



**NTNU – Trondheim**  
Norwegian University of  
Science and Technology

# Modeling of Safety Functions in Quantitative Risk Analysis

**Thien Duy Nguyen**

Master of Science in Product Design and Manufacturing

Submission date: June 2012

Supervisor: Marvin Rausand, IPK

Co-supervisor: Tony Gjerde, Scandpower  
Anne Tomter, Scandpower

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



**MASTER THESIS 2012**  
**for**  
**stud. techn. Thien Duy Nguyen**

**MODELING OF SAFETY FUNCTIONS IN QUANTITATIVE RISK ANALYSIS**  
**(Modellering av sikkerhetsfunksjoner i kvantitative risikoanalyser)**

Safety functions are important issues in all quantitative risk analyses (QRAs). The effects of the safety functions are usually modeled by event trees, where the event tree is pivoting depending on whether the safety function is successful or not. The reliability of each safety function is often modeled by a fault tree, which is again included as part of the event tree. The quantitative analysis of an event tree is usually considered to be a straightforward task, but several challenges prevail. Among these are (i) the pivoting probabilities always dependent of the previous events in the event tree branch leading up to the relevant pivoting event, (ii) the activation sequence of safety functions may not always be obvious, (iii) the various safety functions may have internal dependencies, (iv) the output from a pivoting event may escalate in a way that is difficult to model, and so on.

The overall objective of this Master's thesis is to investigate the effects of the reliability of safety functions on the results from a QRA.

As part of this project thesis the candidate shall:

1. Carry out and document a literature survey on how reliability analyses and QRAs are performed for oil and gas installations on the Norwegian Continental Shelf. The survey should also cover how different disciplines are working together in a QRA, with a special focus on the reliability of safety-instrumented functions.
2. Based on a representative set of performed QRAs, investigate the following questions:
  - a. Are the reliabilities of safety functions significant for the results of the QRA?
  - b. Are the safety functions modeled appropriately, or should more advanced models have been used?
  - c. Which of the safety functions and which elements are most significant related to the QRA results?
  - d. Is the sequence of safety functions adequately modeled and what are the effects of alternative sequences?
  - e. Are dependencies between barrier elements and safety functions modeled adequately? If not, how should this be done?

3. Investigate whether vendor reliability data on safety-instrumented functions (e.g., ESD nodes, ESD valves) in general are too optimistic related to the field performance? If the conclusion is “yes”, what could the main reasons for this be?
4. Develop a best practice for modeling safety functions as part of event tree analysis in a QRA. Among the issues to be considered are:
  - a. How to include vulnerability of safety functions?
  - b. Human factors in case manual operation is needed in order to activate safety functions.
  - c. Dependencies between safety functions

The case QRA studies will be made available by Scandpower and the computer program RiskSpectrum PSA shall be used as basis. The case QRA studies are confidential, and will be presented in the master thesis in an anonymous way.

Following agreement with the supervisors, the various points may be given different weights.

Within three weeks after the date of the task handout, a pre-study report shall be prepared. The report shall cover the following:

- An analysis of the work task’s content with specific emphasis of the areas where new knowledge has to be gained.
- A description of the work packages that shall be performed. This description shall lead to a clear definition of the scope and extent of the total task to be performed.
- A time schedule for the project. The plan shall comprise a Gantt diagram with specification of the individual work packages, their scheduled start and end dates and a specification of project milestones.

The pre-study report is a part of the total task reporting. It shall be included in the final report. Progress reports made during the project period shall also be included in the final report.

The report should be edited as a research report with a summary, table of contents, conclusion, list of reference, list of literature etc. The text should be clear and concise, and include the necessary references to figures, tables, and diagrams. It is also important that exact references are given to any external source used in the text.

Equipment and software developed during the project is a part of the fulfillment of the task. Unless outside parties have exclusive property rights or the equipment is physically non-moveable, it should be handed in along with the final report. Suitable documentation for the correct use of such material is also required as part of the final report.

The student must cover travel expenses, telecommunication, and copying unless otherwise agreed.

If the candidate encounters unforeseen difficulties in the work, and if these difficulties warrant a reformation of the task, these problems should immediately be addressed to the Department.

**The assignment text shall be enclosed and be placed immediately after the title page.**

Deadline: June 11<sup>th</sup> 2012.

Two bound copies of the final report and one electronic (pdf-format) version are required.

Responsible supervisor at NTNU:

Marvin Rausand

Phone: 73 59 25 42

E-mail: [marvin.rausand@ntnu.no](mailto:marvin.rausand@ntnu.no)

Supervisors at Scandpower:

Anne Tomter

P.O.Box 3

Senior consultant

2027 Kjeller

Phone: 92 42 74 61

E-mail: [ato@scandpower.com](mailto:ato@scandpower.com)

Tony Gjerde

Senior consultant

Phone: 91 76 29 60

E-mail: [tgi@scandpower.com](mailto:tgi@scandpower.com)

**DEPARTMENT OF PRODUCTION  
AND QUALITY ENGINEERING**



Per Schjølberg

Associate Professor/Head of Department



Marvin Rausand

Responsible Supervisor



## Preface

The master's thesis is written at the Norwegian University of Science and Technology (NTNU), Department of Production and Quality Engineering, at the request of Scandpower. The thesis is the finalization of a 5-years master's degree, as part of the study program Product Design and Manufacturing, RAMS, spring 2012.

I am indebted to my supervisors. It has been a privilege to have Professor Marvin Rausand at NTNU as supervisor, a man with many years of knowledge about the field of risk assessment. He is also the author of one of the main literatures used. It has been an equally pleasure to have M.Sc. Tony Gjerde and M.Sc. Anne Tomter, senior consultants at Scandpower, as supervisors. They are two young and talented consultants, with knowledge about the industry far exceeding their age. To all three of my supervisors, I am really grateful for your time devoted, helping me carrying out this master's thesis. You have all been an excellent source of knowledge, and our meetings have been of great value. Thank you for the numerous drafts you have read, and for the feedback, which has improved both the technical and linguistic content extensively.

Gratitude is given to Scandpower, gladly putting their facilities, software, and consultants to my disposal. Several helpful conversations have found place within the walls of the company, especially through a workshop with a handful of the consultants.

Trondheim, 2012-06-11



Thien Duy Nguyen

# Summary

Quantitative risk analysis in the offshore industry is mandated by the Norwegian legislation. A literature survey is carried out, related to the current legislation from the Norwegian Petroleum Safety Authority (PSA) and supporting NORSOK standards. Process accidents on offshore installations, operating on the Norwegian continental shelf are emphasized. A risk picture is the synthesis of a risk assessment, describing the risk level. Requirements to the risk picture are discussed, and associated risk measures are presented. The risk measures represent the quantitative parts of a risk picture and the measures are evaluated against risk acceptance criteria. The evaluation can be performed with a mechanistic approach, or more flexibly by using the *as low as reasonably practicable* principle.

Uncertainty is an important aspect that many quantitative risk analyses treat too briefly. Assumptions are always made in risk analyses, and uncertainty therefore becomes an important issue. To put it on the agenda, an introduction to the topic is given.

The main purpose of a risk analysis is to support decision-making and the analysts should keep that in mind when performing the analysis. The field of quantitative risk analysis has received some criticisms, but some of it is unjust. To understand why, the scope of the quantitative risk analysis must be understood. Risk can be considered both from a strategic (long-term) and an operational (day-to-day) perspective. For quantitative risk analyses, a probabilistic view is used, dealing with probabilities and expected values. Strategic decision-making fits with this approach, but renders a day-to-day basis decision-making unsuitable. In addition, quantitative risk analysis copes with several types of hazards, with a long time span. The resources needed to handle all the hazards on an operational level of detail would be tremendous.

Several methods can be used when performing a quantitative risk analysis. The approach used by Scandpower is explored in detail. The main method currently used is event tree analysis. This method has some challenges. A problem addressed is the treatment of dependencies, both within and between event trees. The answer is related to how RiskSpectrum, a fault and event tree software, calculates the end event frequencies. A second problem is the treatment of human reliability, and how it can be implemented in the event tree analyses.

Large investments have been used on fire protection systems, to mitigate the consequences of process accidents. The thesis endeavors to study the importance of these safety systems. The emphasis is how the systems' reliability is modeled and treated in a quantitative risk analysis. To investigate the effects of the safety systems on the risk measures, three quantitative risk analyses are explored in detail. This was executed by using sensitivity analyses.



The sensitivity analyses are performed by altering the failure probabilities to the far ends. Astonishing results arisen. An attempt has been made to understand the mechanisms leading to the results. Possible explanations are discussed, and the three most important are outlined.

An input to the quantitative risk analyses is reliability data of the safety systems, but there can be nonconformity between the data. Vendor data seems to be too optimistic related to the field performance. Possible explanations are discussed in the thesis.

A best practice is presented, formed as an extended conclusion. Topics considered are:

- Challenges when modeling the event trees
- How to include vulnerability of the safety systems
- Uncertainties with the effect of deluge
- Human factors
- Dependencies

# Sammendrag

Kvantitativ risikoanalyse i offshoreindustrien er krevd av den norske lovgivningen. En litteraturstudie er utført, knyttet til det gjeldende regelverket fra det norske Petroleumstilsynet (Ptil) og NORSOK-standardene. Prosessulykker på offshoreinstallasjoner som opererer på norsk sokkel er vektlagt. Et risikobilde er en syntese av en risikovurdering, som beskriver risikonivået. Krav til risikobildet er diskutert, og tilhørende risikomål presentert. Risikomålene representerer den kvantitative delen av et risikobilde, der målene blir evaluert i forhold akseptkriterier for risiko. Evalueringen kan utføres med en mekanistisk tilnærming, eller mer fleksibelt ved å bruke et *så lavt som praktisk mulig* prinsipp.

Usikkerhet er et viktig aspekt som mange kvantitative risikoanalyser behandler for overfladisk. Antagelser er alltid gjort i risikoanalyser, og usikkerhet er dermed et viktig tema. En introduksjon til temaet er gitt for å sette teamet på dagsordenen.

Hovedformålet med en risikoanalyse er å støtte beslutninger, og analytikerne bør ha det i tankene når de utfører analysen. Kvantitativ risikoanalyse har fått noe kritikk, noe av det urettferdig. For å forstå hvorfor må omfanget av kvantitative risikoanalysen bli forstått. Risiko kan betraktes både fra en strategisk (langsiktig) og et operativt (dag-til-dag) perspektiv. En probabilistisk oppfatning er brukt for kvantitative risikoanalyser, for å håndtere sannsynligheter og forventede verdier. Strategiske beslutninger passer med denne tilnærmingen, men gjør en dag-til-dag basis beslutningsprosesser uegnet. I tillegg håndterer kvantitativ risikoanalyse flere typer farer, med en lang tidsperiode. Ressursene som kreves for å håndtere alle disse farene på et operasjonelt detaljnivå vil være enorm.

Flere metoder kan brukes ved utførelse av en kvantitativ risikoanalyse. Tilnærmingen som brukes av Scandpower er utforsket i detalj. Hovedmetoden som brukes i dag er hendelsestreanalyse. Denne metoden har noen utfordringer. Et problem som omtales er behandling av avhengigheter, både innenfor og mellom hendelsestrærne. Svaret er knyttet til hvordan RiskSpectrum, et feil- og hendesetreprogram, beregner frekvensene av slutthendelsene. Et annet problem er behandling av menneskelig pålitelighet, og hvordan det kan bli implementert i hendelsestreanalysene.

Store investeringer har blitt brukt på brannbeskyttelsessystemer for å redusere konsekvensene av prosessulykker. Oppgaven streber etter å studere betydningen av disse sikkerhetssystemene. Fokuset er og utforske hvordan systemets pålitelighet er modellert og behandlet i en kvantitativ risikoanalyse. For å undersøke effekten av sikkerhetssystemene på risikomålene, er tre kvantitative risikoanalyser utforsket i detalj. Dette ble utført ved hjelp av sensitivitetsanalyser. Sensitivitetsanalysene var utført ved å endre på feilsannsynligheter til det

ytterste. Forbløffende resultater oppstod. Det har blitt gjort et forsøk på å forstå mekanismene som førte til resultatene. Mulige forklaringer er diskutert, og de tre viktigste er framhevet.

En inndata til de kvantitative risikoanalysene er pålitelighetsdata til sikkerhetssystemene, men det kan være avvik mellom dataene. Leverandørdata synes å være for optimistiske i forhold til felldata. Mulige forklaringer er omtalt i avhandlingen.

En beste praksis er presentert, utledet som en utvidet konklusjon. Emner vurdert er:

- Utfordringer ved modellering hendelsestrærne
- Hvordan inkludere sårbarheten til sikkerhetssystemene
- Usikkerhet med effekten av brannvann
- Menneskelige faktorer
- Avhengigheter

# Contents

Preface.....	I
Summary .....	II
Sammendrag.....	IV
<b>1 Introduction.....</b>	<b>1</b>
1.1 Background.....	1
1.2 Risk Assessment in Norwegian Regulation.....	3
1.3 Objectives.....	4
1.4 Limitations.....	6
1.5 Literature Survey.....	6
<b>2 Introduction to Quantitative Risk Analysis.....</b>	<b>9</b>
2.1 About Quantitative Risk Analysis.....	9
2.1.1 Quantitative Risk Analysis in a Wider Perspective.....	10
2.1.2 Objectives of a Quantitative Risk Analysis .....	12
2.1.3 A Substitute for Quantitative Risk Analysis?.....	13
2.1.4 Quantitative Risk Analysis, Something Subjective or Objective?.....	13
2.1.5 Strengths and Limitations of Quantitative Risk Analysis .....	15
2.2 Uncertainties in Quantitative Risk Analysis .....	16
2.2.1 Parameter Uncertainty .....	17
2.2.2 Model Uncertainty.....	17
2.2.3 Completeness Uncertainty.....	17
<b>3 The Risk Picture .....</b>	<b>19</b>
3.1 Elements Establishing the Risk Picture.....	19
3.1.1 Risk Categories in Quantitative Risk Analyses .....	19
3.1.2 Establishing the Risk Picture for Personnel Risk .....	20
3.1.3 Addressing Uncertainty when Establishing the Risk Picture .....	21
3.2 Acceptance Criteria.....	22
3.2.1 As Low As Reasonably Practicable .....	22
3.2.2 Cost-Benefit.....	25
3.2.3 Goal-Setting Regime.....	26
3.3 Fatality Risk Measures.....	26
3.3.1 Potential Loss of Life .....	27
3.3.2 Individual Risk Per Annum .....	28
3.3.3 Fatal Accident Rate.....	29
3.3.4 FN Curves .....	29
3.3.5 Typical Acceptance Criteria Used by Norwegian Operators.....	30

3.4	Main Safety Functions.....	31
3.5	Environmental Risk.....	32
3.6	Asset Risk.....	33
3.7	Multi-Discipline Engineering.....	34
<b>4</b>	<b>Quantifying the Risk Picture of Process Accidents.....</b>	<b>35</b>
4.1	Barriers Preventing and Mitigating Process Accidents.....	35
4.1.1	Detection System.....	36
4.1.2	ESD Isolation System.....	37
4.1.3	Blowdown System.....	37
4.1.4	Firewater System.....	38
4.1.5	Activation Sequence of the Safety Systems.....	39
4.2	Event Tree Analysis in Quantitative Risk Analysis.....	40
4.2.1	Modeling Accident Scenarios.....	40
4.2.2	Event Tree Analysis and Supporting Tools.....	40
4.2.3	Sequence Modeling of the Safety Systems.....	41
4.2.4	Event Tree Analysis in Offshore Compared to Nuclear.....	42
4.3	Detailed Representation of a Process Accident.....	43
4.4	Reliability Analysis.....	44
4.5	Hardware Reliability.....	45
4.6	Human Reliability Analysis.....	47
4.7	Integrating Reliability Analysis with Event Tree Analysis.....	49
4.7.1	Integrating Fault Trees.....	49
4.7.2	Integrating Human Reliability Analysis.....	49
4.8	Vulnerability Analysis.....	50
4.8.1	ESD isolation.....	50
4.8.2	Blowdown.....	51
4.8.3	Firewater.....	51
4.8.4	Vulnerability Analysis in Event Trees.....	51
4.9	Dependencies in Event Trees.....	52
4.9.1	Sequence Fault Trees.....	53
4.9.2	Consequence Fault Tree.....	54
4.9.3	Master Fault Tree.....	55
4.9.4	The Ability to Handle Dependencies.....	55
<b>5</b>	<b>Case Study: Safety Functions and Event Tree Analysis – Process Accidents.....</b>	<b>57</b>
5.1	Case Study Presentation.....	57
5.2	The Approach of the Sensitivity Analyses.....	61
5.3	Results.....	62
5.3.1	Fatal Accident Rate.....	62
5.3.2	Main Safety Functions.....	63
5.3.3	Ignited Events.....	64
5.3.4	Importance of the Safety Systems.....	66
5.4	Discussion.....	66
5.4.1	Small Changes to the Fatal Accident Rate.....	66

5.4.2	Three Highlighted Reasons Regarding the Safety Systems .....	75
5.4.3	FAR Distribution – Immediate, Escape and Evacuation.....	75
5.4.4	Substantial Increases of Impairment Frequencies? .....	76
5.4.5	Distribution of Ignited Events .....	77
5.4.6	Contradictions in Safety Systems Importance .....	78
<b>6</b>	<b>Best Practice – Modeling Safety Systems in Event Trees .....</b>	<b>79</b>
6.1	Event Tree Modeling .....	79
6.1.1	Ideal Representation of an Event Tree.....	79
6.1.2	Realistic Event Tree Modeling.....	80
6.1.3	Effect of Deluge .....	82
6.2	Fault Tree Modeling.....	83
6.2.1	Vulnerability of Safety Systems.....	83
6.2.2	Human Errors.....	83
6.2.3	Dependencies between Safety Systems.....	85
6.3	Importance of Event Tree Modeling VS Fault Tree.....	85
<b>7</b>	<b>Conclusions and Recommendations for Further Work.....</b>	<b>87</b>
7.1	Conclusions .....	87
7.2	Discussion.....	89
7.3	Recommendations for Further Work.....	90
<b>A</b>	<b>Abbreviations and Acronyms.....</b>	<b>91</b>
<b>B</b>	<b>Detailed Tables for the Case Study .....</b>	<b>93</b>
B.1	FAR, Impairment of MSF Frequency, and Ignited Events.....	93
B.1.1	Installation A.....	94
B.1.2	Installation B.....	97
B.1.3	Installation B, Escalation Probabilities Set to 0.....	100
B.1.4	Installation C.....	102
B.2	Ignition and Explosion Probabilities – Installation A.....	105
B.2.1	Ignition Probabilities – ESD Isolation.....	105
B.2.2	Explosion Probabilities – ESD Isolation.....	105
B.2.3	Explosion Probabilities – Firewater.....	106
<b>C</b>	<b>Supplementing Figures.....</b>	<b>107</b>
C.1	Fault Tree Symbol Descriptions.....	107
C.2	Example of Master Fault Tree .....	108
C.3	Detailed Event Tree .....	109
	<b>Bibliography .....</b>	<b>110</b>

# Chapter 1

## Introduction

### 1.1 Background

Risk is a colloquially used term; even so, there is no agreed definition of risk. Inconsistency prevails in newspapers and other media. The scientific community is not an exception, and the interpretation is almost as varying as among the general public (Rausand, 2011).

There must a purpose to a risk analysis, which is performed directed against a target group (client). Risk analyses can be used to get a better understanding of risk, where the purpose is to inform. One of the most important target groups is the decision-makers, often the operator of the installation. Other stakeholders can influence the decision process, which the analyst team might have to consider. A suitable definition of risk analysis is provided by Kaplan and Garrik (1981). They express a risk analysis as the process of providing answers to the following three main questions:

1. What can go wrong?
2. What is the likelihood of that happening?
3. What are the consequences?

The risk  $R$  to a system, and the three questions can be deduced to an equation, expressed as a set of triplets (Kaplan & Garrik, 1981):

$$R = \{(s_i, f_i, C_i)\}_{i=1}^n \tag{1.1}$$

The various hazardous events is denoted  $s_1, s_2, \dots, s_n$ . The belonging frequency to the event  $i$  is denoted  $f_i$ , and the consequences  $C_i$ . The consequences are a multidimensional vector which might include damage to people, property, environment, and so on (Rausand, 2011). The frequency can also be replaced by the probability  $p_i$ .

Risk analysis can distinctively be categorized as either qualitative or quantitative. Probabilities and consequences are in qualitative analysis assessed qualitatively, whereas quantitative analysis provides numerical estimations for the probabilities and consequences (Rausand, 2011). As the expected consequence used in quantitative risk analyses (QRAs) is a statistical expression, an observed accident might never lead to the expected value (e.g. 3.4 fatalities is not possible) (Vinnem, 2007). The accident history of offshore activities has shown that the present risk analysis methods and tools are insufficient, major accidents still occur. A major accident is by NORSOK is defined as an

*Acute occurrence of an event such as a major emission, fire or explosion which immediately or delayed, leads to serious consequences to human health and/or fatalities and/or environmental damage and/or larger economic losses. (NORSOK Z-013, 2010, p. 12)*

The fatal accident of Deepwater Horizon (see National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011, for a detailed inquiry of the accident), accompanied by several other accidents<sup>1</sup> has called out for the need of good risk analyses. One of the large developments of QRA in Norway came with the new regulations issued by the Norwegian Petroleum Directorate, which required the performance of QRAs (Vinnem, 2007, cited in NPD, 1980). The importance of QRA as a tool to prevent such accidents was enhanced by Lord Cullen, after the public inquiry of the Piper Alpha accident. The inquiry recommended that QRAs should be introduced into the UK legislation, much in the same way as in Norway (Lord Cullen, 1990).

QRA is still in the process of development, and is far from fully developed. Some have questioned the method and prompted the need of newer methods. Note that no major accidents, related to offshore production installations, have occurred on the Norwegian continental shelf after the capsizing of the Alexander L. Kielland flotel in 1980. Still, several near accidents have occurred.

A problem to address is how the effects of safety systems are reflected in the QRA models. Large investments have been spent on fire protection to mitigate the consequences of

---

<sup>1</sup> E.g. Piper Alpha, Alexander L. Kielland, and Ekofisk B. Refer Vinnem, 2007, Chapter 4, for an introduction to a collection of offshore accidents



process accidents. Emergency shutdown (ESD) isolation systems are implemented to close the feed of hydrocarbons during a leakage/fire scenario, isolating the segments; blowdown to discard the hydrocarbon already in the segment; and firewater systems to extinguish or mitigate the spreading possibility. These safety systems take on the role of risk-reducing measures, but the degree of effects is somewhat uncertain.

## 1.2 Risk Assessment in Norwegian Regulation

The Petroleum Safety Authority Norway (PSA) is the regulatory authority for technical and operational safety, enforcing regulations to control the safety of design and operation of offshore installations. Five of the most central regulations, entered into force January 2011, are:

- *The facilities regulations:* Regulations relating to health, safety and the environment in the petroleum activities and at certain onshore facilities (PSA, 2011c).
- *The management regulations:* Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities (PSA, 2011d).
- *The facilities regulations:* Regulations relating to design and outfitting of facilities, etc. In the petroleum activities (PSA, 2011b).
- *The activities regulations:* Regulations relating to conducting petroleum activities (PSA, 2011a).
- *The technical and operational regulations:* Regulations relating to technical and operational matters at onshore facilities in the petroleum activities, etc. (PSA, 2011e).

Risk analysis is mandated by the management regulations (PSA, 2011d). Note that there have been some formulation changes after the version from 2002. A QRA is no longer explicitly required, but the content from Section 17 (PSA, 2011d) can be interpreted as partly fulfilled by performing a QRA. The risk analyses required are related to major accidents, which are low probability incidents with potential of severe consequences. Major accidents are infrequent and difficult to analyze, but must not be taken easy upon due to the severity. The NORSOK Z-013 (2010) standard is developed as a guideline to comply with the PSA's requirements of risk assessments (see Figure 2.1 regarding differences between risk analysis and assessment). The risk assessment process shall always (NORSOK Z-013, 2010, p. 18):

1. Identify hazardous situations and potential accidental events

2. Identify initiating events and describe their potential causes
3. Analyze accidental sequences and their possible consequences
4. Identify and assess risk-reducing measures
5. Provide a nuanced and overall picture of the risk, presented in a way suitable for the various target groups/users and their specific needs and use

QRA is suggested as a tool to establish the risk picture (risk picture is defined in Section 3.1), but all five presented steps are subsequently based on each other. They can thus sometimes be found together in a QRA report, even though some of the steps are qualitative.

### Section 17

#### Risk analyses and emergency preparedness assessments

The responsible party shall carry out risk analyses that provide a balanced and most comprehensive possible picture of the risk associated with the activities. The analyses shall be appropriate as regards providing support for decisions related to the upcoming operation or phase. Risk analyses shall be carried out to identify and assess contributions to major accident and environmental risk, as well as ascertain the effects various operations and modifications will have on major accident and environmental risk.

Necessary assessments shall be carried out of sensitivity and uncertainty.

The risk analyses shall

- a) identify hazard and accident situations,
- b) identify initiating incidents and ascertain the causes of such incidents,
- c) analyse accident sequences and potential consequences, and
- d) identify and analyse risk-reducing measures.

Risk analyses shall be carried out and form part of the basis for making decisions when e.g.:

- a) classifying areas, systems and equipment,
- b) demonstrating that the main safety functions are safeguarded,
- c) identifying and stipulating design accidental loads,
- d) establishing requirements for barriers,
- e) stipulating operational conditions and restrictions,
- f) selecting defined hazard and accident situations.

Emergency preparedness analyses shall be carried out and be part of the basis for making decisions when e.g.

- a) defining hazard and accident situations,
- b) stipulating performance requirements for the emergency preparedness,
- c) selecting and dimensioning emergency preparedness measures.

(PSA, 2011d)

## 1.3 Objectives

QRA is highly developed in the area of hydrocarbon releases (Spouge, 1999), but the knowledge about the method is far from complete. To gain a better understanding of the method, related to the specific approach used by Scandpower, the deduced objectives of this thesis are:

1. Carry out and document a literature survey on how reliability analyses and QRAs are performed for oil and gas installations on the Norwegian Continental Shelf. The survey should cover how different disciplines work together in a QRA, with a special focus on the reliability of safety-instrumented functions.
2. Based on a representative set of performed QRAs, investigate the following questions:
  - a. Are the reliabilities of safety functions significant for the results of the QRA?
  - b. Are the safety functions modeled appropriately, or should more advanced models have been used?
  - c. Which of the safety functions and which elements are most significant related to the QRA results?
  - d. Is the sequence of safety functions adequately modeled and what are the effects of alternative sequences?
  - e. Are dependencies between barrier elements and safety functions modeled adequately? If not, how should this be done?
3. Investigate whether vendor reliability data on safety-instrumented functions (e.g., ESD nodes, ESD valves) in general are too optimistic related to the field performance? If the conclusion is “yes”, what could the main reasons for this be?
4. Develop a best practice for modeling safety functions as part of event tree analysis in a QRA. Among the issues to be considered are:
  - a. How to include vulnerability of safety functions?
  - b. Human factors in case manual operation is needed in order to activate safety functions
  - c. Dependencies between safety functions

In agreement with the main supervisor, it was decided to reduce the focus on task 3. A comprehensive approach could be to compare historical data with generic vendor data<sup>2</sup>. Instead, a brief presentation of earlier findings and discussions are given.

It was decided to have a larger focus on the event tree modeling in the best practice. This was in agreement with Scandpower, due to the results which prevailed during the case studies.

---

<sup>2</sup> For example, by comparing reliability data from EXIDA [www.exida.com] with the PDS data handbook [www.sintef.no/pds]

## 1.4 Limitations

The scope of a QRA which deals with an offshore installation can be extensive, and cover many possible hazard types. The thesis is mainly concerned with process accidents, defined here as ignited hydrocarbon leaks from process equipment (including pipelines). Locations upstream of the well chokes and outboard of the riser ESD valves are excluded, including other types of hazards. Note that NORSOK Z-013 (2010, Section 5.4.3) has a list of required hazards to be assessed for a QRA. There are requirements related to the various phases, from the concept selection phase to the operational phase. In this context, the operational phase concerned with the reliability of the safety systems, is considered as the most relevant. There are several types of risk measures and calculation approaches, where the approach of Scandpower is emphasized.

The requirements comprised by a QRA changes, and new regulations and standards are presented occasionally. This thesis is limited to the Norwegian continental shelf, and the present Norwegian legislation.

The QRA methodology comprises of several approaches, where the event tree analysis is emphasized. RiskSpectrum<sup>3</sup> is a software program, used to handle the fault and event trees, including interactions with several other tools/software. A detailed presentation and discussion of these tools is considered to be outside the scope of this master's thesis. To have a good understanding of the tools (and process accidents), great knowledge about computational fluid dynamics (CFD) is beneficial (CFD software can be used to simulate fire and explosions). Unfortunately, the author does not possess this knowledge. The number of possible scenarios is unlimited when process accidents are considered; the number of leaks, leak sizes, personnel present and so on. In order to have a comprehensible amount of data, a selection of approximately 1 000 to 10 000 relevant scenarios is often chosen.

The probability assessments of escalation scenarios is influenced by high uncertainties, for example related to the fire integrity of process equipment. The uncertainties and approach when determining the probabilities are too comprehensive to be covered adequately.

## 1.5 Literature Survey

The main literature related to QRA are from NORSOK Z-013 (2010), Vinnem (2007), and Spouge (1999). The literature gives a rather comprehensive presentation of QRA for the Norwegian and British continental shelf. These references are a few years old, such that some of the information is no longer valid. This is due to the extensive research on the topic and the changing legislation.

---

<sup>3</sup> For information about RiskSpectrum, refer:  
[http://www.riskspectrum.com/en/risk/Meny\\_2/RiskSpectrum\\_PSA/](http://www.riskspectrum.com/en/risk/Meny_2/RiskSpectrum_PSA/)

In Norway, the PSA enforces the regulations, with NORSOK Z-013 (2010) as guidance for compliance. NORSOK Z-013 is supplemented by additional standards, some of the most relevant are presented in Table 1.1 (NORSOK Z-013, 2010, p. 7).

Table 1.1: Standards supplementing NORSK Z-013

Standard	Description
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety related systems – Part 1-7
ISO 17776	Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment
ISO/IEC 31000	Risk management - Principles and guidelines
NORSOK S-001	Technical safety
OLF Guideline 070	Guidelines for the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian continental shelf

The reader should have some knowledge about risk assessment, and be familiar with “Risk Assessment: Theory, Methods, and Applications” (Rausand, 2011). Most of the terms and definitions are in compliance with this book, which also describes the theory about the models and methods used in QRA and risk measures.

