilling AS, Bergen, Norway*

ABSTRACT: The Blowout Preventer (BOP) system is used for controlling blowout risks in drilling operations. The system is implemented to shut down an oil and gas well when the well fluids have entered the wellbore. All BOP systems today are operated with Electro-Hydraulic (E/H) controls, and the record shows high number of failures and malfunctions involving hydraulic components (e.g. leakages). Failures of BOP systems have made significant contributions to non-productive time of drilling rigs. This paper introduces a new concept of electro-mechanically operated BOP, which seems to be a candidate to improve reliability and availability of the BOP. The main interest of this paper is to shed light on the new features of the electrical BOP system versus current art qualitatively. In addition, this contribution proposes a method for the BOP availability analysis which may be used in the decision-making about designing optimal BOP systems.

## 1 INTRODUCTION

The petroleum industry has expanded into new areas for oil and gas production. Exploration activities in the North Sea, for example, have gradually moved to the northernmost regions and to ultra-deep waters, typically in the Gulf of Mexico and Brazil to discover more hydrocarbon resources. Drilling activities involve the risk associated with uncontrolled release of well fluids (Corneliussen, 2006), namely kicks. Kicks, if not controlled by the safety barriers, can escalate to a blowout event, where the fluids and gas flow to the surface or into lower pressured subsurface zones. The blowout accident in the Macondo well caused 11 fatalities, abandonment of the drilling rig, and the largest oil spill in the U.S. history. One of the accident causes was the failure of the Blowout Preventer (BOP) system in stopping the pressurized hydrocarbons escalating to the rig.

The subsea BOP system is a secondary well barrier that consists of several well barrier elements (NORSOK D-010, 2013). The BOP system can contain the well fluids and cut off the drill pipe when the containment by the primary well barriers has failed. The BOP is temporarily installed on the wellhead at the seabed. The BOP stack at the seabed is the assembly of preventers, and their auxiliary equipment, including control system equipment. The marine drilling riser is a pipe (typical 21-inch Outer Diameter), that extends from the drilling platform down to the Lower Marine Riser Package at the top of the BOP stack. The upper part of the BOP stack can be disconnected from the lower BOP stack as part of a controlled operation, or in case of emergency. Dangerous failures of BOP components may not be detected before the BOP is locked onto the well head. Failures may be revealed during the periodic testing, and an immediate pulling of the BOP for repair if the faulty components are considered critical (NORSOK D-010, 2013). This introduces non-productive time, while unscheduled pulling of BOPs may increase the well blowout risk (Strand & Lundteigen, 2015). To enhance safety during drilling, it has been suggested in the industry that decision-making related to reliability, availability, and maintenance of BOP systems should be made on credible information on the system performance. Furthermore, such information is expect to determine the optimal design of the BOP systems in long term (IADC, 2016).

The design principle of hydraulic actuation of BOPs has dominated the industry since the 1920`s. A common problem of Electro-Hydraulic (E/H) BOP system is the hydraulic leakages, which can be a single point of failure. Leakage of a valve or connection may eventually require pulling of the BOP to the surface. Deep water drilling has additional problems, such as hydraulic signal delay, pressure and stored energy loss, difficulties of condition monitoring, and heavy weight of subsea hydraulic fluid accumulators.

Acknowledging such aspects of the current BOP systems, the company Electrical Subsea & Drilling AS (ESD) and its R&D partner Kongsberg Maritime are developing a new design concept of electrically operated BOP system. The main idea is to replace all the hydraulic components with equivalent electrical components. Another concept is the technology for Electro-Mechanical (E/M) actuators that are operated without using hydraulic pressure.

The aim of this paper is first to highlight some of the reliability implications of introducing the electrically operated BOP system. The second aim is to suggest an advanced approach for quantitative analysis of the BOP availability. Petri nets are used to consider the effect of regular testing (including repair time), which is not explicitly captured in the previous studies. The case study in section 4 gives a representative example on how to apply this approach in the availability analysis of the current E/H BOP system. The case study is not intended for the electrical BOP, as the currently available reliability data is considered to be insufficient to support the anlysis. Once the data is available, however, the approach can be easily applied for the new design BOP system.

## 2 BOP SYSTEM DESCRIPTION

### 2.1 *BOP well barrier elements*

GL 070 (2004) defines the safety functions of a drilling BOP system; 1) Seal around pipe 2) Seal an open bore 3) Shear drill pipe and seal well off. These functions are achieved by different types of BOP well barrier elements and the items that are necessary to activate (open or close) the preventers (API RP53, 2012). Two types of preventers are used in a BOP system: the ram-type preventer and the annular type preventer. A ram preventer uses a pair of rams that linearly move for sealing the wellbore, or shearing of a drill pipe. The types are: the pipe rams, the Blind Shear Rams (BSR) and the casing shear ram. The BSR is the only type of well barrier element that can shear the pipe and in turn seal the wellbore with rubber packers, such that no fluid can pass through the pipe and the annulus around the pipe. Pipe rams can seal around the drill string of a particular diameter, while the variable bore rams are able to seal the tubulars with different diameters. Pipe rams may also be used to hold the tubular in position during shearing of the pipe. The annular preventer is a flexible rubber sealing element, a so-called 'doughnut' sealing element, as it can embrace and seal any object inside the annular space of the wellbore. It has lower working pressure than the ram type BOPs and is positioned in the LMRP. Typical pressure rating of the annular preventer is 10-ksi in a 15-ksi rated BOP stack.

### 2.2 *Electro-Hydraulic (E/H) control systems*

The BOP control system today is based on E/H control systems, where Programmable Logic Controllers (PLCs) converts operators' command on the panel into electronic signals. The schematic of E/H control is shown in Figure 1. Solenoid valves then convert the electric signal to pilot hydraulic signals. The hydraulic signals are used to direct pressurized hydraulic fluid from the power supply on the topside and the subsea BOP mounted accumulators to operate the preventers. Numerous valves, manifolds, and regulators are used to translate the input from the surface to subsea BOP stacks. For the power supply to operate the preventers and connectors, hydraulic pressure supply is provide by a surface mounted Hydraulic Power Unit (HPU), hydraulic distribution (hoses and hard piping) and subsea hydraulic accumulators.

### 2.3 *Reliability implication of electrical control system*

The new concept of electrically operated BOP includes the use of electrical power supply with batteries to replace hydraulic pressure energy, Electro-Mechanical (E/M) actuators, and the control system consisted of only electrical components. The two types of actuators are being prototyped by the company ESD: 1) ram-type actuator which can be used for pipe rams and BSR 2) ring piston actuator for annular preventers and connectors.

Ring motors are used to power both the ram actuators and the ring piston devices. The output torque from the motor is transferred to the actuation segment through transmission elements based on planetary gears and roller screw technology. The rotary motion of the electric motor is transferred to linear motion of the actuating element. An efficient power transmission is a key to produce sufficient force. Figure 2 is a simple presentation of the ring piston actuator used for annular preventer and connector.

The main focus with respect to ESD's E/M actuator development has been on the blind shear ram application, because that application requires very high force in comparison to other ram functions. Shear rams must generate forces necessary for cutting or sealing tubulars in the wellbore. Normal ram-type BOPs, for example, withstand 15-ksi working pressure, and shear rams are required to have cutting capacity of 900 Metric tons. The possible achievements of electrical BOP systems are: 1) Avoidance of common scenarios involving hydraulic leakages and no discharge of hydraulic fluid to