Event tree analysis (ETA) is one of several approaches for quantification in QRA, and fault trees are often used for reliability analysis. Alternatives to fault trees are Bayesian network and Petri net, where a fault tree can be easily converted to the others (refer Rausand, 2011, for a brief introduction to the methods and conversion from fault tree). All three are graphical and mathematical tools for modeling discrete events systems. The two latter are considered as more comprehensive, and includes additional features, for example, when applied to systems that do not fall into simple failed or working states.

QRA has been criticized for limitations with the use of event chain models, being unable to capture the complexity of a system. Also for its inability to include human errors and organizational factors (Leveson, 2011). Competing analyses are systems-theoretic accident model and processes (STAMP, presented by Leveson, 2011) and barrier and operational risk analysis (BORA, presented by Sklet, 2006). None of these approaches are considered by the author to be replacements of QRA, but rather as supplements. The difference between QRA and BORA is discussed in Section 2.1.3.2. The scientific area of human and organizational factors is wide, and still not settled. Treating this problem in detail is beyond the scope of the thesis, and is a topic with many unresolved questions.



# Chapter 2

## Introduction to Quantitative Risk Analysis

### 2.1 About Quantitative Risk Analysis

The term quantitative risk analysis is not universally accepted, and several alternative terms are used (Vinnem, 2007):

- Quantified Risk Assessment (QRA)
- Probabilistic Risk Assessment (PRA)
- Probabilistic Safety Assessment (PSA)
- Concept Safety Evaluation (CSE)
- Total Risk Analysis (TRA)<sup>4</sup>

The contents are normally similar (the difference between analysis and assessment is illustrated in Figure 2.1), where QRA and TRA are often used in Norway. QRA is not a method restricted to the oil and gas industry, it is also used in the nuclear power plant industry (often called PRA in the nuclear industry). Dependent on the objective of the QRA, the analysis can range from a relatively simple to a very comprehensive study. A substantial amount of resources to perform the study might be required, and the suggested risk-reducing measures costly to implement.

---

<sup>4</sup> In Norwegian: Totalrisikoanalyse (often used by Statoil)

**2.1.1 Quantitative Risk Analysis in a Wider Perspective**

Figure 2.1 illustrates a possible diagram of a risk management process (one of several, without this presentation being necessarily better than others) flow, highly inspired by NORSOK Z-013 (2010, Figure 3) and Spouge (1999, Figure 2.1). A universally “perfect” flow diagram for a risk management process may not exist, where an adaption to the specific area of use is required. The goal is not to present the most ideal process description, but to highlight some important elements.

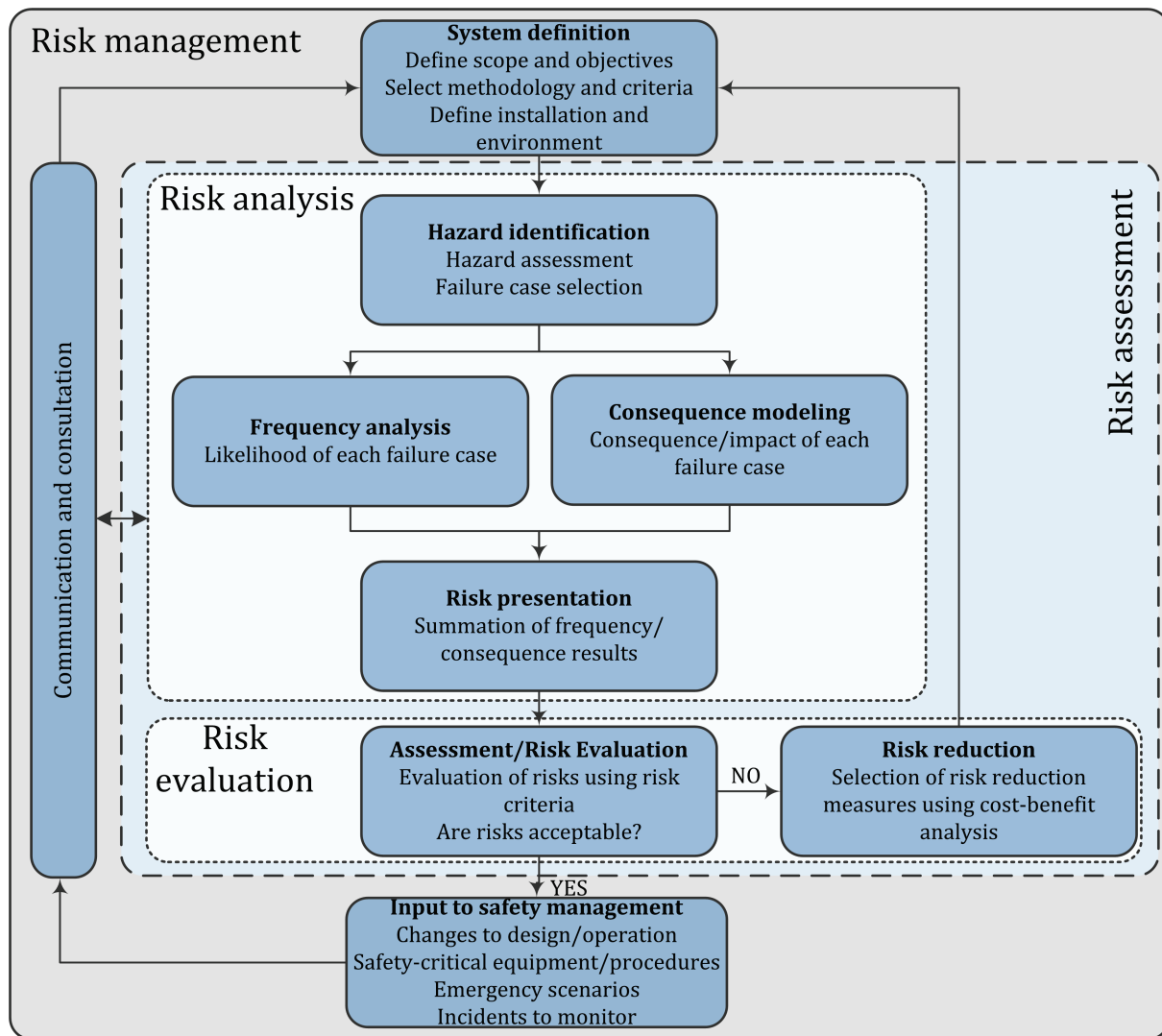


Figure 2.1: Flow diagram for a risk analysis, evaluation and management process

A QRA is mainly outlined within risk analysis, but should also be considered in relation to risk management. Risk analysis is an integrated part of risk management, and should be treated as such. One higher purpose of a risk analysis is to serve as information during decision-makings, which outlines the importance of the activity “input to safety management”. It can be



distinguished between risk-based decision-making (RDBM) and risk-informed decision-making (RIDM). The main difference is that RDBM is solely based on results from probabilistic risk assessment, whereas RIDM also involves deterministic analyses and technical considerations (Rausand, 2011). Figure 2.1 is only concerned with RDBM, but note that QRA can be used in both RDBMs and RIDMs.

A QRA can be comprehensive, thus the decision-maker can be tempted to only rely on the quantitative results, which is often easier to comprehend. Some important information can lie dormant behind the numbers. Communication and consultation is essential to ensure that the necessary information is at hand, when the important decisions take place. There should be a two way communication between the persons performing the QRA (consultants are often hired to perform the analysis, e.g. due to lack of resources, or the need of certain competence) and the decision-makers. Many assumptions are made throughout an analysis. To be able to make good decisions, the operator should be familiar with the assumptions, uncertainties, and important findings. A possible decision-making process is illustrated in Figure 2.2.

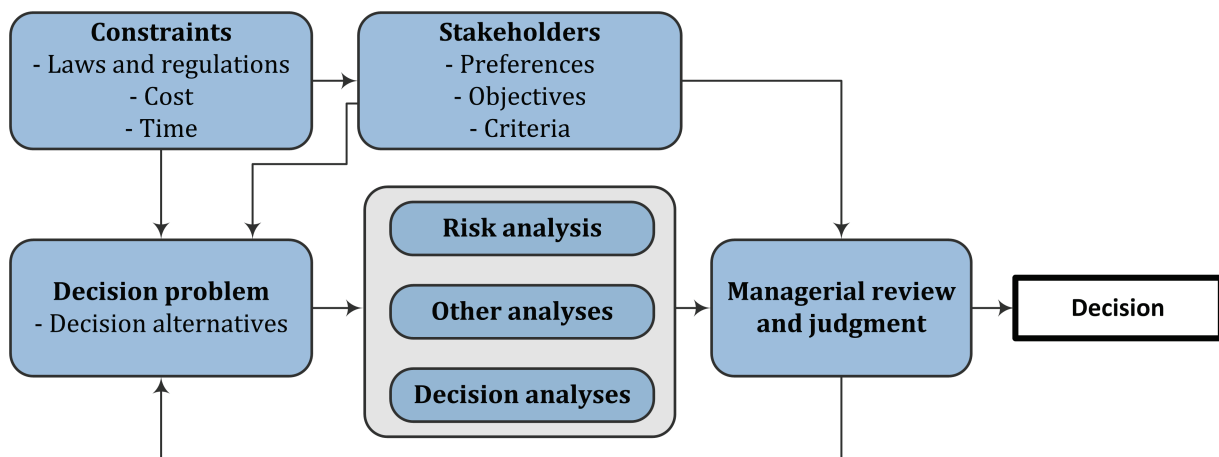


Figure 2.2: Decision-making process (Rausand, 2011)

Risk management should be done continuously, implying an iterative process, shown as a “closed loop” in Figure 2.1. Evaluating and classifying a risk as acceptable does not necessary set a finite end to the risk assessment process. A risk picture is not always static, and can change over time. What once thought to be under control might change, as for example a result of modification of the system, operating conditions, deterioration, and improvement of methods. These factors can contribute to limit the goodness of a QRA, and a new risk analysis becomes required. This outlines the uncertainties related to QRA, and importance of updating a QRA. Other limitations are due to the models and methods used, where a perfect method or model does not exist.

A QRA is not necessarily restricted to give a picture of the past, but can be used to influence the future. As outlined in the management regulations (PSA, 2011d, Section 17), the risk analyses should be used during decision-making related to upcoming operations and phases. New risk analyses should be prepared for each phase of an offshore installation, where NORSOK Z-013 (2010) states the requirements for risk analyses appurtenant to the various phases. The risk analyses belonging to a phase should not be considered isolated, where decisions regarding the next phase should be based on the previous.

### 2.1.2 Objectives of a Quantitative Risk Analysis

Four possible main objectives for an offshore installation QRA are (Vinnem, 1998, p. 40):

1. Estimation of risk in an absolute or relative sense, usually in relation to some kind of risk acceptance criteria
2. Determine design loads and conditions
3. Understanding of hazards causation and potential escalation pathways
4. Ranking of hazards according to risk potential

The listed objectives are only some of many possible objectives (see Spouge, 1999, page 8 for a list of additional possible objectives), and several benefits can be associated with the various objectives. By understanding the hazards causation and potential escalation pathways, risk-reducing measures can be implemented to mitigate the risk. To gain this understanding, identification of the safety-critical procedures and equipment might be needed. Note that all the objectives can be used during decision-makings, which goes beyond to consider if an installation is sufficiently safe or not. A QRA is not used to its fullest if the only purpose is to check certain risk measures against their acceptance criteria. There cannot be put enough emphasis on the benefits from the process of performing a risk assessment. This is why the communication and exchanging of experience and information is important (further discussed in Section 2.1.5.1).

Preventive measures when performing QRAs have surprisingly gained little attention, and the emphasis is often the mitigating measures. Consider the modeling of a process accident, using ETA to calculate the frequency of various consequences (ETA in QRA is discussed in Chapter 4). There is little attention on avoiding the initial events (when dealing with process accidents, the term hazardous event might be more correct) from occurring. The emphasis is on detecting, controlling, and mitigation the hazards. When looking at the hazardous event of hydrocarbon leak, suggestions to prevent the source of hazard, or reducing the frequency, are seldom observed in a QRA. The leak frequencies are often calculated without any means to

reduce the initial event of leakage. The suggested mitigating measures deal often only with the escalation of fire.

### **2.1.3 A Substitute for Quantitative Risk Analysis?**

#### **2.1.3.1 Operational Decisions - Barrier and Operational Risk Analysis**

The barrier and operational risk analysis (BORA) was initiated and developed in Norway from 2003 (Haugen, Seljelid, Sklet, Vinnem, & Aven, 2007). BORA can be used to analyze the causes of process leak, both qualitative and quantitative. The model is developed to consider physical and non-physical barriers, taking technical, human, and organizational causes of leak into consideration. The means of introducing a comprehensive modeling of human and organizational causes is to compensate for a traditionally weak area of QRA. The analysis is able to identify failures and failure combinations which entail risk. This in turn can be used to identify measures to control the risk, and changes to the barriers during special operational activities. An advantage of BORA is the larger focus on proactive risk-reduction.

Refer Rausand (2011) for a brief introduction to the method, or Vinnem, Haugen, Vollen, and Grefstad (2006) and Sklet (2006) for a more thorough presentation.

#### **2.1.3.2 Quantitative Risk Analysis in Relation to Barrier and Operational Risk Analysis**

QRA is usually focused on the event chain after the initial event, where BORA focuses on the prevention of the occurrence of the initial events. This can be explained by the nature of the two methods. QRA should be considered as a strategic tool, for long-term planning, whereas BORA is on the operational level, used for short-term planning. BORA can be used as a proactive method to reduce the leak frequencies, and QRA to predict the long-term risk level, and prevent hazards from escalating. Some of the criticisms of QRA are aimed towards the usability of QRA to consider operational risk. This can be misunderstood as one of the purposes of QRA. QRA is a strategic tool, using long-term risk measures and suggesting risk-reducing measures often not directly linked to the operational level. Regarding the insufficient areas of QRA, additional analyses methods might be needed to fill the gaps. QRA and BORA (or other methods) should supplement each other, rather than substitute.

#### **2.1.4 Quantitative Risk Analysis, Something Subjective or Objective?**

The interpretation of quantitative values emerging from a QRA is closely linked to what probability is regarded as. There are several probability philosophies, the three main approaches are the classical, the frequentist, and the Bayesian (refer Watson, 1994, or Rausand, 2011, for a more detailed discussion of the various probability theories). None of the mentioned

are found to fully comprehend a truly good explanation of the risk estimates from a QRA. The classical approach does hold the attribute of objectivism, but if the probabilities were truly objective, the results from different analytics should be identical. The results from a QRA would then be independent of the individual performing the analysis. A comparison of various teams using the same models concluded significant differences in the results (Rausand, 2011, cited in Linkov & Burmistrov, 2003). If actions are made upon the assumption of objectivity, the results might not be consistent with achieving the defined purposes (Schofield, 1998).

According to Kaplan and Garrik (1981), frequency refers to the outcome of an experiment, involving repeated trials. The approach of the frequentist is for major accidents impossible to satisfy; one cannot expose an offshore installation of hazards to calculate the frequency of the consequences unfolded.

A possibility is to apply the subjective theory of probability (Bayesian approach). The probabilities are then a subjective degree of belief about a system, based on the available information (Schofield, 1998). Using a subjective theory of probability is not necessary a remedy. Do not be deluded to believe that the objectivity wanted is still present, when a subjective approach is used (Watson, 1994). The benefit from a purely subjective analysis might be limited, where nothing can be validated or verified, since they are only personal opinions. From a management point of view, if an analysis is considered as no more than an individual's beliefs, decisions based on that analysis would then be difficult to defend.

The classical QRA relies at the present on a classical/relative frequency interpretation of probability. With this view, an insufficient investment on risk-reducing measures might occur, when handling low probability and high-consequence events (NS-EN ISO 17776, 2002). With a view of probability as objective, the statistical significance of risk results must be addressed (Schofield, 1998), which can be a challenge with limited data.

A suggestion is to construct the QRA as an argument, rather than an expression of truth (Watson, 1994). The degree of certainty would then depend on the analysts performing the analysis. This does not necessarily change the calculations presently used, but how they are presented and interpreted. With this approach, an additional focus on the competence of the analysts prevails. There is plausible evidence that within some fields, the practice at expressing uncertainties as probabilities leads to competence at the task (Murphy & Winkler, 1984). The knowledge and experience of the persons performing the QRA are factors influencing the outcome (completeness uncertainty), and also how certain the provided risk estimate is.

## **2.1.5 Strengths and Limitations of Quantitative Risk Analysis**

### **2.1.5.1 Strengths of QRA**

The most evident benefit from a QRA is the output in terms a risk picture (note that there are uncertainties regarding the establishing of the risk picture, see Section 2.2), expressing possible future damaging events in terms of probabilities. The less evident benefits from the process itself might be more important. QRA can be seen as a vehicle for structured arguments, which provides guidance to the designers and operators on how to reduce the risk (Spouge, 1999). The structured judgment is important to anticipate accidents before they occur (Spouge, 1999), and allocate and handle safety weaknesses by suggesting risk-reducing measures.

A QRA can be powerful as a vehicle to represent a very complex argument, based on a large quantity of data and judgments, providing a discipline for arguments. The risk measures can be useful when comparing the risk associated with different alternatives, thus using the indicators as relative values. There are many uncertainties related to the calculation, where the complexity is an important factor. Should QRA be rejected? Absolutely not, a QRA can contribute to a better understanding of the system object for analysis, with regard to risk and safety. The process of risk analysis gives a deeper understanding of the system at hand, and important inputs to decision-making and risk-reducing measures. Dangerous scenarios can be prevented, and knowledge of an accident gained in advance of its occurrence.

QRA is most fit for major accidents, with low probability and high consequences (Spouge, 1999). The consequences can be catastrophic, potentially involving massive loss of lives, damage to the environment, and financial losses leading to bankruptcy. Major accidents should not be taken easy upon, where QRA can be a tool to address this problem. An example is provided by QRAs in the Norwegian sector, explicitly identifying the risks of gas riser fires several years before the Piper Alpha accident (Pyman & Gjerstad, 1983).

### **2.1.5.2 Limitations of QRA**

A quantitative analysis is not implying objectivity, QRA are in most cases subjective and judgmental. False confidence in the risk measures may take place if the significance of the judgments and assumptions are overlooked. On the other hand, over-emphasizing on the judgmental nature may lead to its potential benefits being disregarded (Spouge, 1999).

The result from a QRA is only as good as the assumptions and data used as inputs. In resemblance with other analysis methods, the potential of QRA is restricted by the lack of plant specific data and data uncertainties. QRA only provides an input to decision-makers about safety issues, and cannot make the decisions itself (Spouge, 1999).

An offshore installation can be considered as a complex system (which is discussable, refer Rosness et al., 2010), equipment and utilities are set up within limited space, leading to tight couplings. When having tight couplings, a change in the system propagates quickly to other parts of the systems (refer Perrow, 1999, for additional reading about complexity and tight couplings within normal accident theory). The blowout incident on Snorre A shows the danger of tight couplings and complex interactions. An example from the incident is the shutdown of the main power supply due to ignition risk during the incident, needed to force drilling mud down into the well to prevent a blowout. This interaction was not predicted before the incident (refer Rosness, et al., 2010, for additional reading about the accident). With complex and tight coupled systems, great danger and uncertainties will follow. The QRA performed in offshore is mainly focused on the consequences. A QRA might thus not be able to address the sequence leading to a hazardous event, or able to prevent it from occurring.

To predict the consequences and their probabilities, QRA relies on a frequency foundation as basis for predicting the initial events. The risk picture presented by the QRA is highly dependent on the initial events, but the data basis can be questioned. If the number of large leaks is too high, the risk picture will be reflected correspondingly (see Section 5.4.1.5 about the topic). The data basis is thus critical. Another challenge is to predict all possible events, due to the complexity. A software program able to handle the large number of scenarios in a systematic manner is required. The large amount of data is often difficult to comprehend, and the overview easy lost.

## 2.2 Uncertainties in Quantitative Risk Analysis

Uncertainties can be categorized as (NUREG-1855, 2009):

1. Parameter uncertainty
2. Model uncertainty
3. Completeness uncertainty

Availability of all possible and accurate information or data is considered a seldom privilege. Assumptions are made throughout a risk analysis, and along with assumptions are often uncertainties. The assumptions can be related to data, methodologies or about the system object for analysis. In the Norwegian legislation, treatment of uncertainties are not explicitly required, except for a discussion of it (NORSOK Z-013, 2010) (brief introduction is given in Section 3.1.3).

### 2.2.1 Parameter Uncertainty

Parameter (data) uncertainties can be due to the effect of small sample sizes, the relevance of generic data to the specific systems, or the effect of limited reporting in relation to failure mode definition (Schofield, 1998). Major accidents are fortunately rare events, but limit the amount of data as a negative consequence. Use of generic data is an option to overcome this problem, but question of the relevance of the data appears. Another challenge is due to nonconformity of classifying and analyzing failures. The nuclear industry, compared to the Norwegian offshore industry, has at the present a more thorough treatment of parameter uncertainty. The current practice is to characterize parameter uncertainty, using probability distributions on the parameter values (NUREG-1855, 2009). Many of the stipulated acceptance criteria are defined such that the appropriate measure for comparison is the mean value of the uncertainty distribution on the corresponding metric (NUREG-1855, 2009). In comparison, there is no tradition for parameter uncertainty in the Norwegian QRA.

### 2.2.2 Model Uncertainty

Risk analyses are based on a large number of models, which always are simplifications of the real situation (Rausand, 2011). When performing a risk analysis, the analyst can choose between a repertoire of methods or models, each with appurtenant strengths and limitations. The suitability is case specific, where the object of the analysis should influence the method or model selected. The typical response to model uncertainties is to choose a certain model when performing a QRA. It is possible to use several alternate models, then provide weights of the results from the various models (NUREG-1855, 2009). This is unusual and requires additional resources. There are some prevailing consensus models<sup>5</sup> in QRA, for example fault tree and event tree analysis. Even so, the adoption of consensus models should not be done unrestricted. The analyst should understand the models, including the belonging assumptions and limitations in its attempt to illustrate the reality. The consequence methodology discussed in detail in this thesis is the ETA.

### 2.2.3 Completeness Uncertainty

Lack of completeness is not uncertainty in itself, but a recognition of limitations (NUREG-1855, 2009). Completeness uncertainties are issues related to the general quality of the risk analysis

---

<sup>5</sup> Consensus model: In the most general sense, “a model that has a publicly available published basis and has been peer reviewed and widely adopted by an appropriate stakeholder group” (NUREG-1855, 2009)

process, its objectives, scope, competence of the research team, and so on. Two main factors influencing the uncertainties are (Rausand, 2011):

- Is the background material for the risk analysis correct and up to date?
- Have all the potential hazardous events been identified?

A large number of drawings and documents are often used in a risk analysis, but the system analyzed will differ from the actual system if they are incorrect or outdated (Rausand, 2011). The dissimilarities can also stem from the realizations phase, where the production, installation or assembly of the installation are not performed in compliance with the drawings.

Sometimes, the limitation is due to resources. It can be difficult to acquire precise data or information, and the level of detail is often decided by resources available. What should for example the tolerance for the drawings be, in the magnitude of millimeter or centimeter?

A challenge is to cover all possible hazards, where uncovered hazards can lie dormant. Some hazards can be deliberately unattended for simplification purposes. It can be time consuming to further analyze all identified hazardous events. The hazards are then at least known by the analyst, more concerning are the unknown hazards, especially if they are substantial. Unknown hazards are of course unattended. Both kinds of omission leads to an incomplete risk picture, where the unattended hazardous events can reduce the conservatism of the computed risk. The real risk picture can thus be more severe than what presented in the risk analysis. The completeness uncertainty are difficult to quantify and represents aspects of the systems that are not treated in the model (NUREG-1855, 2009).

Refer Schofield (1998) and Rausand (2011, Chapter 16) for additional reading about uncertainty, and HSE (2001) for how to take precautions in the face of uncertainty.



# Chapter 3

## The Risk Picture

### 3.1 Elements Establishing the Risk Picture

Risk picture is a term, mainly used by the Norwegian offshore industry. The term is defined as a

*Synthesis of the risk assessment, with the intention to provide useful and understandable information to relevant decision-makers. (NORSOK Z-013, 2010, p. 14)*

The risk picture in a QRA is comprised by the output from a risk analysis, often as estimates of the risk measures. The definition states the risk picture as a source of information to relevant decision-makers, which is an important purpose. A paradox is the simplicity and easiness of using one figure risk measures (point estimates), and the information withheld in such a measure. A risk picture is easy to understand and compare if they are simple, as a drawback, the level of detail is lower and might lack some important information. The synthesis of the risk analyses is not only limited to the risk measures. A good risk picture stretches beyond the summation table of the risk measures. Even though a QRA is mainly quantitative, the analysis can comprise of important qualitative findings.

#### 3.1.1 Risk Categories in Quantitative Risk Analyses

The risk related to accidents can be divided into the sub-categories of (Vinnem, 2007, p. 16):

- Personnel risk
  - o Fatality risk (see Section 3.3)
  - o Impairment risk (see Section 3.4)
- Environmental risk (see Section 3.5)
- Asset risk (see Section 3.6)
  - o Material damage risk
  - o Production delay risk

Which risks categories to assess is decided by the scope of the QRA. The focus of offshore QRAs is often major accidents, where the level of detail is dependent on the scope, and limited by resources. A risk analysis normally includes an assessment of all three sub-categories, when considering offshore installations (NORSOK Z-013, 2010). The focal point is often personnel risk, whereas environmental and asset risk are assessed more briefly. It is sometimes even hardly mentioned. Note that the management regulations (PSA, 2011d, Section 9) requires risk acceptance criteria to be determined by the operator for the first two risk categories.

Risk to personnel can be defined in terms of injury or fatality (Center for Chemical Process Safety, 2000), where only fatality risk is considered in the thesis. An argument for disregarding injuries is the number of possible degrees of injuries and the high uncertainties. When considering fatality risk, the person is either dead or alive. Risk to assets can be considered to comprise of both the direct economic losses (damage to material assets and production/service loss), and damage to the company image. Loss of assets mainly strikes the company itself, and does not directly harm human life or environment.

### **3.1.2 Establishing the Risk Picture for Personnel Risk**

When establishing the risk picture, NORSOK Z-013 (2010) requires a separate calculation and presentation of the following fatality risk contributions (when applicable):

1. Immediate fatalities
2. Offshore transportation fatalities including shuttling
3. Escape fatalities
4. Evacuation and rescue fatalities
5. Off-site risk

For risk to personnel, the elements of risk can be divided into occupational, major, transportation, and diving accidents (Vinnem, 2007). When considering process accidents, only the immediate, escape, and evacuation and rescue fatalities from the list of NORSOK are relevant.

Immediate fatalities occur in the immediate vicinity, or in time, of the initial hazardous event, (Vinnem, 2007). Most of these fatalities will occur within the area of occurrence (Vinnem, 1998). Consider a leak in a process area, subsequently the formation of a gas cloud, ignition and explosion. The immediate fatalities of such an incident are the casualties due to the shock wave and heat, generated from the explosion. Escape to refuge area will be the action after the initial event. Fatalities during this phase are denoted escape fatalities, which occur during escape prior to or immediately after the initial accident, back to a shelter area (Vinnem, 2007). Such fatalities can occur as personnel are trapped by fire or smoke. Safety is still not assured after entrance to the shelter area, fatalities can occur during the evacuation from the installation (Vinnem, 2007). Evacuation fatalities are when people are killed due to failure of the evacuation and rescue system (Spouge, 1999). Some means of evacuations are directly from the installations, such as helicopters or free fall lifeboats. OLF free fall lifeboat project is an ongoing study. A full-scale test drop on the Veslefrikk field revealed, among others, too high strains to the human body during drop (Strauman & Selnes, 2011). Other means of evacuation requires rescue from sea, for example when the personnel jumps of the installation, or using ladders for escape, increasing the risk and introduces new hazards.

### 3.1.3 Addressing Uncertainty when Establishing the Risk Picture

NORSOK Z-013 (2010, p. 25) requires a discussion of the uncertainty, including aspects of:

1. The perspective on risk used in the assessment, e.g. classical, statistical, probability of frequency, combined classical and Bayesian, Bayesian, Predictive approach.
2. The effect and level of uncertainty given the adopted perspective and the context for the assessment (including the “system boundaries” and “system basis”) compared to the “actual” or the “real” systems and/or activities of interest
3. Possible implications for the main results
4. Occurrence of unexpected outcomes, as a result of invalid assumptions and premises, or insufficient knowledge

When performing a QRA, discussion of uncertainty is often taken easy upon. Some analysts are rather using sensitivity analyses as an argumentation for the importance of uncertainty. The uncertainties of parameters can for example be of less importance, if the end

results only have small fluctuations when altering important parameters. Discussion of the three uncertainties presented earlier (parameter, model and completeness) should be able to cover all the aspects listed by NORSOK.

## 3.2 Acceptance Criteria

The PSA does not define the term risk acceptance criteria (PSA, 2011d), but is defined by NORSOK as

*Criteria that are used to express a risk that is considered as the upper limit for the activity in question to be tolerable. (NORSOK Z-013, 2010, p. 13)*

This definition indicates a mechanistic use of the acceptance criteria, by setting a determined value as the criteria, and comparing the risk estimate. Other types of criteria setting is more focused on the process, rather than setting a determined value on the limits (an example is given in Section 3.2.1).

The extracted Section 9 from the management regulations stipulates what an acceptance criteria must be set for (PSA, 2011d). The upper limit of the acceptance criteria are not set by the PSA, except for the impairment frequency of the main safety functions (discussed in Section 3.4). The responsibility is transferred to the operators. Typical acceptance criteria are discussed in Section 3.3.5.

### Section 9

#### Acceptance criteria for major accident risk and environmental risk

The operator shall set acceptance criteria for major accident risk and environmental risk.

Acceptance criteria shall be set for:

- a) the personnel on the offshore or onshore facility as a whole, and for personnel groups exposed to particular risk,
- b) loss of main safety functions as mentioned in Section 7 of the Facilities Regulations for offshore petroleum activities,
- c) acute pollution from the offshore or onshore facility,
- d) damage to third party.

(PSA, 2011d)

### 3.2.1 As Low As Reasonably Practicable

The framework regulation (PSA, 2011c) does not explicitly require the use of the *as low as reasonably practicable* (ALARP<sup>6</sup>) principle, but the requirements described in Section 11 are

---

<sup>6</sup> In other contexts also known as “as low as reasonably achievable”

essentially equal to the UK interpretation of the ALARP principle. In UK, ALARP is part of the legislation as a regulatory requirement by the Health and Safety at Work Act (Jones-Lee & Aven, 2011). Several of the operators on the Norwegian continental shelf have adopted the ALARP principle, even though they are not maintained by law. A brief presentation of the principle is given in NORSOK Z-013 (2010). The principle is an approach which must be adapted to the specific system/situation.

### Section 11

#### Risk-reduction principles

Harm or danger of harm to people, the environment or material assets shall be prevented or limited in accordance with the health, safety and environment legislation, including internal requirements and acceptance criteria that are of significance for complying with requirements in this legislation. In addition, the risk shall be further reduced to the extent possible.

In reducing the risk, the responsible party shall choose the technical, operational or organizational solutions that, according to an individual and overall evaluation of the potential harm and present and future use, offer the best results, provided the costs are not significantly disproportionate to the risk-reduction achieved.

If there is insufficient knowledge concerning the effects that the use of technical, operational or organizational solutions can have on health, safety or the environment, solutions that will reduce this uncertainty, shall be chosen.

Factors that could cause harm or disadvantage to people, the environment or material assets in the petroleum activities, shall be replaced by factors that, in an overall assessment, have less potential for harm or disadvantage.

Assessments as mentioned in this section, shall be carried out during all phases of the petroleum activities.

This provision does not apply to the onshore facilities' management of the external environment.

(PSA, 2011c)

People are often willing to expose themselves to some risk to gain certain benefits. To mitigate the possible undesirable effects, precautions are made if possible. Figure 3.1 illustrates the ALARP principle, where the level of risk increases when moving from bottom to top. The risk can be divided into three levels (HSE, 2001):

- *Unacceptable region:* The red zone indicates unacceptably high risk, activities with risk falling within this region are regarded unacceptable, whatever the benefit. The risk has to be reduced to falls within one of the regions below, or can in extraordinary circumstances be justified.
- *ALARP region:* In the yellow zone, the risk has to be kept as low as reasonably practicable (ALARP criteria). Risk-reducing measures must be implemented unless the cost is grossly disproportionate to the benefit.

- *Broadly acceptable region*: When the risk is negligible or adequately controlled, no further action is required, without the need to demonstrate the ALARP principle.

There is a fundamental difference between the terms “practicable” and “reasonably practicable”. Practicability is limited to technically feasible measures (physically possible), not concerned with cost, whereas reasonable practicable does (Schofield, 1998). There is no doubt that “reasonably practicable” holds fewer measures compared to “physically practicable” (Vinnem, et al., 2006).

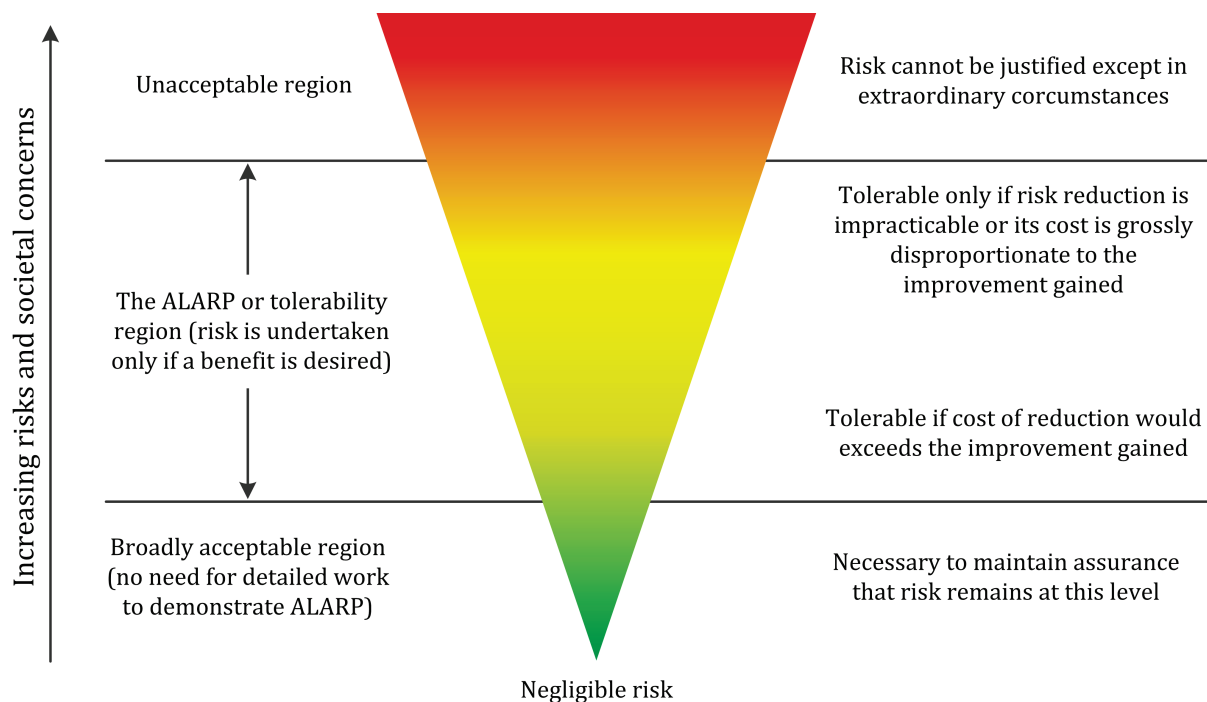


Figure 3.1: The as low as reasonably practicable (ALARP) principle (Modified from HSE, 1992)

Who having the onus of proof is an important aspect, which is not clearly stated by the framework regulation (PSA, 2011c, Section 11). In the UK, the duty holder is responsible to show that the measures rejected are not reasonably practicable. The thrust is then not the regulator. The approach is to implement all reasonably practicable measures. It is not sufficient for the operator to show that the already implemented measures are adequate (unless the risk is negligible), but to show that possible measures are unreasonably practicable. The framework regulation requires that only measures *significantly* disproportionate to the risk-reduction can be disregarded (PSA, 2011c).

The Health and Safety Executive (HSE<sup>7</sup>) uses the term grossly, whereas the PSA (Norway) uses the term significantly, which seems like a stricter criterion. The threshold to disregard a significantly disproportionate measure is usually less compared to grossly.

The approach of ALARP is not always adequate. A good risk-reducing measure might be disregarded, as a worse measure is implemented first. This can occur when the measures are covering some of the same risk, and the measures are expensive.

### 3.2.2 Cost-Benefit

There must be a judgment based decision about what a reasonable risk level constitutes, which can be made through the use of a cost-benefit approach. A disproportion factor  $DF$  is introduced (HSE, 2005):

$$DF = \frac{\text{Cost of risk-reducing measure}}{\text{Benefit of the risk – reduction}} \quad (3.1)$$

The  $DF$  takes usually a value of 1 or greater, and is correlated to the degree of risk. A greater risk calls for a greater  $DF$ . An expected benefit equal to the cost required is found at a  $DF$  of 1. The evaluation of disproportion can be carried out by defining a disproportionate limit  $DF_0$ , where a measure should be implemented if  $DF < DF_0$  (Rausand, 2011). A challenge is to assign a proper value to  $DF_0$ , which reflects a grossly or significantly disproportion. A converging towards an agreed disproportionate limit has not taken place, and  $DF_0$  must be addressed for the specific case. The disproportionate limit is influenced by the willingness to pay, which is constrained by the ability to pay (Jones-Lee & Aven, 2011). The petroleum industry is usually in disposal of large economic resources, and is able to stretch further to secure the safety of their employees. The possibility to invest more to prevent possible future economic losses, is greater compared to many other industries.

One might argue that no human life is worth risking, making it a sensitive issue to place an explicit monetary value on a human life (Rausand, 2011). Resources are not infinite; overcommitting on implementing risk-reducing measures can lead to bankruptcy. The evaluation of a risk-reducing measure will inevitably involve a monetary value of human life.

The cost in monetary terms of implementing a safety improvement is relatively straightforward to specify, though not always easy to estimate beforehand. Estimating the expected benefit can be more challenging. Due to uncertainties, one should not be engrossed by cost-benefits analysis. When considering the risk-reducing measures, the results from such

---

<sup>7</sup> UK's equivalent to the PSA

analysis should only be used in conjunction with good engineering judgment (NS-EN ISO 17776, 2002).

### 3.2.3 Goal-Setting Regime

There is an increasing movement towards a *goal-setting regime* by the Norwegian authorities. This implies a focus on the goals for risk-reduction, rather than specifying the solutions to reach these goals (Vinnem, 1998). The PSA reflects this by not deciding the limit of the acceptance criteria, but requiring the operator to individually set the criteria themselves. The advantages of a goal-setting regime are (Vinnem, 1998, p. 41):

- The industry is more flexible when fulfilling the regulations and can choose the optimal solution under given circumstances
- Preventive and protective systems may be tailored to the hazards that are relevant

With the flexibility, a portion of the responsibility is allocated to the operators. For this approach to be efficient, the flexibility offered must be utilized and not misused. A type of misuse is to set too low limits, to easier meet the acceptance criteria. Another misuse is to set criteria which are never met, where the acceptance criteria are expected to be exceeded, and the project still carried out. To assure a decent risk level, the ALARP principle can be implemented. Note that the flexibility can also be related to the safety systems used, or approaches to reduce the risk.

The operators face new difficulties when the art of engineering is constantly pushed further; for example seeking towards deeper waters. For unconventional concepts, the goal-setting interpretation might be the only possible approach (Vinnem, 1998). A generic solution is not able to give the desired prevention and protection in all possible situations. Another challenge is aging platforms; introducing problems earlier not present, or worsen problems present. An example is the challenge of corrosion, which increases with the age of the installation, requiring additional attention to treat these threats.

## 3.3 Fatality Risk Measures

Risk to people can be distinguished as individual or group risk. Individual risk is concerned with the risk an individual is exposed to, during a specific time limit, under defined fixed relations to the hazard (Rausand, 2011). An individual risk measure can be a point estimate, a set of risk estimates to various types of individuals, or related to geographical locations.



Group risk is concerned with the risk exposed to a group of people, and is a combination of individual risk levels and the number of people at risk (Rausand, 2011). Group risk can be used to draw the risk picture for a certain group, for example related to a specific area on an installation. When members of the public are exposed, group risk can be referred to as a societal risk. The term group risk is often preferred in offshore QRA, where the workers are isolated and the common citizens seldom affected.

When presenting the risk as a point estimate, an application of both group and individual risk might be useful. It is not sufficient to achieve a low average risk, but the risk level of the most exposed individuals should also be minimized (Mannan, 2005). Some operators overcome this problem by stating a separate acceptance criterion for highly exposed groups/individuals.

Several risk measures are used to calculate and express individual and group risk. Although the risk measures are consistent with, and based on the same definitions, the results may be substantially different (Spouge, 1999). One specific risk measure might have several approaches, which might include different interpretations. The same measure can be used as both a measure of individual or group risk, dependent on the perspective (e.g. the PLL). The presented risk measures in this chapter are accommodated for the offshore industry. Generic formulas and explanations of the various measures are discussed by Rausand (2011).

### 3.3.1 Potential Loss of Life

The *potential loss of life* (PLL) is also known as the annual fatality rate (AFR). The PLL is the expected number of fatalities within a specified population, or within a specified area, per annum (refer Rausand, 2011, Section 4.3.8 for additional reading about PLL). PLL is a term proposed by Shell, and emphasizes the inevitability of fatalities, even with good safety management (Spouge, 1999). The PLL is usually a simple group risk indicator. It only considers the expected number of fatalities, and not the distribution of fatalities among the number of accidents. One accident causing 100 deaths, or 100 accidents causing 1 death each, is considered equally (Rausand, 2011). The PLL can also be considered as the probability of an individual losing his or her life.

In relation to offshore platforms, the PLL is also referred to as fatalities per platform year (FPPY), but the term PLL is still commonly used. The PLL is normally used as an intermediate result and not as a risk criterion, since the risk is “reduced” by restricting the number of people (Vinnem, 2007). The PLL can also be expressed through fatality risk assessments (Vinnem, 2007, p. 17):

$$PLL = \sum_{i=1}^m \sum_{j=1}^n (f_{ij} \cdot c_{ij}) \quad (3.2)$$

Where  $f_{ij}$  is the annual frequency of accident scenario  $i$ , with personnel consequence  $j$ . The expected number of fatalities for the respective scenario and personnel consequence is denoted  $c_{ij}$ . The total number of accident scenarios in the event trees is  $m$ , and  $n$  is the total personnel consequence types (e.g. immediate, escape, and evacuation and rescue). The frequency of the various accident scenarios ( $f_{ij}$ ) can be calculated, for example, by using event trees (the approach Scandpower uses is described in Section 4.2 and Chapter 5).

### 3.3.2 Individual Risk Per Annum

The *individual risk per annum* (IRPA) is also known by the name of individual risk (IR) and average individual risk (AIR). Refer Rausand (2011), Section 4.3.1 for additional reading about IRPA. The IRPA can be expressed by the PLL, and vice versa. One approach is to express the IRPA as (Vinnem, 2007):

$$IRPA = \frac{PLL}{\text{Exposed individuals}} = \frac{PLL}{POB_{\text{avg}} \cdot \frac{8760}{H}} \quad (3.3)$$

The PLL is used as an intermediate result to calculate the IRPA equation (3.3).  $POB_{\text{avg}}$  is the average number personnel on board (POB), more specifically the number of personnel on the offshore installation. The exposed number of hours might be based on the actual working hours, or the total hours the personnel are on the installation (Holand, 1997). It is important to state what the exposure hours comprise of. Some risk applies only during working hours, as others are for the whole time spent on the installation. The exposed number of hours is defined as both on- and off-duty in this context. This can be suitable, concerning offshore activities. The personnel are still on the installation, and continuously exposed, even if they are off-duty.  $H$  is the annual number of hours spent offshore per individual, including on- and off-duty hours. The ratio  $8760/H$  is the number of required individuals to fill one position. The value of  $H$  is dependent on the work schedule of the operator. A common schedule in Norway is two weeks “on”, then four weeks “off”. Three persons are then required to fill a position;  $H$  is therefore 2920 hours per year.

### 3.3.3 Fatal Accident Rate

The *fatal accident rate* (FAR) is the expected number of fatalities in a defined population per 100 million hours of exposure. Refer Rausand (2011), Section 4.3.9, for additional reading about FAR (which also includes a table of experienced FAR values in various industries). Consider 1 000 men at the age 20 starts to work with a certain occupation, working 2 500 hours per year. With a FAR of 4, only 996 will leave the profession alive at the age of 60 (Mannan, 2005).

FAR can be used as a measure of overall risk for all personnel at a facility, or for a defined group (NORSOK Z-013, 2010). It is one of the most common risk measures (regarding fatalities per unit time) used in the North Sea (Holand, 1997). To compare the FAR values, the measure has to wear the same definition. This is not always the case, especially regarding the interpretation of exposed hours. The number of exposed hours is often set as the total hours the personnel are on the installation, where the FAR is expressed as (Vinnem, 2007, p. 19):

$$\text{FAR} = \frac{\text{PLL}}{\text{POB}_{\text{avg}} \cdot 8760} \cdot 10^8 \quad (3.4)$$

By comparing the FAR, Equation (3.4), and the IRPA, Equation (3.3), the two indicators are closely correlated with the following relationship (Vinnem, 2007):

$$\text{IRPA} = H \cdot \text{FAR} \cdot 10^{-8} \quad (3.5)$$

FAR is typically in the range of 1 – 30 and is often a more understandable compared to IRPA (Spouge, 1999). When the estimated FAR is installation specific, the foundation of comparison with experienced fatality statistics is lost. This is mainly due to the high impact of low probability incidents, with high number of fatalities (Holand, 1997). This is illustrated in Table 3.1, where the impact of including/excluding the Alexander L. Kielland accident is shown.

Table 3.1: Experienced overall FAR for Norway, January 1980 - January 1994 (Holand, 1997)

Conditions for the FAR calculations	FAR
Total FAR (including Alexander Kielland accident)	47.30
Total FAR (disregarding the Alexander Kielland accident)	8.50

### 3.3.4 FN Curves

Group risk can be expressed as FN curves, presenting the severity/consequence (size of the accident) in relation to the frequencies of accidents. Refer Rausand (2011), Section 4.3.11, for additional reading about FN curves. A FN curve can be used to illustrate both the risk curve and

the acceptance criterion (NORSOK Z-013, 2010). The acceptance criterion specifies the tolerable (left side) and the non-tolerable area (right side). This can be extended to include the ALARP principle, by introducing an upper and lower limit. The axes are normally on a logarithmic scale, and it has been common to plot the cumulative frequency of number of fatalities  $N \geq n$  (Rausand, 2011), where  $n$  is the number of fatalities.

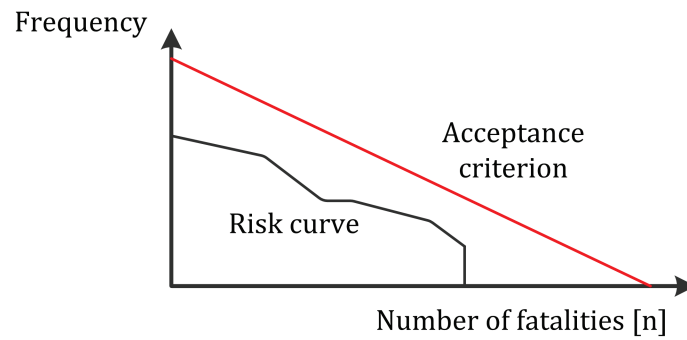


Figure 3.2: Example of FN curve

When performing risk analysis for offshore installations, the method of ETA is often used to calculate the PLL, which subsequently can be used to draw the FN curve. Consider  $n_i$  as the number of fatalities for scenario  $i$ , for that specific scenario. The respective PLL can be expressed as  $PLL_i$ , and  $f_i$  as the frequency.

$$n_i = \frac{PLL_i}{f_i} \quad (3.6)$$

The annual frequency of exactly  $n$  fatalities, denoted  $f(n)$ , can be calculated by summing the frequency of all scenarios with the exact number of  $n$  fatalities:

$$f(n) = \sum_i f_{in} \quad (3.7)$$

Where  $f_{in}$  is the frequency of scenario  $i$ , with exactly  $n$  fatalities. The FN curve can then be constructed using Equation (3.7).

### 3.3.5 Typical Acceptance Criteria Used by Norwegian Operators

Regarding first parties, FAR is typically used by the Norwegian operators. A common stipulated FAR is 10, as an average for the total personnel on the installation. An installation average FAR can be manipulated, making the FAR for groups often more relevant. By only considering the

installation FAR, a reduction of the FAR is achieved when increasing the number of personnel in low FAR-contributing areas (living quarters). With this manipulation, a reduction of the actual risk is not accomplished. In compliance with the management regulation, Section 9, an accept criterion is also set for the most exposed groups (PSA, 2011d). A typical value is  $FAR = 25$ . The purpose of defining a FAR for the most exposed groups, is to prevent a group from exposure to abnormal high level of risks. Even so, the FAR for a group is still an average, applicable for all members in the specified group, without considering the level of risk the various individuals are exposed to (Rausand, 2011).

FN curves are less commonly used in the Norwegian offshore industry, which is also more difficult to satisfy compared to FAR. Using an average FAR does not put any requirements to the distribution. Single value risk measures can often be converted to be reflected in a FN curve. A FN curve can be considered as a distribution of many single value criteria. Taking the distribution into consideration, a single high risk activity cannot be concealed by low risk activities.

When assessing the acceptance criteria, the fatality risk measures presented in this section are often applied in a mechanistic way. This implies that the risk is either acceptable or not, based on the risk estimates calculated, compared to a determined criteria. Thus, the need for principles such as the ALARP principle is present.

### 3.4 Main Safety Functions

Main Safety Functions (MSFs) are used as protective means for personnel in the case of a severe accident (Aven & Vinnem, 2007). According to the facility regulations, concerning permanently manned facilities, the following MSFs must be maintained (PSA, 2011b, Section 7):

1. *Preventing escalation* of accident situations so that personnel outside the immediate accident area are not injured
2. *Maintaining the capacity of load-bearing structures* until the facility has been evacuated
3. *Protecting rooms of significance* to combatting accidents so that they remain operative until the facility has been evacuated
4. *Protecting the facility's secure areas* so that they remain intact until the facility has been evacuated
5. *Maintaining at least one escape route* from every area where personnel are found until evacuation to the facility's safe areas and rescue of personnel have been completed

It is required that no accidental or natural load with a probability of  $10^{-4}$  per annum, or greater, shall result in the loss of an MSF (PSA, 2011b, Section 11). This is interpreted as the impairment frequency of the MSFs never shall exceed  $10^{-4}$  per year, possibly ensured by introducing barriers. The impairment frequency criteria can be considered as a simple mean of judging the personnel risk, without the explicit expression of fatalities (Spouge, 1999). Five accidental and environmental load categories are defined (NORSOK Z-013, 2010, p. 71):

1. Heat loads
2. Smoke and toxic loads
3. Explosion loads (any kind of explosions)
4. Impact loads
5. Extreme environmental loads

Each hazard type and load should be assessed separately against the risk acceptance criteria for loss of MSFs. The OLF guideline 070 (2004, p. 108) states that several operators on the Norwegian continental shelf have chosen to use  $5 \cdot 10^{-4}$  as a criterion for the total five loads. This interpretation does not comply with the NORSOK standard, where *each* of the loads must be considered separately (NORSOK Z-013, 2010, p. 74). By taking the total sum, rather than considering each of the loads separately, the criterion does not ensure an even distribution of the impairment frequencies. For example, operation in stable environments, should not give the opportunity for lack of safeguards against heat loads.

The impairment frequency of MSF  $k$ , denoted  $f_{Impairment,k}$ , can be caused by several scenarios. The frequency of scenario  $i$  is denoted  $f_i$ , and  $I$  indicates the total number accident scenarios. Each of the scenarios has a probability,  $p_{imp,i,k}$ , of causing an impairment of MSF  $k$ . The impairment frequency of an MSF can then be calculated as (Vinnem, 2007, p. 24):

$$f_{Impairment,k} = \sum_i^I f_i \cdot p_{imp,i,k} \quad (3.8)$$

### 3.5 Environmental Risk

The short term impact of an oil spill is devastating, causing extensive damage to the marine and wildlife habitats. Tremendous efforts and money are required to restore the damage done. The long-term effects are more ambiguous, and should thus be treated with caution. Environmental damage from accidents on offshore installations is mainly related to oil spill, dominated by spills

from blowout, pipeline leaks or storage leaks (Vinnem, 2007). The consequences can be measured as the restoration time, which is the time needed to return to a normal state after a spill. Note that environmental risk analyses are mandated (PSA, 2011d, Section 17). The restoration time indicates that damages to the environment are within the possibility of repair. Some specialists claim that the extent of damage can be beyond the repairable (Vinnem, 2007). Carrying capacity is often spoken of as the environment's maximal load regarding overpopulation, but can also be applicable to damage from oil spill.

The Norwegian Oil Industry Association (OLF) has published a guideline for environmental risk analysis, named MIRA<sup>8</sup> (OLF, 2007). The purposes of MIRA are:

- To emphasize the environmental risk with an activity
- To emphasize environmental risk contributing activities or events related to an operation, for the ability to implement risk-reducing measures
- To emphasize or identify naturally courteous resources which will be affected by an immediate spill, for the ability to implement risk-reducing measures

Refer OLF (2007) for additional reading about MIRA. If executed in detail, an environmental risk analysis can be comprehensive. Environmental risk analysis is often given little attention when it is part of a QRA. It is often assumed for process accidents that the oil spill is contained on the offshore installation.

### 3.6 Asset Risk

Asset risk can be associated with the damage to equipment and structures, along with the resulting disruption of production. Usually, expression of asset risk can be either of the following (Vinnem, 2007, p. 25):

- Expected damage to structures and equipment
- Expected duration of production delay
- Frequency of events with similar consequences, either in extent of damage or duration of production delay

Many studies use simplified modeling of asset risk. One of the most uncertain aspects is the relationship between damage to equipment and structure. This is in relation to the

---

<sup>8</sup> Norwegian acronym for environmental risk analysis (Miljørettet RisikoAnalyse)

production delay, due to restoration and repair (Vinnem, 1998). Sometimes, small damage to equipment can cut the production rate over a longer period, due to low availability of spare part and long lead time.

The government is usually not concerned with asset risk; loss of assets (non-human) impacts at first only the company itself. If considered at all, asset risk is often assigned a small portion of a QRA. Performing analyses to cover asset risk is not mandated by the PSA, but are still performed by some operators. An asset risk analysis can be beneficial, for example used by the operator as an argument of safe investment, conveying possible investors.

### 3.7 Multi-Discipline Engineering

For a process accident scheme, Figure 3.3 illustrates how the discipline of QRA can be seen in relation to others. The need for input from other disciplines is decided by the accident type. For other accident types than process accidents, analyses of for example, ship traffic, collision and falling objects might be relevant. Figure 3.3 is for illustrational purposes only, where the disciplines might have different names, dependent on the organization. The QRA discipline has several inputs to consider during an analysis. Some of the inputs have effect on both the frequencies and consequences, and is thus not divided explicitly. This is dependent on the point in time the end event is set. If the end consequence is a fire escalation, a gas dispersion simulation can impact on both the frequency and the consequences of the escalated fire. To be able to present a high quality risk picture, the QRA team is dependent on several other disciplines.

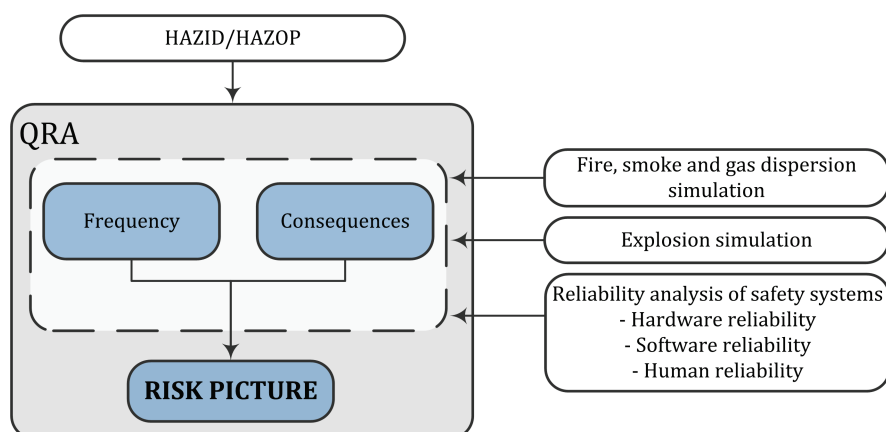


Figure 3.3: Quantitative risk analysis with multi-discipline co-operations



# Chapter 4

## Quantifying the Risk Picture of Process Accidents

### 4.1 Barriers Preventing and Mitigating Process Accidents

To mitigate hazards related to process accidents, fire protections are utilized. Both active and passive fire protections are used on offshore installations. Relevant safety systems (active fire protections) are:

- Detection system
  - o Gas and smoke detection
  - o Fire detection
- ESD isolation system (including ESD isolation valves)<sup>9</sup>
- Blowdown system
- Firewater system
  - o Firefighting, automatic and manual

Actions cannot be executed without the knowledge about the presence of hazards. The detection system could be enlisted as part of the firewater system, but is extracted to emphasize its importance.

---

<sup>9</sup> An ESD can be considered as the initiation of a shutdown, including isolation, blowdown and firewater (among others, see NORSOK S-001, 2008, figure 2, for a principle hierarchy of ESD), it is in this content called ESD isolation when only the isolation function is considered

The purposes of the safety systems are to:

1. Reduce the probability of ignition, and subsequently explosion
2. Mitigate the consequence of fires (prevent escalation) and explosions

The probabilities of ignition and explosion are dependent on the gas dispersion, with the leak rate as one of the main parameters. The positive effect of the safety systems can for example be a reduction of the leak rate, and thus the probability for ignition or explosion.

Passive fire protections, where applied, shall give sufficient fire resistance to structures, piping, and equipment (PSA, 2011b, Section 29). An important passive fire protection is firewalls, used to separate the main areas on the installation (PSA, 2011b, Section 30). Classification of the firewalls and their respective design loads can be found in the PSA facility regulations (2011b, Section 3).

#### **4.1.1 Detection System**

It can be distinguished between gas and fire detection, with the possibility for smoke detection. The detection system enables a fast discovery of hazardous events. The detection can initiate an automatic activation of the safety systems, or alert personnel to perform manual actions. On the contrary, offshore experiences indicate that most fires and explosions (from high pressure equipment) are seen or heard by personnel, who activates the manual call points before the detectors operate (Spouge, 1999).

In general, the technical failure probability of a gas detection system is low. The failure rate is dominated by the probability of the gas reaching the detectors. *ExploRAM*<sup>10</sup> is used to quantify the scenario-dependent gas leak detection probability, at each time step. The tool uses a simple gas detection model (Wiklund & Fossan, 1999). The probability of triggering a detector equals the fraction of the module filled with a gas concentration, higher than the detector set point. The exposure probability is considered independent for each detector.

---

<sup>10</sup> *ExploRAM* is a model for explosion risk assessment (including ignition analyses), only used within Scandpower

### 4.1.2 ESD Isolation System

Purpose of the ESD isolation system (NORSOK S-001, 2008, p. 21):

- ESD valves shall isolate and sectionalize the installations process plant in a fast and reliable manner to reduce the total amount of released hydrocarbons in the event of a leakage

The released amount of hydrocarbons influences the escalation probabilities, subsequently the intensity and duration of the fire. A reduction of the amount of hydrocarbons leaked implies a lower escalation probability, due to reduced amount of fuel. In addition to limit the amount of hydrocarbons leaked out in the segments, the ESD isolation system can have a positive effect on the leak rate. By choking the flow from upstream process system, the pressure can be maintained, naturally decreasing with the volume of the pipes. An important factor regarding ignition probabilities is the duration the cloud is between the lower and upper flammable limit. The larger the gas cloud size, the more likely it is to encounter an ignition source (Spouge, 1999). The ignition probability related to the gas cloud size is thus decreased by the ESD isolation system. The explosion load and probability is also influenced by the gas cloud size.