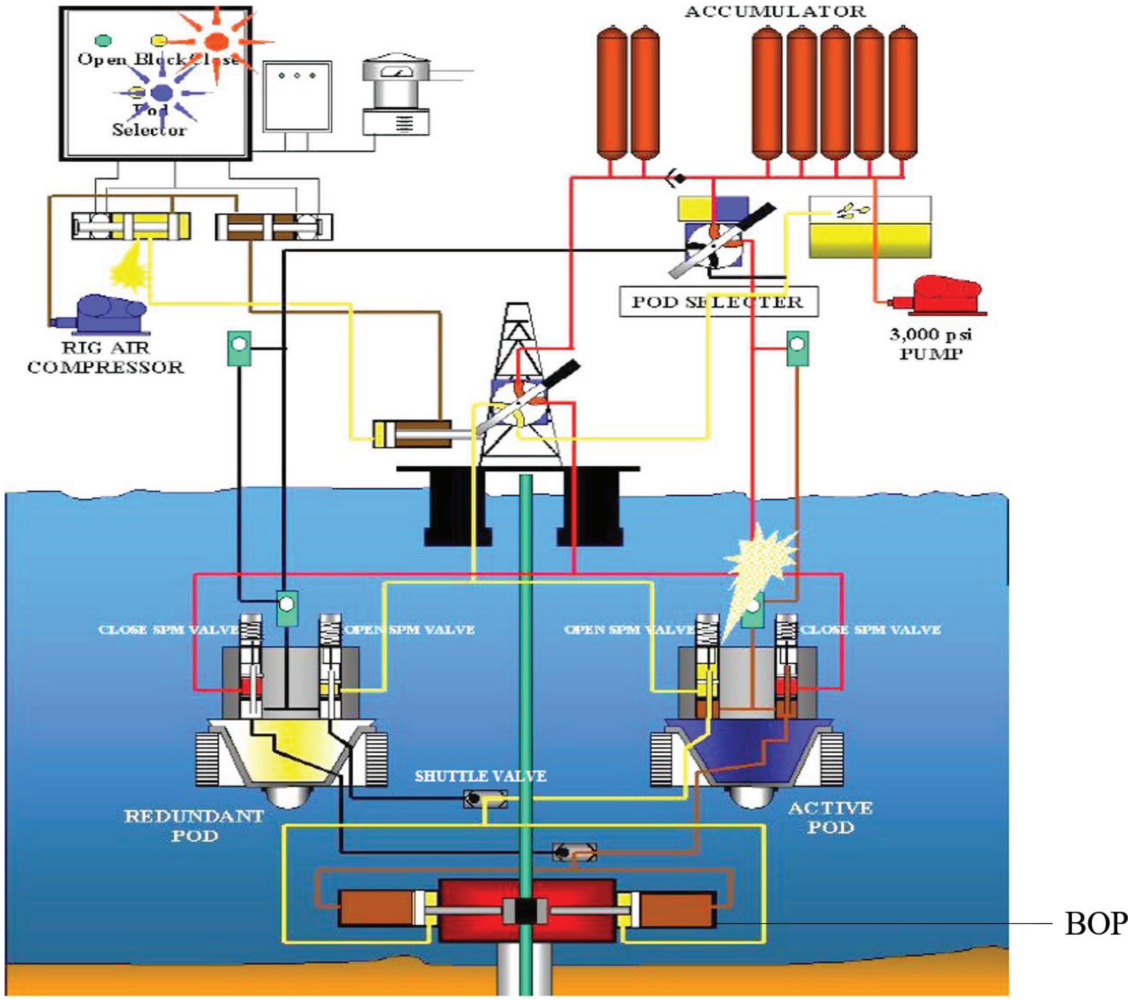



Figure 1. Schematic of electro-hydraulic control and power supply used in the contemporary BOP control systems. Hydraulics fluids are transmitted to the BOPs for activation. Borrowed from Mærsk drilling center (2009).


Figure 2. Electro-mechanical ring piston concept by ESD. The rotary motion of the electric motor is transmitted to the linear motion of the activation segment. Hydraulic modules can be removed with this design concept (Dale, 2013).

the environment 2) no power loss due to increased ambient pressure at deep water, reduced weight and space, increased redundancy 3) Improvement in condition monitoring, instrumentation system: electronic and electro-mechanical components are inherently easier to accurately monitor than the hydraulic components.

E/M actuators are claimed to provide high force with dual redundant rotating motors, fast cutting, precise control and monitoring of stroke position/ applied force. An important, practical advantage of E/M operation is also that it is possible to have exact control over the applied force to provide the optimum operation during stripping operations through the annular preventer. The control system will automatically adjust the rubber element contraction and "back-off" during tool-joint passage. Applied force is measured and regulated with control of electrical motor power and direction.

## 3 SAFETY ANALYSIS OF BOP

A BOP, whether it is electrically or hydraulically operated, has some generic design and operational characteristics that must be addressed in a reliability

analysis. Some examples of such characteristic are what are the safety-critical functions, what performance measures are relevant for safety, how to account for different types of regular testing (including repair time), and the efficiency of these tests. The mentioned topics are elaborated more in the following.

### 3.1 *BOP safety functions*

The BOP system may perform safety functions upon kick detection. The functions can be carried out either by manual or automatic activation of BOPs, depending on the operational conditions. In the normal operational mode, the operators activates one pod to control the hydraulic power supply. The pod is comprised of Subsea Electronic Modules (SEM) with PLCs and the hydraulic unit. The pod also sends information such as electronic riser angle indicator, BOP stack temperature, BOP stack pressure and accumulator pressure readback (Holand & Awan, 2012).

The BOP system can be considered to perform Safety Instrumented Functions (SIF) despite operational modes with the manual activation by operators. The BOP is operated in low demand mode, and the average Probability of a dangerous Failure on Demand ($PFD_{avg}$) is used to determine the Safety Integrity Level (SIL) (IEC 61508, 2010). $PFD_{avg}$ can be understood as the mean proportion of downtime in an interval, and it is interpreted as the probability of an item not being able to function upon demand (Rausand & Høyland, 2004). Minimum SIL 2 of the critical BOP SIFs is required by GL-070 (2004).

### 3.2 *BOP testing*

Testing is performed to confirm correct response to failures, and retain correct performance of a SIS (Rausand, 2014). Current BOP systems requires two types of regular tests: Function Test (FT) and the Pressure Test (PT) (NORSOK D-010, 2013; API RP 53, 2012). A function test is carried out to verify BOP operability. Dangerous failure modes involving closing and opening of BOPs and the pump capability for hydraulic supply are tested. A pressure test is to verify the pressure containment capability by applying pressure to BOPs. FT is required to be carried out every 7 days. PT is required to be performed every 14 days by BSEE regulation (2014), while API RP 53 (2012) requires the interval of 21 days. NORSOK D-010 has revised the requirements from the interval of 14 to 21 days, on the ground that running of tools and pressure testing can be a high risk activity before the bore is cased off. It should be noted that rated pressure is applied for the PT and it cannot be considered as proof testing of cutting ability of ram preventers.

### 3.3 *Possible improvement for the safety functions*

Electronic and electro-mechanical components are inherently easier to accurately monitor than the hydraulic counterparts. The improved BOP instrumentation features is expected to enhance real time safety and management during the operation of the BOP system, and drastically reduce the time consumed for in-between well maintenance through the Condition monitoring functionality:

1. All CPUs, communication lines and electrical wiring will be continuously controlled by a health monitoring system. The fault of electrical equipment shall be monitored, data to be stored locally and sent to the vessel's Control System & Information Management System. For example, an accelerometer shall be mounted in the electrical motor compartment to measure the vibration
2. System performance, such as stroke, speed and torque of all actuators and motors shall be controlled, monitored and logged.
3. Sensors for wellhead fatigue measurement can be implemented in the BOP wellhead connector and be interfaced with a riser monitoring system. Addressing wellhead fatigue issues and proving sufficient margin for drilling operations has been a growing challenge for the oil and gas industry over the last decade. The subsea control system hardware shall be fitted in cylindrical canisters that can be separately pulled and replaced during operation.
4. For redundancy, back-up Hydro-acoustic controls to be interfaced with the new solution All retrievable devices shall be connected with ROV operated connectors. All retrievable devices shall be connected with ROV operated connectors

## 4 QUANTITATIVE ANALYSIS

### 4.1 *Reliability Block Diagram (RBD) driven Petri Nets*

A Reliability Block Diagram (RBD) can be used to illustrate a system safety function that are broken down to component functions. A RBD gives the logical relationship between component functions by structuring each block (rectangle or square) that represents binary states (functioning/failed) (Rausand, 2014). It is possible to combine Petri Net analysis (which allows modeling of multiple states of components) with RBDs (that maintain a structure which is easier read), which is referred to

as RBD driven Petri nets. In a Petri net transitions between different states can be either stochastic or deterministic, and the stochastic transitions allow different types of distributions. RBD driven Petri nets can add dynamic features by taking into account effects of tests and repair, operational strategies in the presence of component failures, and component reliability.