### 4.1.3 Blowdown System

Purposes of the blowdown system (NORSOK S-001, 2008, p. 25):

- In the event of a fire to reduce the pressure in exposed process segments to reduce the risk of rupture and escalation
- Reduce the leak rate and leak duration and thereby ignition probability
- In some cases avoid leakage at process upsets, e.g. in case of loss of compressor seal oil/seal gas
- Route gases from atmospheric vent lines to safe location, or through the flare system to safe location (flare knock out drum and flare tip)

Especially the two first and the last point are relevant when considering process accidents. The build-up of a gas cloud decreases with a smaller leak rate and shorter duration. With the blowdown system operative, a positive reduction of the gas cloud can take place. This can reduce ignition and explosion probability. Figure 4.1 is an example of leak rates, with and without the blowdown system. The pipes are often pressurized, causing a possibility for rupture

of the pipes, which would increase the leak rate substantially. By depressurizing the pipes, a rupture can be prevented, and subsequently the fire spreading to other segments. The probability of spreading to other neighboring segments decreases by emptying them of hydrocarbons. The system is designed for a load higher than the feed rate. Given a functional blowdown system, the leak rate should decrease during failure of the ESD isolation. In addition, a failure of the process shutdown valves should not lead to overpressure of the flare system (NORSOK S-001, 2008).

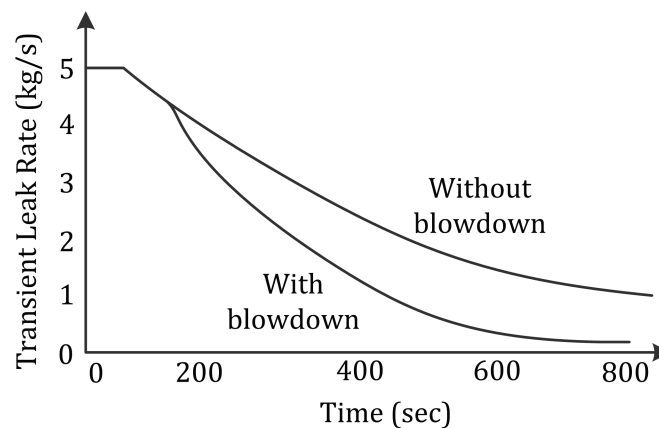


Figure 4.1: Example of time based development of a leak rate, with and without blowdown

#### 4.1.4 Firewater System

Purpose of the firewater (firefighting) system (NORSOK S-001, 2008, p. 54):

- Provide quick and reliable means for fighting fires and mitigate explosion effects

The final elements of the firewater system are usually either deluge or sprinkle valves, where deluge are often used in process areas. In addition, a foam system can be part of the firewater system.

After the outbreak of fire, a positive effect can be achieved by the firewater system; cooling of equipment, controlling the flames, and reducing the heat loads (Hankinson & Lowesmith, 2004). In some scenarios, the effect of the firewater system is small or non-present (e.g. objects impacted by a natural gas jet) (Hankinson & Lowesmith, 2004). Conflicting evidences prevail about the effect of the firewater system on the ignition probability, previous to a fire. This stated both by Spouge (1999) and the HSE (2009a). The system might increase the ignition probability, by causing sparks due to static or shorting of electrical equipment (Spouge, 1999), but might also reduce the intensity of heat sources (e.g. hot surfaces) appearing as

ignition sources. The positive effect is more conspicuous when considering explosion probabilities (intensity). A reduction of explosion overpressure can be achieved (if activated upon gas detection), but the effectiveness is dependent on the module venting configuration (among other factors) (HSE, 2009a).

#### 4.1.5 Activation Sequence of the Safety Systems

NORSOK S-001 (2008) presents generic requirements to when the safety systems should be activated. The actions can depend on the area of detection, detection of gas or fire, alarm or confirmed hazard, and the voting of the detectors. Note that the ESD isolation and blowdown system is activated by a common ESD node. Both automatically and manually activated systems are used, depending on the installation. The specific activation strategy for an installation should be found in the fire and explosion strategy plan. A simplified summary of the activation strategy for the safety systems is presented in Table 4.1. How this is reflected in the ETA is described in Section 4.2.3. It is more complicated if the systems are activated manually, where the activation can take place at any time.

Table 4.1: Requirements for activation of the safety systems (NORSOK S-001, 2008)

Safety system	Gas detection	Fire detection
ESD isolation	Automatically activated	Automatically activated
Blowdown	Automatic activation should be evaluated, or else manual activation is required	Automatically activated (manual on some old installations)
Firewater	If mitigating effects on explosion	Automatically activated

An ESD isolation should be activated both during gas and fire detection. Automatic depressurization is not required, but should be evaluated as a mean to avoid the use of passive fire protections (NORSOK S-001, 2008). The blowdown systems are on some older platforms initiated manually. In case of manual blowdown, the time from gas detection to activation of blowdown can be substantial. The initiation might even be after the occurrence of fire. In some scenarios, the positive effects of blowdown on ignition probabilities might thus not be present. Where effective for explosion mitigation, the firewater systems should be automatically activated upon gas detection (NORSOK S-001, 2008, p. 57). Otherwise, the system should be automatically activated upon fire detection.

## 4.2 Event Tree Analysis in Quantitative Risk Analysis

### 4.2.1 Modeling Accident Scenarios

Accidental event development on offshore installations are some of the most difficult to analyze (Vinnem, 2007). A variety of methods which can be used to model the accident scenarios are:

- Event tree analysis
- Event sequence diagrams
- Cause-consequence analysis
- Consequence analysis methods

Refer Rausand (2011, Chapter 11) for additional reading about the methods. ETA is widely used within QRA as a systematic approach, to calculate the frequency of the various consequence classes. The consequence classes are defined based on the specific analysis, and directly related to the initial event. The accident scenario modeling can be used to estimate the risk, in terms of the risk measures (presented in Section 3.3). The method of ETA is far from flawless, which is further discussed in the chapter.

### 4.2.2 Event Tree Analysis and Supporting Tools

As carried out by Scandpower, modeling of process accidents is mainly constructed around ETA (see Section 5.1 for an example of a process accident event tree). The preferred software is RiskSpectrum<sup>11</sup>, which has incorporated the ability to use fault tree analysis (FTA) as input to the pivotal events. Note that a pivotal event is also known as branch question or node. A consequence matrix is an add-on to RiskSpectrum. The consequence matrix is similar to an Excel spreadsheet, but is integrated closely to the event trees. The matrix features the ability for a systematic assigning of the consequences, for the various sequences in the event trees. For process accidents, the consequences are determined in terms of fatalities.

Outputs from several additional tools are used as input to RiskSpectrum. Figure 4.2 shows a coarsely illustrated process of a QRA, with emphasis on the tools utilized. Examples of outputs used in the event trees are leak frequencies, safety systems' reliabilities, and ignition and explosion probabilities. The use of additional tools involves additional limitations, assumptions, and non-transparent transformation of data. This can introduce uncertainties, not handled properly when later used by the event trees. The process becomes more fragmented,

---

<sup>11</sup> RiskSpectrum has the ability to assign the probabilities to the pivotal events with uncertainty distributions

and the overview easily lost. Several inputs can be fed into a tool, whereas only one output to the ETA is produced. A single ignition probability can be based on input from gas dispersion analyses, reliability of the safety systems, ignition source control, and so on. A lot of the information is thus “lost” when that output is later fed into the event tree as a pivotal event probability (discussed in Section 5.4.1.1). At the same time, merging all the tools into a single software program could make the software too complicated. A load of bloated features is not always beneficial. This is not practically achievable either. There is no single tool able to consider all aspects, where the software/tools are often state-of-the-art in their respective disciplines. The more automatic and comprehensive a software program becomes, the less does the user understand.

An argument for this approach is to incorporate the necessary aspects needed to conceive a more detailed risk analysis. The amount of information can be large and inadequately processed without the use of external tools and the calculations powers of computers.

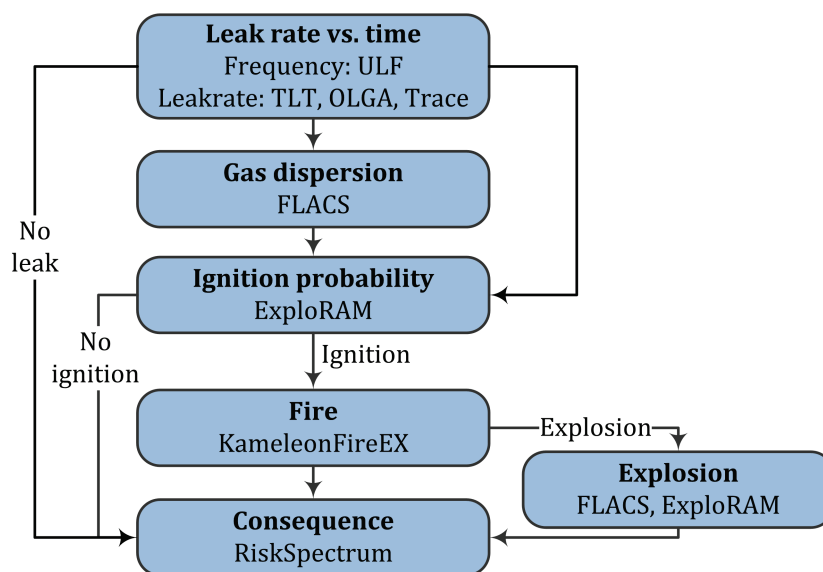


Figure 4.2: Flow diagram of modeling process accidents and supporting tools/software<sup>12</sup>

### 4.2.3 Sequence Modeling of the Safety Systems

Modeling the activation sequence of barriers is an important and difficult task. Accordance between the sequence and the time the events occur in the accident scenario is crucial (Rausand, 2011). Some challenges with sequence modeling in event trees are (Vinnem, 2007, p. 175):

<sup>12</sup> Modification of a figure from Scandpower’s intranet

- Encompassing the right sequence as it is normally highly time dependent
- Escalation involves complex interactions between different processes and different equipment
- Human intervention may have extensive effects on the development of accidents
- Small differences in circumstances may lead to vastly different end events
- ETA is static, and usually not suitable to handle the dynamics of detailed accident sequences

The same barrier might be activated in several pathways, which is described in Section 4.1.5. The pivotal events are conditional probabilities, where the probabilities are based on the previous events. Having the wrong sequence, or omitting parts of it, results in a wrong foundation when the conditional probabilities are determined. Consider the ignition, explosion, and escalation probabilities. The activation sequence of the safety systems in the event can have a great impact these probabilities. Omitting or giving wrong credibility to a system can make these probabilities either too high or too low. If initiated too late, the effect (purpose) of a safety system can be ceased. Consider the blowdown system during a process accident, which can be activated automatically upon either gas or fire detection, in addition to manually at any point of time. How the sequence of the accident unfolds, can be influenced by when the blowdown is activated. An early activation is likely to reduce the ignition and explosion probabilities, whereas the positive effect is reduced, if activated after the ignition occurs.

#### **4.2.4 Event Tree Analysis in Offshore Compared to Nuclear**

ETA was introduced with the WASH-1400 report (Rasmussen, 1975), a study aimed towards the nuclear power industry. The event tree approach has later been used and adapted to several industries, and the suitability can be questioned when used within the oil and gas industry. The equivalent to a QRA is in the nuclear power industry called a probabilistic risk assessment (PRA), with an overall aim of estimating the probabilities and severity of radiological consequences. The focus of PRA has been to prevent radiological consequences at all costs, focusing more on fault trees, with less focus on event trees. The emphasis has been operational safety, whereas the offshore QRA has been focused on the consequences and the long term risk. As an effect, the use of importance measures is more applicable in the nuclear industry to identify the important safety systems, compared to offshore.

The use of event trees in offshore application is challenging, due to the many different consequences and severity of each consequence. When used for process accidents on offshore installations, the consequences of a fire are within a wide spectrum of outcomes. Many



unpredictable scenarios can occur, and there are unlimited possibilities for fires to propagate. The QRA can thus not be used for operational risks in the same way as for the nuclear industry. By changing the status of a safety system, a new FAR can be calculated, but how can this be used to assess the current risk level? The FAR is an average of a range of different consequences; it is not suitable to use such an average as a presentation of the real time risk picture.

### 4.3 Detailed Representation of a Process Accident

Figure 4.3 (refer Appendix C.3 for a larger version) is a possible highly detailed event tree, for a process accident. The figure only shows a single leak scenario, where an event tree has to be modeled for each like rate. The number of event trees is thus dependent on the discretization of the leak rate. The standard hydrocarbon leak frequency (SHLF) model, used by Scandpower, divides the leak rates into 4 leak categories (see Table 5.1). Note that the level of detail is greatly limited by the static nature of the ETA. Human interactions are thus left out (discussed in Section 0 and 4.5). Such factors can be complex and difficult to explicitly incorporate adequately in the event trees. Human interventions might occur at almost any given time, and the amount possible actions are high and unpredictable during special working conditions.

As the present practice in Scandpower, only strong explosions are considered in the event trees, disregarding smaller explosions (these are considered as fires). Even though the explosion force can be described with a continuous distribution, explosions are treated in the way as the leak frequencies. To include several types of explosions and increasing the level of detail, the pivotal event of explosion can be split into multiple branches. This is not performed in Figure 4.3, it can be observed that the number of end events is huge, and the event tree would be far more complicated if additional categorization of explosion was done. A strong explosion is here defined as an explosion with pressure exceeding the design pressure (e.g. of firewalls).

Another challenge is modeling of the ESD isolation and blowdown valves. To gain a high level of detail, each significant valve should be modeled as a pivotal event, where the end event is dependent on the combination of valves failing. The leak rate, affecting the ignition probability, is dependent on the number of failed valves, the size of the respective pipe segment (thus volume of hydrocarbons), the location of valves, and so on. A simplified approach is to only consider critical failures. Even with the simplified approach, the detailed event tree is comprehensive. This can be observed in Figure 4.3. Even though the detailed event tree is simplified to an extent, the number of end events is still 285. A tremendous effort is required to determine the contribution from all events. This shows how comprehensive an event tree can

be. Simplifications must thus be used. A discussion about the practicability regarding the level of detail of an event tree is discussed in Section 6.1.2.

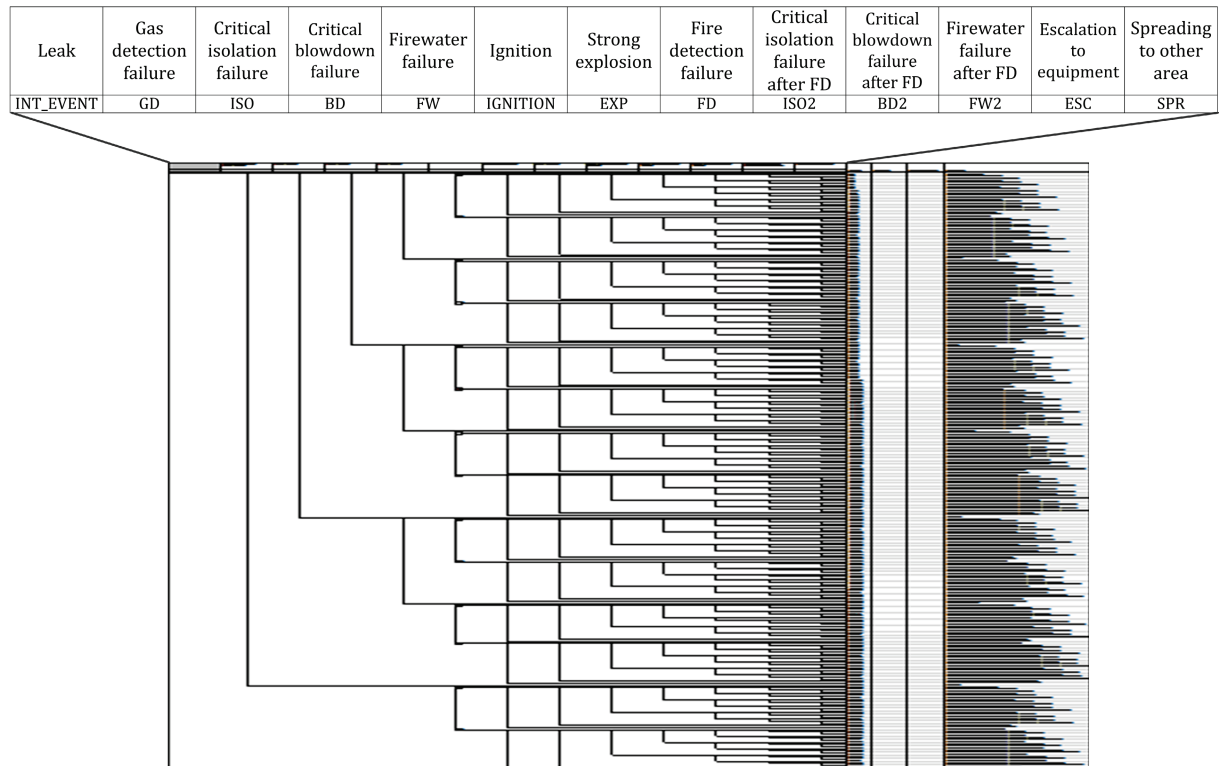


Figure 4.3: High detailed event tree of process accident

## 4.4 Reliability Analysis

The offshore industry has used extensive resources on safety systems, with considerable capacity and redundancy. Still, the availability of the system during an incident cannot be assured at all times. To predict the reliability of a system, a reliability analysis can be used. Reliability analysis can be divided into (Rausand & Høyland, 2004):

- Hardware reliability
- Software reliability
- Human reliability

Industrial accidents indicate that the performance of complex sociotechnical system is dependent on the interaction of technical, human, social, organizational, managerial, and environmental elements (Schönbeck, Rausand, & Rouvroye, 2010, p. 311). All three types of reliability analysis can (and should) be applied as input to a QRA, but the level of detail and

usefulness are often restricted by resources. Safety systems consist often of hardware parts, and controlled by computers (or programmable logics), which calls for the need of both hardware and software reliability analysis. Human reliability might be forgotten, but investigations indicate that nearly all incidents are initiated or exacerbated by human errors (Spouge, 1999). The blame on humans might be unjust. Some failures were initially due to hardware failures, but unfortunately worsened by human errors. When considering process accidents, the most evident and easiest (but far from easy) might be the hardware reliability analysis of the safety systems.

Many methods can be applied when reliability analyses are performed, some of the relevant methods related to QRAs are (refer Spouge, 1999, for a brief introduction to the various methods):

- Failure mode, effects and criticality analysis (FMECA)
- Fault tree analysis
- Event tree analysis
- Reliability simulation (Monte Carlo simulation)
- Human reliability analysis (HRA)

The methods have their strengths and weaknesses. Their suitability is dependent on the field of application, and the methods can be used to supplement one another. When for example considering hardware reliability, fault trees are often used, which can be supplemented with outputs from FMECA, or human error probabilities from HRA.

A challenge with the methods is the input data, referring to the uncertainties related to data estimation or collection (Section 2.2.1). There are several sources to reliability data<sup>13</sup>. As earlier discussed, a trade-off between having plant specific data and a sufficient amount of data, in order to obtain statistically significant failure rates, must be made. The confidence to the data applied can be questioned, and a discussion about the uncertainties of the reliability data can be useful.

## 4.5 Hardware Reliability

Safety instrumented systems are used to provide a specific risk-reduction, but unrealistic failure rates can lead to unsafe comfort. A philosophy is to calculate a risk-reduction, which reflects the

---

<sup>13</sup> Examples are OREDA [[www.oreda.com](http://www.oreda.com)], EXIDA [[www.exida.com](http://www.exida.com)], PDS Data handbook [[www.sintef.no/pds](http://www.sintef.no/pds)], and RNNP [[www.ptil.no/risikonivaa-rnnp/category20.html](http://www.ptil.no/risikonivaa-rnnp/category20.html)]

actual risk-reduction experienced in the operational phase (Hauge, Lundteigen, Hokstad, & Håbrekke, 2009). Another philosophy, by IEC 61508 (2010), is only concerned with random hardware failures when predicting the failure rates. Systematic failures are then handled separately and qualitatively. The latter approach will inevitably lead to lower failure rates. This can be preferred by some manufacturers, claiming a specification appearing better on paper. Failure rates for systematic failures are often hard to predict, depending on the particular application (Hauge, et al., 2009). Some manufacturers convey the responsibility to the operator, claiming no influence to the systematic failure introduced in operating phase.

IEC 61508 (2010, p. 23) suggest two approaches regarding hardware safety integrity architectural constraints, based on<sup>14</sup>:

1. Hardware fault tolerance and safe failure fraction concepts
2. Component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels

A problem is exaggerated performance claimed by the manufacturers (Summers, 2008). Many manufacturers provided in-service and accelerated test failure data prior to the release of IEC 61508 (Summers, 2008). After the approval of IEC 61508, an increase of product approval was based on a shelf-state analysis with seemingly perfect operating environment conditions, to calculate the safe failure fraction. To overcome this, a change was made in the present version of IEC 61508: "Failure rates used for quantifying the effect of random hardware failures and calculating safe failure fraction or diagnostic coverage shall take into account the specified operating conditions" (IEC 61508, 2010, part 2, p. 32). Angela Summers (Summers, 2008) did criticize the approach of IEC 61508. The standard gave the manufacturers opportunities of imprecise prediction of equipment- and analysis boundaries, incorrect failure classification or too optimistic predictions of the diagnostic coverage factor. Note that at least some of the topics are covered by the present version of the IEC 61508. For example concerning manipulation of diagnostic safe failure fraction, by using undefined failure classifications (e.g. no-effect), categorized as safe failures to increase the safe failure fraction. It is now stated that no-effect and no-part failures shall not play any part in the calculation of the diagnostic coverage factor, or the safe failure fraction (IEC 61508, 2010, part 2, p.71).

Concerning the second approach, regarding hardware integrity, the reliability data should be (IEC 61508, 2010, part 2, p. 31):

---

<sup>14</sup> Denoted route 1<sub>H</sub> and route 2<sub>H</sub> in the IEC 61508 standard

- Based on field feedback for elements in use in a similar application and environment
- Based on data collected in accordance with international standards (e.g., IEC 60300-3-2 or ISO 14224)
- Evaluated according to:
  - o The amount of field feedback
  - o The exercise of expert judgment
  - o The undertaking of specific tests (where needed)

There are some challenges related to this approach. When the data is based on field feedback, then the manufacturers are dependent on feedback from the operators. Recording of data can be a comprehensive task. The recorded data might be insufficient, due to operators not being dedicated to record and share the failure data. Only a portion of the failures might be reported back to the manufacturer. Some operators might only return information during the period of warranty, or omitting small failures easily fixed by them self. Due to the lack of feedback, the product might be considered by the manufacturer to have experienced fewer failures compared to the actual number. This can lead to optimistic failure rates.

Unless there is consensus among the international standards on how the data collection should be performed, inconsistency can occur. Possible topics are: failure classification, which failures are covered or not, information needed, comparable application and environment, how to perform the collection, and how to treat human errors.

## 4.6 Human Reliability Analysis

A common understanding governs about the effect human error has on safety, but the estimate of the contribution to system failures vary (Schönbeck, et al., 2010). Several issues are related to humans: the perceptual, physical, and mental capabilities; the interactions of individuals with their jobs and the working environments; the influence of equipment and system design on human performance; and the organizational characteristics that influence safety related behavior at work (Skogdalen & Vinnem, 2011, p. 470). It is difficult to anticipate human reactions, especially in the incident of an accident. Human performance can be important in QRA. Significant improvements can be made through identifying areas of poor performance, and implementing the needed measures (Spouge, 1999). A large proportion of the benefits from a HRA, and QRA likewise, is lost if they are executed for quantitative purposes only.

The three main inputs from HRA, that might be used in a QRA are (Spouge, 1999, p.81):

- Hazard identification
- Incident development probabilities
- Escape and evacuation success probabilities

The task of identifying hazards related to human error (identification, description, and analysis of possible erroneous actions) can be denoted as *human error (mode) identification* (Rausand, 2011). The analysis must be carried out, tailored for the specific installation. Possible methods are action error mode analysis (AEMA), human HAZOP, and systematic human error reduction and prediction approach (SHERPA) (refer Rausand, 2011, Section 13.3, for additional reading).

When the hazardous tasks have been identified, a decomposition approach can be used to determine the success rate. The operator's ability to perform a given task successfully is assigned a human error rate (Spouge, 1999), also possibly a human error probability (HEP). This can be incorporated in a reliability method (e.g. fault tree or event tree), and the human error rate can be considered as a constant failure rate. It can be controversial to put a failure rate on human activities. The subsequent sequence of an accident following an error is not modeled accurately, as a consequence of treating human errors similar to hardware failures (Acosta & Siu, 1993). Still, there has been an attempt to model the incident development probabilities, in terms of human error rates. HRA methods may be classified as either first and second generation (Rausand, 2011). The first generation was developed to provide input to quantitative risk analyses, whereas the second attempted to consider the context and errors of commission in human error prediction (Rausand, 2011, cited in HSE, 2009b). The first generation is usually easier to implement in risk analyses. Both the technique for human error rate prediction (THERP) and the human error assessment and reduction technique (HEART) stem from the first generation. THERP was earlier developed for the nuclear industry, but has later been widely used within the offshore industry. A question is how suitable the method is for this area of application. The practical use is discussed in Section 6.2.2.

The success of escape and evacuation depend on how the personnel act in the presence of hazards (e.g. incorrect release of life boats), stressing the need for escape and evacuation drills.

## 4.7 Integrating Reliability Analysis with Event Tree Analysis

### 4.7.1 Integrating Fault Trees

Reliability analysis can be used as input to the ETA. Regarding the safety systems, fault trees can be used to calculate the reliability of the system. The reliability is then applied as failure probabilities for the pivotal events. Figure 4.4 illustrates the interface.

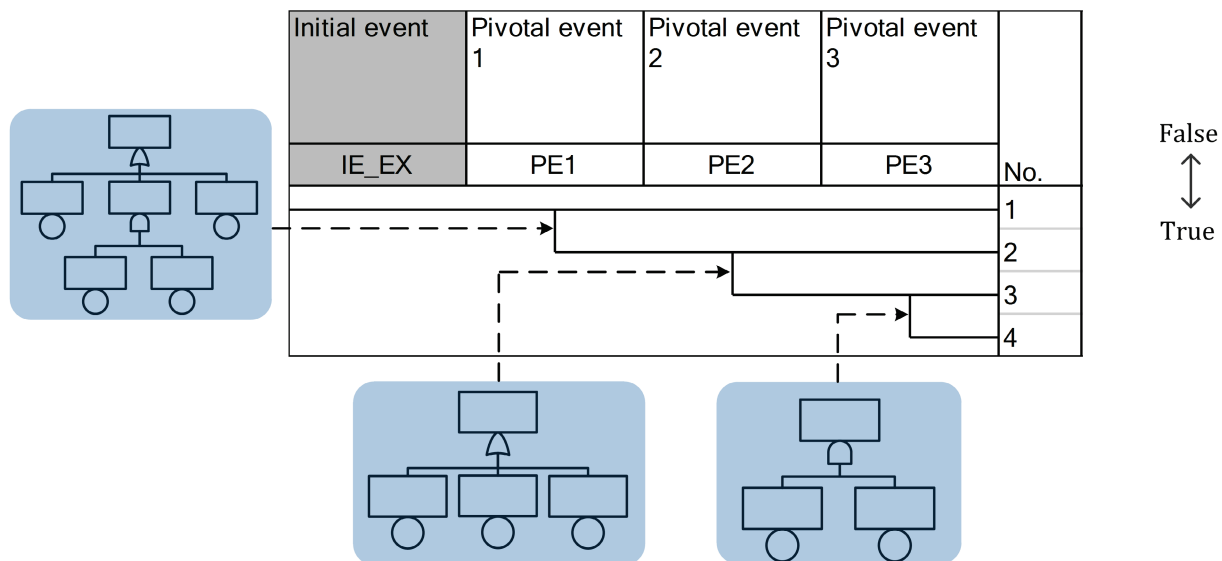


Figure 4.4: Fault trees as input to an event tree

### 4.7.2 Integrating Human Reliability Analysis

The development of an accident can be altered by human intervention, which is difficult to incorporate in a static event tree. The intervention might occur at any given time, with both a negative and positive effect. There can be situations where the operator shuts down a correct activation of a safety system, due to misinterpretation of what thought to be a spurious alarm. Other intervention, non-related to the safety systems can also take place. Examples are manual firefighting, or special activities (e.g. maintenance), which changes the consequences or development of an accident sequence. Consider the approach of the first generation HRA methods, and a process accident with the need of manual activation of the safety systems. Probabilistic value can be determined for the inability of the operator to act correctly. This can then be incorporated in a fault tree, along with the respective safety function, as shown in Figure 4.5. The dynamic response after an error is not treated explicitly with this approach.

The basic event "HUMAN\_ERROR", can for a process accident be the need for the operator to manually activate the blowdown system. This is discussed in detail in Section 6.2.2.

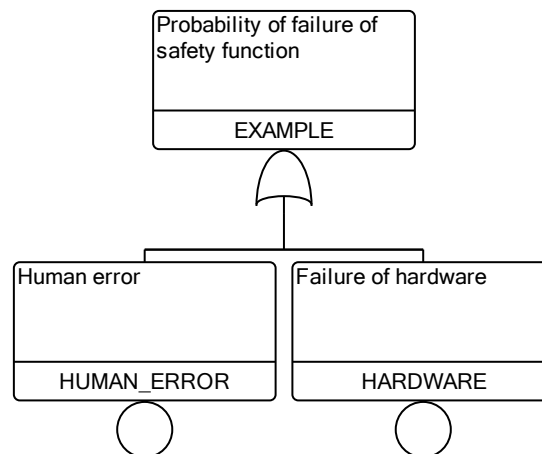


Figure 4.5: Example of fault tree with human error

## 4.8 Vulnerability Analysis

Vulnerability analysis is in this context related to the robustness of a safety system (hardware components). A qualitative vulnerability analysis can be performed for the safety systems (as a standalone analysis), to evaluate the vulnerability. The purpose of a vulnerability analysis is to study the ability of a barrier, to withstand a design accidental load (DAL). It can be distinguished between the design and operational phase. The chosen systems during the design phase should be able to withstand the DAL. A system can though fail to maintain its integrity in the operational phase, due to for example deterioration or inadequate maintenance. Since the pivotal events are conditional probabilities, the previous events (mainly explosion and fire for process accidents) which affect the reliability of the safety systems should be considered. A vulnerability analysis, performed during the operational phase, can indicate weaknesses. The weaknesses should be reflected by the reliability data used for the safety systems.