### 4.2 *Case study*

A component or a module of the RBDs can be replaced with Petri nets. An example of a RBD for each BOP system with different operating principles is shown in the Figure 3. Petri Nets model is carried out to represent the states of components in the RBD. The traditional (electro-hydraulic operated) BOP system has chosen to be the subject of this analysis due to the availability of reliability data repair in Holand (2009), Holand & Awan, (2012) and Hauge et al. (2012). The input data such as failure rates and time consumed for testing is shown in Table 2.

The focus of this case study is to estimate the unavailability of the function of a BSR that are under the effect of two types of regular testing and repairs. GRIF workshop demonstration version (GRIF, 2016) is used for the configuration of Petri Net and the simulation for obtaining the average Probability of Failure on Demand ($PFD_{avg}$). Figure 4 illustrates the Petri net model built to treat Function Testing (FT) and Pressure Testing (PT) of a ram-type preventer. It is assumed that FT can reveal the failures of preventer and the associated

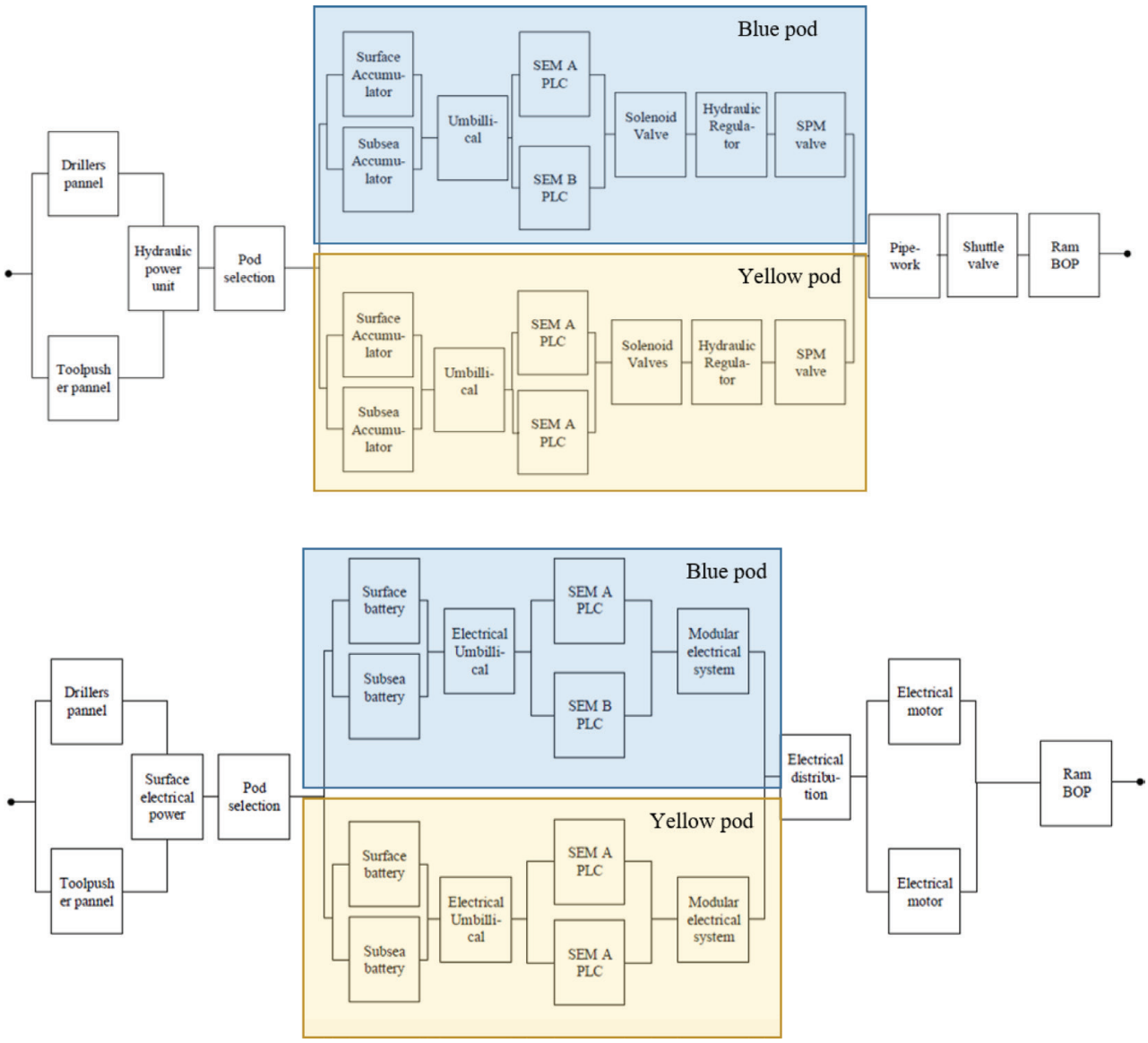



Figure 3. Simplified RBDs for a E/H BOP control system (above) and an electrical BOP system (below).

Table 1. Places and transitions in the Petri nets.

| Element | State (with a place holding a token) /Event |
|---|---|
| Place: Working_FT_A | State: no fault that can be revealed by FT |
| Transition: Fail_FT_A | Event: occurrence of a failure that can be revealed by FT |
| Place: Working_PT_A | State: no fault that is only revealed by PT |
| Transition: Fail_PT_A | Event: occurrence of a failure that can be revealed by PT |
| Transition: Repair_FT | Event: fix of the fault revealed by FT |
| Transition: Repair_PT | Event: fix of the fault revealed by PT |
| Transition: FT | Event: Function test |
| Transition: PT | Event: Pressure test |

Table 2. Input data.

| Parameter | Value |
|---|---|
| Function testing interval | 168 hours (7 days) |
| Pressure testing interval (1) | 336 hours (14 days) |
| Pressure testing interval (2) | 504 hours (21 days) |
| Average time consumed for pressure testing | 14.33 (hours) |
| Average time consumed for function testing | 0.71 (hours) |
| Failure rate $\lambda$ | 4.3·10–5 (Per hour) |
| Failure rate $\lambda$PT (detected by PT) | 2.8·10–5 (Per hour) |
| Failure rate $\lambda$FT (detected by FT) | 1.5·10–5 (Per hour) |
| Average time consumed for Repair | 6.1 (hours) |

control devices involving opening and closing of BOP. The ability of preventer to withhold the well pressure is tested in FT. The FT in this Petri nets does not cover the cutting ability of BSR.

Two type of variables, predicates and assertions are used. Predicate represent the pre-condition of transition, while assertion denotes the result of transition. For instance, '? pfail == 0' and ! pfail = pfail+1' imply that the working component A can move to the failed state (pfail = 1) as a result of the stochastic transition. And Table 1 describes the Petri net model.

Jin and Rausand (2013) demonstrates the $PFD_{avg}$ of a *k*-out-of-*n* (*koon*) system that is subjected to both periodic PST and the Proof Test (PT). Formula (1) is $PFD_{avg}$ derived without considering Common Cause Failure (CCF).