Some of the significant (possible) damages to the safety systems, subject for vulnerability analysis, are discussed in Section 4.8.1-4.8.3 (Spouge, 1999, is used as reference for those sections).

### 4.8.1 ESD isolation

- Explosion distorting the valve and preventing it from sealing
- Prolonged fire affecting the valves

The consequence of both incidents could lead to additional leakage. Such failure can allow hydrocarbons from adjacent segments to merge with an existing fire.



### 4.8.2 Blowdown

- Explosion jamming the blowdown valves or puncturing the piping
- Prolonged fire affecting the blowdown line

Either of the two can introduce additional leak points. If the leaks are ignited, a subsequent exposure of other pipes can occur, and propagate further.

### 4.8.3 Firewater

- Damage to the firewater pumps, their control system or power supply
- Explosion damage to the ring main and deluge heads
- Fire damage to the ring main and deluge heads (jet fire could be impinge on the deluge piping, but failure is unlikely if water is flowing through the pipes)

There have been attempts to prevent some of the scenarios. An example is the requirement to route the firewater ring main outside the areas of exposure, to prevent explosion damage (NORSOK S-001, 2008). Explosion can still be a hazard, destroying for example the deluge nozzle, or other parts (e.g. pipes) of the deluge system.

### 4.8.4 Vulnerability Analysis in Event Trees

Vulnerability can be integrated into ETA by changing the reliability of the affected components modeled in the fault trees. It is also possible to use a probabilistic approach, with a basic event in the fault tree (in an OR-gate with the TOP event of the safety system failure), representing a probability of having a certain load leading to failure of the safety system. The reliability depends on the possible previous event, for example explosion or fire. The reliability must also be considered in relation to the initial event. A large leak is more likely to have a more severe fire (possibly explosion) compared to smaller leaks. Several sets of fault trees with different failure rates can be used to calculate the probabilities of the pivotal events. A challenge is to quantify the exact impact an accidental load has on the reliability of a safety system.

Plant specific reliability data are at times extracted from the historical data of an installation. This approach might give a representative picture of the equipment during normal operation, but does not take the vulnerability from accident loads into consideration. Leaks from process equipment are inevitably relatively frequent events (Spouge, 1999), but larger accidents, causing explosion and escalated fires are more seldom. As they are seldom observed, the effects of these events are rarely represented in the historical reliability data. The approach implies that the data do not take the previous events of explosion or fire into consideration.

## 4.9 Dependencies in Event Trees

A challenge with event trees is dependency. This is also Related problems are (Rausand, 2011, p.346):

- Same components present in two or more barriers
- Environmental dependencies causing several “independent” barriers to fail
- Functional dependencies on other systems, utilities, components, or operator actions
- Dependencies between hazardous event and the pivotal events
- Dependencies between pivotal events

When using FTA as input to an event tree, some basic events can be shared by several fault and/or event trees. Consider an ESD isolation and a blowdown system, activated in the respective sequence. Both systems can be connected to the same ESD node (logic), and modeled using fault trees. If the ESD isolation failure is due to an ESD node failure, then the subsequent closure of the blowdown valves is assured to fail. When the safety systems have shared components, the conditional probability of a safety system failing is based on the outcome of the previous system. This is especially important if the shared component is critical, such as the ESD node. Note that the dependency is not limited to components, but can be any kind of basic event (e.g. human error). The frequency of the end events, now denoted  $\text{Freq}(\text{EE})$ , in an event tree can be calculated with a traditional approach:

$$\text{Freq}(\text{EE}) = \text{Freq}(\text{IE}) \cdot \Pr(\text{PE}_1/\text{PE}_1^*) \cdot \Pr(\text{PE}_2/\text{PE}_2^*) \cdot \dots \cdot \Pr(\text{PE}_n/\text{PE}_n^*) \quad (4.1)$$

The frequency of the initial event is denoted  $\text{Freq}(\text{IE})$ , and the probability of the pivotal event  $\Pr(\text{PE}_i/\text{PE}_i^*)$ . Note that the slash is a substitute for “or”, indicating either the probability of  $\text{PE}_i$  or  $\text{PE}_i^*$ . Though not explicitly expressed,  $\Pr(\text{PE}_i/\text{PE}_i^*)$  is a conditional probability.

When using RiskSpectrum, a different approach is used when the frequencies of the end events are calculated. How RiskSpectrum treats dependencies is related to the approach used to calculate the end events frequency. RiskSpectrum started mainly as a fault tree software program, and adapted the fault tree method to calculate the frequencies of the event trees. This approach seems to be more competent when handling dependencies. Following is an explanation of how RiskSpectrum calculates the frequencies of a consequence, which also is the key to how dependencies are handled. The approach requires a tremendous effort if it should be performed by hand.

### 4.9.1 Sequence Fault Trees

A sequence is the path which leads to a specific and distinct end event. Note that several end events can be of the same consequence type, but still distinguished by different paths. Figure 4.6 illustrates an event tree with “OK” occurring three times, all with different sequences.

Initial event	Pivotal event 1	Pivotal event 2	Pivotal event 3	Pivotal event 4			
IE_EX	PE1	PE2	PE3	PE4	No.	Freq.	Conseq.
False ↑↓ True					1		NOT_OK
					2		OK_
					3		NOT_OK
					4		OK_
					5		OK_

Figure 4.6: Example of event tree 1

Consider the consequence “NOT\_OK” from Figure 4.6, with sequence number 3. To end up at the third end event, the only possible outcome is the first and second pivotal event (PE1 and PE2) being false, and the third and fourth (PE3 and PE4) true. This specific sequence can be converted into an equivalent fault tree structure, illustrated by Figure 4.7 (Scandpower, 2008).

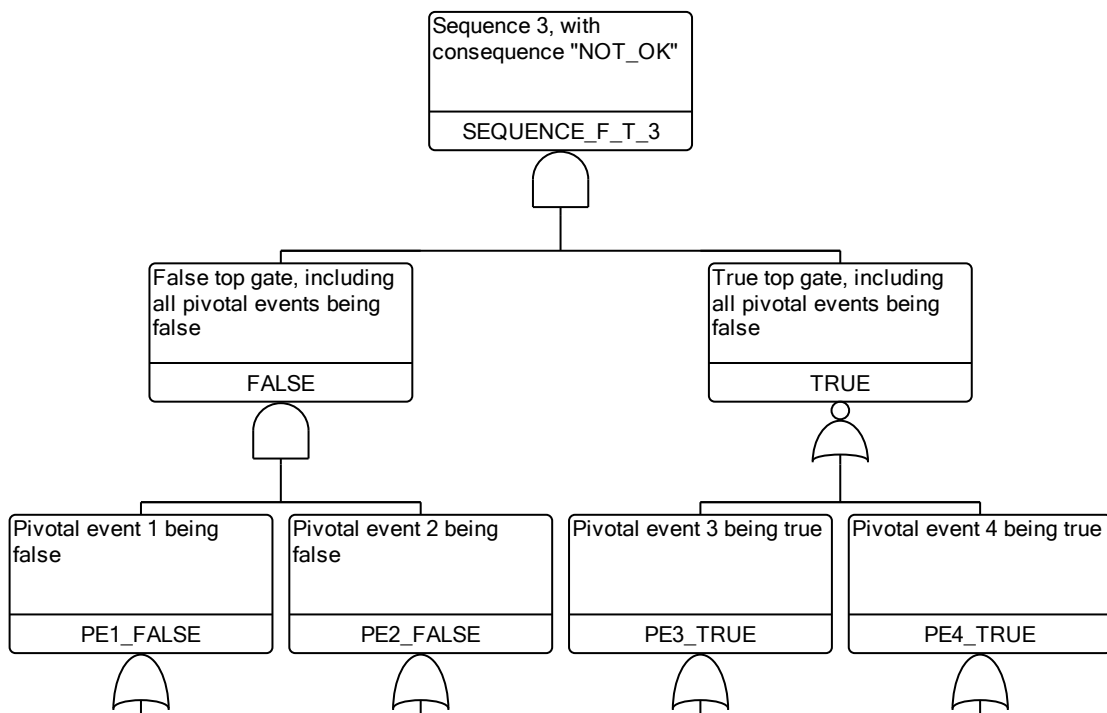


Figure 4.7: Example of sequence fault tree

The FALSE-gate is an AND-gate with all the “false” pivotal events beneath (pivotal event 1 and 2), and corresponding for the TRUE top gate (pivotal event 3 and 4). The number of gates below the TRUE or FALSE-gate is dependent on the number of pivotal events, along with their status as either true or false. If the “NOT\_OK” consequence from sequence number 1 was the objective, then there would be four gates below the FALSE-gate, and none below TRUE. The type gate on the lowest level is dependent on the input of the pivotal event. If a fault tree is used as input, the TOP event of that tree (e.g. failure of blowdown system) would be replaced with for example the PE1\_FALSE-gate. The simplest input is a basic event, representing a probability of the pivotal event being false. See Appendix C.1 for description of the symbols used in the fault tree.

### 4.9.2 Consequence Fault Tree

To take all sequences leading to the wanted consequence into consideration, a consequence fault tree is established. The consequence fault tree starts with an AND-gate, having the initial event of the event tree as an input, in addition to an OR-gate. The OR-gate has all relevant sequence fault trees, resulting in the specified consequence as input. This is illustrated in Figure 4.8, where the “NOT\_OK” consequence can be found two places, at first and third sequence.

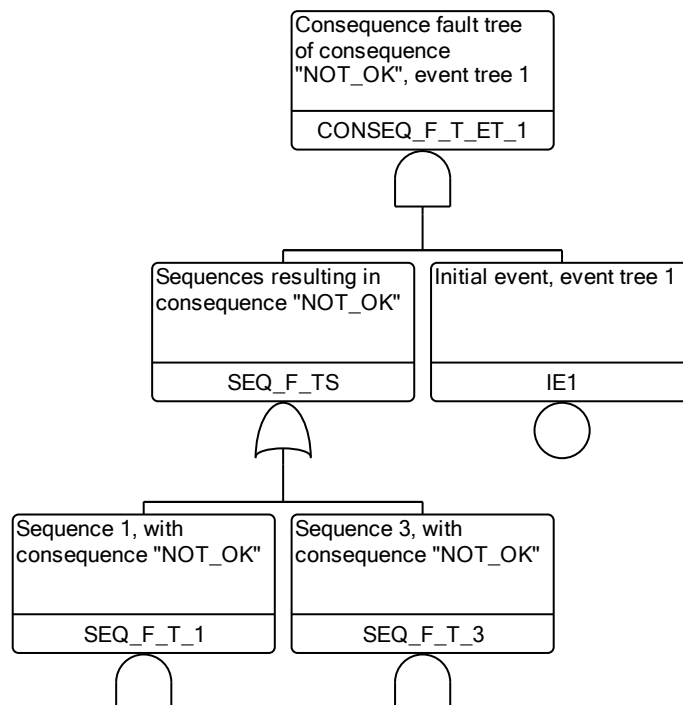


Figure 4.8: Example of consequence fault tree, for event tree 1

### 4.9.3 Master Fault Tree

If the consequence is found in more than one event tree, a master fault tree can be constructed as an OR-gate. The gate will have all relevant event trees with the specified consequence as input. Figure 4.9 shows a master fault tree, finding the frequency of the consequence "NOT\_OK", which can be found in for example two different event trees, 1 and 2. Extra event trees can be added if the consequence is found in additional trees. See Appendix C.2 for an example of a master fault tree, including consequence and sequence fault trees.

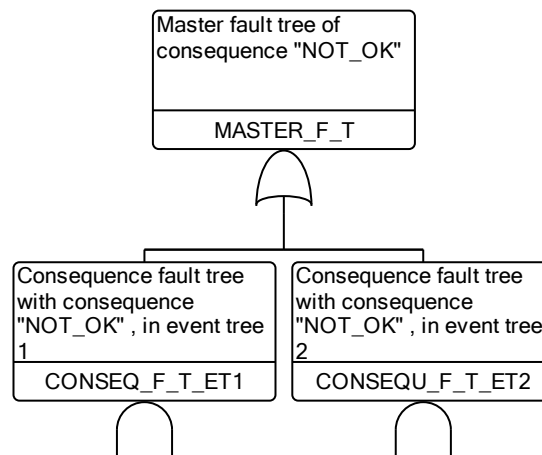


Figure 4.9: Example of a master fault tree

### 4.9.4 The Ability to Handle Dependencies

After the conversion from event trees to fault trees, using RiskSpectrum, the ability to handle dependencies is then decided by the fault trees' ability. The TOP event of a consequence fault tree equals the frequency of a consequence. This frequency can be a point-estimate calculated by using minimal cut sets (a common approach when using fault trees), which handles dependencies decently. When using this approach, independency between all basic events in a minimal cut set is assumed, this is generally not the case. A basic event is often a member of several minimal cut sets, which is often acceptable when using a conservative formula, called upper bound approximation (refer Rausand, 2011, for additional reading about the approach of minimal cut sets). The fault tree is able to handle both dependencies within and between event trees, as long as the dependent basic events are modeled in the same fault tree, which is always the case during the conversion from event tree to fault tree.

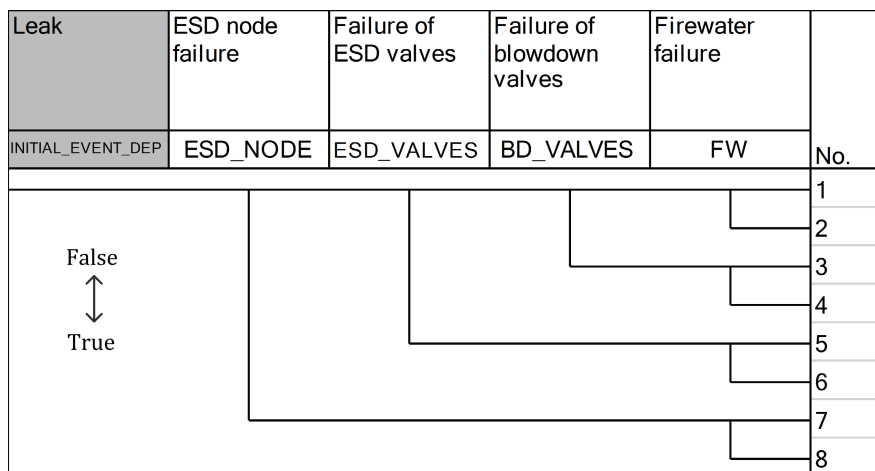


Figure 4.10: Example of extracted dependent component from fault tree to event tree

Another approach to handle dependencies is to extract the components from the fault tree, and introduce them as a pivotal event. This approach is mostly relevant if the component is of high importance, and needs to be modeled explicitly. Note that the event tree becomes more complicated with many pivotal events. This approach can be used both for the traditional calculation method, and the RiskSpectrum method. Figure 4.10 shows how this is done for an ESD node, which is shared by an ESD isolation and a blowdown system.

# Chapter 5

## Case Study: Safety Functions and Event Tree Analysis – Process Accidents

### 5.1 Case Study Presentation

Three QRA for different offshore installation performed by Scandpower (installation A, B, and C) have been selected as basis for the case study. Only process accidents are treated, focusing on the modeling of safety systems and how they impact the risk picture. The selected cases are performed by different analysts, which increase the differences between the analyses, due to subjective assumptions and assessments. The consideration of consequences of escalation is particularly difficult, which is highly judgmental and difficult to generalize (Spouge, 1999). The analyses are separated by several years, where the “best practice” has changed from the oldest to newest analysis.

Table 5.1: Leak categories with respective leak rates

Category	Leak rate [kg/s]
Small	0.1 – 1
Medium	1 – 10
Major	10 – 30
Large	30 – 300 000

For process accidents, the initial vent is a hydrocarbon leak. The initial events are categorized according to leak sizes, as shown in Table 5.1. Note that the number of initial events, and thus the number of event tree, increases with the number of leak categories and segments ( $\# \text{ initial events} = \# \text{ leak categories} \cdot \# \text{ segments}$ ). The number of events trees for each of the installations was in the range of thousands.

Figures 5.1, 5.2, and 5.3 present the event trees of process accidents on installation A, B, and C, respectively. The event trees<sup>15</sup> are to a degree simplified, where some of the pivotal events have additional events implicitly implemented in the probabilities. For example, the probabilities of ignition and explosion, dependent on the failure or success of the safety systems. They are rather considered by other tools (discussed in Section 4.1), but not explicitly expressed in the events trees.

Leak	Ignition	Strong explosion	Critical ESD isolation failure	Blowdown failure	Firewater failure	Escalation to equipment within area	Spreading to other area	No.	Freq.	Conseq.
INITIAL_EVENT_A	IGNITION	EXP	ISO	BD	FW	ESC	SPR			
								1		OK_
								2		FII
								3		FEI
								4		FSI
								5		FII
								6		FEI
								7		FSI
								8		FII
								9		FEI
								10		FSI
								11		FII
								12		FEI
								13		FSI
								14		FII
								15		FEI
								16		FSI
								17		FII
								18		FEI
								19		FSI
								20		EXI
								21		FIE
								22		FEE
								23		FSE
								24		FIE
								25		FSE
								26		FSE
								27		FIE
								28		FEE
								29		FSE
								30		FIE
								31		FEE
								32		FSE
								33		FIE
								34		FEE
								35		FSE
								36		FIE
								37		FEE
								38		FSE
								39		EXE

Figure 5.1: Event tree of a process accident on installation A

<sup>15</sup> It is recommended that each pivotal event is formulated as a “negative” statement, with upper branch as “true” and lower as “false”, arranging the most serious accidents scenarios upwards in the event tree (Rausand, 2011), note that this is not done in RiskSpectrum.



The event trees of installation A and B are almost identical, whereas installation C differs a little. It is for installation A and B considered that the probability of having a simultaneous critical ESD isolation and blowdown failure is negligible. This assumption is not made for installation C. Here, the effect of the firewater system is now assumed negligible when ESD isolation and blowdown has failed. In addition, a pivotal event called “ESD node” is explicitly modeled for this installation. This can be similar to explicitly modeling the dependent failure of the ESD node for the ESD isolation and blowdown system, according to Section 4.9.4. The presented assumptions are observable in the events trees. The failures related to the safety systems are critical failures only. Some of the segments have for example ESD isolation valves preventing a relatively small volume of hydrocarbons. The failure of such valves is assumed less important and has a negligible contribution to the risk picture.

Leak	Ignition	Strong explosion	Critical ESD isolation failure	Blowdown failure	Firewater failure	Escalation to equipment within area	No.	Freq.	Conseq.
INITIAL_EVENT_B	IGNITION	EXP	ISO	BD	FW	ESC			
							1		OK_
							2		FII
							3		FEI
							4		FII
							5		FEE
							6		FIE
							7		FEI
							8		FII
							9		FEI
							10		FII
							11		FEI
							12		FII
							13		FEI
							14		EXI
							15		FIE
							16		FEE
							17		FIE
							18		FEE
							19		FIE
							20		FEE
							21		FIE
							22		FEE
							23		FIE
							24		FEE
							25		FIE
							26		FEE
							27		EXE

Figure 5.2: Event tree of a process accident on installation B

Note that two types of ignition are considered, no ignition, local ignition (ignited within the area where the leak was initiated), or external ignition (ignited outside the area when the

leak was initiated). Only strong explosions are considered, with severe consequences, neutralizing the effects from the safety systems. It is not explicitly distinguished between immediate and late ignition in the event tree. The consideration is done by ExploRAM, during the evaluation of strong explosions (strong explosions needs the buildup of a gas cloud).

Leak	Ignition	Strong explosion	ESD node failure	Critical ESD isolation failure	Blowdown failure	Firewater failure	Escalation to equipment within area			
INITIAL_EVENT_C	IGNITION	EXP	ESD_NODE	ISO	BD	FW	ESC	No.	Freq.	Conseq.
								1		OK_
								2		FII
								3		FEI
								4		FII
								5		FEI
								6		FII
								7		FEI
								8		FII
								9		FEI
								10		FII
								11		FEI
								12		FII
								13		FEI
								14		FEI
								15		FEX
								16		EXI
								17		FIE
								18		FEE
								19		FIE
								20		FEE
								21		FIE
								22		FEE
								23		FIE
								24		FEE
								25		FIE
								26		FEE
								27		FIE
								28		FEE
								29		FEE
								30		FEX
								31		EXE

Figure 5.3: Event tree of a process accident on installation C

Installation B is the only event tree containing the pivotal event of “spreading to other area”. The two other installations uses another approach, where the probability of escalation is treated by consequence matrixes instead (consequence matrix is described in Section 4.2.2). Based on the knowledge of the analyst (e.g. knowledge about the scenario or end event, the area and probability of personnel present, the impairment of MSFs), the consequences of each end event can be assigned, and PLL calculated. The consequence codes used are as follow:

- OK<sub>-</sub> – No ignition, environmental consequences only
- FII – Local fire due to internal ignition
- FIE – Local fire due to external ignition
- FEI – Escalated fire due to internal ignition
- FEE – Escalated fire due to external ignition
- FEX<sup>16</sup> – Escalated fire with failure of ESD node
- EXI – Explosion due to internal ignition
- EXE – Explosion due to external ignition

## 5.2 The Approach of the Sensitivity Analyses

The sensitivity analyses were performed by changing the failure probabilities to the safety systems to the far ends. Table 5.2 presents a summary of the sensitivity analyses performed, with reference to the respective sections. Base case denotes the original analysis, with original failure rates for the safety systems. “Failure probability 0/1” indicates the failure probability set for the systems listed under. Failure probability 0 implies a 100 % probability of functionality. Failure probability 1 indicates the opposite. The failure probability of the ESD node is *not* set to 1. The ESD node failure leads to failure of both the ESD isolation and the blowdown system, for *all* segments, which is considered to be catastrophic. Consequences considered for an ESD node is thus set high. To prevent the ESD node failure from dominating the risk picture, a 10 times higher failure rate is used, instead of failure probability 1.

Table 5.2: Summary of sensitivity analyses performed

Installation	Case	Parameters changed	FAR	MSF	Ignited event
A,B, C	All safety systems	Failure probability 0/1: - ESD isolation - Blowdown - Firewater  Failure rate x0/x10: - ESD node	Section 5.3.1	Section 5.3.2	Section 5.3.3
A,B, C	ESD Isolation	Failure probability 0/1: - ESD isolation	Section 5.3.4	Appendix B.1.1-B.1.4	Appendix B.1.1-B.1.4
A,B, C	Blowdown	Failure probability 0/1: - Blowdown			
A,B, C	Firewater	Failure probability 0/1: - Firewater			
C	ESD node	Failure rate x0/x10: - ESD node			

<sup>16</sup> Only applies for installation C

## 5.3 Results

### 5.3.1 Fatal Accident Rate

Tables 5.3, 5.4, and 5.5 present the summary of sensitivity analyses, regarding the effect of the safety systems on the FAR. A minimal (virtually identical) decrease of the FAR due to process accident can be observed when all safety systems are set to function (failure probability of 0). The original failure probabilities of the safety systems in the base case are relatively small, approximately in the range of 3-5 %. The gap between the original failure probabilities and a failure probability of 0 is thus small. This is reflected by a small change in the FAR values when comparing “base case” and “failure probability 0”. The gap between the “base case” and the “failure probability 1” will thus be larger. Note that the failure probabilities in the base case are unequal for the various installations. If a safety system has a failure probability of 5 % on installation A, but 10 % on B, then the installation A is likely to have smaller changes to the FAR when going from “base case” to “failure probability 0”. The findings will likely be opposite when moving from “base case” to “failure probability 1”.

Table 5.3: Sensitivity analysis of the safety systems, FAR, installation A

	Base case	Failure probability 0	% change from base case	Failure probability 1	% change from base case
<b>FAR</b>					
FAR due to process accidents	1.39	1.39	-0.05 %	1.45	4.29 %
<b>FAR distribution</b>					
FAR immediate	0.80	0.80	-0.10 %	0.84	5.72 %
FAR escape	0.39	0.39	-0.02 %	0.40	3.75 %
FAR evacuation	0.21	0.21	0.05 %	0.21	-0.12 %

Table 5.4: Sensitivity analysis of the safety systems, FAR, installation B

	Base case	Failure probability 0	% change from base case	Failure probability 1	% change from base case
<b>FAR</b>					
FAR due to process accidents	2.39	2.39	-0.09 %	2.42	0.93 %
<b>FAR distribution</b>					
FAR immediate	1.66	-0.08 %	1.69 %	1.26 %	1.66 %
FAR escape	0.39	-0.22 %	0.39 %	0.35 %	0.39 %
FAR evacuation	0.35	0.04 %	0.35 %	0.00 %	0.35 %

Table 5.5: Sensitivity analysis of the safety systems, FAR, installation C

	Base case	Failure probability 0	% change from base case	Failure probability 1	% change from base case
<b>FAR</b>					
FAR due to process accidents	0.48	0.46	-3.18 %	0.72	50.69 %
<b>FAR distribution</b>					
FAR immediate	0.35	0.35	0.12 %	0.35	0.12 %
FAR escape	0.05	0.05	-1.76 %	0.09	92.78 %
FAR evacuation	0.08	0.07	-18.60 %	0.28	250.10 %

### 5.3.2 Main Safety Functions

Tables 5.6, 5.7, and 5.8 present the impairment frequencies of the MSFs for installation A, B, and C, respectively. A small reduction of the impairment frequency, for all three installations, can be observed when all safety systems function (failure probability 0). The same trend was observed for the FAR values, which can have the same explanation (small difference for the failure probabilities when going from “base case” with 3-5 % to “failure probability 0”). A more significant increase can be observed for the impairment frequencies when the failure probabilities are set to 1. The degree of increase seems highest for installation C, subsequently A, and almost non-existing for installation B.

Table 5.6: Sensitivity analysis of the safety systems, impairment of MSFs, installation A

	Base case	Failure probability 0	% change from base case	Failure probability 1	% change from base case
<b>MSFs (impairment frequency due to fire)</b>					
Spreading of fire from Drilling and wellhead area to another main area	3.16E-05	3.09E-05	-2.10 %	4.99E-05	58.11 %
Spreading of fire from Lower process area to another main area	0	0	n/a	0	n/a
Spreading of fire from Upper process area to another main area	2.23E-04	2.14E-04	-4.24 %	3.11E-04	39.24 %
Escalation of fire within Drilling and wellhead area	1.54E-04	1.51E-04	-2.13 %	2.46E-04	59.71 %
Escalation of fire within Lower process area	6.54E-05	6.51E-05	-0.48 %	8.22E-05	25.64 %
Escalation of fire within Upper process area	2.32E-04	2.22E-04	-4.22 %	3.43E-04	47.69 %
Escape from Drilling and wellhead area	2.31E-04	2.31E-04	-0.02 %	2.41E-04	4.47 %
Escape from Lower process area	6.11E-05	6.11E-05	0.00 %	6.11E-05	0.00 %
Escape from Upper process area	9.73E-05	9.73E-05	0.03 %	9.73E-05	0.03 %

Table 5.7: Sensitivity analysis of the safety systems, impairment of MSFs, installation B

	Base case	Failure probability 0		Failure probability 1	
			% change from base case		% change from base case
<b>MSFs (impairment frequency due to heat loads)</b>					
Evacuation means (lifeboats on the west side)	3.38E-04	3.38E-04	-0.01 %	3.38E-04	0.01 %
Spreading of fire from Process area to another main area	1.18E-04	1.18E-04	-0.13 %	1.19E-04	1.00 %
Escape from drilling rig	1.64E-04	1.64E-04	-0.01 %	1.64E-04	0.01 %
Escape from drilling shaft South	3.38E-04	3.38E-04	-0.01 %	3.38E-04	0.01 %
<b>MSFs (impairment frequency due to smoke)</b>					
Evacuation means (lifeboats on the west side)	2.10E-04	2.10E-04	0.00 %	2.10E-04	0.00 %
Escape from drilling rig	9.83E-04	9.81E-04	-0.18 %	1.02E-03	3.33 %
Escape from drilling shaft South	2.26E-04	2.26E-04	-0.02 %	2.26E-04	0.00 %

Table 5.8: Sensitivity analysis of the safety systems, impairment of MSFs, installation C

	Base case	Failure probability 0		Failure probability 1	
			% change from base case		% change from base case
<b>MSFs (impairment frequency due to fire)</b>					
Spreading from process area	8.05E-05	7.58E-05	-5.73 %	2.10E-04	160.70 %
Escape from pontoon and columns	6.01E-05	5.88E-05	-2.30 %	1.14E-04	88.85 %
Escape from drilling area	9.62E-06	9.36E-06	-2.68 %	2.40E-05	149.62 %
Escape from utility area	1.07E-05	1.07E-05	-0.44 %	1.48E-05	37.99 %

### 5.3.3 Ignited Events

Consequences in the event trees are established as ignited events, ranging from “OK” to “explosion”, as presented in Section 5.1. The type of ignited event indicates how severe an incident is. A strong explosion has a higher potential of causing more damage, compared to a local fires (non-escalating fires). Both the FAR and the impairment frequencies of the MSFs are reflected by the distribution of the type of ignited events. Thus a high increase in explosion frequencies should result in a higher FAR and impairment frequencies of the MSFs.

Tables 5.9, 5.10, and 5.11 are results from the sensitivity analyses with focus on the ignited events. The frequencies of non-ignited events are constant for all installations, since the ignition probabilities are not altered (thus not presented in the tables). The frequency of an initial event in an event tree will always be equal to the sum of the frequencies of the various consequences. The sum is thus constant for all the installations, but the distribution is changed when altering the reliability of the safety systems. Increased reliability should shift the distribution in favor of the less severe consequences, resulting in a decrease of the severe

consequences (escalation and explosion), and accordingly an increase of local fires. An opposite distribution is expected when the reliability decreases.

Table 5.9: Sensitivity analysis of the safety systems, ignited events, installation A

	Base case	Failure probability 0		Failure probability 1	
	Frequency	Frequency	% change in frequency from base case	Frequency	% change in frequency from base case
<b>Ignited events (process fires)</b>					
Local fire due to internal ignition (FII)	1.66E-03	1.68E-03	0.88 %	1.43E-03	-14.01 %
Local fire due to external ignition (FIE)	7.92E-05	7.93E-05	0.08 %	7.77E-05	-1.85 %
Escalated fire due to internal ignition (FEI)	3.10E-04	3.06E-04	-1.15 %	4.47E-04	44.33 %
Escalated fire due to external ignition(FEE)	1.72E-06	1.68E-06	-2.36 %	3.13E-06	82.18 %
Spread fire internal (FSI)	1.43E-04	1.33E-04	-7.02 %	2.40E-04	67.17 %
Spread fire external (FSE)	4.15E-09	0	-100.00 %	7.86E-08	1795.2 %
Strong explosion due to internal ignition (EXI)	1.02E-04	1.02E-04	0.00 %	1.02E-04	0.00 %
Strong explosion due to external ignition (EXE)	1.59E-07	1.59E-07	0.00 %	1.59E-07	0.00 %

Table 5.10: Sensitivity analysis of the safety systems, ignited events, installation B

	Base case	Failure probability 0		Failure probability 1	
	Frequency	Frequency	% change in frequency from base case	Frequency	% change in frequency from base case
<b>Ignited events (process fires)</b>					
Local fire due to internal ignition (FII)	1.51E-03	1.52E-03	0.77 %	1.37E-03	-8.79 %
Local fire due to external ignition (FIE)	2.60E-04	2.61E-04	0.38 %	2.41E-04	-7.57 %
Escalated fire due to internal ignition (FEI)	8.49E-04	8.39E-04	-1.25 %	9.83E-04	15.70 %
Escalated fire due to external ignition(FEE)	2.87E-05	2.79E-05	-2.54 %	4.86E-05	69.64 %
Strong explosion due to internal ignition (EXI)	6.31E-04	6.31E-04	0.00 %	6.31E-04	0.00 %
Strong explosion due to external ignition (EXE)	6.58E-04	6.58E-04	0.00 %	6.58E-04	0.00 %

Table 5.11: Sensitivity analysis of the safety systems, ignited events, installation C

	Base case	Failure probability 0		Failure probability 1	
	Frequency	Frequency	% change in frequency from base case	Frequency	% change in frequency from base case
<b>Ignited events (process fires)</b>					
Local fire due to internal ignition (FII)	4.90E-04	5.03E-04	2.76 %	0	-100.00 %
Local fire due to external ignition (FIE)	3.13E-04	3.23E-04	3.15 %	0	-100.00 %
Escalated fire due to internal ignition (FEI)	2.49E-04	2.39E-04	-3.94 %	7.17E-04	187.73 %
Escalated fire due to external ignition(FEE)	2.34E-04	2.27E-04	-3.03 %	5.32E-04	126.95 %
Escalated fire, ESD failure (FEX)	4.52E-06	0	-100.00 %	4.43E-05	879.24 %
Strong explosion due to internal ignition (EXI)	7.90E-05	7.90E-05	0.00 %	7.90E-05	0.00 %
Strong explosion due to external ignition (EXE)	4.88E-05	4.88E-05	0.00 %	4.88E-05	0.00 %

### 5.3.4 Importance of the Safety Systems

The FAR for all three installations, when the reliability of one safety system is altered at a time, is shown in Table 5.12. Note that the sensitivity analyses were performed with the same approach as earlier. One safety systems at a time was set to either failure probability 0 or 1, where the others were unchanged. ESD isolation, “failure probability 0”, was for example performed by using the base case, setting all failure probabilities related to the ESD isolation to 0, where the other parameters were untouched. The ESD node for installation C was still changed by altering the failure rate to 10 times higher.

## 5.4 Discussion

### 5.4.1 Small Changes to the Fatal Accident Rate

The changes to the FAR (and impairment frequencies of main safety functions) are surprisingly small for installation A and B (a change of 4.29 % and 0.93 % respectively) when all safety functions are set to fail (failure probability 1). Refer Table 5.3 and 5.4. The changes were more evident for installation C, with an increase of 50 %, possibly due to consequences related to failure of the ESD node. Even so, it should not at this stage be concluded that the safety systems have negligible effects. Possible explanations to why the effects or the FAR values are so low are:

1. The safety systems are too coarsely modeled when estimating the ignition and explosion probabilities
2. Conservative fire simulations, which are not taking firewater into consideration
3. High escalation probabilities in the base case, also when all safety systems are functioning
4. Generally high degree of conservatism
5. The estimate of the number of larges (which dominate the risk picture) is too high

Not all of the explanations can be related to the safety systems. The three most important explanations, when the emphasis is the effects of the safety system, are discussed in Section 5.4.2.



Table 5.12: Sensitivity analysis comparing safety systems, FAR. Installation A, B and C

Base case	ESD Isolation				Blowdown				Firewater				ESD Node				
	Failure prob 0		Failure prob 1		Failure prob 0		Failure prob 1		Failure prob 0		Failure prob 1		Failure prob 0		Failure rate x10		
		% change from base case		% change from base case		% change from base case		% change from base case		% change from base case		% change from base case		% change from base case		% change from base case	
<b>FAR due to process accidents</b>																	
Inst. A	1.39	1.39	0.00 %	1.40	0.90 %	1.39	0.00 %	1.41	1.40 %	1.39	-0.06 %	1.44	3.15 %	n/a	n/a	n/a	n/a
Inst. B	2.39	2.39	0.01 %	2.40	0.12 %	2.39	-0.10 %	2.50	4.50 %	2.39	0.00 %	2.40	0.45 %	n/a	n/a	n/a	n/a
Inst. C	0.48	0.48	-0.07 %	0.51	5.40 %	0.48	-0.53 %	0.50	3.78 %	0.48	0.01 %	0.49	1.21 %	0.47	-2.69 %	0.59	23.62 %

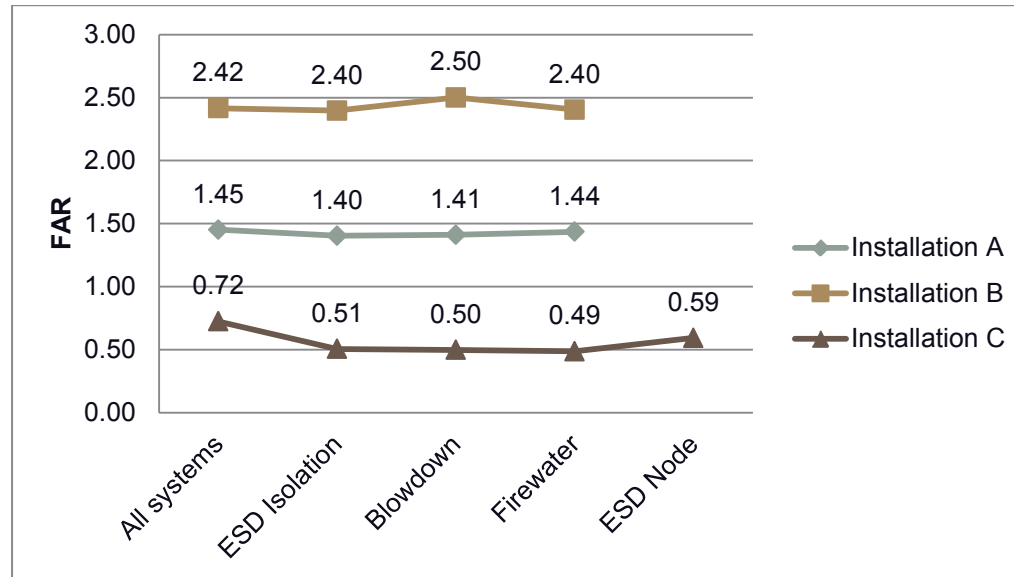


Figure 5.4: Comparing the FAR values for the various safety systems when failure probability is 1

### 5.4.1.1 Ignition and Explosion Probabilities

The calculation of ignition and explosion probabilities is performed in ExploRAM, only used within Scandpower, which is based on gas and dispersion analysis (Scandpower, 2012). The gas and dispersion analyses are dependent on the ESD isolation, blowdown, and firewater systems, affecting, among others, the leak rate, duration, and gas concentration.

The safety systems are in the present approach not modeled explicitly as pivotal events antecedent of the ignition event. The effects of the systems are rather incorporated implicitly into the ignition and explosion probabilities. By reducing the number of pivotal events, the event tree becomes less complex, reducing the number of end events. As a consequence, a change in the reliability of the safety systems will not be explicitly reflected by a change in the ignition and explosion probabilities, used in the event tree. Later changes of the reliability must be coped with by recalculating and importing new values from ExploRAM, which was not done in the sensitivity analyses. Changes to the reliabilities were fault tree related only, only affecting the escalation and spreading probabilities, whereas the ignition and explosion probabilities also should have been affected. The reliabilities of the safety systems have to be in agreement when the systems modeled twice in the event trees (before ignition, and once again before escalation). This does not imply identical values. The pivotal events between the first and second activation might alter the reliabilities (e.g. explosion, or already activated), making them worse.

Table 5.13: Summary of how the safety systems are considered for ignition and explosion probabilities in ExploRAM

Safety system	Ignition probability	Explosion probability
ESD isolation	User defined failure probability	User defined failure probability
Blowdown	Input (transient leak rate) from TLT <sup>17</sup> , normal practice to use transient leak rates corresponding to a failure probability 1	Input (transient leak rates) from TLT, normal practice to use transient leak rates corresponding to a failure probability 1
Firewater	Not considered	Input from explosion load simulations in FLACS <sup>18</sup> , normal practice to use loads corresponding to failure probability 1

Table 5.13 is a summary of how the safety systems are considered by ExploRAM. See Section 4.1 for a brief review of the effects the safety systems have. The analyst has the

<sup>17</sup> A tool used to determine the duration of process leak, and transient leak rates

<sup>18</sup> A CFD explosion and dispersion modeling software

opportunity to insert the reliability of the ESD isolation into the tool, which subsequently considers the reliability when calculating the ignition and explosion probabilities.

The functionality of blowdown can be considered by ExploRAM, decided by the leak frequency development. The duration and transient leak rate can reflect a leak with/without blowdown. For the three installations, ExploRAM used *only* input corresponding to functional blowdown, which is non-conservative. The possibility for non-functioning blowdown was not considered. Figure 4.1 showed an example of the positive effect of blowdown on the leak rate. The amount of released hydrocarbons and the size of the gas cloud can be reduced, thus the probability of ignition and severity of a possible explosion. This assumption is important for older platforms, with manual activation. The time before blowdown activates can be substantial, reducing the effect on ignition and explosion probabilities. Thus the blowdown system is non-conservatively credited for some of the installations.

As discussed in Section 4.1.4, the effect of firewater is ambiguous, and is thus not considered for the ignition probability. The firewater system is considered analogous to the blowdown system, where the input from FLACS decides the functionality of firewater on the explosion loads. The input is in terms of explosion simulations, obtaining the relationship between the explosion load and the size of the ignited gas cloud (Wiklund & Fossan, 1999). To quantify the frequency of strong explosions, ExploRAM combines the frequency distribution for the equivalent gas cloud size, with the probability that the explosion load exceeds the design criteria (loads corresponding to a strong explosion). The inputs used for the three installations corresponded to a non-presence of the firewater system. Note that this approach is conservative. Immediate and delayed ignitions are included in the probability distribution for ignited gas clouds, where a delayed ignition enables sufficient time for a larger gas cloud to form. The frequencies of strong explosions are unchanged as a result of not changing the explosion probabilities (can be observed in Table 5.9, 5.10, and 5.11). It is likely that an increase of explosions would result in a significant increase of the immediate FAR and the impairment of MSFs. This outlines the importance of modeling strong explosions properly, and the danger of omitting changes to the explosion probabilities.

Table 5.14: Difference in ignition probabilities with and without isolation, in percentage points

Segment	Leak size			
	Small	Medium	Major	Large
A1	0.00 %	0.31 %	1.35 %	0.68 %
A2	0.00 %	0.08 %	0.55 %	0.36 %
A3	0.00 %	0.25 %	0.65 %	0.22 %
A4	0.01 %	0.24 %	2.20 %	1.06 %
A5	0.00 %	0.52 %	2.24 %	2.80 %
A6	0.00 %	0.09 %	0.30 %	0.45 %
A7	0.01 %	0.72 %	3.21 %	4.18 %
A8	0.01 %	0.72 %	3.21 %	4.18 %
A9	0.00 %	0.15 %	0.61 %	0.84 %
A10	0.01 %	1.07 %	5.11 %	3.07 %

The ignition probabilities are one of the most critical elements, where the risk results are normally directly dependent on the probability of ignition (Vinnem, 2007). If the ignition and explosion probabilities were modeled more accurately, the effect of safety systems might have been more revealing in the risk measure. This might lead to greater changes to the FAR, impairment frequency of the MSFs, and distribution of the ignited events. Table 5.14 shows the differences for ignition probabilities, for a selected number of segments (numbered A1-A10) for installation A (see Appendix B.2 for the complete set of the data). Note that the values are in percentage points, and not percentage. Insignificant changes can be observed for the smaller leak sizes, but more distinctly for the larger leaks. Though the changes in percentage points are small, they are significant, some probabilities were doubled and far beyond (some of the changes in percentage were in the range of hundred thousands, changes in percentage points are thus used for easier readability).

Table 5.15: Difference in strong explosion probabilities given ignition, with and without isolation, in percentage points

Segment	Leak size			
	Small	Medium	Major	Large
A1	0.00 %	9.64 %	23.15 %	12.51 %
A2	0.00 %	1.60 %	6.10 %	5.91 %
A3	0.00 %	2.88 %	10.19 %	5.23 %
A4	0.00 %	17.00 %	16.28 %	0.00 %
A5	0.00 %	31.10 %	53.68 %	13.73 %
A6	0.00 %	4.38 %	7.72 %	1.73 %
A7	0.00 %	45.28 %	85.35 %	7.28 %
A8	0.00 %	45.28 %	85.35 %	7.28 %
A9	0.00 %	8.89 %	16.32 %	1.26 %
A10	0.00 %	30.48 %	47.02 %	1.68 %

Table 5.15 shows for the same segments the differences in probabilities of having a strong explosion given ignition, with and without ESD isolation. Similar (but a little more evident) findings, as with the ignition probabilities, can be observed with the strong explosion probabilities. Based on these findings, it is believed that a much larger change in the FAR values (among others risk measures) would have been observed if the ignition and explosion probabilities were recalculated to take credit for the safety systems.

Table 5.16: Difference in strong explosion probabilities given ignition, with and without firewater, in percentage points

Segment	Leak size			
	Small	Medium	Major	Large
A1	0.00 %	0.16 %	0.15 %	0.02 %
A2	0.00 %	0.19 %	0.22 %	0.08 %
A3	0.00 %	0.15 %	0.14 %	0.02 %
A4	0.00 %	0.01 %	0.00 %	0.00 %
A5	0.00 %	0.15 %	0.10 %	0.00 %
A6	0.00 %	0.08 %	0.03 %	0.00 %
A7	0.00 %	0.07 %	0.03 %	0.00 %
A8	0.00 %	0.07 %	0.03 %	0.00 %
A9	0.00 %	0.04 %	0.01 %	0.00 %
A10	0.00 %	0.04 %	0.02 %	0.00 %

Table 5.16 presents the differences in percentage points for the explosion probabilities, with and without firewater. Most surprisingly are the small changes to the probabilities. Based on the results, the mitigating effects of firewater on explosions are almost non-existing. This indicates that the firewater system has small mitigating effects on the explosion probabilities (might be plant specific, based on the geometry of the segments, ventilations, and so on), or that the effects are not handled properly by FLACS and/or ExploRAM. Note that the table does not show how great the effect of firewater has on the explosion load; all loads below the strong explosion limit might be increasing significantly without firewater.

#### 5.4.1.2 Fire Simulations without Firewater

After the ignition and a possible explosion, fire simulations are performed to anticipate the subsequent development. In the case studies, the fire simulations were performed without firewater, in accordance with the facility regulations (PSA, 2011b), Section 29, and NORSOK S-001 (2008). The facility regulations states that the cooling effect from firefighting equipment shall not be credited when considering passive fire protection. NORSOK states that the effect of deluge shall not be considered for the main structural elements and fire partitions. An exception

of the NORSOK statement is that firewater can be considered for process piping/equipment, if proper documentation is provided.

It is likely that the firewater system reduces the severity of a fire, for example by reducing the heat flux the personnel and equipment is exposed to, which reduces the probability of fatalities and escalation. The time before the effects are appreciable can be significant, which unable the reduction the immediate fatalities. It is not possible for the risk analyst to reveal the impact the firewater has on the risk measures, since the fire simulations are performed without firewater. The effect of firewater in the fire simulations is assumed to have a greater effect on the impairment of the escape routes and/or lifeboats, hence fatalities during escape (and/or evacuation fatalities). With the fatal heat flux covering a larger area due to simulation without firewater, impairment of the escape routes becomes more likely. Personnel are inhibited from escaping from the exposed segment, and from other segments. Another factor is the increased danger during rescue attempts of wounded personnel which are affected by the initial blast. The topic of firewater is further discussed in Section 6.1.3.

#### 5.4.1.3 High Escalation Probabilities

Even with the successful activation of all the safety systems, the possibility of a fire escalating is still present. The escalation probabilities can often be assessed as relatively high. For example due to deteriorated passive fire protection, easily exposed equipment, conservative precautions, reducing the benefits of the safety systems. It was for installation B determined high escalation probabilities, mainly due to deteriorated passive fire protection. To see the effect of smaller escalation probabilities, an additional sensitivity analysis is performed for installation B.

Table 5.17: Sensitivity analysis of the safety systems with low escalation probabilities, FAR, installation B

	Base case	Failure probability 0	% change from base case	Failure probability 1	% change from base case
<b>FAR</b>					
FAR due to process accidents, low escalation probabilities	2.26	2.24	-0.55 %	2.42	7.10 %
FAR due to process accidents, original escalation probabilities	2.39	2.39	-0.09 %	2.42	0.93 %

The escalation probabilities, when having successful activation of the ESD isolation, blowdown, and firewater system, is set to 0 (observed in Figure 5.2, where the pivotal event of escalation, leading to sequence number 3 and 16 is set to 0). This implies that if all three safety systems function, no escalation will occur. The other escalation probabilities are untouched. The

results are shown in Table 5.17, with a comparison of the original FAR values. As expected, changes are not observable for the case of “failure probability 1”, both with a FAR of 2.42, since they were not affected by the parameters changed. The change in percentage when moving from “base case” to “failure probability 1” increased to 7.10 %, when applying low escalation probabilities. The original study with normal escalation probabilities had only an increase of 0.93 %. This indicates that the escalation probabilities have a great impact on the end results. It is likely that the escalation probabilities themselves are not the reason for small changes to the FAR values. Changes to the impairment frequencies of the MSFs seem to still be far lower compared to installation A and C, even with lower escalation probabilities (Appendix B.1.3).

#### **5.4.1.4 Generally High Degree of Conservatism**

The preferred approach is usually to give an accurate and best estimate of the risk picture, which is the closest “representation” of the real world. Due to uncertainties, conservatisms are often used when performing QRAs, as an act of precaution. Almost all uncertainties are countered by the analyst with conservatism. The conservatism can be related to the leak frequencies, reliability of safety systems, consequences, etc. The completeness uncertainty is important to consider. Overextending the conservatism in other areas can be looked as a compensation for forgotten or unknown hazardous not catered for. The conservatism can be exaggerated, and propagate to the end results, which dominates the risk picture. The degree of conservatism of the QRAs used in the case study is unknown, and the degree might also vary among the analyses. A better understanding might have been given if the detailed uncertainty analyses were available.

#### **5.4.1.5 Overestimated Number of Large Leaks**

In the Norwegian petroleum industry, the leak frequencies are calculated based on the SHLF model, prepared by Det Norske Veritas (Det Norske Veritas, 2010). This approach might give a too high estimate of the leak frequencies, at least based on the observations from the Norwegian continental shelf in the recent years (Scandpower, 2011).

Figure 5.5 illustrates the correlation between the leak rate, the frequency and the consequence. A leak with a high leak rate releases more hydrocarbons. For a delayed ignition scenario, a larger gas cloud is formed, increasing the probability for ignition and explosion, and the likelihood of causing severe consequences. For an immediate ignition scenario, a jet fire is likely to occur, where a larger leak rate produces a more extreme jet fire stream. A large leak increases the probabilities of equipment being exposed, and the occurrence of escalation. The presented fire and explosion events are simplified, as the ignition of a hydrocarbon release can

have several more outcomes<sup>19</sup> (Spouge, 1999). Fortunately, large leaks are far more seldom than smaller leaks. The effects of the safety systems are mostly relevant for smaller leaks, mitigating the effects of a fire, and the probability of explosion. Fires occurring from large leaks are, on the other hand, assumed to be so extreme that the effectiveness of the safety systems is greatly reduced. The effect of the safety systems is therefore dependent on the distribution of smaller or larger leaks, and more substantial if the proportion of smaller leaks is high. The risk picture is often dominated by large leaks, where a high proportion of, for example the FAR, is from large leaks. An overestimation of the smaller leaks is usually not critical, which has a smaller contribution to the risk measures. By additionally overestimating the frequency of large leaks, the domination can be exaggerated. The effects of the safety systems on smaller leaks can by this be undermined.

The number of hazardous event is for process accidents the number of leaks, fewer leaks implies fewer hazardous events, reducing the probability of having fatalities. It is thus believed that the frequency of the initial events, especially the frequency of large leaks has an important effect on the FAR. Note that there are leaks are directly related to human errors (e.g. during maintenance), having an impact on the leak frequency basis used when performing a QRA. Recall that the QRA are used for strategic purposes, with a long-term horizon. It is not suitable to use a QRA to evaluate the risk of an upcoming maintenance activity.

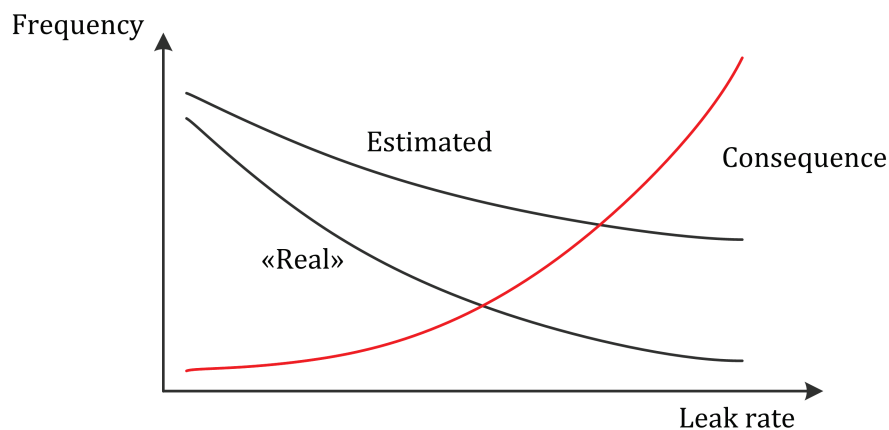


Figure 5.5: Estimated and “real” presentation of leak rate, frequency and consequence

<sup>19</sup> Dependent on the type of material, rate and nature of the release, time of ignition, and the nature of the surrounding structure (Spouge, 1999). Possible outcomes are jet fire, pool fire, flash fire, fireball, explosion and gas plume.



### 5.4.2 Three Highlighted Reasons Regarding the Safety Systems

All five explanations, discussed in Section 5.4.1, contribute to the small effects on the FAR values, and potentially also the impairment frequencies of the MSFs. A descending ranking of what is thought as the three most important explanations, when considering the safety systems, are:

1. The safety systems are too coarsely modeled when estimating the ignition and explosion probabilities
2. High escalation probabilities in the base case, also when all safety systems are functioning
3. Conservative fire simulations, which are not taking firewater into consideration

The presented results do *not* conclude inapplicability of risk measures used in QRAs. In the base case, the safety systems are to an extent considered in the ignition, explosion and escalation probabilities. The estimates from the original QRAs can thus be close the “real” risk.

The ignition and explosion probabilities were chosen as the most important. Ignition and explosion are early pivotal events in the fault trees. Errors made in the early stage can propagate further back in the event tree. If the number of fires were optimistically high, then the correctness of fire simulation and escalation probabilities would be of less importance.

The escalation probabilities are important, since they decide how great the mitigating effects of the safety systems are. The degree of conservatism and the probability of escalation are dependent on the subjective view from the analyst. High escalation probabilities do not necessarily imply a conservative approach. This might be due to hidden hazards, or optimistic parameters.

By not modeling the release of firewater in the fire simulations, the effect of firewater is not included during the determination of the consequences of the end events (fire). The effect of the firewater can be covered by comparing simulations with and without firewater. It is more important to get the frequency and distribution of the end events correct, thus the firewater chosen as the least important of the three explanations. If for example the number of large leaks and explosions were overestimated, then the simulation with firewater would be less relevant, as the severity would be far beyond the “true” values.

### 5.4.3 FAR Distribution – Immediate, Escape and Evacuation

The FAR during evacuation seems virtually unaffected by the change by the reliability of the safety systems, when moving from “base case” to “failure probability 1”. FAR related to

immediate fatalities and fatalities during escape seems more affected. There is again an exception for installation C, where the FAR evacuation increased with 250 %.

The results tend towards a higher contribution from FAR immediate, compared to escape and evacuation. Still, history (for all types of accidents) has shown that the fatalities from escape and evacuation dominate the fatality picture (Vinnem, 2007), but this is highly dependent on the type of accident. Blowout is not likely to cause many immediate fatalities, but is more likely to induce escape or evacuation fatalities. Process accidents are assumed to have a higher contribution from immediate fatalities, occurring during the ignition (and explosion). The escalation is assumed to be slow enough (due to fire protection, firewalls, etc.) to give sufficient time to escape or evacuate. The process area is also usually at the far end of an installation, distanced from safe (shelter) areas located such that few people are affected by the loss of escape routes.

There have been major process accidents leading to a high number of escape and evacuation fatalities. The Piper Alpha accident caused a high number of fatalities, mainly due to bad communication. People found refuge at the shelter area, as instructed, awaiting helicopter rescue. This was not executable due to fire and smoke without the information being transmitted to the awaiting personnel. Operators had fled the radio room, impairing the ability of communication (Vinnem, 2007). Major accidents of this magnitude are often disregarded when looking at the risk picture (FAR values), which can also be done for the fatality distribution in this context.

#### **5.4.4 Substantial Increases of Impairment Frequencies?**

An exception is installation B, which had far less changes compared to the other two. The small changes for installation B can be explained by the already high escalation probabilities. This is discussed in Section 5.4.1.3.

One can be deluded when only looking at the high changes in percentage. The frequencies handled are small, many in the magnitude of  $10^{-4}$  per year or less, thus the absolute change in the values seems less substantial. Most of the MSFs maintain their acceptable status regarding impairment frequency, when moving to case of “failure probability 1”. Of all MSFs, only two functions from installation C moved from the region of acceptable to unacceptable (from below, to above  $10^{-4}$ ). This is partly due to many of the MSFs already being unacceptably high in the base case. Note that for installation A and C, the heat and smoke loads have been merged into one load, denoted fire. Using an acceptance criterion of  $10^{-4}$  for fire loads is then conservative as fire should be considered as two loads, heat and smoke. Using a criterion of  $2 \cdot 10^{-4}$  is not entirely correct either (as discussed in Section 3.4). It would be preferable to

distinguish between heat and smoke loads. An argument for using one criterion of  $10^{-4}$ , treating the two loads as one, is the concurrent presence of smoke and heat.

The results indicate that the safety systems have a significant effect on the impairment frequencies, but the changes are not critical (regarding acceptance criteria). More severe changes might be observed if the listed points in Section 5.3.1 are handled properly, given the frequencies are comparable to the FAR values.

#### **5.4.5 Distribution of Ignited Events**

An expected increase of local fires (FIE and FIE) is observable when all safety systems function (failure probability 0), having a higher frequency of less severe ignited events (refer Tables 5.9, 5.10, and 5.11). The frequency of escalated and spread fires (FEI, FEE, FSI, and FSE) is reduced as a direct consequence. Opposite results can be observed when all safety systems are set to fail, where the non-presence of the systems implies a higher probability of escalation (thus frequency of escalated fires). The results are related to how the event trees are modeled. Note that the installations are modeled differently, with different assumptions. Installation A and B assumes that simultaneous failure of ESD isolation and blowdown cannot occur, whereas installation C assumes that an escalated fire occurs if the ESD isolation and blowdown fails. Thus, the installation C leads to more extreme numbers when doing the sensitivity analyses.

The distribution between local and escalated fires is conceived as expected, but the magnitude is more diffuse. Some of the increases, in percentage, are high (in the magnitude of  $10^3$ ), this due to handling of small frequencies (some in the magnitude of  $10^{-9}$ ). Small changes in the absolute value result thus in large changes in percentage. Should the changes to the frequencies be more extreme?

The changes are once again most evident for installation C, subsequently A, then B, similar to the findings regarding the FAR and impairment frequencies of the MSFs. This is possibly due to the same explanations, discussed in Section 5.4.1. This indicates a correlation between those measures, but not directly as all the measures are decided by the consequence cohered to the type of ignited event (and escalation probabilities). The consequences are determined, based on the installation itself (geometry for simulations, equipment present, criticality of safety systems, etc.), including the subjectivity of the analyst's knowledge about it. An escalated fire can in an accident constitute great damage, where in another do less damage. There is no fixed correlation (correlation factor) between the ignited events and the other two measures, but there are in general a correlation between the distribution of ignited events and the risk measures.

#### 5.4.6 Contradictions in Safety Systems Importance

The results are contradicting when trying to outline the most important safety system (refer Table 5.12), when based solely on the FAR values. For installation A, the failure of the firewater gave the highest increase of the FAR, blowdown for installation B, and the ESD node for installation C. Note that the FAR value for installation B, when *only* the blowdown system has failed (FAR = 2.50 [value from Table 5.12]), exceeds the FAR for when all safety systems have failed (FAR = 2.42 [value from Table 5.4]). This is explained by how the safety systems are modeled in the event tree, in combinations with the consideration of the consequences (severity) of the end events. A simultaneous failure of both the ESD isolation and blowdown was never considered in the event tree. It was assumed that the simulations failure of both those systems were highly unlikely, thus neglected. With the ESD isolation being modeled first, setting all failure probabilities to 1 implies the failure of only ESD isolation and firewater, disregarding blowdown. For installation B, the failure of blowdown was considered more severe than the simultaneous failure of both the other two systems, leading to the observed results. This shows that the event trees, as they are modeled, are not proper for the sensitivity analyses.

For installation C, the ESD node had the greatest effect on the FAR, which is related to the high and conservative consequences of a failure of the node. The consequences were determined conservatively, based on the knowledge about the event being of low probability. This shows how the consequence determinations affect the risk measures. The determination can be difficult and important, which also make the comparing the sensitivity analyses difficult. The most important safety system is clearly dependent on how the consequences are determined.