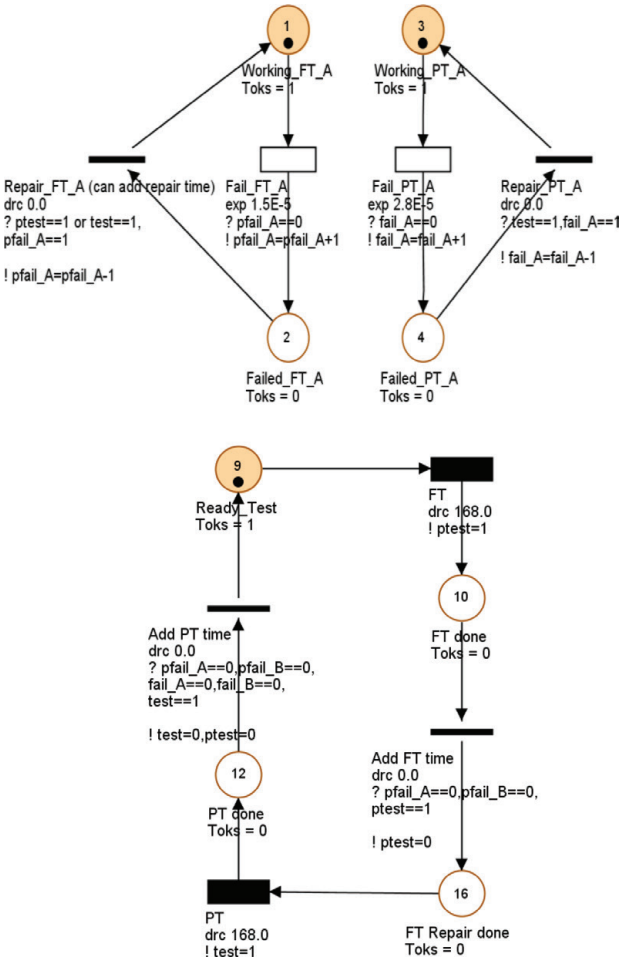



Figure 4. Example of a Petri nets for a ram-type preventer.

$$PFD_{avg} \approx \frac{1}{m}\left(\begin{array}{l}\sum_{i=1}^{m}\sum_{j=0}^{n-k}\binom{n}{j}\left((i-1)(i-\theta)\lambda\tilde{\tau}\right)^{j} \\ \quad \times \frac{(n-j)!(\lambda\tilde{\tau})^{n-j-k+1}}{(n-j-k+2)!(k-1)!} \\ \quad + \sum_{i=1}^{m}\sum_{j=n-k+1}^{n}\binom{n}{j}\left((i-1)(i-\theta)\lambda\tilde{\tau}\right)^{j}\end{array}\right) \quad (1)$$

where $\theta$ = PST coverage; $\tilde{\tau}$ = PST interval $\tau = m\tilde{\tau}$; and (m–1) = number of PSTs in each PT interval;

The main assumptions are:

1. The channels in *koon* system are identical with the constant DU failure rate.
2. All the tests are carried out simultaneously for n channels, and testing and repair
3. Repair time is negligible. Once a failure is revealed by PST, it is repaired immediately
4. The failure revealed by PT is not affected by PST

Table 3. Simulation result.

| | Formula (PT interval 14 days) | Simulation 1 (PT interval 14 days) | Simulation 2 (PT interval 21 days) |
|---|---|---|---|
| 1oo1 | 5,96E-03 | 5.923E-3 | 8.253E-3 |
| 1oo2 | 4,545E-05 | 4,437E-05 | 9.291E-5 |

Table 4. Simulation result with PT interval 14 days.

| | Simulation 1–1 (with repair time) | Simulation 1–2 (testing time) | Simulation 1–3 (both testing and repair time) |
|---|---|---|---|
| 1oo1 | 6.193E-3 | 6.192E-3 | 6.473–3 |
| 1oo2 | 4.842E-5 | 4.900E-5 | 5.127 E-5 |

Table 5. Simulation result with PT interval 21 days.

| | Simulation 2–1 (with repair time) | Simulation 2–2 (testing time) | Simulation 2–3 (both testing and repair time) |
|---|---|---|---|
| 1oo1 | 8,521E-3 | 8,521E-3 | 8.804E-3 |
| 1oo2 | 9.292E-5 | 9.400E-5 | 9.918E-5 |

### 4.3 *Result*

The estimated $PFD_{avg}$ of 1oo1 BSR and 1oo2 BSRs are attained from the Monte Carlo simulation in GRIF. The simulation duration is set to be 3 years, since the BOP overhaul interval is 3 to 5 years. Firstly, estimation of $PFD_{avg}$ without including of testing and repair times are shown in Table 3, which exhibits close values with the approximation formula (1). The extended PT test interval from 14 to 21 days gives the increase in $PFD_{avg}$, but without changing the exponents of the numbers. Table 4 and Table 5 show simulation results of three different cases with consideration of: 1) repair time 2) consumed time for testing 3) both repair time and consumed time for testing. It is shown that the repair and testing times result in small increment of the $PFD_{avg}$.

## 5 DISCUSSION

The case study is applied to a single device of E/H BOP system. The approach is the point of departure which can eventually extend to a system level model, where the whole the BOP system function from the initiation to closure of minimum number of BOP actuating devices, in light of the mode of operation. The result shows that the shorter test interval gives higher availability. However, risk introduced by performing test and cost of non-productive time are not analyzed. On the other hand, the company ESD addresses that electrical BOP should have different testing strategies. Preventive and corrective maintenance on the control system can be triggered based on condition monitoring mentioned in the section 3.3. According to the ESD's claim, electrical BOP can reduce the time consumed for testing and the preparations prior to operations by means of early detection of any degraded performance. It is expected that less failures are reported with electrical actuation, as all the hydraulic and electro/hydraulic valves are removed. Less unscheduled stops and lifting of BOP to the rig can be also assumed. This aspect therefore presents the need to investigate testing efficiency and repair and restoration times with new operational strategy of an electrical BOP. Besides, the new BOP system will have various sensors, which continuously provide feedback to the control system and the motor control that provide actuation data. Such new components will introduce new failure modes, and these must be carefully analyzed to calculate the associated reliability parameter.

## 6 SUMMARY AND CONCLUSION

This paper identifies key characteristics of electrical BOP system. This new design may improve safety availability of BOP systems and contribute to the risk reduction during drilling. The case study demonstrates Petri net modelling for availability analysis for an E/H BOP to consider two types of regular testing with different intervals. To apply the method for an electrical BOP, it is necessary to make reasonable estimates for failure rates based on qualification testing, since no operational experience has not yet been obtained for such systems. Despite the uncertainty, it is important to develop and carry out quantitative analyses that can support decision-making for optimizing the design and operation of the BOP systems.

## ACKNOWLEDGMENT

The authors are grateful for the valuable comments from G.-O. Strand.

## REFERENCES

API 53 (2012). API Standard 53 Blowout Prevention Equipment Systems for Drilling Wells. American Petroleum Institute (API), API Publishing services, Washington, DC.

BSEE, *Code of Federal Regulations*. 2014, Bureau of Safety and Environmental Enforcement: http://www.bsee.gov/.

Corneliussen, K. (2006). Well safety; Risk control in the operational phase of offshore wells. PhD thesis. Norwegian University of Science and Technology (NTNU). Trondheim, Norway.

Dale. J (2013). BOP control features "All electric controls". [Powerpoint slide].

Hauge S., Håbrekke S., Kråkenes T., Lundteigen, M.A. & Merz M. (2012). Barriers to prevent and limit acute releases to sea — Environmental barrier indicators, SINTEF Rapport A22763. SINTEF, Trondheim, Norway.

Holand, P. & Awan, H. (2012) Reliability of Deepwater Subsea BOP Systems and Well Kicks. Exprosoft.

Holand, P. (2009). Effektivisering av BOP testing. [PowerPoint slides]. Retrieved from esra.no/wp-content/uploads/2015/04/Kl-1110-Effektivisering-av-testing-av-subsea-BOP_Per-Holand_ExproSoft.pdf

GRIF, 2016. GRIF Workshop: http://grif-workshop.com/

NORSOK D-010 (2013). Well integrity in drilling and well operations, Norsok standard, Standard Norge, Oslo, Norway.

Norsk olje og gass. (2004). GL 070 — Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry.

Rausand, M. and Høyland, A. (2004). System Reliability Theory: Models, Statistical Methods, and Applications. Wiley, Hoboken, NJ, 2nd edition.

Rausand, M. (2014). Reliability of Safety-Critical Systems: Theory and Applications. Wiley, Hoboken, NJ.

Signoret, J.P., Dutuit, Y., Cacheux, P.J., Folleau, C., Collas, S., & Thomas, P. (2013). Make your petri nets understandable: Reliability block diagrams driven petri nets. Reliability Engineering & System Safety, 113, 61–75.

Strand, G.O. & Lundteigen, M.A. (2015). Risk control in the well drilling phase: BOP system reliability assessment. European Safety and Reliability Conference, 2015.