It is not possible to conclude which of the safety system being most important based on the sensitivity analyses, due to the contradicting results. It is possible that the answer is also installation and incident specific, without the possibility to outline a system to focus on, when modeling the reliability of the safety systems.

# Chapter 6

## Best Practice – Modeling Safety Systems in Event Trees

### 6.1 Event Tree Modeling

The chapter presents a proposed best practice, mainly based on the findings throughout the thesis.

#### 6.1.1 Ideal Representation of an Event Tree

The results from an analysis are dependent on how the process accidents are modeled in the event trees, where the event tree shall reflect the transient development of an initial event. It is important to always consider the previous events when assessing the probabilities of the next. Only the pivotal events modeled in the event trees are considered. As discussed in Section 4.3, a detailed sequence of the pivotal events in an event tree could be as presented in Figure 6.1.

Leak	Gas detection failure	Critical isolation failure	Critical blowdown failure	Firewater failure	Ignition	Explosion	Fire detection failure	Isolation failure after FD	Blowdown failure after FD	Firewater failure after FD	Escalation of fire
INT_EVENT	GD	ISO	BD	FW	IGNITION	EXP	FD	ISO2	BD2	FW2	ESC

Figure 6.1: Possible pivotal events in a detailed event tree

The safety systems are modeled twice in the event tree, once after gas detection, and secondly after fire detection. By modeling the safety systems twice, activations on gas and/or fire detection can be considered. Table 4.1 shows a summary of the requirements to when the safety systems should be activated, whereas Table 5.13 shows how they are considered by the ignition and explosion probabilities in ExploRAM. Note that the requirements might differ from

the installation subject for analysis. When modeling an event tree, bear in mind that a system activated upon gas detection does not need to be activated again upon fire detection. An unwanted event after gas detection can occur, which makes the activation on fire detection useful, for example during a problem with receiving/transmitting signals. The fire detection can be considered as a redundancy to activate the systems not triggered during gas detection. The effect of a safety system is dependent on when it is activated; systems first activated on fire detection do not have any effects on the ignition and explosion probabilities. It can be distinguished between the effect on ignition and explosion probabilities, and secondly on escalation probabilities. When the safety systems are modeled twice, the effect on either ignition and explosion, or escalation can be considered independently. A blowdown system might have mitigating effect on the ignition and explosion probabilities, but due to damage from an explosion, not be available to reduce the escalation probabilities.

Explosions can be categorized by the load. At the present, only strong explosions are considered, with the definition based on the design pressure of the firewalls. The probability of immediate fatalities is to an extent correlated to the explosion pressure. A more rightful picture of fatalities can be achieved if several explosion loads are considered. Introduction of several explosion loads can be evaluated. If another category of explosion is introduced (e.g. medium) including the existing strong explosion, vulnerability analyses in QRAs might be more relevant.

### **6.1.2 Realistic Event Tree Modeling**

Simplifications are needed to find the optimal trade-off between the utility value of resources (manpower, computational speed, etc.), and the level of detail gained. Figure 6.2 illustrates how the utility value of resources is correlated to the level of detail. At first, little effort is needed to gain a significant higher level of detail. The utility value will decline at a certain point, without the level of detail increasing considerably. A disproportion between the level of detail gained, compared to the resources needed will occur. Significantly more resources are needed for a small gain of additional information, or effort to make the models more precisely, is needed to increase the level of detail. Still, the data and models could be distorted by uncertainty (refer Section 2.2 for a discussion about uncertainty). It is for example unnecessarily to double the resources to be able to calculate a FAR value of 7.31, compared to 7.3. The utility value is also dependent on the operator (customer), deciding the amount of resources fed into the analysis. The optimal is at the peak before the utilization drops, which might not be easy to find, as it fluctuates from project to project. The client might set a limit before the peak is reached. If the client is interested in a coarse analysis, the level of detail will suffer. Sometimes, a certain level of detail is required, and the utility value of resources can be disregarded.

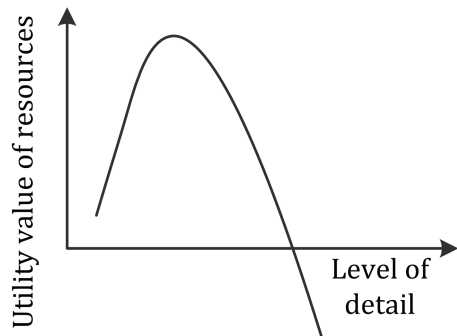


Figure 6.2: Utility value of resources VS level of detail

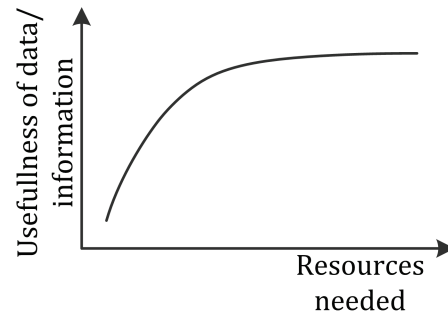


Figure 6.3: Utility value of data/information VS level of detail

When modeling an accident scenario, the resources needed is increasing exponentially with the usefulness of the data/information. Note that a perfect reflection of the real world is never achievable. Figure 6.3 shows how the usefulness of the data or information changes with the resources expended. Additional data is never destructive (unless the data or information is falls), but the gain is minimal after a certain point. A large and detailed event tree does not ensure the correctness of the analysis, where uncertainties once again are a factor. The results from an ETA are influenced by many assumptions and evaluations, especially when considering the consequences, where subjective evaluations are made. If a QRA is executed with a too high level of detail, the working hours required would be extending beyond the reasonable. There must, at the same time, be put sufficient effort in the analysis to achieve a sufficient confidence in the results. Comparing the more simple approach from Figure 5.1 (8 pivotal events) with the more comprehensive approach from Figure 4.3 (13 pivotal events), the number of end events increased from approximately 40 to 285.

Leak	Gas detection failure	Critical isolation failure	Critical blowdown failure	Firewater failure	Ignition	Explosion	Fire detection failure	Escalation of fire
INT_EVENT	GD	ISO	BD	FW	IGNITION	EXP	FD	ESC

Figure 6.4: Possible pivotal events in a simplified event tree

Figure 6.4 illustrates a simplified version of a process event tree. The number of end events can potentially be doubled (or more, if multiple branches are used) with each introduced pivotal event. The work load can be substantially reduced by cutting the number of events. This simplification should only be performed if possible. Some information will be lost, and the omitted events should be the least important. The sequence of an incident should to a degree be

intact, without losing highly possible or important end events. For example omitting the pivotal event of ignition would entirely alter the results in an optimistic manner.

If a simplified approach is used and the safety systems only modeled once, prefer to have the relevant safety systems as early as possible. Then, the non-presence/presence of a safety system is considered for most relevant pivotal events as possible. The safety systems should for process accidents affect all the probabilities of ignition, explosion, and escalation. This is only beneficial if the effects from the safety systems are considered properly in these probabilities. At the present, the input fed into ExploRAM is often corresponding to 100 % functionality of the blowdown system, and no effect of firewater on ignition probability (and usually not on explosion probabilities either). This can be countered by assigning a higher consequence (fatalities) for the end events without blowdown or firewater.

The use of event trees make the analyses mainly deterministic, representing a selection of possible initial events and outcomes by discrete scenarios (Spouge, 1999). Consider leak frequencies. The more correct approach is to estimate the leak frequency as a continuous function, but they are more challenging to derive and use (Spouge, 1999). To have a limited number of initial events (type of leaks), the leak frequencies are fixed in categories (usually by leak size or rate). This is widely used, and the advantage is simplicity. A challenge is to ensure that all analysts (within the whole industry and not only a company) use the same set of categories. If not, the analyses become less comparable.

### 6.1.3 Effect of Deluge

Effects of deluge are per today normally not considered during fire simulations, leading to conservative estimation of consequences for both fatalities and impairment of MSFs. The effect of deluge is unclear, but there is an ongoing project by SINTEF. The overall aim for the project is to *"establish the basis of predictive methods for the abilities of the active systems in terms of fire fighting effect in case of an accident"*<sup>20</sup> (SINTEF, 2005).

If the calculation of fatalities is considered by the area percentage of a module exposed to fatal loads, with the average of personnel present, a reduction of for example the heat load can be significant. Consider a fatal heat load initially covering 20 % (without firewater) of a module, reduced to 15 % with firewater, the fatalities would as a consequence be cut by a quarter. The FAR value can be considerably lowered, if similar findings were found for all segments (dependent on the effect of firewater system, which again is dependent on e.g. the leak size).

---

<sup>20</sup> For additional reading, refer to the latest report published: "Documentation of active fire fighting systems as a fire safety design parameter" (Brandt, Opstad, & Wighus, 2012).



Substantial reduction of the impairment frequencies, especially for escape routes, is possible when taking firewater into consideration. For some reasons (possibly due to insufficient knowledge about the effect firewater), PSA and NORSOK state that the effect of firewater should not be credited (discussed in Section 5.4.1.2).

## 6.2 Fault Tree Modeling

### 6.2.1 Vulnerability of Safety Systems

Section 4.8 summarizes the recommended approach regarding vulnerability.

### 6.2.2 Human Errors

For some installations, the blowdown system must be manually activated. Additional reading about HRA is found in Section 4.6. Human errors can be treated as a basic event and introduced to the fault tree co-existing with hardware failures, as shown in Figure 6.5.

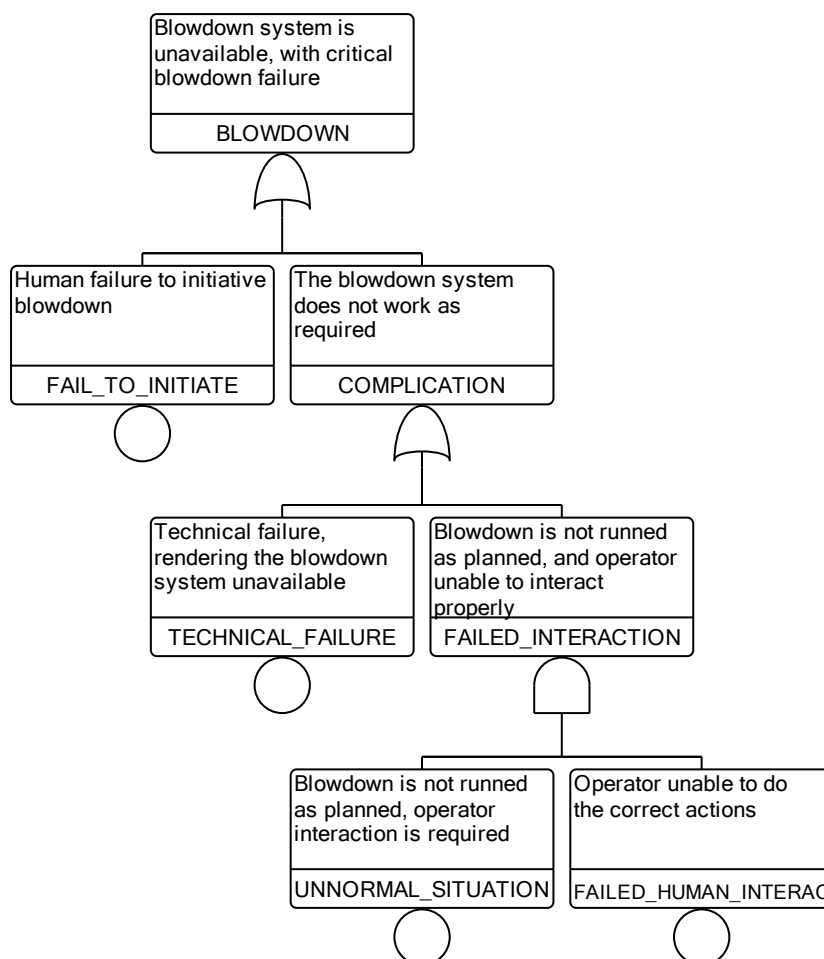


Figure 6.5: Fault tree of critical blowdown failure

Two possible approaches when determining the HEP are:

1. Generic HEP
2. HEP from a HRA study

Table 6.1 is a simple approach when assigning a HEP. The task under study is matched with the generic task description and the corresponding HEP. 10 % is for example a HEP which can be used for the basic event of “fail\_to\_initiate”. A probability for the basic event “failed\_human\_interac” can be set higher. The circumstances are more extraordinary and unexpected, and the numbers of correct actions are limited. This might be some kind of overriding of the system, since it does not operate as expected.

THERP and HEART are common HRA methods which can be used to estimate a HEP. The use of HEPs from such studies is beneficial to increase the confidence of the QRA. If possible, combine a HRA study with QRA, taking the benefit from the synergy. As with QRA, there are many benefits from HRA beyond the quantitative results, for example to suggest risk-reducing-measures. Refer Rausand (2011) for introduction to the topic of HRA. It is *not* recommended to initiate a HRA study with the solely purpose of estimating a HEP, which is likely to give a bad utility value of the resources.

Table 6.1: Example generic human error probabilities (Vinnem, 2007, cited in Hunns & Daniels, 1980)

Error type	Type of behavior	Human error probability
1	Extraordinary errors: of the type of difficult to conceive how they could occur: stress free, powerful cues initiating for success	$10^{-5}$
2	Error in regularly performed, commonplace simple tasks with minimum stress	$10^{-4}$
3	Errors of commission such as operating wrong button or reading wrong display. More complex task, less time available, some cues necessary	$10^{-3}$
4	Errors of omission where dependence is placed on situation cues and memory. Complex, unfamiliar task with little feedback and some distractions	$10^{-2}$
5	Highly complex task, considerable stress, little time to perform it	$10^{-1}$
6	Process involving creative thinking, unfamiliar complex operation where time is short, stress is high	$10^{-1} - 1$

### 6.2.3 Dependencies between Safety Systems

Possible dependencies considered in a process accident are:

- ESD isolation valves
- Blowdown valves
- Deluge valves
- Diesel engine
- Firewater pumps

The dependencies are handled automatically and decently through the calculation approach used by RiskSpectrum, as described in Section 4.9. Note that this approach of treating dependencies does not explicitly take the consequences of the basic events into consideration. Consider blowdown valves in a segment, a failure of one critical valve is sufficient for the blowdown system to be considered to have failed. The severity of all valves failing would normally be perceived as higher, but a distinguishing between the two events are not made in the modeling of the event trees. Similarities might be observed from the installation point of view. The perceived consequence (setting the number of fatalities) of a blowdown failure affecting *all* segments, could be considered much more severe, compared to when each segments are assessed individually and the sum taken. A PLL determined by the analyst for an ESD node failure (which all blowdown valves are dependent on) leading to a blowdown failure affecting all segments, might be higher compared to the PLL calculated by summing the contribution from a blowdown failure at each segments (given the events trees are divided by segments).

## 6.3 Importance of Event Tree Modeling VS Fault Tree

With the current practice of event tree modeling, the case study showed marginal effects on the risk picture when assigning the reliability of the safety systems as input to the pivotal events. The analyst might thus almost unconcernedly set a reasonable failure probability (e.g. no big difference between 1.5 or 3.0 % on the end results). It may be more important to emphasize on the effect of the safety systems on the pivotal events, early in the event tree (ignition and explosion). Rather than using efforts on modeling the reliability of the systems accurately in complex fault trees. The focus should be on how to model the event trees most correctly, especially the sequence, and which pivotal events to include. The initial event of leak does not really become a hazardous event until an ignition occurs. If the modeling of safety systems has a significant effect on the ignition and explosions, try to model it more correctly. When the

modeling of the event trees is more correct, the effect of the safety systems might become more evident.

There are indications that the consequence setting is more important than the reliability modeling of the safety systems (at the current practice). Spending resources to precisely model the reliability of the safety systems becomes unnecessary, if the severity (PLL) determination of the consequence classes are uncertain (which they usually are). The reliability of the safety systems are usually differing in the range of a few percent, but the consequences might differ a lot more. Setting a high consequence is likely to give larger effects, compared to changing the reliability of the safety systems with a couple of percent.

# Chapter 7

## Conclusions and Recommendations for Further Work

### 7.1 Conclusions

The field of QRA is vast, and the literature survey can only cover parts of it. QRA is known by many names, where QRA and TRA are commonly used in Norway. An important factor regarding risk analysis is uncertainty; distinguishing between parameter, model, and completeness uncertainty (discussed in Section 2.2). There is no existing tradition of thorough treatment of the topic in Norwegian QRAs. When performing a QRA, the requirement is just a discussion of the uncertainty.

QRA can be used to evaluate risk to personnel, environment, and assets. The emphasis of an offshore QRA is normally personnel risk. Risk measures are used to present the risk picture (treated in Chapter 3). To consider individual risk, the most commonly used risk measure is FAR (the risk measures are presented in Section 3.3). The benefits from a QRA are beyond using the risk measures to evaluate the acceptability of a risk. The process itself is important, providing guidance for the designers and operators on how to reduce the risk (strengths and limitations discussed in Section 2.1.5). Performing a QRA can be a comprehensive task, and the quality dependent on the analyst. Regarding process accidents, the support from other disciplines is needed, with knowledge about CFD simulations, safety systems, and human factors.

A case study of three different installations has been performed (presented in Chapter 6). The effect of the reliability of the safety systems on the main risk results is investigated. The results indicated marginal effects of the safety systems (ESD isolation, blowdown and firewater) on the risk. The FAR values were mainly changed in the order of 1/100. Installation C was an

exception, due to a different modeling of the event tree. The ESD node was modeled explicitly as a pivotal event, with a failure causing high severities. The impairment frequencies of the MSFs were significantly changed in percentage, but most of the MSFs did not alter from an acceptable to the intolerable area. Many of the MSFs were already in the intolerable area during the base case. The acceptance criterion for two of the loads (heat and smoke) was considered as one (fire), which is a possible explanation. Still, negligible effect of safety systems is *not* concluded. Three possible explanations in a descending order of importance are (discussed in Section 5.4.2):

1. The safety systems are too coarsely modeled when estimating the ignition and explosion probabilities
2. High escalation probabilities in the base case, also when all safety systems are functioning
3. Conservative fire simulations, which are not taking firewater into consideration

The findings were ambiguous about the most important safety systems, which indicate the answer as installation specific. Possible contributing factors to the importance are the modeling of the event tree, and the subjective consequence evaluations by the analyst. The consequences determined are influenced by the skills and knowledge of the analyst. Two analysts can determine the severity of the same blowdown failure differently.

The time dependency required in an event tree forces the safety systems to be modeled in their respective activation sequence. The sequence is installation (and situation) specific and dependent on if the systems are activated automatically or manually (discussed in Section 4.1.5). The time of activation should be specified in the fire and explosion strategy plan (see Table 4.1 for a summary of the generic requirements). Deciding the probability of a pivotal event must be based on the previous events; an incorrect sequence will affect the judgment negatively. Altering the sequence incorrectly can lead to illogical sequences (e.g., explosion before ignition). The event trees are only simplifications of the real world. The effect of the simplification is dependent on many factors: type of initial events, parameters as input of the pivotal events, and especially the pivotal events omitted to reduce the size of the event tree. As performed by Scandpower, the safety systems are not modeled explicitly previous to the events of ignition and explosion. This diffuses the contribution of the safety systems. An external tool, ExploRAM, is used to calculate these probabilities. The effects of the safety systems are considered by the tool, but are not visualized in the event trees. A summary of how the safety systems are included is

presented in Table 5.13. To have a full dataset, enabling a more precise modeling of the effects of the safety systems, ExploRAM must be run multiple times. There are 6 combinations regarding failure/success of the safety systems. The effects on the escalation probabilities are clearer, where the safety systems are modeled more adequately.

RiskSpectrum has a more unorthodox approach when calculating the end event frequencies (discussed in Section 4.9). The event trees are first converted into fault trees. The ability to handle dependencies is then decided by the ability of the fault tree (more specific the approach of minimal cut sets), which is a decent approach.

Vendor reliability data is often found to be more optimistic compared to what experienced in the field (discussed in Section 4.5). The explanation is with the interpretation of the content of a failure rate. The IEC 61508, which many manufacturers adhere to, does not include systematic failures when predicting the failure rate. The actual risk-reduction from the safety systems will, due to systematic failures, be lower compared to the predicted.

A suggestion to the best practice is presented in Chapter 6. The emphasis should be the event tree modeling (including the determination of consequences), before the effects of the safety systems might become more evident. A detailed modeling of the safety systems can become wasted if the consequences determined by the analyst are too uncertain. As the QRA is for strategic purposes, handling human reliability similar to hardware failures can be adequate. Vulnerability is most relevant during the operational phase, and can be included by altering the failure rates. The best practice is only a suggestion, and further work should be based on the presented.

## 7.2 Discussion

It is expected that the safety systems have large effects on the risk picture, but is the expectations correct? The systems might, for all we know, actually have limited effects on the risk. It might also at times worsen the situation. The expectations might just be something we are lead to believe. The present conclusion about the importance of the safety systems are based on one specific approach of sensitivity analyses of three specific QRA studies. The selection is not sufficient for a statistic significance to be concluded. The focus of the thesis was shifted towards event tree due to the prevailed results. How the safety systems were modeled in the event trees was of interest, rather than the importance of the fault trees. The thesis shows how important the conditional probabilities of the pivotal events are. The end results can be off target if the antecedent events are not taken into consideration.

### 7.3 Recommendations for Further Work

It is important to have a correct frequency basis (leak frequencies in this thesis) before performing the QRA. The basis seems vague, and the industry should have a common agreement on which datasets to use. Subsequently, the effect of the safety system on the ignition and explosion probabilities can be studied more in detail. How changes to these probabilities can propagate in the event tree and affect the end results seems unclear.

A topic which can be explored further is uncertainty. The nuclear industry seems to be far ahead. Can something be learned and adapted? It might also be that uncertainty is unsuitable for QRAs.

Dependencies of the safety systems could be investigated further, to verify if the fault tree approach of handling dependencies is adequate. An interesting topic would be common cause failures in the event trees, how they are treated during the conversion to fault trees. Another aspect is how common cause failures are considered during the consequence determination. Dependencies can introduce simultaneous hazardous sequences, interacting and increasing the severity. This might not be considered properly when each event tree is treated individually.



# Appendix A

## Abbreviations and Acronyms

<b>AEMA</b>	Action Error Mode Analysis
<b>AFR</b>	Annual Fatality Rate
<b>AIR</b>	Average Individual Risk
<b>ALARP</b>	As Low As Reasonably Practicable
<b>BORA</b>	Barrier and Operational Risk Analysis
<b>CFD</b>	Computational Fluid Dynamics
<b>CSE</b>	Concept Safety Evaluation
<b>DAL</b>	Design Accidental Load
<b>ESD</b>	Emergency ShutDown
<b>ETA</b>	Event Tree Analysis
<b>FAR</b>	Fatal Accident Rate
<b>FMECA</b>	Failure Mode, Effects and Criticality Analysis
<b>FPPY</b>	Fatalities Per Platform Year
<b>FTA</b>	Fault Tree Analysis
<b>HAZID</b>	Hazard Identification
<b>HAZOP</b>	Hazard and Operability Analysis
<b>HEP</b>	Human Error Probability
<b>HSE</b>	Health and Safety Executive
<b>IR</b>	Individual risk

<b>IRPA</b>	Individual Risk Per Annum
<b>MSF</b>	Main Safety Function
<b>OLF</b>	The Norwegian Oil Industry Association
<b>PLL</b>	Potential Loss of Life
<b>POB</b>	Personnel On Board
<b>PRA</b>	Probabilistic Risk Assessment
<b>PSA</b>	Petroleum Safety Authority (Norway)
<b>QRA</b>	Quantitative Risk Analysis
<b>RBDM</b>	Risk Based Decision-Making
<b>RIDM</b>	Risk Informed Decision-Making
<b>SHERPA</b>	Systematic Human Error Reduction and Prediction Approach
<b>SHLF</b>	Standard Hydrocarbon Leak Frequency
<b>TRA</b>	Total Risk Analysis

# **Appendix B**

## **Detailed Tables for the Case Study**

### **B.1 FAR, Impairment of MSF Frequency, and Ignited Events**

The following tables are summaries of results from the case studies.

**B.1.1 Installation A**

Table B.1: Sensitivity analysis of the safety systems, FAR and impairment of MSFs, installation A

	Isolation				Blowdown				Firewater			
	Prob 0		Prob 1		Prob 0		Prob 1		Prob 0		Prob 1	
		% change from base case		% change from base case		% change from base case		% change from base case		% change from base case		% change from base case
<b>FAR</b>												
FAR due to process accidents	1.39	0.00 %	1.40	0.90 %	1.39	0.00 %	1.41	1.40 %	1.39	-0.06 %	1.44	3.15 %
<b>FAR distribution</b>												
FAR immediate	0.80	-0.03 %	0.81	1.53 %	0.80	-0.01 %	0.81	2.33 %	0.80	-0.06 %	0.83	3.72 %
FAR escape	0.39	0.04 %	0.39	0.10 %	0.39	0.00 %	0.39	0.30 %	0.39	-0.07 %	0.40	3.74 %
FAR evacuation	0.21	0.04 %	0.21	-0.02 %	0.21	0.00 %	0.21	-0.09 %	0.21	0.00 %	0.21	-0.10 %
<b>MSFs (impairment frequency due to fire)</b>												
Spreading of fire from Drilling and wellhead area to another main area	3.10E-05	-1.71 %	4.21E-05	33.31 %	3.16E-05	-0.03 %	4.41E-05	39.54 %	3.15E-05	-0.24 %	3.94E-05	24.80 %
Spreading of fire from Lower process area to another main area	0	0.00 %	0	0.00 %	0	0.00 %	0	0.00 %	0	0.00 %	0	0.00 %
Spreading of fire from Upper process area to another main area	2.16E-04	-3.23 %	2.98E-04	33.59 %	2.23E-04	-0.09 %	2.38E-04	6.80 %	2.22E-04	-0.69 %	3.04E-04	36.08 %
Escalation of fire within Drilling and wellhead area	1.51E-04	-1.71 %	2.06E-04	33.77 %	1.54E-04	-0.04 %	2.16E-04	39.95 %	1.54E-04	-0.26 %	1.94E-04	25.94 %
Escalation of fire within Lower process area	6.53E-05	-0.18 %	6.71E-05	2.61 %	6.54E-05	-0.04 %	6.71E-05	2.55 %	6.53E-05	-0.27 %	7.49E-05	14.49 %
Escalation of fire within Upper process area	2.25E-04	-3.01 %	3.05E-04	31.68 %	2.32E-04	-0.11 %	2.50E-04	7.93 %	2.30E-04	-0.88 %	3.38E-04	45.93 %
Escape from Drilling and wellhead area	2.31E-04	0.05 %	2.31E-04	0.02 %	2.31E-04	0.00 %	2.32E-04	0.36 %	2.31E-04	-0.08 %	2.41E-04	4.49 %
Escape from Lower process area	6.11E-05	0.00 %	6.11E-05	0.00 %	6.11E-05	0.00 %	6.11E-05	0.00 %	6.11E-05	0.00 %	6.11E-05	0.00 %
Escape from Upper process area	9.73E-05	0.02 %	9.73E-05	0.02 %	9.73E-05	0.00 %	9.73E-05	0.00 %	9.73E-05	0.00 %	9.73E-05	0.00 %



Table B.3: Sensitivity analysis of the safety systems, ignited events in relation with PLL, installation A

	Base case		Prob 0				Prob 1			
	Frequency	PLL	Frequency	% change in frequency from base case	PLL	% change in PLL from base case	Frequency	% change in frequency from base case	PLL	% change in PLL from base case
<b>Ignited events (process fires)</b>										
Local fire due to internal ignition (FII)	1.66E-03	1.86E-02	1.68E-03	0.88 %	1.87E-02	0.92 %	1.43E-03	-14.01 %	1.67E-02	-11.45 %
Local fire due to external ignition (FIE)	7.92E-05	1.96E-04	7.93E-05	0.08 %	1.97E-04	0.21 %	7.77E-05	-1.85 %	1.85E-04	-6.16 %
Escalated fire due to internal ignition (FEI)	3.10E-04	5.42E-03	3.06E-04	-1.15 %	5.37E-03	-0.94 %	4.47E-04	44.33 %	7.39E-03	26.61 %
Escalated fire due to external ignition(FEE)	1.72E-06	2.91E-05	1.68E-06	-2.36 %	2.84E-05	-2.30 %	3.13E-06	82.18 %	5.24E-05	44.44 %
Spread fire internal (FSI)	1.43E-04	2.38E-03	1.33E-04	-7.02 %	2.24E-03	-6.24 %	2.40E-04	67.17 %	3.71E-03	35.91 %
Spread fire external (FSE)	4.15E-09	6.15E-08	0	-100.00 %	0	- 100.00 %	7.86E-08	1795.24 %	1.17E-06	94.72 %
Strong explosion due to internal ignition (EXI)	1.02E-04	6.07E-03	1.02E-04	0.00 %	6.07E-03	0.00 %	1.02E-04	0.00 %	6.07E-03	0.00 %
Strong explosion due to external ignition (EXE)	1.59E-07	9.64E-06	1.59E-07	0.00 %	9.64E-06	0.00 %	1.59E-07	0.00 %	9.64E-06	0.00 %

**B.1.2 Installation B**

Table B.4: Sensitivity analysis of the safety systems, FAR and impairment of MSFs, installation B