*Safety and Reliability – Theory and Applications – Čepin & Briš (Eds)*
*© 2017 Taylor & Francis Group, London, ISBN 978-1-138-62937-0*

# A new design concept of Blowout Preventer for decision support

S. Lee, M.A. Lundteigen, N. Paltrinieri & Y. Liu
*NTNU, Trondheim, Norway*

M. Rød & J. Dale
*Electrical Subsea and Drilling AS, Bergen, Norway*

ABSTRACT: The Blowout Preventer (BOP) system is used for controlling blowout risks in drilling operations. The system is implemented to shut down an oil and gas well when the well fluids have entered the wellbore. All BOP systems today are operated with Electro-Hydraulic (E/H) controls, and the record shows high number of failures and malfunctions involving hydraulic components (e.g. leakages). Failures of BOP systems have made significant contributions to non-productive time of drilling rigs. This paper introduces a new concept of electro-mechanically operated BOP, which seems to be a candidate to improve reliability and availability of the BOP. The main interest of this paper is to shed light on the new features of the electrical BOP system versus current art qualitatively. In addition, this contribution proposes a method for the BOP availability analysis which may be used in the decision-making about designing optimal BOP systems.

## 1 INTRODUCTION

The petroleum industry has expanded into new areas for oil and gas production. Exploration activities in the North Sea, for example, have gradually moved to the northernmost regions and to ultra-deep waters, typically in the Gulf of Mexico and Brazil to discover more hydrocarbon resources. Drilling activities involve the risk associated with uncontrolled release of well fluids (Corneliussen, 2006), namely kicks. Kicks, if not controlled by the safety barriers, can escalate to a blowout event, where the fluids and gas flow to the surface or into lower pressured subsurface zones. The blowout accident in the Macondo well caused 11 fatalities, abandonment of the drilling rig, and the largest oil spill in the U.S. history. One of the accident causes was the failure of the Blowout Preventer (BOP) system in stopping the pressurized hydrocarbons escalating to the rig.

The subsea BOP system is a secondary well barrier that consists of several well barrier elements (NORSOK D-010, 2013). The BOP system can contain the well fluids and cut off the drill pipe when the containment by the primary well barriers has failed. The BOP is temporarily installed on the wellhead at the seabed. The BOP stack at the seabed is the assembly of preventers, and their auxiliary equipment, including control system equipment. The marine drilling riser is a pipe (typical 21-inch Outer Diameter), that extends from the drilling platform down to the Lower Marine Riser Package at the top of the BOP stack. The upper part of the BOP stack can be disconnected from the lower BOP stack as part of a controlled operation, or in case of emergency. Dangerous failures of BOP components may not be detected before the BOP is locked onto the well head. Failures may be revealed during the periodic testing, and an immediate pulling of the BOP for repair if the faulty components are considered critical (NORSOK D-010, 2013). This introduces non-productive time, while unscheduled pulling of BOPs may increase the well blowout risk (Strand & Lundteigen, 2015). To enhance safety during drilling, it has been suggested in the industry that decision-making related to reliability, availability, and maintenance of BOP systems should be made on credible information on the system performance. Furthermore, such information is expect to determine the optimal design of the BOP systems in long term (IADC, 2016).

The design principle of hydraulic actuation of BOPs has dominated the industry since the 1920`s. A common problem of Electro-Hydraulic (E/H) BOP system is the hydraulic leakages, which can be a single point of failure. Leakage of a valve or connection may eventually require pulling of the BOP to the surface. Deep water drilling has additional problems, such as hydraulic signal delay, pressure and stored energy loss, difficulties of condition monitoring, and heavy weight of subsea hydraulic fluid accumulators.

Acknowledging such aspects of the current BOP systems, the company Electrical Subsea & Drilling AS (ESD) and its R&D partner Kongsberg Maritime are developing a new design concept of electrically operated BOP system. The main idea is to replace all the hydraulic components with equivalent electrical components. Another concept is the technology for Electro-Mechanical (E/M) actuators that are operated without using hydraulic pressure.

The aim of this paper is first to highlight some of the reliability implications of introducing the electrically operated BOP system. The second aim is to suggest an advanced approach for quantitative analysis of the BOP availability. Petri nets are used to consider the effect of regular testing (including repair time), which is not explicitly captured in the previous studies. The case study in section 4 gives a representative example on how to apply this approach in the availability analysis of the current E/H BOP system. The case study is not intended for the electrical BOP, as the currently available reliability data is considered to be insufficient to support the anlysis. Once the data is available, however, the approach can be easily applied for the new design BOP system.

## 2 BOP SYSTEM DESCRIPTION

### 2.1 *BOP well barrier elements*

GL 070 (2004) defines the safety functions of a drilling BOP system; 1) Seal around pipe 2) Seal an open bore 3) Shear drill pipe and seal well off. These functions are achieved by different types of BOP well barrier elements and the items that are necessary to activate (open or close) the preventers (API RP53, 2012). Two types of preventers are used in a BOP system: the ram-type preventer and the annular type preventer. A ram preventer uses a pair of rams that linearly move for sealing the wellbore, or shearing of a drill pipe. The types are: the pipe rams, the Blind Shear Rams (BSR) and the casing shear ram. The BSR is the only type of well barrier element that can shear the pipe and in turn seal the wellbore with rubber packers, such that no fluid can pass through the pipe and the annulus around the pipe. Pipe rams can seal around the drill string of a particular diameter, while the variable bore rams are able to seal the tubulars with different diameters. Pipe rams may also be used to hold the tubular in position during shearing of the pipe. The annular preventer is a flexible rubber sealing element, a so-called 'doughnut' sealing element, as it can embrace and seal any object inside the annular space of the wellbore. It has lower working pressure than the ram type BOPs and is positioned in the LMRP. Typical pressure rating of the annular preventer is 10-ksi in a 15-ksi rated BOP stack.

### 2.2 *Electro-Hydraulic (E/H) control systems*

The BOP control system today is based on E/H control systems, where Programmable Logic Controllers (PLCs) converts operators' command on the panel into electronic signals. The schematic of E/H control is shown in Figure 1. Solenoid valves then convert the electric signal to pilot hydraulic signals. The hydraulic signals are used to direct pressurized hydraulic fluid from the power supply on the topside and the subsea BOP mounted accumulators to operate the preventers. Numerous valves, manifolds, and regulators are used to translate the input from the surface to subsea BOP stacks. For the power supply to operate the preventers and connectors, hydraulic pressure supply is provide by a surface mounted Hydraulic Power Unit (HPU), hydraulic distribution (hoses and hard piping) and subsea hydraulic accumulators.

### 2.3 *Reliability implication of electrical control system*

The new concept of electrically operated BOP includes the use of electrical power supply with batteries to replace hydraulic pressure energy, Electro-Mechanical (E/M) actuators, and the control system consisted of only electrical components. The two types of actuators are being prototyped by the company ESD: 1) ram-type actuator which can be used for pipe rams and BSR 2) ring piston actuator for annular preventers and connectors.

Ring motors are used to power both the ram actuators and the ring piston devices. The output torque from the motor is transferred to the actuation segment through transmission elements based on planetary gears and roller screw technology. The rotary motion of the electric motor is transferred to linear motion of the actuating element. An efficient power transmission is a key to produce sufficient force. Figure 2 is a simple presentation of the ring piston actuator used for annular preventer and connector.

The main focus with respect to ESD's E/M actuator development has been on the blind shear ram application, because that application requires very high force in comparison to other ram functions. Shear rams must generate forces necessary for cutting or sealing tubulars in the wellbore. Normal ram-type BOPs, for example, withstand 15-ksi working pressure, and shear rams are required to have cutting capacity of 900 Metric tons. The possible achievements of electrical BOP systems are: 1) Avoidance of common scenarios involving hydraulic leakages and no discharge of hydraulic fluid to

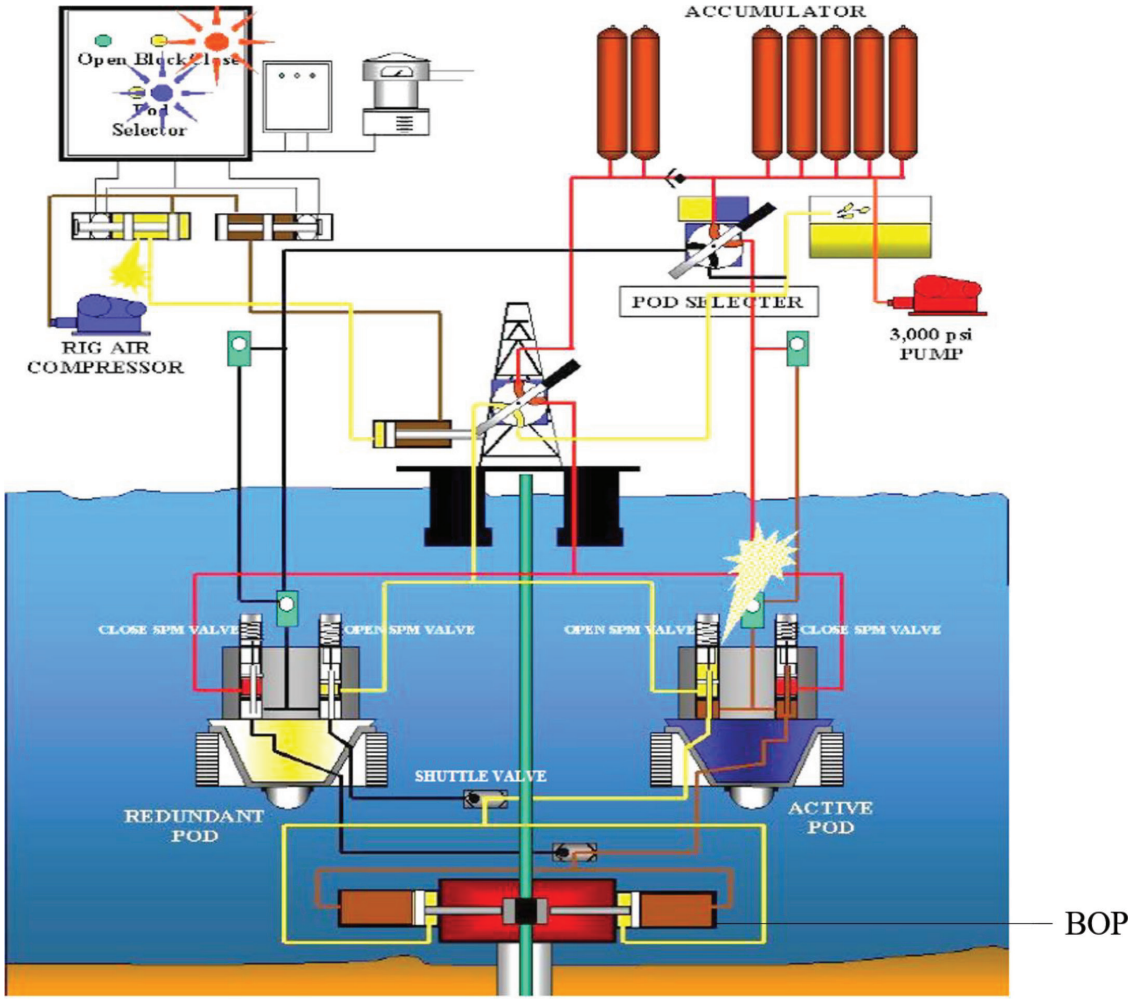



Figure 1. Schematic of electro-hydraulic control and power supply used in the contemporary BOP control systems. Hydraulics fluids are transmitted to the BOPs for activation. Borrowed from Mærsk drilling center (2009).


Figure 2. Electro-mechanical ring piston concept by ESD. The rotary motion of the electric motor is transmitted to the linear motion of the activation segment. Hydraulic modules can be removed with this design concept (Dale, 2013).

the environment 2) no power loss due to increased ambient pressure at deep water, reduced weight and space, increased redundancy 3) Improvement in condition monitoring, instrumentation system: electronic and electro-mechanical components are inherently easier to accurately monitor than the hydraulic components.

E/M actuators are claimed to provide high force with dual redundant rotating motors, fast cutting, precise control and monitoring of stroke position/ applied force. An important, practical advantage of E/M operation is also that it is possible to have exact control over the applied force to provide the optimum operation during stripping operations through the annular preventer. The control system will automatically adjust the rubber element contraction and "back-off" during tool-joint passage. Applied force is measured and regulated with control of electrical motor power and direction.

## 3 SAFETY ANALYSIS OF BOP

A BOP, whether it is electrically or hydraulically operated, has some generic design and operational characteristics that must be addressed in a reliability

analysis. Some examples of such characteristic are what are the safety-critical functions, what performance measures are relevant for safety, how to account for different types of regular testing (including repair time), and the efficiency of these tests. The mentioned topics are elaborated more in the following.

### 3.1 *BOP safety functions*

The BOP system may perform safety functions upon kick detection. The functions can be carried out either by manual or automatic activation of BOPs, depending on the operational conditions. In the normal operational mode, the operators activates one pod to control the hydraulic power supply. The pod is comprised of Subsea Electronic Modules (SEM) with PLCs and the hydraulic unit. The pod also sends information such as electronic riser angle indicator, BOP stack temperature, BOP stack pressure and accumulator pressure readback (Holand & Awan, 2012).

The BOP system can be considered to perform Safety Instrumented Functions (SIF) despite operational modes with the manual activation by operators. The BOP is operated in low demand mode, and the average Probability of a dangerous Failure on Demand ($PFD_{avg}$) is used to determine the Safety Integrity Level (SIL) (IEC 61508, 2010). $PFD_{avg}$ can be understood as the mean proportion of downtime in an interval, and it is interpreted as the probability of an item not being able to function upon demand (Rausand & Høyland, 2004). Minimum SIL 2 of the critical BOP SIFs is required by GL-070 (2004).

### 3.2 *BOP testing*

Testing is performed to confirm correct response to failures, and retain correct performance of a SIS (Rausand, 2014). Current BOP systems requires two types of regular tests: Function Test (FT) and the Pressure Test (PT) (NORSOK D-010, 2013; API RP 53, 2012). A function test is carried out to verify BOP operability. Dangerous failure modes involving closing and opening of BOPs and the pump capability for hydraulic supply are tested. A pressure test is to verify the pressure containment capability by applying pressure to BOPs. FT is required to be carried out every 7 days. PT is required to be performed every 14 days by BSEE regulation (2014), while API RP 53 (2012) requires the interval of 21 days. NORSOK D-010 has revised the requirements from the interval of 14 to 21 days, on the ground that running of tools and pressure testing can be a high risk activity before the bore is cased off. It should be noted that rated pressure is applied for the PT and it cannot be considered as proof testing of cutting ability of ram preventers.

### 3.3 *Possible improvement for the safety functions*

Electronic and electro-mechanical components are inherently easier to accurately monitor than the hydraulic counterparts. The improved BOP instrumentation features is expected to enhance real time safety and management during the operation of the BOP system, and drastically reduce the time consumed for in-between well maintenance through the Condition monitoring functionality:

1. All CPUs, communication lines and electrical wiring will be continuously controlled by a health monitoring system. The fault of electrical equipment shall be monitored, data to be stored locally and sent to the vessel's Control System & Information Management System. For example, an accelerometer shall be mounted in the electrical motor compartment to measure the vibration
2. System performance, such as stroke, speed and torque of all actuators and motors shall be controlled, monitored and logged.
3. Sensors for wellhead fatigue measurement can be implemented in the BOP wellhead connector and be interfaced with a riser monitoring system. Addressing wellhead fatigue issues and proving sufficient margin for drilling operations has been a growing challenge for the oil and gas industry over the last decade. The subsea control system hardware shall be fitted in cylindrical canisters that can be separately pulled and replaced during operation.
4. For redundancy, back-up Hydro-acoustic controls to be interfaced with the new solution All retrievable devices shall be connected with ROV operated connectors. All retrievable devices shall be connected with ROV operated connectors

## 4 QUANTITATIVE ANALYSIS

### 4.1 *Reliability Block Diagram (RBD) driven Petri Nets*

A Reliability Block Diagram (RBD) can be used to illustrate a system safety function that are broken down to component functions. A RBD gives the logical relationship between component functions by structuring each block (rectangle or square) that represents binary states (functioning/failed) (Rausand, 2014). It is possible to combine Petri Net analysis (which allows modeling of multiple states of components) with RBDs (that maintain a structure which is easier read), which is referred to

as RBD driven Petri nets. In a Petri net transitions between different states can be either stochastic or deterministic, and the stochastic transitions allow different types of distributions. RBD driven Petri nets can add dynamic features by taking into account effects of tests and repair, operational strategies in the presence of component failures, and component reliability.