	Isolation				Blowdown				Firewater			
	Prob 0	% change from base case	Prob 1	% change from base case	Prob 0	% change from base case	Prob 1	% change from base case	Prob 0	% change from base case	Prob 1	% change from base case
<b>FAR</b>												
FAR due to process accidents	2.39	0.01 %	2.40	0.12 %	2.39	-0.10 %	2.50	4.50 %	2.39	0.00 %	2.40	0.45 %
<b>FAR distribution</b>												
FAR immediate	1.66	0.00 %	1.67	0.18 %	1.66	-0.08 %	1.73	4.06 %	1.66	0.00 %	1.67	0.56 %
FAR escape	0.39	0.03 %	0.39	-0.02 %	0.39	-0.25 %	0.43	10.58 %	0.39	0.00 %	0.39	0.38 %
FAR evacuation	0.35	0.01 %	0.35	0.01 %	0.35	0.02 %	0.35	-0.17 %	0.35	0.01 %	0.35	-0.01 %
<b>MSFs (impairment frequency due to heat loads)</b>												
Evacuation means (lifeboats on the west side)	3.38E-04	0.00 %	3.38E-04	0.01 %	3.38E-04	-0.01 %	3.39E-04	0.38 %	3.38E-04	0.00 %	3.38E-04	0.01 %
Spreading of fire from Process area to another main area	1.18E-04	0.02 %	1.18E-04	-0.10 %	1.18E-04	-0.14 %	1.25E-04	6.25 %	1.18E-04	-0.01 %	1.19E-04	0.85 %
Escape from drilling rig	1.64E-04	0.00 %	1.64E-04	0.01 %	1.64E-04	-0.01 %	1.64E-04	0.35 %	1.64E-04	0.00 %	1.64E-04	0.01 %
Escape from drilling shaft South	3.38E-04	0.00 %	3.38E-04	0.01 %	3.38E-04	-0.01 %	3.40E-04	0.38 %	3.38E-04	0.00 %	3.38E-04	0.01 %
<b>MSFs (impairment frequency due to smoke)</b>												
Evacuation means (lifeboats on the west side)	2.10E-04	0.00 %	2.10E-04	0.00 %	2.10E-04	0.00 %	2.10E-04	0.00 %	2.10E-04	0.00 %	2.10E-04	0.00 %
Escape from drilling rig	9.83E-04	0.01 %	9.83E-04	0.03 %	9.82E-04	-0.13 %	1.04E-03	5.38 %	9.82E-04	-0.05 %	9.95E-04	1.20 %
Escape from drilling shaft South	2.26E-04	0.00 %	2.26E-04	-0.01 %	2.26E-04	-0.02 %	2.28E-04	0.92 %	2.26E-04	0.00 %	2.26E-04	0.01 %





Table B.6: Sensitivity analysis of the safety systems, ignited events in relation with PLL, installation B

	Base case		Prob 0				Prob 1			
	Frequency	PLL	Frequency	% change in frequency from base case	PLL	% change in PLL from base case	Frequency	% change in frequency from base case	PLL	% change in PLL from base case
<b>Ignited events</b>										
Local fire due to internal ignition (FII)	1.51E-03	1.33E-02	1.52E-03	0.77 %	1.34E-02	0.93 %	1.37E-03	-8.79 %	1.19E-02	-11.74 %
Local fire due to external ignition (FIE)	2.60E-04	3.62E-03	2.61E-04	0.38 %	3.63E-03	0.38 %	2.41E-04	-7.57 %	3.33E-03	-8.72 %
Escalated fire due to internal ignition (FEI)	8.49E-04	1.12E-02	8.39E-04	-1.25 %	1.10E-02	-1.57 %	9.83E-04	15.70 %	1.31E-02	14.31 %
Escalated fire due to external ignition(FEE)	2.87E-05	4.27E-04	2.79E-05	-2.54 %	4.16E-04	-2.77 %	4.86E-05	69.64 %	7.41E-04	42.34 %
Strong explosion due to internal ignition (EXI)	6.31E-04	1.11E-02	6.31E-04	0.00 %	1.11E-02	0.00 %	6.31E-04	0.00 %	1.11E-02	0.00 %
Strong explosion due to external ignition (EXE)	6.58E-04	1.01E-02	6.58E-04	0.00 %	1.01E-02	0.00 %	6.58E-04	0.00 %	1.01E-02	0.00 %

**B.1.3 Installation B, Escalation Probabilities Set to 0**

Table B.7: Sensitivity analysis of the safety systems with low escalation probabilities, FAR and impairment of MSFs, installation B

	Base case	Prob 0	% change from base case	Prob 1	% change from base case
<b>FAR</b>					
FAR due to process accidents	2.26	2.24	-0.55 %	2.42	7.10 %
<b>FAR</b>					
FAR immediate	1.55	1.55	-0.61 %	1.69	8.53 %
FAR escape	0.36	0.36	-0.87 %	0.39	8.14 %
FAR evacuation	0.35	0.35	0.06 %	0.35	-0.38 %
<b>MSFs (impairment frequency due to heat loads)</b>					
Evacuation means (lifeboats on the west side)	3.37E-04	3.37E-04	-0.03 %	3.38E-04	0.28 %
Spreading of fire from Process area to another main area	9.42E-05	9.21E-05	-2.25 %	1.19E-04	26.30 %
Escape from drilling rig	1.63E-04	1.63E-04	-0.02 %	1.64E-04	0.27 %
Escape from drilling shaft South	3.37E-04	3.37E-04	-0.03 %	3.38E-04	0.28 %
<b>MSFs (impairment frequency due to smoke)</b>					
Evacuation means (lifeboats on the west side)	2.10E-04	2.10E-04	0.00 %	2.10E-04	0.00 %
Escape from drilling rig	9.44E-04	9.39E-04	-0.53 %	1.02E-03	7.60 %
Escape from drilling shaft South	2.26E-04	2.26E-04	-0.04 %	2.26E-04	0.24 %

Table B.8: Sensitivity analysis of the safety systems with low escalation probabilities, ignition events, installation B

	Base case	Prob 0		Prob 1	
	Frequency	Frequency	% change in frequency from base case	Frequency	% change in frequency from base case
<b>Ignited events (process fires)</b>					
Local fire due to internal ignition (FII)	2.29E-03	2.36E-03	2.80 %	1.35E-03	-41.08 %
Local fire due to external ignition (FIE)	2.86E-04	2.89E-04	0.96 %	2.40E-04	-16.27 %
Escalated fire due to internal ignition (FEI)	6.37E-05	0	-100.00 %	1.01E-03	1479.51 %
Escalated fire due to external ignition (FEE)	2.49E-06	0	-100.00 %	4.94E-05	1881.78 %
Strong explosion due to internal ignition (EXI)	6.31E-04	6.31E-04	0.00 %	6.31E-04	0.00 %
Strong explosion due to external ignition (EXE)	6.58E-04	6.58E-04	0.00 %	6.58E-04	0.00 %





Table B.11: Sensitivity analysis of the safety systems, ignited events in relation with PLL, installation C

	Base case		Prob 0				Prob 1			
	Frequency	PLL	Frequency	% change in frequency from base case	PLL	% change in PLL from base case	Frequency	% change in frequency from base case	PLL	% change in PLL from base case
<b>Ignited events</b>										
Local fire due to internal ignition (FII)	4.90E-04	8.06E-04	5.03E-04	2.76 %	8.28E-04	2.68 %	0	-100.00 %	0	n/a
Local fire due to external ignition (FIE)	3.13E-04	5.41E-04	3.23E-04	3.15 %	5.58E-04	3.00 %	0	-100.00 %	0	n/a
Escalated fire due to internal ignition (FEI)	2.49E-04	8.21E-04	2.39E-04	-3.94 %	7.86E-04	-4.40 %	7.17E-04	187.73 %	2.59E-03	68.31 %
Escalated fire due to external ignition(FEE)	2.34E-04	7.53E-04	2.27E-04	-3.03 %	7.31E-04	-3.02 %	5.32E-04	126.95 %	1.79E-03	57.90 %
Escalated fire, ESD failure (FEX)	4.52E-06	1.64E-04	0	-100.00 %	0	n/a	4.43E-05	879.24 %	1.60E-03	89.79 %
Strong explosion due to internal ignition (EXI)	7.90E-05	1.61E-03	7.90E-05	0.00 %	1.61E-03	0.00 %	7.90E-05	0.00 %	1.61E-03	0.00 %
Strong explosion due to external ignition (EXE)	4.88E-05	1.02E-03	4.88E-05	0.00 %	1.02E-03	0.00 %	4.88E-05	0.00 %	1.02E-03	0.00 %

## B.2 Ignition and Explosion Probabilities – Installation A

### B.2.1 Ignition Probabilities – ESD Isolation

Table B.12: Ignition probabilities with ESD isolation

Segment	Leak size			
	Small	Medium	Major	Large
A1	0.05 %	0.34 %	2.11 %	2.23 %
A2	0.05 %	0.45 %	2.62 %	2.50 %
A3	0.05 %	0.35 %	2.05 %	2.31 %
A4	0.05 %	0.20 %	1.29 %	1.18 %
A5	0.05 %	0.22 %	1.63 %	1.28 %
A6	0.05 %	0.26 %	1.77 %	1.48 %
A7	0.05 %	0.21 %	1.56 %	1.22 %
A8	0.05 %	0.21 %	1.56 %	1.22 %
A9	0.05 %	0.23 %	1.64 %	1.30 %
A10	0.05 %	0.14 %	1.15 %	1.17 %

Table B.13: Ignition probabilities without ESD isolation

Segment	Leak size			
	Small	Medium	Major	Large
A1	0.05 %	0.65 %	3.46 %	2.90 %
A2	0.05 %	0.53 %	3.17 %	2.86 %
A3	0.05 %	0.60 %	2.70 %	2.53 %
A4	0.06 %	0.44 %	3.48 %	2.24 %
A5	0.05 %	0.74 %	3.87 %	4.08 %
A6	0.05 %	0.35 %	2.07 %	1.93 %
A7	0.06 %	0.93 %	4.77 %	5.39 %
A8	0.06 %	0.93 %	4.77 %	5.39 %
A9	0.05 %	0.37 %	2.26 %	2.15 %
A10	0.06 %	1.21 %	6.26 %	4.24 %

### B.2.2 Explosion Probabilities – ESD Isolation

Table B.14: Explosion probabilities with ESD isolation

Segment	Leak size			
	Small	Medium	Major	Large
A1	0.00 %	9.40 %	16.90 %	11.23 %
A2	0.00 %	11.97 %	24.53 %	16.28 %
A3	0.00 %	8.39 %	15.94 %	13.70 %
A4	0.00 %	1.09 %	0.09 %	0.00 %
A5	0.00 %	3.44 %	5.13 %	0.02 %
A6	0.00 %	5.61 %	9.04 %	0.47 %
A7	0.00 %	2.74 %	3.42 %	0.00 %
A8	0.00 %	2.74 %	3.42 %	0.00 %
A9	0.00 %	3.74 %	5.56 %	0.03 %
A10	0.00 %	0.00 %	0.00 %	0.00 %

Table B.15: Explosion probabilities without ESD isolation

Segment	Leak size			
	Small	Medium	Major	Large
A1	0.00 %	19.04 %	40.05 %	23.74 %
A2	0.00 %	13.58 %	30.63 %	22.19 %
A3	0.00 %	11.27 %	26.13 %	18.93 %
A4	0.00 %	18.10 %	16.37 %	0.00 %
A5	0.00 %	34.55 %	58.81 %	13.74 %
A6	0.00 %	9.98 %	16.75 %	2.20 %
A7	0.00 %	48.02 %	88.77 %	7.28 %
A8	0.00 %	48.02 %	88.77 %	7.28 %
A9	0.00 %	12.63 %	21.88 %	1.30 %
A10	0.00 %	30.48 %	47.02 %	1.68 %

### B.2.3 Explosion Probabilities – Firewater

Table B.16: Explosion probabilities with firewater

Segment	Leak size			
	Small	Medium	Major	Large
A1	0,00 %	10,42 %	19,60 %	12,75 %
A2	0,00 %	12,04 %	25,28 %	17,14 %
A3	0,00 %	9,05 %	18,68 %	15,16 %
A4	0,00 %	2,21 %	1,17 %	0,00 %
A5	0,00 %	9,49 %	15,71 %	2,74 %
A6	0,00 %	5,99 %	9,82 %	0,65 %
A7	0,00 %	5,68 %	9,08 %	0,49 %
A8	0,00 %	5,68 %	9,08 %	0,49 %
A9	0,00 %	4,47 %	6,97 %	0,14 %
A10	0,00 %	2,60 %	4,07 %	0,15 %

Table B.17: Explosion probabilities without firewater

Segment	Leak size			
	Small	Medium	Major	Large
A1	0,00 %	10,58 %	19,75 %	12,77 %
A2	0,00 %	12,23 %	25,50 %	17,22 %
A3	0,00 %	9,20 %	18,82 %	15,18 %
A4	0,00 %	2,23 %	1,17 %	0,00 %
A5	0,00 %	9,63 %	15,82 %	2,75 %
A6	0,00 %	6,07 %	9,85 %	0,65 %
A7	0,00 %	5,75 %	9,10 %	0,49 %
A8	0,00 %	5,75 %	9,10 %	0,49 %
A9	0,00 %	4,51 %	6,98 %	0,14 %
A10	0,00 %	2,65 %	4,08 %	0,15 %



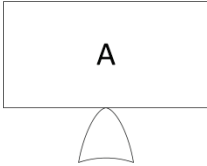
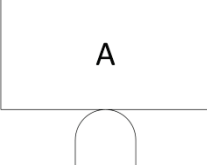
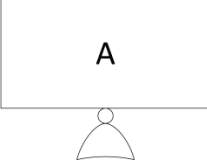
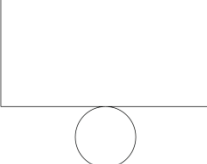
# Appendix C

## Supplementing Figures

### C.1 Fault Tree Symbol Descriptions

Most of the description are from Rausand (2011, Table 10.2), except the NOR-gate, taken from Scandpower (2008).

Table C.1: Fault tree analysis symbol description

	Symbol	Description
OR-gate		The OR-gate indicates that the output event A occurs if any of the input events occur
AND-gate		The AND-gate indicates that the output event A occurs only when all the input events occur at the same time
NOR (NOT OR)-gate		NOR-gate, indicates the output of event A occurs if all the input events do <i>not</i> occur
Basic event		The basic event represents a basic equipment failure that requires no further development of failure causes

### C.2 Example of Master Fault Tree

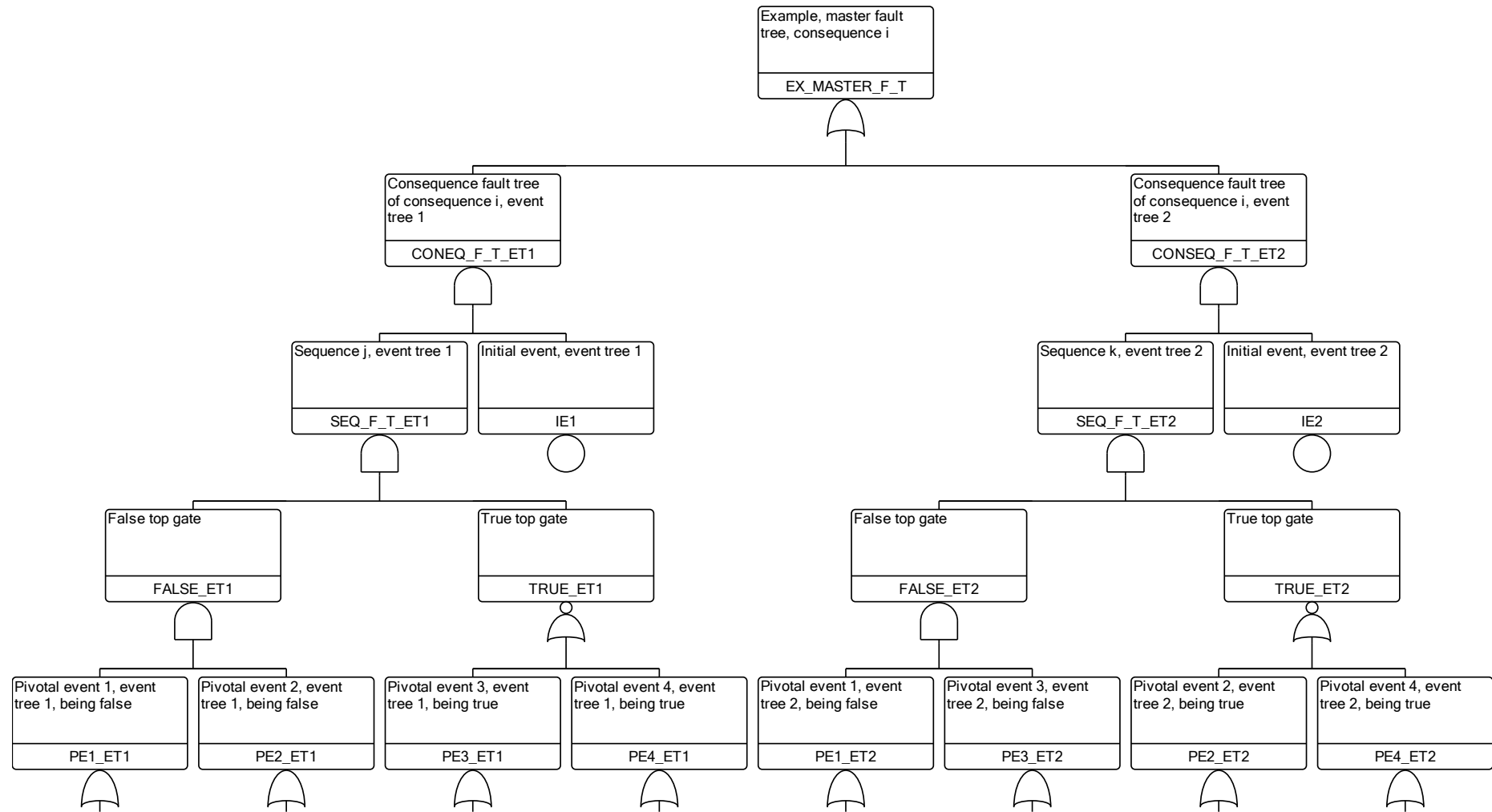


Figure C.1: Example of a master fault tree

### C.3 Detailed Event Tree

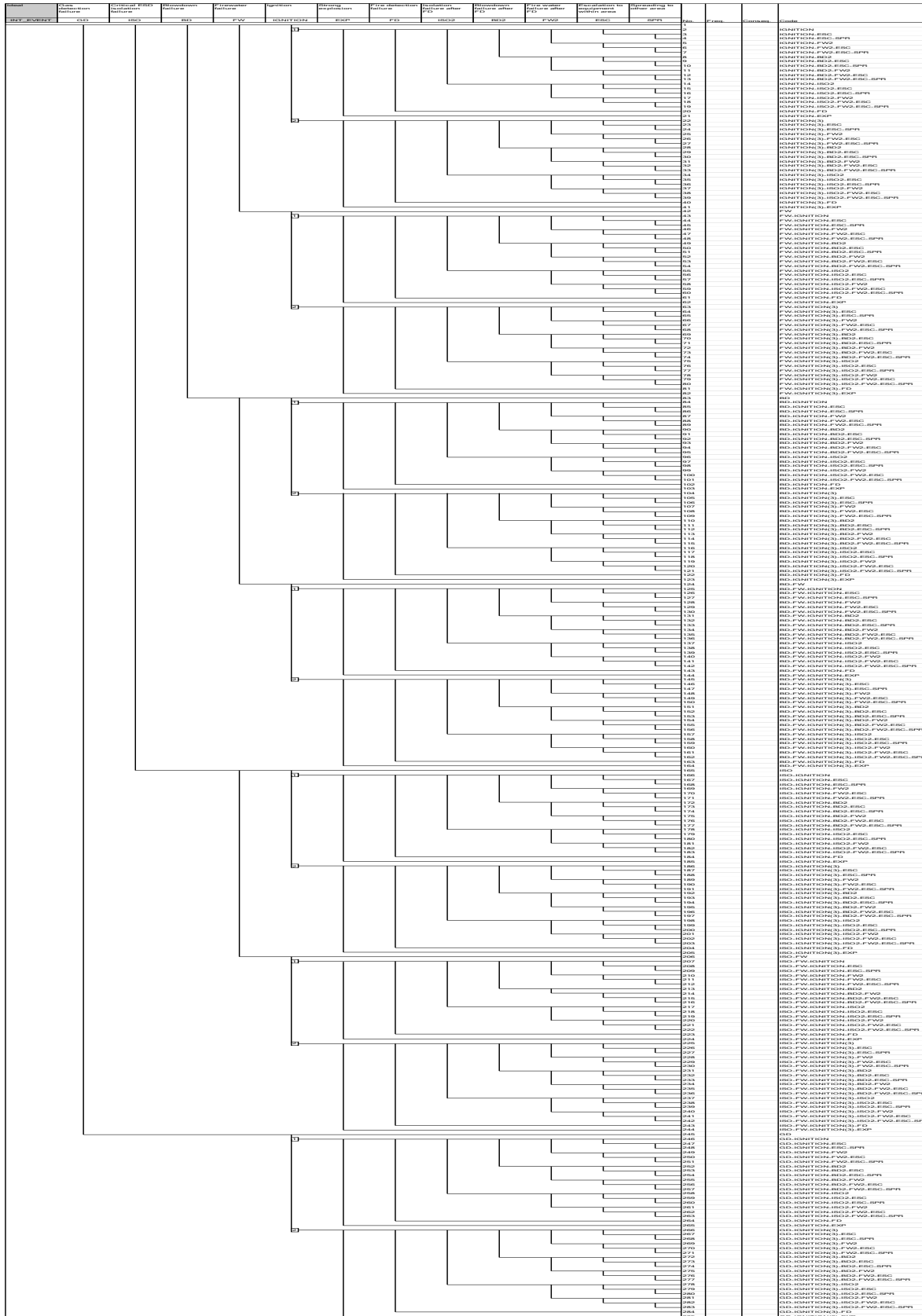


Figure C.2: Example of a highly detailed event tree for a process accident

# Bibliography

- Acosta, C., & Siu, N. (1993). Dynamic Event Trees in Accident Sequence Analysis: Application to Steam Generator Tube Rupture. *Reliability Engineering and System Safety*, 41, 135-154.
- Aven, T., & Vinnem, J. E. (2007). *Risk management with applications from the offshore petroleum industry*. London: Springer.
- Brandt, A. W., Opstad, K., & Wighus, R. (2012). Documentation of active fire fighting systems as a fire safety design parameter - Tests with different deluge nozzles in 3 m diameter rig (NBL A12110). Trondheim: SINTEF NBL as.
- Center for Chemical Process Safety. (2000). *Guidelines for chemical process quantitative risk analysis* (2nd ed.). New York: Wiley-AIChE.
- Det Norske Veritas (2010). Offshore QRA - Standardised Hydrocarbon Leak Frequencies (Rev.1) (Report/DNV reg. no 2008-1768/1241Y35-14). Høvik: DNV.
- Hankinson, G., & Lowesmith, B. J. (2004). Effectiveness of area and dedicated water deluge in protecting objects impacted by crude oil/gas jet fires on offshore installations. *Journal of Loss Prevention in the Process Industries*, 17, 119-125.
- Hauge, S., Lundteigen, M., Hokstad, P., & Håbrekke, S. (2009). Reliability Prediction Method for Safety Instrumented Systems: PDS Method Handbook, 2010 Edition (A13503). Trondheim: SINTEF.
- Haugen, S., Seljelid, J., Sklet, S., Vinnem, J. E., & Aven, T. (2007). Operational Risk Analysis: Total Analysis of Physical and Non-Physical Barriers (Research report 200254-07). Bryne: Preventor.
- Holand, P. (1997). *Offshore Blowouts* (2nd ed.). Burlington: Gulf Professional Publishing.
- HSE (1992). The Tolerability of Risk from Nuclear Power Stations. London: HMSO.
- HSE (2001). Reducing risks, protecting people: HSE's decision-making process. Norwich: HMSO.
- HSE (2005). Cost Benefit Analysis (CBA) Checklist. Retrieved 10. Jun., 2012, from <http://www.hse.gov.uk/risk/theory/alarpcheck.htm>
- HSE (2009a). Prevention, Control and Mitigation of Explosions. Retrieved 10. Jun., 2012, from <http://www.hse.gov.uk/offshore/strategy/mitigation.htm>
- HSE (2009b). Review of Human Reliability Assessment Methods (Research report RR679). London: Health and Safety Executive.

- Hunns, D. M., & Daniels, B. K. (1980). The Method of Paired Comparisons. Symposium on Advances in Reliability Technology (NCSR R23). Bradford: Bradford National Centre of Systems Reliability.
- IEC 61508 (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Parts 1-7. Geneva: International Electrotechnical Commission.
- Jones-Lee, M., & Aven, T. (2011). ALARP: What does it really mean? *Reliability Engineering and System Safety*, 96(8), 877-882.
- Kaplan, S., & Garrik, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, 1(1), 11-27.
- Leveson, N. G. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, Massachusetts: MIT Press.
- Linkov, I., & Burmistrov, D. (2003). Model Uncertainty and choices Made by Modelers: Lessons Learned from the International Atomic Energy Agency Model Intercomparisons. *Risk Analysis*, 23, 1297-1308.
- Lord Cullen. (1990). *The Public Inquiry into the Piper Alpha Disaster*. London: Her Majesty's Stationery Office.
- Mannan, S. (2005). *Lee's Loss Prevention in the Process Industries: Hazard Identification, Assessment, and Control* (3rd ed. Vol. 1). Amsterdam ; Boston: Elsevier Butterworth-Heinemann.
- Murphy, A. H., & Winkler, R. L. (1984). Probability Forecasting in Meterology. *Journal of the American Statistical Association*, 79(387), 489-500.
- National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2011). Deep Water - The Gulf Oil Disaster and the Future of Offshore Drilling (Report to the President).
- NORSOK S-001 (2008). Technical Safety (4th ed.). Oslo: Standards Norway.
- NORSOK Z-013 (2010). Risk and emergency preparedness assessment. Oslo: Standards Norway.
- NPD (1980). Guidelines for conceptual evaluation of platform design. Stavanger: Norwegian Petroleum Directorate.
- NS-EN ISO 17776 (2002). Petroleum and Natural Gas Industries - Offshore Production Installations - Guidelines on Tools and Techniques for Hazard Identification and Risk Assessment. Geneva: International Organization for Standardization.
- NUREG-1855 (2009). Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making. Washington, DC: U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.

- OLF 070 (2004). Application of IEC 61508 and IEC 61511 in The Norwegian Petroleum Industry (2nd rev.). Stavanger: The Norwegian Oil Industry Association.
- OLF (2007). Metode for Miljørettet Risikoanalyse (MIRA) Revisjon 2007 (Report 2007-0063). Høvik: Det Norske Veritas AS.
- Perrow, C. (1999). *Normal Accidents: Living With High-Risk Technologies* (Updated ed.). New Jersey: Princeton University Press.
- PSA (2011a). The Activities Regulations. Stavanger: Petroleum Safety Authority, Norwegian Pollution Control Agency, and Norwegian Social and Health Directorate.
- PSA (2011b). The Facilities Regulations. Stavanger: Petroleum Safety Authority, Norwegian Pollution Control Agency, and Norwegian Social and Health Directorate.
- PSA (2011c). The Framework Regulations. Stavanger: Petroleum Safety Authority, Norwegian Pollution Control Agency, and Norwegian Social and Health Directorate.
- PSA (2011d). The Management Regulations. Stavanger: Petroleum Safety Authority, Norwegian Pollution Control Agency, and Norwegian Social and Health Directorate.
- PSA (2011e). Technical and Operational Regulations. Stavanger: Petroleum Safety Authority, Norwegian Pollution Control Agency, and Norwegian Social and Health Directorate.
- Pyman, M. A. F., & Gjerstad, T. (1983). Experience in Applying Assessment Techniques Offshore in the Norwegian Sector. *Symposium Series, 81*.
- Rasmussen, N. C. (1975). Reactor Safety Study: An Assessment of Accident in U.S. Commercial Nuclear Power Plants (WASH-1400, NUREG-75/104). Rockville, MD: U.S. Nuclear Regulatory Commission.
- Rausand, M. (2011). *Risk Assessment: Theory, Methods, and Applications*. Hoboken, NJ: Wiley.
- Rausand, M., & Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications* (2nd ed.). Hoboken, NJ: Wiley-Interscience.
- Rosness, R., Grøtan, T. O., Guttormsen, G., Herrera, I. A., Steiro, T., Størseth, F., Tinmannsvik, R. K., & Wærby, I. (2010). Organisational Accidents and Resilient Organisation: Six Perspectives. Revision 2 (A17034). Trondheim: SINTEF.
- Scandpower (2008). RiskSpectrum Analysis Tools: Theory Manual. Version 3.0.0 Kjeller: Relcon Scandpower AB.
- Scandpower (2011). Benchmarking and Leak Frequency Model With Respect to RNNP Dataset (101192). Trondheim: Scandpower.

- Scandpower (2012). ExploRAM - Explosion Risk Assessment Model (Fact sheet). Kjeller: Scandpower. Retrieved from <http://www.scandpower.com/documents/203777-factsheet-08-exploram-explosion-risk-assessment-model.aspx>
- Schofield, S. (1998). Offshore QRA and the ALARP principle. *Reliability Engineering and System Safety*, 61(1-2), 31-37.
- Schönbeck, M., Rausand, M., & Rouvroye, J. (2010). Human and Organisational Factors in the Operational Phase of Safety Instrumented systems: A New Approach. *Safety Science*, 48, 310-318.
- SINTEF (2005). Deluge systems as a fire safety design parameter. Retrieved 10. Jun., 2012, from <http://www.sintef.no/home/Building-and-Infrastructure/SINTEF-NBL-as/Key-projects-and-topics/Deluge-systems-as-a-fire-safety-design-parameter/>
- Sklet, S. (2006). Hydrocarbon Releases on Oil and Gas Production Platforms: Release scenarios and safety barriers. *Journal of Loss Prevention in the Process Industries*, 19(5), 494-506.
- Skogdalen, J. E., & Vinnem, J. E. (2011). Quantitative risk analysis offshore: Human and organizational factors. *Reliability Engineering and System Safety*, 96(4), 468-479.
- Spouge, J. (1999). A Guide to Quantitative Risk Assessment for Offshore Installations (Technical report). London: The Centre for Marine and Petroleum Technology.
- Strauman, K. J., & Selnes, P. O. (2011). OLF free fall lifeboat project - methodology for slamming and headway/propulsion analysis (Summary report). Stavanger: The Norwegian Oil Industry Association.
- Summers, A. E. (2008). IEC 61508 Product Approvals - Veering Off Course. *Article posted 11.06.08 on [www.controlglobal.com](http://www.controlglobal.com)*.
- Vinnem, J. E. (1998). Evaluation of methodology for QRA in offshore operations. *Reliability Engineering and System Safety*, 61(1-2), 39-52.
- Vinnem, J. E. (2007). *Offshore Risk Assessment: Principles, Modelling, and Applications of QRA Studies* (2nd ed.). London: Springer.
- Vinnem, J. E., Haugen, S., Vollen, F., & Grefstad, J. E. (2006). ALARP-prosesser: Gjennomgang og drøfting av erfaringer og utfordringer (200584-03). Bryne: Preventor.
- Watson, S. R. (1994). The meaning of probability in probabilistic safety analysis. *Reliability Engineering and System Safety*, 45(3), 261-269.
- Wiklund, J., & Fossan, I. (1999). Model for Explosion Risk Quantification (Presentation). Kjeller: Scandpower.