### 4.2 *Case study*

A component or a module of the RBDs can be replaced with Petri nets. An example of a RBD for each BOP system with different operating principles is shown in the Figure 3. Petri Nets model is carried out to represent the states of components in the RBD. The traditional (electro-hydraulic operated) BOP system has chosen to be the subject of this analysis due to the availability of reliability data repair in Holand (2009), Holand & Awan, (2012) and Hauge et al. (2012). The input data such as failure rates and time consumed for testing is shown in Table 2.

The focus of this case study is to estimate the unavailability of the function of a BSR that are under the effect of two types of regular testing and repairs. GRIF workshop demonstration version (GRIF, 2016) is used for the configuration of Petri Net and the simulation for obtaining the average Probability of Failure on Demand ($PFD_{avg}$). Figure 4 illustrates the Petri net model built to treat Function Testing (FT) and Pressure Testing (PT) of a ram-type preventer. It is assumed that FT can reveal the failures of preventer and the associated

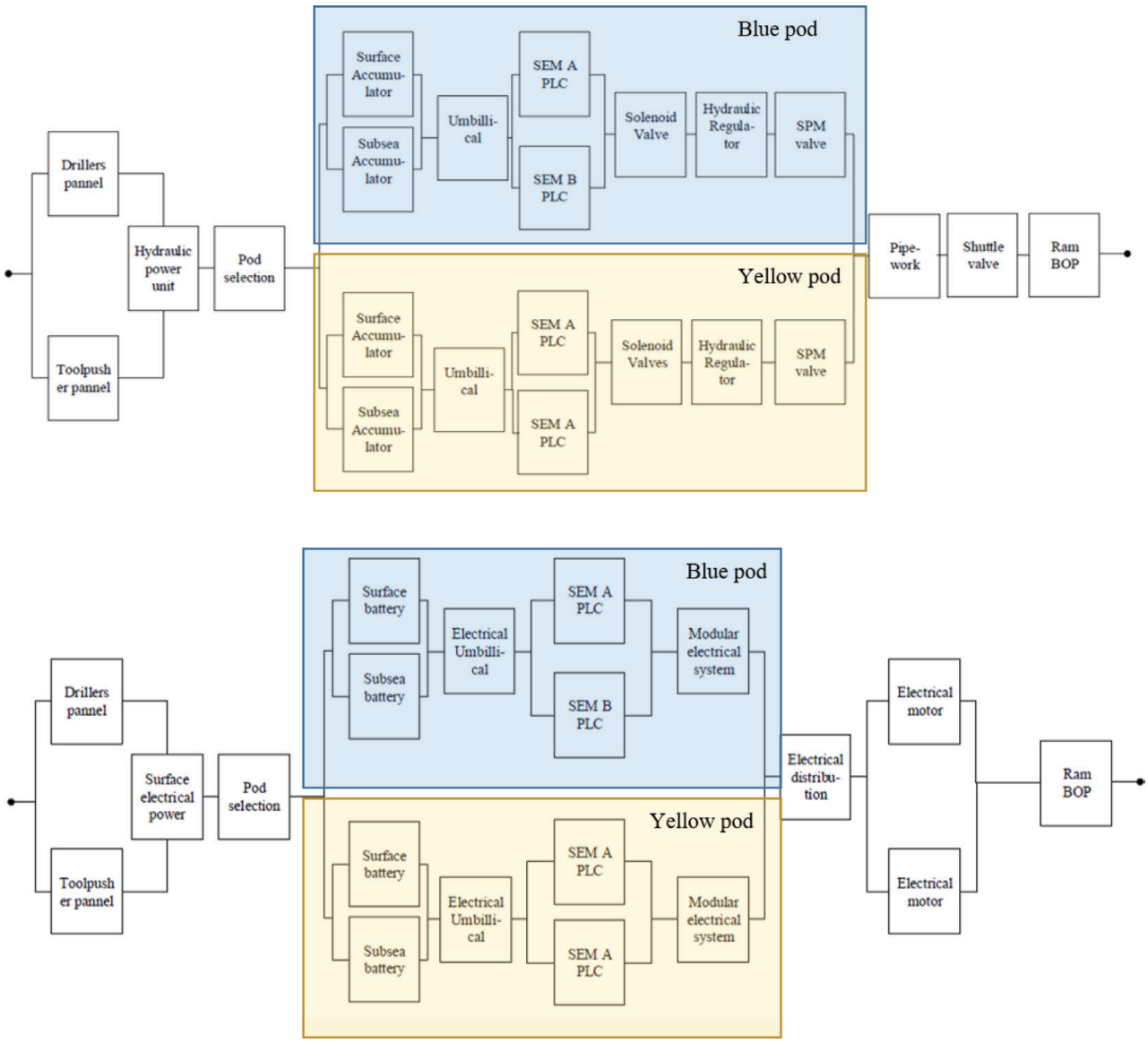



Figure 3. Simplified RBDs for a E/H BOP control system (above) and an electrical BOP system (below).

Table 1. Places and transitions in the Petri nets.

| Element | State (with a place holding a token) /Event |
|---|---|
| Place: Working_FT_A | State: no fault that can be revealed by FT |
| Transition: Fail_FT_A | Event: occurrence of a failure that can be revealed by FT |
| Place: Working_PT_A | State: no fault that is only revealed by PT |
| Transition: Fail_PT_A | Event: occurrence of a failure that can be revealed by PT |
| Transition: Repair_FT | Event: fix of the fault revealed by FT |
| Transition: Repair_PT | Event: fix of the fault revealed by PT |
| Transition: FT | Event: Function test |
| Transition: PT | Event: Pressure test |

Table 2. Input data.

| Parameter | Value |
|---|---|
| Function testing interval | 168 hours (7 days) |
| Pressure testing interval (1) | 336 hours (14 days) |
| Pressure testing interval (2) | 504 hours (21 days) |
| Average time consumed for pressure testing | 14.33 (hours) |
| Average time consumed for function testing | 0.71 (hours) |
| Failure rate $\lambda$ | 4.3·10–5 (Per hour) |
| Failure rate $\lambda$PT (detected by PT) | 2.8·10–5 (Per hour) |
| Failure rate $\lambda$FT (detected by FT) | 1.5·10–5 (Per hour) |
| Average time consumed for Repair | 6.1 (hours) |

control devices involving opening and closing of BOP. The ability of preventer to withhold the well pressure is tested in FT. The FT in this Petri nets does not cover the cutting ability of BSR.

Two type of variables, predicates and assertions are used. Predicate represent the pre-condition of transition, while assertion denotes the result of transition. For instance, '? pfail == 0' and ! pfail = pfail+1' imply that the working component A can move to the failed state (pfail = 1) as a result of the stochastic transition. And Table 1 describes the Petri net model.

Jin and Rausand (2013) demonstrates the $PFD_{avg}$ of a *k*-out-of-*n* (*koon*) system that is subjected to both periodic PST and the Proof Test (PT). Formula (1) is $PFD_{avg}$ derived without considering Common Cause Failure (CCF).

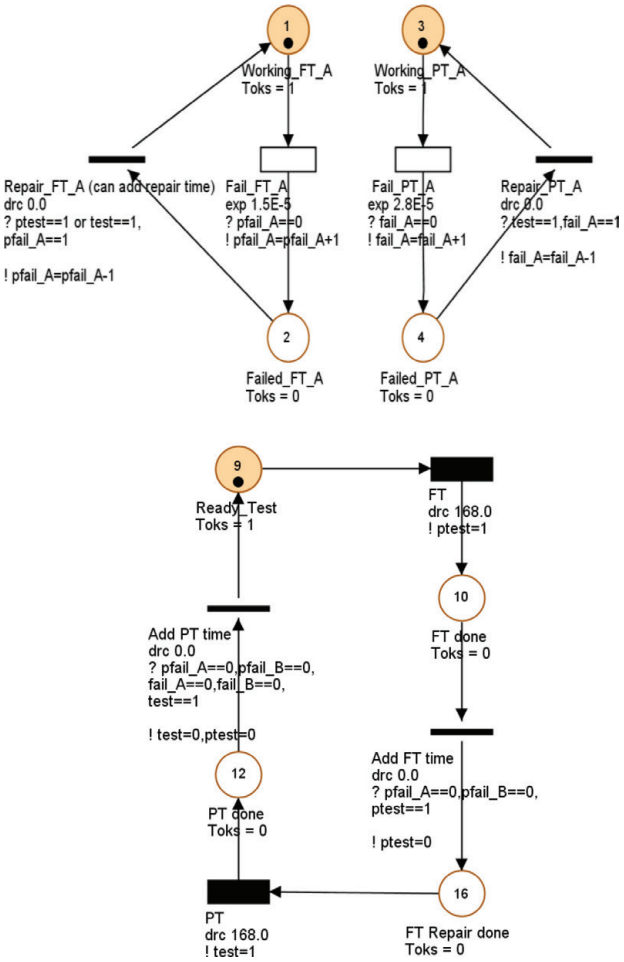



Figure 4. Example of a Petri nets for a ram-type preventer.

$$PFD_{avg} \approx \frac{1}{m}\left(\begin{array}{l}\sum_{i=1}^{m}\sum_{j=0}^{n-k}\binom{n}{j}\left((i-1)(i-\theta)\lambda\tilde{\tau}\right)^{j} \\ \quad\times\dfrac{(n-j)!(\lambda\tilde{\tau})^{n-j-k+1}}{(n-j-k+2)!(k-1)!} \\ \quad+\sum_{i=1}^{m}\sum_{j=n-k+1}^{n}\binom{n}{j}\left((i-1)(i-\theta)\lambda\tilde{\tau}\right)^{j}\end{array}\right) \quad (1)$$

where $\theta$ = PST coverage; $\tilde{\tau}$ = PST interval $\tau = m\tilde{\tau}$; and (m–1) = number of PSTs in each PT interval;

The main assumptions are:

1. The channels in *koon* system are identical with the constant DU failure rate.
2. All the tests are carried out simultaneously for n channels, and testing and repair
3. Repair time is negligible. Once a failure is revealed by PST, it is repaired immediately
4. The failure revealed by PT is not affected by PST

Table 3. Simulation result.

| | Formula (PT interval 14 days) | Simulation 1 (PT interval 14 days) | Simulation 2 (PT interval 21 days) |
|---|---|---|---|
| 1oo1 | 5,96E-03 | 5.923E-3 | 8.253E-3 |
| 1oo2 | 4,545E-05 | 4,437E-05 | 9.291E-5 |

Table 4. Simulation result with PT interval 14 days.

| | Simulation 1–1 (with repair time) | Simulation 1–2 (testing time) | Simulation 1–3 (both testing and repair time) |
|---|---|---|---|
| 1oo1 | 6.193E-3 | 6.192E-3 | 6.473–3 |
| 1oo2 | 4.842E-5 | 4.900E-5 | 5.127 E-5 |

Table 5. Simulation result with PT interval 21 days.

| | Simulation 2–1 (with repair time) | Simulation 2–2 (testing time) | Simulation 2–3 (both testing and repair time) |
|---|---|---|---|
| 1oo1 | 8,521E-3 | 8,521E-3 | 8.804E-3 |
| 1oo2 | 9.292E-5 | 9.400E-5 | 9.918E-5 |

### 4.3 *Result*

The estimated $PFD_{avg}$ of 1oo1 BSR and 1oo2 BSRs are attained from the Monte Carlo simulation in GRIF. The simulation duration is set to be 3 years, since the BOP overhaul interval is 3 to 5 years. Firstly, estimation of $PFD_{avg}$ without including of testing and repair times are shown in Table 3, which exhibits close values with the approximation formula (1). The extended PT test interval from 14 to 21 days gives the increase in $PFD_{avg}$, but without changing the exponents of the numbers. Table 4 and Table 5 show simulation results of three different cases with consideration of: 1) repair time 2) consumed time for testing 3) both repair time and consumed time for testing. It is shown that the repair and testing times result in small increment of the $PFD_{avg}$.

## 5 DISCUSSION

The case study is applied to a single device of E/H BOP system. The approach is the point of departure which can eventually extend to a system level model, where the whole the BOP system function from the initiation to closure of minimum number of BOP actuating devices, in light of the mode of operation. The result shows that the shorter test interval gives higher availability. However, risk introduced by performing test and cost of non-productive time are not analyzed. On the other hand, the company ESD addresses that electrical BOP should have different testing strategies. Preventive and corrective maintenance on the control system can be triggered based on condition monitoring mentioned in the section 3.3. According to the ESD's claim, electrical BOP can reduce the time consumed for testing and the preparations prior to operations by means of early detection of any degraded performance. It is expected that less failures are reported with electrical actuation, as all the hydraulic and electro/hydraulic valves are removed. Less unscheduled stops and lifting of BOP to the rig can be also assumed. This aspect therefore presents the need to investigate testing efficiency and repair and restoration times with new operational strategy of an electrical BOP. Besides, the new BOP system will have various sensors, which continuously provide feedback to the control system and the motor control that provide actuation data. Such new components will introduce new failure modes, and these must be carefully analyzed to calculate the associated reliability parameter.

## 6 SUMMARY AND CONCLUSION

This paper identifies key characteristics of electrical BOP system. This new design may improve safety availability of BOP systems and contribute to the risk reduction during drilling. The case study demonstrates Petri net modelling for availability analysis for an E/H BOP to consider two types of regular testing with different intervals. To apply the method for an electrical BOP, it is necessary to make reasonable estimates for failure rates based on qualification testing, since no operational experience has not yet been obtained for such systems. Despite the uncertainty, it is important to develop and carry out quantitative analyses that can support decision-making for optimizing the design and operation of the BOP systems.

## ACKNOWLEDGMENT

The authors are grateful for the valuable comments from G.-O. Strand.

## REFERENCES

API 53 (2012). API Standard 53 Blowout Prevention Equipment Systems for Drilling Wells. American Petroleum Institute (API), API Publishing services, Washington, DC.

BSEE, *Code of Federal Regulations*. 2014, Bureau of Safety and Environmental Enforcement: http://www.bsee.gov/.

Corneliussen, K. (2006). Well safety; Risk control in the operational phase of offshore wells. PhD thesis. Norwegian University of Science and Technology (NTNU). Trondheim, Norway.

Dale. J (2013). BOP control features "All electric controls". [Powerpoint slide].

Hauge S., Håbrekke S., Kråkenes T., Lundteigen, M.A. & Merz M. (2012). Barriers to prevent and limit acute releases to sea — Environmental barrier indicators, SINTEF Rapport A22763. SINTEF, Trondheim, Norway.

Holand, P. & Awan, H. (2012) Reliability of Deepwater Subsea BOP Systems and Well Kicks. Exprosoft.

Holand, P. (2009). Effektivisering av BOP testing. [PowerPoint slides]. Retrieved from esra.no/wp-content/uploads/2015/04/Kl-1110-Effektivisering-av-testing-av-subsea-BOP_Per-Holand_ExproSoft.pdf

GRIF, 2016. GRIF Workshop: http://grif-workshop.com/

NORSOK D-010 (2013). Well integrity in drilling and well operations, Norsok standard, Standard Norge, Oslo, Norway.

Norsk olje og gass. (2004). GL 070 — Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry.

Rausand, M. and Høyland, A. (2004). System Reliability Theory: Models, Statistical Methods, and Applications. Wiley, Hoboken, NJ, 2nd edition.

Rausand, M. (2014). Reliability of Safety-Critical Systems: Theory and Applications. Wiley, Hoboken, NJ.

Signoret, J.P., Dutuit, Y., Cacheux, P.J., Folleau, C., Collas, S., & Thomas, P. (2013). Make your petri nets understandable: Reliability block diagrams driven petri nets. Reliability Engineering & System Safety, 113, 61–75.

Strand, G.O. & Lundteigen, M.A. (2015). Risk control in the well drilling phase: BOP system reliability assessment. European Safety and Reliability Conference, 2015.